OpenManage Integration for Microsoft System Center Version 7.3 für Microsoft Endpoint Configuration Manager und System Center Virtual Machine Manager

Einheitliches Benutzerhandbuch

Juni 2021
Rev. A00

DELL EMC

Hinweise, Vorsichtshinweise und Warnungen

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

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

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

Inhaltsverzeichnis

1

Einführung in OMIMSSC

Bei diesem Dokument handelt es sich um ein einheitliches Benutzerhandbuch, das alle Informationen zu Verwendung, Installation und bewährten Verfahren von OMIMSSC enthält.

OpenManage Integration for Microsoft System Center (OMIMSSC) wird als Appliance mit Integration für die Microsoft System Center-Produktreihe ausgeliefert. OMIMSSC ermöglicht ein komplettes Lebenszyklusmanagement von Dell EMC PowerEdge-Servern durch die Anwendung des Integrated Dell Remote Access Controller (iDRAC) mit Lifecycle Controller (LC).

OMIMSSC ermöglicht die Bereitstellung von Betriebssystemen, Dell EMC HCI-Lösungen für Microsoft Windows Server, Hardware-Patching, Firmwareaktualisierung und Wartung von Servern und Modularsystemen. Integrieren Sie OMIMSSC mit Microsoft Endpoint Configuration Manager (MECM), zuvor bekannt unter System Center Configuration Manager (SCCM), für die Verwaltung der Dell PowerEdge-Server in herkömmlichen Rechenzentren oder integrieren Sie OMIMSSC mit Microsoft System Center Virtual Machine Manager (SCVMM) für die Verwaltung der Dell PowerEdge-Server in virtuellen und Cloud-Umgebungen.

Informationen zu Änderungen der MECM-, SCVMM-und SCCM-Markennamen finden Sie in der Microsoft-Dokumentation.

Themen:

Neuheiten

- Support für Microsoft Endpoint Configuration Manager (MECM) Version 2103.
- Support für Microsoft Endpoint Configuration Manager (MECM) Version 2010.
- Support für Microsoft Endpoint Configuration Manager (MECM) Version 2006.
- Support für System Center Virtual Machine Manager (SCVMM) 2019 UR3.
- Support für System Center Virtual Machine Manager (SCVMM) 2019 UR2.
- Support für System Center Virtual Machine Manager (SCVMM) 2016 UR10.
- Support für die Verwaltung des nutzerdefinierten SSL-Zertifikats.
- Clusterfähige Aktualisierungen für HCI- und Failover-Cluster beinhalten jetzt die Möglichkeit, Treiberaktualisierungen in Kombination mit BIOS und Firmware für Windows Server-basierte Cluster durchzuführen.
- Support für neue Intel-basierte und iDRAC 9-basierte PowerEdge-Server.
  - R750
  - R750xa
  - R650
  - C6520
  - MX750c
  - XE2420
- Support für die Erstellung von Windows Server-basierten HCI-Clustern, Verwaltung und Cluster-Aware-Aktualisierung von AX-Nodes und S2D Ready-Nodes.
  - AX6515
  - AX740xd
  - AX640
  - R440
- Support für die WinPE-Treiber-Injektion mithilfe des Dell EMC OpenManage Server-Treiberpakets.

  ANMERKUNG: DTK ist ein Auslaufprodukt von Dell EMC. Verwenden Sie das Dell EMC OpenManage Server-Treiberpaket für WinPE-Treiber.
- Support für die ESXi Betriebssystem Bereitstellungen der Versionen 7.0 U2, 7.0 U1 und 6.7 U3.
- Support für RHEL-Betriebssystem-Bereitstellungen der Versionen 7.9, 8.0, 8.3 und 8.4.
- Neustrukturiertes Benutzerdokument. (Installationsanleitung, Benutzerhandbuch und Fehlerbehebungsinformationen in einem einzigen vereinheitlichten Dokument zusammengefasst).

- Support für die Bereitstellung der Dell EMC OMIMSSC-Appliance für OpenManage Integration für Microsoft Endpoint Configuration Manager (MECM) und System Center Virtual Machine Manager (SCVMM) Version 7.3 auf den folgenden VMware ESXi-Versionen mit der. .ova-Datei:
  - Version 6.5
  - Version 6.7
  - Version 7.0

zusammen mit der vorhandenen Unterstützung für die Bereitstellung der Dell EMC OMIMSSC-Appliance für MECM und SCVMM auf Hyper-V mit der .vhd-Datei.

2

OMIMSSC Lizenz

OMIMSSC verfügt über zwei Arten von Lizenzen:

- Testlizenz: Dies ist eine Testversion der Lizenz, die eine Testlizenz für fünf Server (Hosts oder nicht zugeordnete) enthält, die nach der Installation automatisch importiert wird. Dies gilt nur für die 11. und spätere Generationen der Dell EMC-Server.
- Produktionslizenz: Sie können eine Produktionslizenz von Dell EMC für eine beliebige Anzahl von Servern erwerben, die von OMIMSSC verwaltet werden. Diese Lizenz umfasst Produktunterstützung und Updates der OMIMSSC-Appliance.

Wenn Sie die Lizenzdatei kaufen, können Sie die XML-Datei (Lizenzschlüssel) über das digitale Schließfach von Dell herunterladen. Wenn Sie keine Lizenzschlüssel herunterladen können, wenden Sie sich an den Dell Support. Die Telefonnummer für das regionale Dell Supportteam für Ihr Produkt finden Sie unter `dell.com/support/softwarecontacts`.

Sie können Server in OMIMSSC mithilfe einer einzelnen Lizenzdatei ermitteln. Wenn ein Server in OMIMSSC erkannt wird, wird eine Lizenz verwendet. Wenn ein Server gelöscht wird, wird eine Lizenz freigegeben. Im Aktivitätsprotokoll von OMIMSSC wird für die folgenden Aktivitäten ein Eintrag vorgenommen:

- Lizenzdatei wird importiert
- Der Server wird aus OMIMSSC gelöscht und die Lizenz wird freigegeben.
- Lizenz wird nach dem Erkennen eines Servers verbraucht.

Nach dem Upgrade von einer Testlizenz auf eine Produktionslizenz wird die Testlizenz mit der Produktionslizenz überschrieben. Die Anzahl der **lizenzierten Knoten** entspricht der Anzahl der erworbenen Produktionslizenzen.

Themen:

Unterstützte Optionen für die Lizenzfunktion

Nachfolgend sind die Optionen aufgeführt, die für die Lizenzfunktion unterstützt werden in OMIMSSC

Erwerben einer neuen Lizenz

Bei der Aufgabe einer Bestellung zum Kauf einer neuen Lizenz wird von Dell eine E-Mail mit der Bestellbestätigung gesendet und Sie können die neue Lizenzdatei über den Dell Digital Store 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.

Stapeln mehrerer Lizenzen

Sie können mehrere Produktionslizenzen stapeln, um die Anzahl der unterstützten Server auf die Summe der Server in den hochgeladenen Lizenzen 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 OMIMSSC-Appliances erforderlich ist.

Wenn Sie bereits mehrere Lizenzen hochgeladen haben, ist die Anzahl unterstützter Server die Summe der Server in den nicht abgelaufenen Lizenzen zu dem Zeitpunkt, zu dem die letzte Lizenz hochgeladen wurde.

Ersetzen von Lizenzen

Wenn bei Ihrer Bestellung ein Problem auftritt oder wenn Sie versuchen, eine geänderte oder beschädigte Datei hochzuladen, wird eine entsprechende Fehlermeldung angezeigt. Sie können eine weitere Lizenzdatei vom Dell Digital Locker anfordern. Wenn Sie eine Ersatzlizenz erhalten, enthält die Ersatzlizenz dieselbe Berechtigungs-ID wie die vorherige Lizenz. Beim Hochladen einer Ersatzlizenz wird eine bereits mit der gleichen Berechtigungs-ID hochgeladene Lizenz ersetzt.

Erneutes Importieren von Lizenzen

Wenn Sie versuchen, dieselbe Lizenzdatei zu importieren, wird eine Fehlermeldung angezeigt. Erwerben Sie eine neue Lizenz und importieren Sie die neue Lizenzdatei.

Importieren mehrerer Lizenzen

Sie können mehrere Lizenzdateien mit unterschiedlichen Berechtigungs-IDs importieren, um die Anzahl der Server zu erhöhen, die Sie in OMIMSSC ermitteln und verwalten können.

Erweiterungslizenzen

Sie sind berechtigt, mit OMIMSSC und der vorhandenen Lizenzdatei für alle unterstützten Servergenerationen zu arbeiten. Wenn die Lizenzdatei die neueste Servergeneration nicht unterstützt, erwerben Sie neue Lizenzen.

Testlizenz

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

Lizenzverbrauch in OMIMSSC nach Server Ermittlung

Wenn Sie versuchen, einen Host hinzuzufügen oder einen Bare-Metal-Server zu erkennen, werden Sie vor ihrer Nutzung gewarnt und es wird empfohlen, dass Sie unter den folgenden Umständen neue Lizenzen erwerben:

- Wenn die Anzahl der lizenzierten Server die Anzahl der erworbenen Lizenzen überschreitet
- Wenn Sie festgestellt haben, dass die Server der Anzahl der erworbenen Lizenzen entspricht
- Wenn Sie die Anzahl der erworbenen Lizenzen überschreiten, erhalten Sie eine zeitweilig verlängerte Lizenz.
- Wenn Sie die Anzahl der erworbenen Lizenzen und alle zeitweilig verlängerten Lizenzen überschritten haben.

ANMERKUNG: Die zeitweilig verlängerte Lizenz beträgt 20 Prozent der Gesamtanzahl der erworbenen Lizenzen. Die tatsächlichen Lizenzen, die Sie in OMIMSSC verwenden können, entsprechen der Gesamtzahl der erworbenen Lizenzen plus der zeitweilig verlängerten Lizenzen.

Importieren der Lizenz in OMIMSSC

Importieren Sie nach dem Kauf einer Lizenz diese mit den folgenden Schritten in OMIMSSC:

1. Klicken Sie im OMIMSSC-Verwaltungsportal auf **Lizenz-Center**.
2. Klicken Sie auf **Lizenz importieren** und wählen Sie die aus dem Dell Digital Store heruntergeladene Lizenzdatei aus.

   ANMERKUNG: Sie können nur gültige Lizenzdateien importieren. Wenn die Datei beschädigt oder manipuliert ist, wird eine entsprechende Fehlermeldung angezeigt. Laden Sie die Datei erneut aus dem Dell Digital Store herunter oder wenden Sie sich an einen Vertreter von Dell, um eine gültige Lizenzdatei zu erhalten.

Ansicht des Lizenz-Centers

1. Öffnen Sie einen Browser und geben Sie die URL der OMIMSSC-Appliance an.
   Daraufhin wird die Anmeldeseite des OMIMSSC-Verwaltungsportals angezeigt.
2. Klicken Sie auf **Lizenzcenter**.

   Auf der Seite werden die folgenden Informationen angezeigt:

   Lizenzzusammenfassung: zeigt die Lizenzdetails für OMIMSSC an.
   - **Lizenzierte Nodes**: Gesamtzahl der erworbenen Lizenzen
   - **Verwendete Nodes**: Anzahl der Server, die ermittelt wurden und die Lizenz genutzt haben

- **Verfügbare Nodes**: verbleibende lizenzierte Nodes, die Sie in OMIMSSC erkennen können.

Managen von Lizenzen: zeigt die jeweils importierten Lizenzdateien zusammen mit den Details an, wie z. B. Berechtigungs-ID, Produktbeschreibung, Zeitpunkt, zu dem die Lizenzdatei importiert wurde, Zeitpunkt, seit dem die Lizenzdatei gültig ist, und Liste aller unterstützten Servergenerationen von der Lizenz.

3

OMIMSSC Komponenten

Im folgenden finden Sie eine Liste der OMIMSSC-Komponenten und deren Namen, die in diesem Handbuch verwendet werden:

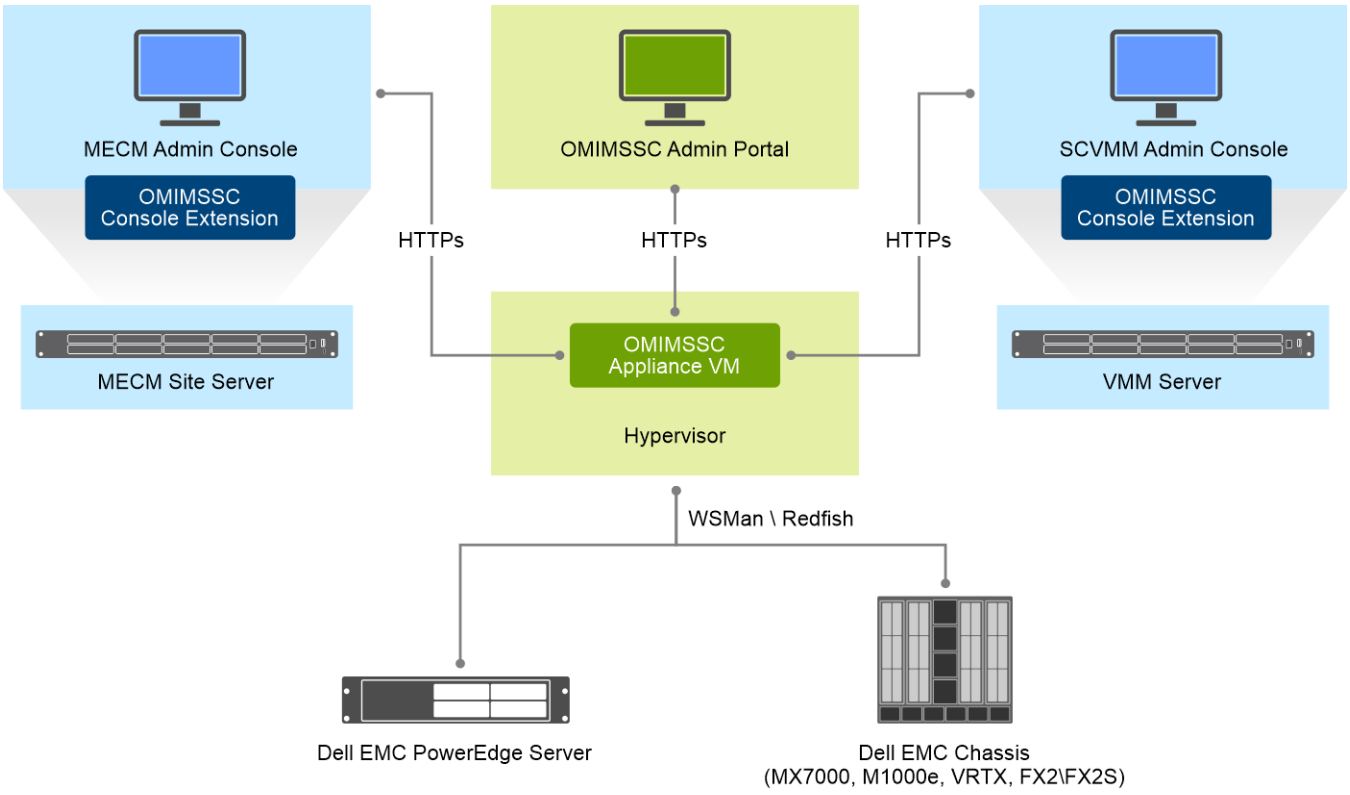
Tabelle 1. Komponenten in OMIMSSC

Komponenten	Beschreibung
OpenManage Integration for Microsoft System Center Virtuelle Maschine der Appliance, auch bekannt als OMIMSSC Appliance.	Hostet die OMIMSSC-Appliance auf einer Hyper-V als virtuelle Maschine, die auf CentOS basiert, und führt die folgenden Aufgaben aus: ● Interagiert mit den Dell EMC Servern über iDRAC mithilfe des Web Services-Management (WSMAN). ● Interagiert mit Dell EMC PowerEdge MX7000-Geräten über OpenManage Enterprise Module (OME-Modular) mithilfe von REST API-Befehlen.
Verwaltungsportal	Aufgaben, die über das Verwaltungsportal verwaltet werden, sind: ● Lizenzverwaltung ● System Center-Registrierung bei OMIMSSC ● Appliance-Management ● Upgrade und Backup der Appliance ● Download des Appliance-Protokolls
OpenManage Integration for Microsoft System Center Konsole, auch bekannt als OMIMSSC Konsole.	Dieselbe Konsolenerweiterung wird auf MECM- und SCVMM-Konsolen verwendet. Sie ist auch bekannt als: ● OMIMSSC Konsolenerweiterung für MECM ● OMIMSSC Konsolenerweiterung für SCVMM

Verwaltungssysteme sind Systeme, auf denen OMIMSSC und seine Komponenten installiert sind.

Verwaltete Systeme sind die von OMIMSSC verwalteten Server.

OMIMSSC Architektur



4

Supportmatrix für OMIMSSC

Themen:

Unterstützte System Center-Versionen

Alle verfügbaren MECM-und SCVMM-Versionen für OMIMSSC lauten wie folgt:

OMIMSSC **Unterstütztes System Center**

- Microsoft System Center Configuration Manager (SCCM) 2012 R2
- Microsoft System Center Configuration Manager (SCCM) 2012 R2 SP1
- Microsoft System Center Configuration Manager (SCCM) Version 1809
- Microsoft System Center Configuration Manager (SCCM) Version 1810
- Microsoft System Center Configuration Manager (SCCM) Version 1902
- Microsoft System Center Configuration Manager (SCCM) Version 1906
- Microsoft Endpoint Configuration Manager (MECM) version 1910
- Microsoft Endpoint Configuration Manager (MECM) version 2002
- Microsoft Endpoint Configuration Manager (MECM) version 2103
- Microsoft Endpoint Configuration Manager (MECM) version 2010
- Microsoft Endpoint Configuration Manager (MECM) version 2006
- Microsoft System Center Virtual Machine Manager (SCVMM) 2012 R2
- Microsoft System Center Virtual Machine Manager (SCVMM) 2016
- Microsoft System Center Virtual Machine Manager (SCVMM) 2016 UR8
- Microsoft System Center Virtual Machine Manager (SCVMM) 2016 UR9
- Microsoft System Center Virtual Machine Manager (SCVMM) 2016 UR3
- Microsoft System Center Virtual Machine Manager (SCVMM) 2019
- Microsoft System Center Virtual Machine Manager (SCVMM) 2019 UR1
- Microsoft System Center Virtual Machine Manager (SCVMM) 2019 UR2
- Microsoft System Center Virtual Machine Manager (SCVMM) 2019 UR10

Tabelle 2. Unterstützte Geräte

Dell EMC System	Unterstützte Version
iDRAC 9-basierte PowerEdge-Server	• BS-Treiberpaket für unterstützte Plattformen: ○ R750, R750xa und R650 - 21.03.10 und höher ○ XE2420 - 20.11.04 ○ R6515, R7515, C6525 und R6525 - 19.12.08 ○ R7525 - 19.12.07 ○ C6520 – 21.03.10 oder höher ○ MX750c – 21.03.10 oder höher • Lifecycle Controller Version und Integrated Dell EMC Remote Access Controller Version für unterstützte AMD-Plattformen: ○ R750, R750xa und R650 - 4.40.20.00 und höher ○ XE2420 - 4.40.10.00

Tabelle 2. Unterstützte Geräte (fortgesetzt)

Dell EMC System	Unterstützte Version
	○ C6520 – 4.40.20.0 oder höher ○ MX750c – 4.40.20.0 oder höher ● Dell EMC OpenManage Server Driver Pack version 10.0.1 ● **MECM** ○ R6515 und R7515 - 3.40.40.40 oder höher ○ C6525 und R6525 - 3.42.42.42 oder höher ○ R7525 - 4.10.10.10 oder höher ● **SCVMM** ○ R6515, R7515, C6525, R6525 und R7525-4.30.30.30 oder höher **ANMERKUNG:** Betriebssystembereitstellung mit Start zu vFlash \ Stage zu vFLash-Methode und Serverprofil-Backup-Funktionen werden nicht unterstützt.
PowerEdge Server 14. Generation	● BS-Treiberpaket: 17.05.21 ● Lifecycle Controller Version und Integration Dell EMC Remote Access Controller Version – 3.00.00.00 oder höher ● Dell EMC OpenManage Server Driver Pack version 10.0.1
PowerEdge Server 13. Generation	● BS-Treiberpaket: 16.08.13 ● Lifecycle Controller Version – 2.40.40.40 oder höher ● Integration Dell Remote Access Controller-Version – 2.40.40.40 oder höher ● Dell EMC OpenManage Server Driver Pack version 10.0.1
PowerEdge Server der 12. Generation	● BS-Treiberpaket: für Server R220 und FM120 - 16.08.13 ● Andere unterstützte Plattformen BS-Treiberpaket: 15.07.07 ● Lifecycle Controller Version 2.40.40.40 oder höher ● Integration Dell Remote Access Controller Version 2.40.40.40 oder höher ● Dell EMC OpenManage Server Driver Pack version 10.0.1
Chassis Management Console (CMC)	● FX2 1.4 oder höher ● M1000e 5.2 oder höher ● VRTX 2.2 oder höher
Dell EMC OpenManage Enterprise-Modular	● PowerEdge MX7000 Chassis 1.0
Unterstützte AX- und/oder Storage Spaces Direct Ready-Nodes (mit Windows Serverbetriebssystem) als Ziel-Nodes für Dell EMC HCI-Lösungen für Microsoft Windows Server	AX-Nodes: AX-640, AX-740xd und AX-6515 Storage Spaces Direct Ready-Nodes: R440, R640, R740xd und R740xd2

ANMERKUNG: Die Unterstützung für die 11. Generation von PowerEdge-Servern ist ab der OMIMSSC-Version 7.2.1 veraltet.

Tabelle 3. Unterstützte Betriebssysteme (Bereitstellung):

Betriebssysteme	Unterstützte Version
Microsoft Windows	● Windows Server 2019 ● Windows Server 2016 ● Windows Server 2012 R2
Betriebssysteme, die nicht von Windows unterstützt werden	● RHEL 8.0, 8.3, 8.4 ● RHEL 7.2, 7.3, 7.4, 7.5 ● RHEL 6.9
VMWare ESXi	● ESXi 7.0 U2 - A00 ● ESXi 7.0 U1 - A05 ● ESXI 6.7 U3 - A10

Tabelle 3. Unterstützte Betriebssysteme (Bereitstellung): (fortgesetzt)

Betriebssysteme	Unterstützte Version
	• ESXi 6.7 - A06 • ESXi 6.5 U3 • ESXi 6.5 U1 - A11 • ESXi 6.5 - A03 • ESXi 6.0 U3 - A15 • ESXi 6.0 - A02 **ANMERKUNG:** Laden Sie das Image von https://www.dell.com/support/ herunter, beziehen Sie sich auf die Seite Treiber und Downloads des spezifischen Servermodells gemäß den von OMIMSSC unterstützten Versionen.

OMIMSSC Unterstützte Cluster

- Erstellen und Verwalten von Windows 2016 und 2019 Windows Server HCI-fähigen Clustern auf SCVMM-Konsole
- Verwaltung von Windows 2012 R2, 2016 und 2019 Hyper-V-Host-Clustern auf der SCVMM-Konsole

Netzwerkanforderungen

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

Tabelle 4. Virtual Appliance

Portnummer	Protokolle	Schnittstellen-Typ	Maximale Verschlüsselungsstufe	Richtung	Ziel	Verwendung	Beschreibung
53	DNS	TCP	Keine	Ausgang	OMIVV-Appliance zu DNS-Server	DNS-Client	Verwendet als Konnektivität zum DNS-Server oder Auflösen der Hostnamen.
68	DHCP	UDP	Keine	Eingang	DHCP-Server zu OMIVV-Appliance	Dynamische Netzwerkkonfiguration	Um die Netzwerkdetails wie IP, Gateway, Netzmaske und DNS abzurufen.
69	TFTP	UDP	128 Bit	Ausgang	OMIMSSC zu iDRAC	Einfache Dateiübertragung	Wird verwendet, um den Bare-Metal-Server auf die erforderliche Mindestversion der Firmware zu aktualisieren.
123	NTP	UDP	Keine	Eingang	NTP zu OMIMSSC-Appliance	Zeitsynchronisation	Zum Synchronisieren mit einer bestimmten Zeitzone.
80/443	HTTP oder HTTPS	TCP	Keine	Ausgang	OMIMSSC-Appliance zu Internet	Dell Online-Datenzugriff	Verwendet als Konnektivität zu Online-Service (Internet), Firmware und aktuellen RPM-Informationen.
443	HTTPS	TCP	128 Bit	Eingang	OMIMSSC-Benutzeroberfläche zu OMIMSSC-Appliance	HTTPS-Server	Von OMIMSSC angebotene Webdienste. Diese Webdienste werden vom vSphere Client und Dell Admin-Portal genutzt.
443	HTTPS	TCP	128 Bit	Eingang	ESXi-Server zu OMIVV-Appliance	HTTPS-Server	Wird im Betriebssystem-Bereitstellungsprozess für Skripts nach der Installation zur Kommunikation mit der OMIMSSC-Appliance verwendet.
443	HTTPS	TCP	128 Bit	Eingang	iDRAC zu OMIVV-Appliance	Automatische Ermittlung	Bereitstellungsserver, der für die automatische Ermittlung von

Tabelle 4. Virtual Appliance (fortgesetzt)

Portnummer	Protokolle	Schnittstellen-Typ	Maximale Verschlüsselungsstufe	Richtung	Ziel	Verwendung	Beschreibung
							verwalteten Knoten verwendet wird.
443	WSMAN	TCP	128 Bit	Ein/Aus	OMIVV-Appliance zu oder von iDRAC	iDRAC-Kommunikation	iDRAC-, CMC- oder OME-Modular-Kommunikation; wird zur Verwaltung und Überwachung der verwalteten Knoten verwendet.
111	HTTPS	TCP	Keine	Eingang	iDRAC zu OMIVV-Appliance	Aufruf eines Remote-Verfahrens	Wird verwendet, um die Adresse der RPC-Funktion zu bestimmen.
4433	HTTPS	TCP	Keine	Eingang	iDRAC zu OMIVV-Appliance	Automatische Ermittlung	Wird für die automatische Ermittlung verwendet.
445/139	SMB	TCP	128 Bit	Ausgang	OMIVV-Appliance zu CIFS	CIFS-Kommunikation	Für die Kommunikation mit Windows-Freigaben.
2049	NFS	UDP/TCP	Keine	Ein/Aus	OMIVV-Appliance zu NFS	Öffentliche Freigabe	Öffentliche NFS-Freigabe, die von der OMIMSSC-Appliance für die verwalteten Knoten verfügbar gemacht und für Firmwareaktualisierungs- und Betriebssystem-Bereitstellungsprozesse verwendet wird.
4001 bis 4004	NFS	UDP/TCP	Keine	Ein/Aus	OMIVV-Appliance zu NFS	Öffentliche Freigabe	Diese Ports müssen offen gehalten werden zur Ausführung der statd, quotd, lockd, und mountd Dienstleistungen durch den V2 und V3-Protokolle der NFS-Server.
Nutzerdefinierte	beliebig	UDP/TCP	Keine	Ausgang	OMIVV-Appliance zu Proxyserver	Proxy	Für die Kommunikation mit dem Proxyserver

Tabelle 5. Verwaltete Knoten (ESXi)

Portnummer	Protokolle	Schnittstellen-Typ	Maximale Verschlüsselungsstufe	Richtung	Ziel	Verwendung	Beschreibung
443	WSMAN	TCP	128 Bit	Eingang	OMIVV-Appliance zu ESXi	iDRAC-Kommunikation	Wird verwendet, um Informationen für die Management Station bereitzustellen. Dieser Port muss über ESXi geöffnet werden.
443	HTTPS	TCP	128 Bit	Eingang	OMIVV-Appliance zu ESXi	HTTPS-Server	Wird verwendet, um Informationen für die Management Station bereitzustellen. Dieser Port muss über ESXi geöffnet werden.

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

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

Infrastructure administration using Microsoft System Center Console

Microsoft System Center user account privileges

All the required account privileges to use OMIMSSC are as follows:

User must be member of the following groups in System Center Consoles for Account privileges to use OMIMSSC console extension.

Table 6. User accounts with required privileges

Users	Privileges/Roles
For enrollment	• Account used to enroll the MECM console with OMIMSSC should be a full admin or an administrator in MECM. • Account used to enroll the SCVMM console with OMIMSSC should be a member of administrator role in SCVMM. • Domain user. • Member of Local Administrator group in system center machine.
For logging in to console extensions	• Account used to enroll the MECM console with OMIMSSC should be a full admin or an administrator in MECM. • Account used to enroll the SCVMM console with OMIMSSC should be a delegated admin or an administrator in SCVMM. • Domain user. • Member of Local Administrator group in system center machine.

Systemanforderungen für OMIMSSC

Stellen Sie vor der Installation von OMIMSSC sicher, dass Sie die folgenden Softwarevoraussetzungen auf der Grundlage der drei aufgeführten OMIMSSC-Komponenten erfüllen:

- OMIMSSC Appliance:
  - Installieren Sie Windows Server und aktivieren Sie die Hyper-V-Rolle.
  - Sie können jetzt eine beliebige Anzahl von MECM- oder SCVMM-Konsolen an eine OMIMSSC-Appliance registrieren, da OMIMSSC die Multikonsolenregistrierung unterstützt. Basierend auf der Anzahl der Konsolen, die Sie anmelden möchten, gelten folgende Hardwareanforderungen:

    Tabelle 7. Hardwareanforderungen

Komponenten	Für eine MECM- oder SCVMM-Konsole	Für eine beliebige Anzahl von MECM- oder SCVMM-Konsolen
RAM	8 GB	8 GB*N
Prozessoranzahl	4	4*N

- Installieren Sie eine der folgenden Versionen des Windows-Betriebssystems:
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
- Installieren Sie eine der folgenden Versionen von ESXi:
  - Version 6.5
  - Version 6.7
  - Version 7.0
- OMIMSSC Verwaltungsportal: Installieren Sie einen der folgenden unterstützten Browser:
  - Internet Explorer 10 oder höher

- Mozilla Firefox 30 oder höher
- Google Chrome 23 oder höher
- Microsoft Edge

Systemanforderungen der OMIMSSC-Konsolenerweiterung für SCVMM

So installieren Sie die OMIMSSC-Konsolenerweiterung für SCVMM:

- Installieren Sie die gleichen Versionen von SCVMM-Verwaltungskonsole und SCVMM-Server.
- Die Funktion "Failoverclustering" ist auf dem SCVMM-Server aktiviert.
- Der registrierte Nutzer sollte über Administratorrechte auf dem SCVMM-Server verfügen.
- Der registrierte Nutzer sollte über Administratorrechte auf dem verwalteten Cluster verfügen.

5

Bereitstellen OMIMSSC

Themen:

Download von OMIMSSC aus dem Internet

Zum Herunterladen von OMIMSSC von https://www.dell.com/support führen Sie folgende Schritte durch:

1. Klicken Sie auf **alle Produkte Durchsuchen** > **Software** > **Enterprise Systems Management** > **OpenManage Integration for Microsoft System.**
2. Wählen Sie die erforderliche Version des OMIMSSC.
3. Klicken Sie auf die Registerkarte **Treiber & Downloads**.
4. Laden Sie die vhd-Datei für OMIMSSC herunter.
5. Extrahieren Sie die vhd-Datei und richten Sie dann die OMIMSSC Appliance ein.
   Die Größe der VHD-Datei beträgt ca. 5 GB. die Bereitstellung dauert ca. 5 bis 10 Minuten.
6. Geben Sie den Speicherort zum Entpacken der Dateien an und klicken Sie auf die Schaltfläche zum Extrahieren von Dateien:
   - **OMIMSSC_<Dateiversion>_für_VMM_und_ConfigMgr**

OMIMSSC-Appliance auf Hyper-V einrichten

Stellen Sie sicher, dass die folgenden Anforderungen auf dem Hyper-V, auf dem Sie das OMIMSSC-Gerät einrichten, erfüllt sind:

- Der virtuelle Switch ist konfiguriert und verfügbar.
- Weisen Sie Speicher für die OMIMSSC-Appliance-VM basierend auf der Anzahl der Microsoft-Konsolen zu, die Sie registrieren möchten. Weitere Informationen dazu finden Sie unter Allgemeine Anforderungen.

So richten Sie die OMIMSSC-Appliance ein:

1. Stellen Sie die OMIMSSC-Appliance-VM mit folgenden Schritten bereit:
   a. Wählen Sie unter **Windows Server** im **Hyper-V Manager** im Menü **Aktionen** die Option **Neu** und klicken Sie auf **Virtual Machine Manager**.
      Der **Assistent für neue virtuelle Maschinen** wird angezeigt.
   b. Klicken Sie in **Bevor Sie beginnen** auf **Weiter**.
   c. Geben Sie in **Name und Speicherort angeben** einen Namen für die virtuelle Maschine an.

      Wenn Sie die VM an einem anderen Speicherort speichern möchten, wählen Sie **Die virtuelle Maschine an einem anderen Speicherort speichern** aus, klicken Sie auf **Durchsuchen** und navigieren Sie zum neuen Speicherort.
   d. Wählen Sie in **Generation angeben 1. Generation**, und klicken Sie dann auf **Weiter**.
   e. Weisen Sie unter **Arbeitsspeicher zuweisen** die in der Voraussetzung angegebene Speicherkapazität zu.
   f. Wählen Sie unter **Netzwerk konfigurieren** in **Verbindung** das Netzwerk aus, das Sie verwenden möchten, und klicken Sie dann auf **Weiter**.
   g. Wählen Sie in **Virtuelle Festplatte verbinden Eine vorhandene virtuelle Festplatte verwenden** aus, navigieren Sie an den Speicherort, auf dem die **OMIMSSC_<file version>_for_VMM_and_ConfigMgr** VHD-Datei vorhanden ist, und wählen Sie die Datei aus.

      Die Größe der VHD-Datei beträgt ca. 5 GB. die Bereitstellung dauert ca. 5 bis 10 Minuten.
   h. Bestätigen Sie in **Zusammenfassung** die von Ihnen eingegebenen Details, und klicken Sie auf **Fertigstellen**.
   i. Legen Sie die **Anzahl der virtuellen Prozessoren** auf 4 fest. Standardmäßig ist die Anzahl der Prozessoren auf 1 gesetzt.

So legen Sie den Wert für die Prozessoranzahl fest:

i. Klicken Sie mit der rechten Maustaste auf die OMIMSSC-Appliance und wählen Sie **Einstellungen** aus.
ii. Wählen Sie in **Einstellungen** die Option **Prozessor** aus und legen Sie die **Anzahl der virtuellen Prozessoren** auf `4` fest.

2. Führen Sie nach dem Start der OMIMSSC-Appliance die folgenden Aufgaben aus:

   ANMERKUNG: Es wird empfohlen, dass Sie fünf Minuten warten, bevor Sie sich als **Administrator** anmelden, damit alle Dienste gestartet werden.

   a. In **Localhost-Anmeldung**: Geben Sie admin ein.
   b. In **Neues Administratorkennwort eingeben**: Geben Sie ein Kennwort ein.

      ANMERKUNG: Dell EMC empfiehlt, sichere Kennwörter zu konfigurieren und zu verwenden, um die `admin` Benutzer- und Konsolen-Erweiterung der Appliance zu authentifizieren.

   c. In **Neues Administratorkennwort bestätigen**: Geben Sie das Kennwort erneut ein und drücken Sie zum Fortfahren die **Eingabetaste**.
   d. Wählen Sie in den aufgelisteten Optionen **Netzwerk konfigurieren** aus, drücken Sie die **Eingabetaste**, und führen Sie die folgenden Unterschritte aus:
      - Wählen Sie unter **NetworkManagerTUI** die Option **System-Hostname festlegen**, geben Sie den Namen der OMIMSSC-Appliance an und klicken Sie auf **OK**.

        Beispiel: `Hostname.domain.com`

        ANMERKUNG: Sie können die IP-Adresse der OMIMSSC-Appliance ändern, indem Sie die Option **Netzwerk konfigurieren** auswählen. Sie können die IP-Adresse oder den Hostnamen der OMIMSSC-Appliance ab diesem Zeitpunkt nicht mehr ändern.
      - Wenn Sie eine statische IP-Adresse angeben, wählen Sie **Verbindung bearbeiten** und dann **Ethernet0**.

        Wählen Sie **IPv4-KONFIGURATION**, wählen Sie **Manuell** und klicken Sie auf **Anzeigen**. Geben Sie die IP-Konfigurationsadresse, Gateway-Adresse und die DNS-Server-IP ein und klicken Sie auf **OK**.

   e. Notieren Sie sich die URL des OMIMSSC-Admin-Portals der OMIMSSC-Appliance.

      ANMERKUNG: Fügen Sie die IP-Adresse und den vollqualifizierten Domainnamen des OMIMSSC-Geräts in Zonen für Vorwärtsauflösung und Zonen für Rückwärtsauflösung in DNS hinzu.

      ANMERKUNG: Appliance-Protokolle sind für Nicht-Admin-Benutzer zugänglich. Diese Protokolle enthalten jedoch keine vertraulichen Informationen. Schützen Sie als Workaround die URL der Appliance.

Einrichten der OMIMSSC-Appliance auf ESXi

Stellen Sie vor der Bereitstellung von OMIMSSC mithilfe von ESXi sicher, dass Sie die OVA-Datei aus der komprimierten ZIP-Datei auf ein lokales Laufwerk extrahieren. Gehen Sie zum Bereitstellen von OMIMSSC auf ESXi wie folgt vor:

1. Starten Sie ESXi mithilfe der IP-Adresse.

   Die VMware ESXI-Anmeldeseite wird angezeigt.
2. Geben Sie Ihren Nutzernamen und Ihr Kennwort ein und klicken Sie dann auf Anmelden.
3. Wählen Sie im linken Fensterbereich auf Virtuelle Maschinen aus.
4. Um eine VM zu erstellen, wählen Sie VM erstellen/registrieren aus.

   Der Assistent für neue virtuelle Maschinen wird angezeigt.

   a. Wählen Sie im Abschnitt Erstellungsart auswählen die Option Virtuelle Maschine aus OVF- oder OVA-Datei bereitstellen aus.
   b. Klicken Sie auf Weiter.
   c. Geben Sie in OVF- und VMDK-Dateien auswählen einen Namen für die virtuelle Maschine ein, die Sie erstellen möchten.
   d. Klicken Sie, um Dateien auszuwählen oder per Drag-and-Drop zu verschieben.
   e. Doppelklicken Sie auf die Datei OMIMSSC_xx.ova. Das OVA Management Pack wird in den Installationsprozess hochgeladen.
   f. Klicken Sie auf Weiter.
   g. Wählen Sie im Abschnitt Storage auswählen den Storage oder Datenspeicher aus, in dem Sie die Konfigurations-und VD-Dateien speichern möchten.
   h. Klicken Sie auf Weiter.
   i. Wählen Sie im Abschnitt Bereitstellungsoptionen die erforderlichen Netzwerkzuordnungen aus.

- Standardmäßig ist die Funktion für die Festplattenbereitstellung als Thin ausgewählt.
- Die Option zum automatischen Einschalten der virtuellen Maschine ist aktiviert.

j. Klicken Sie auf Weiter.

k. Überprüfen Sie im Abschnitt Bereit zur Fertigstellung die festgelegte Einstellung und klicken Sie dann auf Fertig stellen.

Der VM-Erstellungsprozess wird gestartet. Sie können den Status in Letzte Aufgaben anzeigen.

5. Aktivieren Sie die Option Gast und Host synchronisieren auf der VM, die auf ESXi gehostet wird:
   a. Wählen Sie die VM aus und klicken Sie auf Bearbeitungsoptionen.
   b. Wählen Sie VM-Optionen aus.
   c. Wählen Sie VMware-Tools>Zeit>Gast und Host synchronisieren aus.

Registrieren mehrerer Microsoft-Konsolen

Verwalten Sie die OMIMSSC-Appliance-Ressourcen, wenn mehrere Microsoft-Konsolen bei OMIMSSC registriert sind.

Stellen Sie anhand der Anzahl der Microsoft-Konsolen, die Sie an der OMIMSSC-Appliance anmelden möchten, sicher, dass die Hardwareanforderungen erfüllt sind. Weitere Informationen finden Sie unter Allgemeine Systemanforderungen für OMIMSSC.

Zum Konfigurieren von Ressourcen für mehrere Microsoft Konsolen führen Sie folgende Schritte durch:

1. Starten Sie die OMIMSSC-Appliance und melden Sie sich an.
2. Navigieren Sie zu **Registrierungsparameter konfigurieren** und drücken Sie die **Eingabetaste**.
3. Geben Sie die Anzahl der Konsolen an, die Sie an der OMIMSSC-Appliance registrieren möchten.
   Die erforderlichen Ressourcen werden aufgelistet.

Starten des OMIMSSC-Verwaltungsportals zum Download der OMIMSSC-Komponenten

1. Starten Sie einen Browser und melden Sie sich beim OMIMSSC-Admin-Portal unter Verwendung der gleichen Zugangsdaten an, die bei der Anmeldung am OMIMSSC-Gerät verwendet wurden.

   Format: `https://<IP address or FQDN>`

   ANMERKUNG: Fügen Sie die URL des OMIMSSC-Admin-Portals unter **lokaler Intranetstandort** hinzu. Weitere Informationen finden Sie unter Hinzufügen der OMIMSSC-IP-Adresse im Browser
2. Klicken Sie auf **Downloads** und klicken Sie auf **Installationsprogramm herunterladen** zum Herunterladen der erforderlichen Konsolenerweiterung.

Installieren der OMIMSSC-Konsolenerweiterung für MECM

- Stellen Sie sicher, dass Sie OMIMSSC auf dem MECM-Standortserver installieren, bevor es auf der MECM-Verwaltungskonsole verwendet wird.
- Es wird empfohlen, dass Sie Configuration Manager schließen, bevor Sie die OMIMSSC-Konsolenerweiterung für MECM installieren, aktualisieren oder deinstallieren.

1. Doppelklicken Sie auf `OMIMSSC_MECM(SCCM)_Console_Extension.exe`.
   Der **Startbildschirm** wird angezeigt.
2. Klicken Sie auf **Weiter**.
3. Wählen Sie im Bildschirm **Lizenzvereinbarung** die Option **Ich stimme den Bedingungen der Lizenzvereinbarung zu** aus, und klicken Sie dann auf **Weiter**.
4. Auf der Seite **Zielordner** wird standardmäßig ein Installationsordner ausgewählt. Klicken Sie zum Ändern des Speicherorts auf **Ändern** und wechseln Sie zu einem neuen Speicherort. Klicken Sie anschließend auf **Weiter**.
5. Klicken Sie auf der Seite **Zur Installation des Programms bereit** auf **Installieren**.

   Der folgende Ordner wird nach der Installation der Konsolenerweiterung erstellt:
   - Log: Dieser Ordner enthält protokollbezogene Protokollinformationen.
6. Klicken Sie unter **Installation erfolgreich abgeschlossen** auf **Fertigstellen**.

Empfehlung: Ausgehend von den installierten MECM 2103-Setups muss die Option **nur Konsolenerweiterungen zulassen, die für die Hierarchie genehmigt wurden** in den Einstellungen der **MECM-Hierarchie** deaktiviert werden, um den Startpunkt der OMIMSSC-Konsole in der MECM-Konsole anzuzeigen. Weitere Informationen finden Sie im Abschnitt zur Configuration Manager-Konsole in der Microsoft-Dokumentation.

Installieren von OMIMSSC-Konsolenerweiterung für SCVMM

- Installieren Sie die OMIMSSC-Konsolenerweiterung auf dem SCVMM-Managementserver und der SCVMM-Konsole. Erst nach der Installation der OMIMSSC-Konsole können Sie die Konsolenerweiterung in SCVMM importieren.

1. Doppelklicken Sie auf die Datei `OMIMSSC_SCVMM_Console_Extension.exe`.
   Der **Startbildschirm** wird angezeigt.
2. Klicken Sie auf **Weiter**.
3. Wählen Sie im Bildschirm **Lizenzvereinbarung** die Option **Ich stimme den Bedingungen der Lizenzvereinbarung zu** aus, und klicken Sie dann auf **Weiter**.
4. Auf der Seite **Zielordner** wird standardmäßig ein Installationsordner ausgewählt. Klicken Sie zum Ändern des Speicherorts auf **Ändern** und wechseln Sie zu einem neuen Speicherort. Klicken Sie anschließend auf **Weiter**.
5. Klicken Sie auf der Seite **Zur Installation des Programms bereit** auf **Installieren**.

   Die folgenden Ordner werden nach der Installation der Konsolenerweiterung erstellt:
   - Log: Dieser Ordner enthält protokollbezogene Protokollinformationen.
   - OMIMSSC_UPDATE: Dieser Ordner enthält alle Aktivitäten, die für das Cluster Aware Update (CAU) erforderlich sind. Dieser Ordner verfügt nur über Lese- und Schreibberechtigungen für CAU-Vorgänge. WMI-Berechtigungen (Windows Management Instrumentation) sind für diesen Ordner konfiguriert. Weitere Informationen finden Sie in der Microsoft-Dokumentation.
6. Klicken Sie auf der Seite **InstallShield-Assistent abgeschlossen** auf **Fertigstellen**.
7. Importieren Sie die OMIMSSC-Konsolenerweiterung für SCVMM in die SCVMM-Konsole. Weitere Informationen finden Sie unter Importieren der OMIMSSC-Konsolenerweiterung für SCVMM.

6

Registrieren der Microsoft-Konsole in OMIMSSC

Stellen Sie sicher, dass die folgenden Voraussetzungen und die erforderlichen Kontoberechtigungen erfüllt sind:

- Für MECM-Benutzer ist die OMIMSSC-Konsolenerweiterung für die MECM-Konsole installiert.
- Für SCVMM-Nutzer ist die OMIMSSC-Konsolenerweiterung für SCVMM installiert.

Stellen Sie sicher, dass die folgenden Informationen verfügbar sind:

- Benutzerzugangsdaten für das System, auf dem Microsoft System Center eingerichtet wird, siehe erforderliche Kontoberechtigungen.
- FQDN von MECM oder FQDN von SCVMM.

Führen Sie die folgenden Schritte aus, um eine MECM- oder SCVMM-Konsole bei OMIMSSC zu registrieren:

1. Melden Sie sich beim OMIMSSC-Verwaltungsportal an.
2. Klicken Sie auf **Einstellungen**, auf **Konsolenregistrierung** und dann auf **Registrieren**.
   Daraufhin wird die Seite **Konsole registrieren** angezeigt.
3. Geben Sie einen Namen und eine Beschreibung für die Konsole ein.
4. Geben Sie den FQDN vom MECM-Standortserver oder SCVMM-Server und die Zugangsdaten ein.
5. Klicken Sie auf **Neu erstellen**, um ein Windows-Anmeldeinformationsprofil für den Zugriff auf die MECM- oder SCVMM-Konsole zu erstellen.
   - Wählen Sie den **Typ des Zugangsdatenprofils** als **Windows-Zugangsdatenprofil** aus.
   - Geben Sie einen Profilnamen und eine Beschreibung ein.
   - Geben Sie unter **Zugangsdaten** den Nutzernamen und das Kennwort ein.
   - Geben Sie die Domänendetails unter **Domain** ein.

   ANMERKUNG: Geben Sie den Domänennamen mit Details zur Top-Level-Domain (TLD) an, während Sie das Berechtigungsprofil für die Konsolenregistrierung erstellen.

   ANMERKUNG: Wenn sich die Zugangsdaten für das Domainadministratorkonto und das lokale Administratorkonto unterscheiden, verwenden Sie das Domainadministratorkonto nicht zur Anmeldung bei MECM oder SCVMM. Verwenden Sie stattdessen ein anderes Domainnutzerkonto, um sich bei MECM oder SCVMM anzumelden.

   Wenn der Domänenname beispielsweise `mydomain` ist und TLD `com` ist, geben Sie den Domänennamen im Zugangsdatenprofil wie folgt an: `mydomain.com`.
6. Um die Verbindungen zwischen der OMIMSSC-Appliance und der Microsoft-Konsole zu überprüfen, klicken Sie auf **Verbindung testen**.
7. Klicken Sie auf **Registrieren**, um die Konsole nach einer erfolgreichen Testverbindung zu registrieren.
   Nach der Registrierung erstellt OMIMSSC ein Konto in SCVMM mit dem Namen **Registrierungsprofil für OMIMSSC-SCVMM-Konsolenerweiterung**. Stellen Sie sicher, dass dieses Profil nicht gelöscht wird, da Sie in OMIMSSC keine Vorgänge ausführen können, wenn dieses Profil gelöscht wird. Registrieren Sie den MECM-Standortserver zur Verwendung der OMIMSSC-Konsolenerweiterung in der MECM-Verwaltungskonsole.

Themen:

Zugriff auf OMIMSSC über registrierte Microsoft-Konsole

Starten Sie OMIMSSC über registrierte MECM- oder SCVMM-Konsole.

Hinzufügen der OMIMSSC-FQDN-Adresse im Browser

Vor dem Starten von OMIMSSC fügen Sie die FQDN-Adresse von OMIMSSC als Voraussetzung in die Standortliste **Lokales Intranet** ein, indem Sie die folgenden Schritte ausführen:

1. Klicken Sie auf **IE-Einstellungen** und anschließend auf **Internetoptionen**.
2. Klicken Sie auf **Erweitert** und suchen Sie unter **Einstellungen** nach dem Abschnitt **Sicherheit**.
3. Deaktivieren Sie die Option **Verschlüsselte Seiten nicht auf der Festplatte speichern** und klicken Sie auf **OK**.

Starten der OMIMSSC-Konsolenerweiterung für MECM

Zeigen Sie die unter Kontoberechtigungen erwähnte Tabelle der Benutzerrechte an.

Klicken Sie in der MECM-Konsole auf **Bestand und Einhaltung**, klicken Sie auf **Übersicht** und klicken Sie dann auf die **OMIMSSC-Konsolenerweiterung für MECM**.

ANMERKUNG: Wenn Sie über Remote Desktop Protocol (RDP) eine Verbindung zur MECM-Konsole herstellen, wird die OMIMSSC-Sitzung möglicherweise beendet, wenn das RDP geschlossen wird. Melden Sie sich daher nach dem erneuten Öffnen der RDP-Sitzung erneut an.

Entfernen der OMIMSSC-Konsolenerweiterung für SCVMM

Führen Sie die folgenden Schritte aus, um die OMIMSSC-Konsolenerweiterung für SCVMM zu importieren:

1. Starten Sie die SVMM-Konsole entweder mit Administratorrechten oder als delegierter Administrator.
2. Klicken Sie auf **Einstellungen** und dann auf **Konsolen-Add-In importieren**.
   Der Assistent für **Konsolen-Add-In importieren** wird angezeigt.
3. Klicken Sie auf **Durchsuchen** und wählen Sie die. zip-Datei unter `C:\Program Files\OMIMSSC\VMM Console Extension` aus. Klicken Sie auf **Weiter** und dann auf **Fertigstellen**.
   Stellen Sie sicher, dass das Add-In gültig ist.

Starten der OMIMSSC-Konsolenerweiterung für SCVMM

1. Wählen Sie in der SCVMM-Konsole **Struktur** und dann die Servergruppen **Alle Hosts** aus.

   ANMERKUNG: Um OMIMSSC zu starten, können Sie eine beliebige Hostgruppe auswählen, für die Sie eine Zugriffsberechtigung haben.

2. Wählen Sie in der Multifunktionsleiste **Home** die Option **DELL EMC OMIMSSC**.

7

Verwalten von OMIMSSC und seine Komponenten

Themen:

Anzeigen der OMIMSSC-Appliance-Details

1. Starten Sie das OMIMSSC-Verwaltungsportal über einen Browser.
2. Melden Sie sich beim OMIMSSC-Verwaltungsportal an, indem Sie dieselben Zugangsdaten verwenden, die auch bei der Anmeldung an der OMIMSSC-Appliance-VM verwendet wurden, und klicken Sie auf **Appliance-Details**. Die IP-Adresse und der Hostname der OMIMSSC-Appliance werden angezeigt.

Anzeigen der OMIMSSC-Nutzerverwaltung

1. Starten Sie das Verwaltungsportal OMIMSSC über einen Browser.
2. Melden Sie sich beim Verwaltungsportal OMIMSSC an, indem Sie dieselben Zugangsdaten verwenden, die auch bei der Anmeldung an der OMIMSSC-Appliance-VM verwendet wurden, und klicken Sie auf **OMIMSSC-Nutzerverwaltung**. Der Status der Benutzer, die zuvor in MECM oder SCVMM angemeldet waren, wird angezeigt.

Verwalten von HTTPS-Zertifikaten

OMIMSSC verwendet x.509-PKI-standardbasierte Zertifikate für den sicheren HTTP-Zugriff (HTTPS).

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

Für eine höhere Sicherheit wird empfohlen, die von der Zertifizierungsstelle oder der Enterprise-Zertifizierungsstelle (intern) signierten Zertifikate zu verwenden.

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

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

- Selbstsigniertes Zertifikat

  OMIMSSC erzeugt selbstsignierte Zertifikate nach der Konfiguration des Hostnamens der Appliance.

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

Aktualisieren von Zertifikaten für registrierte OMIMSSC-Server

OMIMSSC erstellt mithilfe der OpenSSL API das CSR (Certificate Signing Request) mit dem RSA-Verschlüsselungsstandard und einer Schlüssellänge von 2048 Bit.

Das von OMIMSSC generierte CSR ruft ein digital signiertes Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle ab. Mit dem digitalen Zertifikat aktiviert OMIMSSC auf dem Webserver HTTPS für die sichere Datenübertragung. Sie können das von der Zertifizierungsstelle signierte Zertifikat über das Verwaltungsportal hochladen.

Weitere Informationen über die HTTPS-Zertifikatverwaltung in OMIMSSC finden Sie im *Benutzerhandbuch zu OpenManage Integration für Microsoft System Center Version 7.3 für Microsoft Endpoint Configuration Manager und System Center Virtual Machine Manager 7.3 unter* https://www.dell.com/support.

Zertifikatsignierungsanforderung (CSR) erstellen

Das Erstellen einer neuen CSR verhindert, dass Zertifikate mit zuvor erstellten CSR auf das Gerät hochgeladen werden.

ANMERKUNG: Stellen Sie sicher, dass die Option **Herunterladen von Dateien** aktiviert ist, um eine CSR herunterzuladen. Diese Option gilt für **Internet Explorer**-Benutzer und kann über *Internetoptionen -> Sicherheit -> Internet > Nutzerdefinierte Stufe -> Downloads* aktiviert werden.

Um eine CSR zu erstellen, führen Sie die folgenden Schritte aus:

1. Wählen Sie auf der Seite **VerwaltungsportalEinstellungen ->Sicherheit** aus und klicken Sie auf **Zertifikatsignierungsanforderung erstellen** im Bereich **SSL-Zertifikate**. Eine Meldung zeigt an, dass bei der Erstellung einer neuen Zertifikatsignierungsanforderung Zertifikate, die mit der vorherigen Zertifikatsignierungsanforderung erstellt wurden, nicht mehr auf das Gerät hochgeladen werden.
2. Wenn Sie mit der Anforderung fortfahren, geben Sie im Dialogfenster **Zertifikatsignierungsanforderung erstellen** Informationen zum allgemeinen Namen, die Organisation, den Ort, das Bundesland, das Land, den Primären Alternativen Antragstellernamen, den Sekundären Alternativen Antragstellernamen und die E-Mail-Adresse an. Klicken Sie auf **Erstellen**.
3. Klicken Sie auf **Herunterladen** und speichern Sie das resultierende CSR an einem zugänglichen Speicherort.

HTTPS-Zertifikat hochladen

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

Die HTTPS-Zertifikate werden für die sichere Kommunikation zwischen der OMIMSSC-Appliance und Hostsystemen oder OMIMSSC verwendet. Um diese Art der sicheren Kommunikation einzurichten, senden Sie das CSR-Zertifikat an eine signierende Zertifizierungsstelle und laden Sie dann das resultierende signierte Zertifikat über die Verwaltungskonsole hoch.

1. Klicken Sie auf der Seite **Verwaltungsportal** auf **Einstellungen>Sicherheit** und klicken Sie dann auf **Zertifikat hochladen** im Bereich **SSL-Zertifikate**.
2. Wählen Sie Optionen aus dem Dialogfeld **Zertifikat hochladen** aus.
3. Klicken Sie zum Hochladen des gewünschten Zertifikats auf **Durchsuchen** und dann auf **Hochladen**.
4. Ein Dialogfeld wird angezeigt, das darauf hinweist, dass das Hochladen des Zertifikats abgeschlossen ist.

ANMERKUNG: Während das Zertifikat hochgeladen wird, reagiert die OMIMSSC-Appliance möglicherweise einige Minuten lang nicht, während die Services neu gestartet werden. Es wird empfohlen, alle vorhandenen Browsersitzungen des OMIMSSC-Verwaltungsportals und des OMIMSSC-Konsolen-Plug-ins auf den MECM-/SCVMM-Konsolen zu schließen. Melden Sie sich erneut beim OMIMSSC-Verwaltungsportal an, um das hochgeladene Zertifikat anzuzeigen.

Standardmäßiges HTTPS-Zertifikat wiederherstellen

1. Wählen Sie auf der Seite **Verwaltungsportal** die Option **Einstellungen–>Sicherheit** aus und klicken Sie auf „Standardmäßiges Zertifikat wiederherstellen“ im Bereich **SSL-Zertifikate**.
2. Klicken Sie im Dialogfeld **STANDARDMÄSSIGES ZERTIFIKAT WIEDERHERSTELLEN** auf **Ja**.

ANMERKUNG: Während das Standardzertifikat wiederhergestellt wird, reagiert die OMIMSSC-Appliance möglicherweise für einige Minuten nicht, während die Services neu gestartet werden. Es wird empfohlen, den Browser-Cache zu löschen und die vorhandenen Browsersitzungen des OMIMSSC-Verwaltungsportals und des OMIMSSC-Konsolen-Plug-ins auf den MECM-/SCVMM-Konsolen zu schließen. Melden Sie sich erneut beim OMIMSSC-Verwaltungsportal an, um das aktualisierte Zertifikat anzuzeigen.

Anzeigen oder Aktualisieren von registrierten Konsolen

Sie können alle registrierten Microsoft-Konsolen mit OMIMSSC anzeigen. Führen Sie dazu die folgenden Schritte durch:

1. Klicken Sie im OMIMSSC-Verwaltungsportal auf Einstellungen und dann auf **Konsolenregistrierung**.
   Alle registrierten Konsolen werden angezeigt.
2. Klicken Sie auf **Einstellungen** und dann auf **Konsolenregistrierung**.
   Alle registrierten Konsolen werden angezeigt.
3. Zum Anzeigen der aktuellen Liste der registrierten Konsolen klicken Sie auf **Aktualisieren**.

Ändern des Kennworts der OMIMSSC-Appliance

Führen Sie die folgenden Schritte aus, um das Kennwort der OMIMSSC-Appliance-VM-Konsole zu ändern:

1. Starten Sie die OMIMSSC-Appliance-VM-Konsole und melden Sie sich mit den alten Zugangsdaten an.
2. Navigieren Sie zu **Administratorkennwort ändern** und drücken Sie die **Eingabetaste**.
   Der Bildschirm zum Ändern des Kennworts wird angezeigt.
3. Geben Sie Ihr aktuelles Kennwort ein und geben Sie dann ein neues Kennwort ein, das den aufgeführten Kriterien entspricht. Geben Sie das neue Kennwort erneut ein und drücken Sie die **Eingabetaste**.
   Der Status nach dem Ändern des Passworts wird angezeigt.
4. Um zur Startseite zurückzukehren, drücken Sie die **Eingabetaste**.

ANMERKUNG: Die Appliance wird nach dem Ändern des Kennworts neu gestartet.

Neustarten der OMIMSSC-Appliance

Führen Sie die folgenden Schritte aus, um das OMIMSSC-Gerät neu zu starten:

1. Starten Sie die OMIMSSC-Appliance-VM und melden Sie sich an.
2. Navigieren Sie zu **Dieses virtuelle Gerät neu starten** und drücken Sie die **Eingabetaste**.
3. Um zu bestätigen, klicken Sie auf **Ja**.
   Das OMIMSSC-Gerät wird zusammen mit allen erforderlichen Diensten neu gestartet.
4. Melden Sie sich nach dem Neustart der VM bei der OMIMSSC-Appliance an.

Ändern von MECM-und SCVMM-Konten im OMIMSSC-Verwaltungsportal

Mit dieser Option können Sie die Kennwörter von MECM- und SCVMM-Konten in der OMIMSSC-Konsole ändern.

Sie können die MECM- und SCVMM-Administratorkennwörter vom OMIMSSC-Verwaltungsportal aus ändern. Dieser Prozess ist eine sequentielle Aktivität.

1. Ändern Sie das Kennwort des MECM- oder SCVMM-Administratorkontos in Active Directory.
2. Ändern Sie das Kennwort in OMIMSSC.

Führen Sie die folgenden Schritte aus, um das MECM- oder SCVMM-Administratorkonto in OMIMSSC zu ändern:

1. Klicken Sie im OMIMSSC-Verwaltungsportal auf **Einstellungen** und dann auf **Konsolenregistrierung**.
   Die angemeldeten Konsolen werden angezeigt.
2. Klicken Sie auf **Einstellungen** und dann auf **Konsolenregistrierung**.
   Die angemeldeten Konsolen werden angezeigt.
3. Wählen Sie eine zu bearbeitende Konsole aus und klicken Sie auf **Bearbeiten**.
4. Geben Sie das neue Kennwort ein und klicken Sie auf **Fertig stellen**, um die Änderungen zu speichern.

Starten Sie nach dem Aktualisieren des Kennworts die Microsoft-Konsole und die OMIMSSC-Konsolenerweiterungen mit den neuen Zugangsdaten erneut.

Reparieren oder Ändern von Installationsprogrammen

Informationen zum Reparieren von Installationsdateien finden Sie in den folgenden Themen:

- Reparieren der OMIMSSC-Konsolenerweiterung für MECM
- Reparieren der OMIMSSC-Konsolenerweiterung für SCVMM

Reparieren der OMIMSSC-Konsolenerweiterung für MECM

Führen Sie die folgenden Schritte aus, um die OMIMSSC-Dateien zu reparieren, falls sie beschädigt sind:

1. Führen Sie die OMIMSSC-Konsolenerweiterung für MECM-Installer aus.
   Der **Startbildschirm** wird angezeigt.
2. Klicken Sie auf **Weiter**.
3. Wählen Sie unter **Programmwartung** die Option **Reparieren** aus und klicken Sie auf **Weiter**.
   Das Fenster **Bereit zur Reparatur des Programms** wird angezeigt.
4. Klicken Sie auf **Installieren**.
   Ein Verlaufsbildschirm zeigt den Fortschritt der Installation an. Wenn die Installation abgeschlossen ist, wird das Fenster **InstallShield-Assistent abgeschlossen** angezeigt.
5. Klicken Sie auf **Fertigstellen**.

Reparieren der OMIMSSC-Konsolenerweiterung für SCVMM

Führen Sie die folgenden Schritte aus, um die OMIMSSC-Dateien zu reparieren, falls sie beschädigt sind:

1. Führen Sie die *OMIMSSC*-Konsolenerweiterung für SCVMM-Installer aus.
2. Wählen Sie unter **Programmwartung** die Option **Reparieren** aus und klicken Sie auf **Weiter**.
3. Klicken Sie unter **Bereit zum Reparieren oder Entfernen des Programms** auf **Reparieren**.
4. Wenn die Reparatur abgeschlossen ist, klicken Sie auf **Fertigstellen**.

8

Backup und Wiederherstellung der OMIMSSC Appliance

Speichern Sie mithilfe der Option **Gerätedaten sichern** vom OMIMSSC-Gerät OMIMSSC-Informationen wie registrierte Microsoft-Konsolen, erkannte Geräte, Profile, Update-Quellen, Betriebsvorlagen, Lizenzen und abgeschlossene Jobs in OMIMSSC-Konsolenerweiterungen.

Themen:

OMIMSSC-Appliance sichern

Mit dieser Funktionalität können die OMIMSSC-Appliance-Datenbank und wichtige Konfigurationen gesichert werden. Die Backup-Datei wird auf dem CIFS-Freigabepfad mit einem verschlüsselten Passwort gespeichert, das vom Benutzer bereitgestellt wird. Es wird empfohlen, die Gerätedaten regelmäßig zu sichern.

Voraussetzungen:

- Stellen Sie sicher, dass Sie eine CIFS-Freigabe mit Zugangsberechtigungen erstellen und Lese- und Schreibberechtigungen zulassen.
- Stellen Sie sicher, dass sowohl für die Sicherung als auch für die Wiederherstellung dasselbe Verschlüsselungspasswort verwendet wird. Das Verschlüsselungskennwort kann nicht wiederhergestellt werden.

Führen Sie die folgenden Schritte aus, um die OMIMSSC Appliance-Daten auf der CIFS-Freigabe zu sichern.

ANMERKUNG: Diese Funktion ist ab OMIMSSC-Version 7.2.1 verfügbar und nicht auf der Appliance-VM-Konsole verfügbar.

1. Klicken Sie im OMIMSSC-Admin-Portal auf **Einstellungen** und dann auf **Gerät wiederherstellen**.
2. Geben Sie auf der Seite **Sicherungseinstellungen und Details** den CIFS-Freigabepfad für die Sicherung im `\\<IP address or FQDN>\<folder name>`-Format an.
3. Wählen Sie das **Zugangsdatenprofil für die CIFS-Freigabe** aus dem Dropdown-Menü.
4. Geben Sie das Verschlüsselungspasswort in die Felder **Kennwort** und **Kennwort erneut eingeben** ein.
5. Klicken Sie auf **Verbindung testen**, um die Konnektivität zwischen der OMIMSSC-Appliance und der CIFS-Freigabe zu überprüfen. Stellen Sie sicher, dass der genannte Backup-Ordner existiert und zugänglich ist
6. Klicken Sie auf **Backup**, um die OMIMSSC-Appliance-Daten zu sichern.

Nächste Schritte

Um zu bestätigen, dass das Backup erfolgreich ist, wechseln Sie zum Backup-Ordner. Es werden zwei Dateien im Backup-Ordner im folgenden Format erstellt:

- Dell_OMIMSSC_VM_Backup_<date_and_time>.tar.gz
- Dell_OMIMSSC_VM_Backup_<date_and_time>.tar.gz.sum

ANMERKUNG: Datum und Uhrzeit in den Sicherungsdateien zeigen an, wann die Sicherung erstellt wurde. Benennen Sie die Sicherungsdatei nicht um.

ANMERKUNG: Überprüfen Sie, ob die Appliance-Daten erfolgreich gesichert werden und die Größe der Backup-Datei mehr als 1 KB beträgt. Wenn die Dateigröße weniger als 1 KB beträgt, starten Sie die Appliance neu. Sichern Sie nach dem Neustart der Appliance die OMIMSSC-Appliance-Daten.

OMIMSSC-Gerät wiederherstellen

- Der Wiederherstellungsvorgang muss nur auf einer neu bereitgestellten Appliance durchgeführt werden. Stellen Sie sicher, dass kein Vorgang auf dem neuen Gerät durchgeführt wurde.

- Entfernen Sie das alte Konsolen-Add-in aus der SCVMM-Konsole und führen Sie ein Upgrade des OMIMSSC-Konsolen-Add-Ins durch, indem Sie das neue Installationsprogramm herunterladen. Weitere Informationen finden Sie im Abschnitt der einheitlichen Benutzerhandbuchs *Aktualisieren der OMIMSSC-Konsolenerweiterung für MECM/SCVMM in der OpenManage Integration für Microsoft System Center*.

Stellen Sie die OMIMSSC-Gerätedaten in einem der folgenden Szenarien wieder her:

- Vor der Aktualisierung auf eine neue Version von OMIMSSC
- Vor der Migration von einem OMIMSSC-Gerät zu einem anderen OMIMSSC-Gerät.

Voraussetzungen:

Stellen Sie sicher, dass Sie die Daten wiederherstellen, bevor Sie Vorgänge am neuen OMIMSSC-Gerät durchführen.

Führen Sie die folgenden Schritte aus, um alte OMIMSSC-Gerätedaten auf einem neuen OMIMSSC-Gerät wiederherzustellen:

1. Klicken Sie im OMIMSSC-Admin-Portal auf **Einstellungen** und dann auf **Gerät wiederherstellen**.
2. Für die Wiederherstellung von Gerätedaten stehen zwei Optionen zur Verfügung.
   - `Option 1: Restore using IP address`

     Diese Option muss verwendet werden, um Daten aus den OMIMSSC-Versionen 7.2 und 7.2.1 wiederherzustellen.

     Geben Sie unter IP-Adresse die IP-Adresse der alten OMIMSSC-Appliance an und klicken Sie auf Wiederherstellen.

     ANMERKUNG: Die Daten werden auf der neuen OMIMSSC-Appliance wiederhergestellt.
   - Option 2: Wiederherstellung unter Verwendung einer nutzerdefinierten CIFS-Freigabe

     Diese Option sollte verwendet werden, um Daten ab Version 7.2.1 wiederherzustellen.

     ANMERKUNG: CIFS-Freigabezugangsdaten werden in der Datenbank als Zugangsdatenprofil gespeichert. Für zusätzliche Sicherheitsmaßnahmen sollte ein Verschlüsselungspasswort zum Entschlüsseln der gesicherten Datei bereitgestellt werden.

   a. Geben Sie den CIFS-Freigabepfad im Format `\\<IP address or FQDN>\<folder name>\<filename>.tar.gz` an.
   b. Wählen Sie das Zugangsdatenprofil für die CIFS-Freigabe aus dem Dropdown-Menü.
   c. Geben Sie das Passwort für die Dateiverschlüsselung ein und klicken Sie auf Wiederherstellen.

   Die Seite **Wiederherstellen** wird automatisch abgemeldet.
3. So zeigen Sie den Wiederherstellungsstatus nach dem Neustart der OMIMSSC-Appliance an:

   Es wird empfohlen, dass Sie einige Minuten warten, bevor Sie sich anmelden, damit alle Dienste gestartet werden.

   a. Melden Sie sich beim OMIMSSC-Admin-Portal an.
   b. Erweitern Sie **Einstellungen** und klicken Sie dann auf **Protokolle**.
   c. Laden Sie die Datei dlciappliance_main.log herunter und suchen Sie nach der folgenden Nachricht nach einer erfolgreichen Wiederherstellung:

   ```
   Successfully restored OMIMSSC Appliance
   ```
4. Im Falle einer SCVMM-Konsole importieren Sie das neue Konsolen-Add-in neu, nachdem Sie den Wiederherstellungsvorgang auf der OMIMSSC-Appliance erfolgreich durchgeführt haben.

Führen Sie nach dem Wiederherstellen des alten OMIMSSC-Geräts die folgenden Schritte aus:

- Es wird empfohlen, die geplanten Aufträge nach dem Wiederherstellen des alten OMIMSSC-Geräts neu zu erstellen.
- Stellen Sie für die Hypervisor-Profile, die aus einer früheren Version von OMIMSSC exportiert wurden, sicher, dass Sie das Profil bearbeiten, um den ISO-Dateipfad und das Windows-Zugangsdatenprofil anzugeben.
- Erstellen Sie eine neue CSR-Anfrage und importieren Sie ein gültiges Zertifikat.

9

Deinstallation OMIMSSC

So deinstallieren Sie OMIMSSC:

1. Heben Sie die Registrierung für die OMIMSSC-Konsole über das OMIMSSC-Verwaltungsportal auf. Weitere Informationen finden Sie unter Registrierung der OMIMSSC-Konsole aufheben.
2. Deinstallieren Sie die OMIMSSC-Konsolenerweiterung für die registrierte Microsoft-Konsole. Weitere Informationen finden Sie unter Deinstallieren der OMIMSSC-Konsolenerweiterung für MECM oder Deinstallieren der OMIMSSC-Konsolenerweiterung für SCVMM.
3. Appliance-VM entfernen. Weitere Informationen finden Sie unter Entfernen der OMIMSSC-Appliance-VM.
4. Entfernen Sie die gerätespezifischen Konten. Weitere Informationen finden Sie unter Weitere Deinstallationstasks.

Themen:

Aufheben der Registrierung der Microsoft-Konsole OMIMSSC

Wenn Sie mehrere Microsoft-Konsolen an einer OMIMSSC-Appliance angemeldet haben, können Sie eine Konsole abmelden und weiterhin mit OMIMSSC arbeiten. Informationen zur vollständigen Deinstallation finden Sie im *Benutzerhandbuch zu OpenManage Integration für Microsoft System Center*.

Führen Sie die folgenden Schritte aus, um die Registrierung einer Microsoft-Konsole aufzuheben:

1. Klicken Sie in OMIMSSC auf **Konsolenregistrierung**.
   Alle Konsolen, die an der OMIMSSC-Appliance registriert sind, werden angezeigt.
2. Wählen Sie die Konsole aus und klicken Sie auf **Registrierung aufheben**, um die Registrierung der Konsole auf Appliance zu entfernen.
3. Deinstallieren Sie das Konsolen-Plug-in.

   ANMERKUNG:
   - Nach dem Aufheben der Registrierung einer Konsole und ihrer Deinstallation werden die Host-Server, die der Konsole zugeordnet sind, in die Liste der nicht zugewiesenen Server in OMIMSSC verschoben.

4. (Optional) Wenn die Konsole nicht erreichbar ist, klicken Sie auf **Ja**, wenn Sie aufgefordert werden, die Konsole zwangsweise abzumelden.
   - Wenn eine OMIMSSC-Konsole während dem Aufheben der Registrierung bereits geöffnet ist, schließen Sie die Microsoft-Konsole, um die Aufhebung abzuschließen.
   - Für SCVMM-Benutzer:
     - Wenn Sie die Registrierung der SCVMM-Konsole am OMIMSSC zwangsweise aufheben, wenn der SCVMM-Server nicht erreichbar ist, löschen Sie das **Anwendungsprofil** in SCVMM manuell.

Installieren der OMIMSSC-Konsolenerweiterung für MECM

Doppelklicken Sie auf `OMIMSSC_MECM(SCCM)_Console_Extension.exe`, wählen Sie **Remove** aus und folgen Sie den Anweisungen auf dem Bildschirm.

Deinstallieren der OMIMSSC-Konsolenerweiterung für SCVMM

So deinstallieren Sie die OMIMSSC-Konsolenerweiterung für SCVMM:

1. Entfernen Sie die Konsolenerweiterung für **Programm deinstallieren**.
   - Klicken Sie in der **Systemsteuerung** auf **Programme** und dann auf **Programm deinstallieren**.
   - Wählen Sie **Konsolen-Add-In für SCVMM** aus und klicken Sie auf **Deinstallieren**.
2. Entfernen Sie die Konsolenerweiterung in SCVMM.
   - Klicken Sie in der SCVMM-Konsole auf **Einstellungen**.
   - Klicken Sie mit der rechten Maustaste auf OMIMSSC und wählen Sie **Entfernen**.

Weitere Schritte zur Deinstallation

Um die OMIMSSC-Konsolenerweiterung aus SCVMM zu entfernen, löschen Sie die folgenden Konten und Profile:

- Appliance-spezifische ausführende Konten
- OMIMSSC Anwendungsprofil

Löschen von Appliance-spezifischen ausführenden Konten

So löschen Sie gerätespezifische „Ausführen als“-Konten aus der SCVMM-Konsole.

1. Klicken Sie in der SCVMM-Konsole auf **Einstellungen**.
2. Klicken Sie auf **Als Konten ausführen**.
3. Löschen Sie gerätespezifische Konten aus der Liste von Konten.
   Appliance-spezifische Konten haben das Präfix `Dell_`.

Löschen von OMIMSSC-Anwendungsprofilen

1. Klicken Sie in der SCVMM-Konsole auf **Bibliothek**, **Profile** und klicken Sie dann auf die **Anwendungsprofile**.
   Alle in SCVMM verwendeten Anwendungsprofile werden angezeigt.
2. Wählen Sie das **OMIMSSC-Registrierungsprofil** aus und löschen Sie es.

Entfernen von Appliance-VM

So entfernen Sie die Appliance VM:

1. Klicken Sie in **Windows Server** in **Hyper-V Manager** mit der rechten Maustaste auf die Appliance-VM und klicken Sie dann auf **Deaktivieren**.
2. Klicken Sie mit der rechten Maustaste auf die Appliance-VM und klicken Sie dann auf **Löschen**.

ANMERKUNG: Bevor Sie die Appliance-VM entfernen, müssen Sie eine Sicherungskopie erstellen, da dies die letzte Chance für ein Backup ist, bevor Sie die Appliance-VM entfernen.

10

Aktualisieren von OMIMSSC

Sie können die OMIMSSC-Appliance auf die neueste Version durch das Backup der OMIMSSC Appliance-Daten (einschließlich Einstellungen und Konfigurationen) und die anschließende Wiederherstellung der gesicherten Datei in der neuesten Version der OMIMSSC Appliance aktualisieren.

Weitere Informationen zum Sichern und Wiederherstellen der OMIMSSC-Appliance finden Sie in den Abschnitten Sichern der OMIMSSC-Appliance und OMIMSSC-Gerät wiederherstellen.

Die folgende Tabelle enthält den Aktualisierungspfad für die OMIMSCC-Appliance-Version 7.3. Für einige Versionen ist eine Zwischenaktualisierung vor dem Upgrade auf die Version 7.3 notwendig:

Tabelle 8. Aktualisierungspfad für die OMIMSCC-Appliance-Version 7.3

Aktuelle Version der OMIMCC-Appliance	Zwischenaktualisierungsversion	Zielversion von OMIMSCC
7.2.1	N/A (oder direktes Upgrade)	7.3
7.2	N/A oder direktes Upgrade)	7.3
7.1.1	7.2.1	7.3
7.1	7.2.1	7.3

11

Verwalten von Anmeldedaten und Hypervisor-Profilen

Profile enthalten alle Daten, die zur Ausführung von Operationen in OMIMSSC erforderlich sind.

Themen:

Zugangsdatenprofil in MECM und SCVMM

Zugangsdatenprofile vereinfachen die Verwendung und Verwaltung von Nutzerzugangsdaten durch die Authentifizierung der rollenbasierten Funktionen des Benutzers. Jedes Zugangsdatenprofil enthält einen Nutzernamen und ein Kennwort für ein einzelnes Nutzerkonto.

OMIMSSC verwendet ein Zugangsdatenprofil zur Verbindung mit dem iDRAC der verwalteten Systeme.

Sie können vier Typen von Zugangsdatenprofilen erstellen:

- Profil für Geräte-Zugangsdaten: Wird verwendet, um sich bei iDRAC oder CMC anzumelden. Mit diesem Profil können Sie auch einen Server ermitteln, Synchronisierungsprobleme beheben und ein Betriebssystem bereitstellen. Dieses Profil ist spezifisch für eine Konsole. Sie können dieses Profil nur in einer Konsole verwenden und verwalten, in der es erstellt wurde.
- Windows-Zugangsdatenprofil: wird für den Zugriff auf Freigabeordner im Windows-Betriebssystem verwendet
- Proxyserver-Zugangsdaten: wird für die Bereitstellung von Proxy-Zugangsdaten für den Zugriff auf FTP-Sites für Aktualisierungen verwendet.

  ANMERKUNG: Alle Profile außer dem Geräteprofil sind freigegebene Ressourcen. Sie können diese Profile von allen registrierten Konsolen aus verwenden und verwalten.

Zugangsdatenprofil erstellen

Berücksichtigen Sie die folgenden Punkte, bei der Erstellung eines Profils mit Zugangsdaten:

- Wenn während der automatischen Ermittlung ein Standardprofil mit Zugangsdaten nicht für iDRAC verfügbar ist, wird der Standardwert für die iDRAC-Zugangsdaten verwendet. Der Standardnutzername für iDRAC ist `root` und das Kennwort lautet `calvin`.

  ANMERKUNG: Bevor Sie einen Server ermitteln, empfiehlt Dell EMC die Erstellung eines standardmäßigen iDRAC-Zugangsdatenprofils mit einem sicheren Kennwort. Das Standard-Zugangsdatenprofil wird für die automatische Ermittlung verwendet. Weitere Informationen zu den Anforderungen an die Kennwortrichtlinie finden Sie im iDRAC-Benutzerhandbuch.
- Um Informationen zu den modularen Systemen zu erhalten, wird auf den modularen Server mit dem Standard-CMC-Profil zugegriffen. Der Nutzername des Standard-CMC-Profils ist `root` und das Kennwort lautet `calvin`.
- (Nur für SCVMM-Nutzer) Wenn ein Gerätetyp-Zugangsdatenprofil erstellt wird, wird ein zugehöriges **ausführendes Konto** in **SCVMM** zur Verwaltung des Geräts angelegt. Der Name dieses **ausführenden Kontos** ist `Dell_CredentialProfileName`.
- Stellen Sie sicher, dass Sie das **ausführende Konto** in SCVMM nicht bearbeiten oder löschen.

1. Führen Sie in OMIMSSC einen der folgenden Schritte aus, um ein **Zugangsdatenprofil** zu erstellen:
   - Klicken Sie im OMIMSSC-Dashboard auf **Zugangsdatenprofil erstellen**.
   - Klicken Sie im Navigationsbereich auf **Profile** > **Zugangsdatenprofil** und klicken Sie dann auf **Erstellen**.
2. Klicken Sie auf **Erstellen**.
   Die Seite **Zugangsdatenprofil** wird angezeigt.
3. Wählen Sie unter **Anmeldetyp** den Typ des Zugangsdatenprofils aus, den Sie verwenden möchten.
4. Geben Sie einen Profilnamen und eine Beschreibung ein.

ANMERKUNG: Die Option **Standardprofil für** gilt nur für ein Zugangsdatenprofil des Gerätetyps.

5. Geben Sie unter **Zugangsdaten** den Nutzernamen und das Kennwort ein.
   - Wenn Sie ein **Profil für Geräte-Zugangsdaten** erstellen, legen Sie dieses Profil als Standardprofil für die Anmeldung bei iDRAC oder CMC fest, indem Sie die Option **Standardprofil für** auswählen. Wählen Sie **Kein**, wenn Sie das Profil nicht als Standardprofil festlegen möchten.

     ANMERKUNG: Das Standard-Zugangsdatenprofil ist nicht spezifisch für die Konsole. Wenn das Zugangsdatenprofil als Standard in der aktuellen Konsole ausgewählt ist, sind die anderen Konsolen für den ausgewählten Typ nicht standardmäßig ausgewählt.
   - Wenn Sie ein **Windows-Zugangsdatenprofil** erstellen, geben Sie die Domaindetails in **Domain** an.

     ANMERKUNG: Wenn der NETBIOS-Name in Active Directory (AD) konfiguriert ist, geben Sie bei der Erstellung des Zugangsdatenprofils für die Konsolenregistrierung den NETBIOS-Namen als Domäne an. Wenn der NETBIOS-Name nicht im AD konfiguriert ist, geben Sie den Domänennamen mit Angaben zur Top Level Domain (TLD) an.

     Wenn der Domänenname beispielsweise `mydomain` ist und TLD `com` ist, geben Sie den Domänennamen im Zugangsdatenprofil wie folgt an: `mydomain.com`
   - Wenn Sie **Proxyserver-Zugangsdaten** erstellen, geben Sie die Proxyserver-URL im Format `http://hostname:port` oder `http://IPaddress:port` unter **Proxyserver-URL** an.
6. Um das Profil zu erstellen, klicken Sie auf **Fertig stellen**.

ANMERKUNG: Wenn Sie ein Geräte-Zugangsdatenprofil in SCVMM erstellen, wird ein entsprechendes **„Ausführen als“-Konto** mit einem Namen erstellt, der **Dell_** als Präfix hat. Stellen Sie sicher, dass der registrierte Nutzer Zugriff auf die entsprechenden **„Ausführen als“-Konto**vorgänge hat, wie z. B. auf die Betriebssystembereitstellung, die das erstellte Zugangsdatenprofil für das Gerät verbraucht.

Ändern eines Zugangsdatenprofils

Berücksichtigen Sie Folgendes, bevor Sie ein Zugangsdatenprofil ändern:

- Nach dem Erstellen können Sie den Typ eines Zugangsdatenprofils nicht mehr ändern. Sie können jedoch andere Felder ändern.
- Sie können ein Zugangsdatenprofil nicht ändern, wenn es verwendet wird.

ANMERKUNG: Die Schritte zum Ändern eines beliebigen Zugangsdatenprofiltyps sind gleich.

1. Wählen Sie das Zugangsdatenprofil aus, das Sie ändern möchten, klicken Sie auf **Bearbeiten** und aktualisieren Sie das Profil nach Bedarf.
2. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Aktualisieren Sie die Seite **Zugangsdatenprofil**, um die vorgenommenen Änderungen anzuzeigen.

Löschen von Zugangsdatenprofilen

Berücksichtigen Sie Folgendes, wenn Sie ein Zugangsdatenprofil löschen möchten:

- Wenn ein Geräte-Zugangsdatenprofil gelöscht wird, wird das zugehörige **„Ausführen als“-Konto** ebenfalls aus SCVMM gelöscht.
- Nachdem das **ausführende Konto** aus SCVMM gelöscht wurde, ist das entsprechende Zugangsdatenprofil nicht mehr in OMIMSSC verfügbar.
- Wenn Sie ein Zugangsdatenprofil löschen möchten, das im Rahmen einer Serverermittlung verwendet wird, löschen Sie zuerst die ermittelten Server und anschließend das Zugangsdatenprofil.
- Wenn Sie ein Geräte-Zugangsdatenprofil löschen möchten, das im Rahmen einer Bereitstellung verwendet wird, löschen Sie zuerst die in der SCVMM-Umgebung bereitgestellten Server und anschließend das Zugangsdatenprofil.
- Sie können ein Zugangsdatenprofil, das in einer Aktualisierungsquelle verwendet wird, nicht löschen.

ANMERKUNG: Die Schritte zum Löschen eines beliebigen Zugangsdatenprofiltyps sind gleich.

Wählen Sie das Zugangsdatenprofil aus, das Sie löschen möchten, und klicken Sie dann auf **Löschen**.

Aktualisieren Sie die Seite **Zugangsdatenprofil**, um die vorgenommenen Änderungen anzuzeigen.

Hypervisor-Profil in SCVMM

Ein Hypervisor-Profil enthält ein nutzerdefiniertes WinPE-ISO-Protokoll (WinPE-ISO wird für die Hypervisor-Bereitstellung verwendet), eine Hostgruppe und ein Hostprofil, die aus SCVMM stammen, und LC-Treiber für die Injektion. Nur eine OMIMSSC-Konsolenerweiterung für SCVMM-Benutzer kann Hypervisor-Profile erstellen und verwalten.

Erstellen eines Hypervisor-Profils

Erstellen Sie ein Hypervisor-Profil und verwenden Sie das Profil zum Bereitstellen von Hypervisoren.

- Aktualisieren Sie das WinPE-ISO-Image und erhalten Sie Zugriff auf den Freigabeordner, in dem das Image gespeichert ist. Informationen zum Aktualisieren des WinPE-Images finden Sie unter WinPE-Aktualisierung.

  Aktualisieren Sie das WinPE-ISO-Image und erhalten Sie Zugriff auf den Freigabeordner, in dem das Image gespeichert ist. Informationen zum Aktualisieren des WinPE-Images finden Sie im Abschnitt WinPE-Aktualisierung im einheitlichen Benutzerhandbuch *OpenManage Integration for Microsoft System Center für Configuration Manager und Virtual Machine Manager*.

- Erstellen Sie eine Hostgruppe, ein Hostprofil oder ein physisches Computerprofil in SCVMM. Informationen zum Erstellen von Hostgruppen in SCVMM finden Sie in der Microsoft-Dokumentation.

1. Führen Sie in OMIMSSC einen der folgenden Tasks aus:
   - Klicken Sie im OMIMSSC-Dashboard auf **Hypervisor-Profile erstellen**.
   - Klicken Sie im linken Navigationsbereich auf **Profile und Vorlagen**, dann auf **Hypervisor-Profil** und schließlich auf **Erstellen**.

   Der **Assistent "Hypervisor-Profil"** wird angezeigt.
2. Klicken Sie auf der **Startseite** auf **Weiter**.
3. Geben Sie unter **Hypervisor-Profil** einen Namen und eine Beschreibung für das Profil ein und klicken Sie dann auf **Weiter**.
4. Auf der **SCVMM-Informationsseite**
   a. Wählen Sie für **SCVMM-Hostgruppenziel** eine SCVMM-Hostgruppe aus dem Dropdownmenü aus, um den Host dieser Gruppe hinzuzufügen.
   b. Wählen Sie unter **SCVMM-Hostprofil/Physisches Computerprofil** ein Hostprofil oder ein physisches Computerprofil aus SCVMM aus, das Konfigurationsinformationen enthält, die auf Servern angewendet werden sollen.

      Wählen Sie in SCVMM eine der folgenden Festplattenpartitionsmethoden in einem **physischen Computerprofil** aus:
      - Wenn Sie im UEFI-Modus starten, wählen Sie die Option **GUID Partition Table (GPT)**.
      - Wählen Sie beim Booten im BIOS-Modus die Option **Master Board Record (MBR)**.
5. Geben Sie in der **WinPE-Start-Image-Quelle** die folgenden Details an und klicken Sie auf **Weiter**.
   a. Geben Sie für **Netzwerk-WinPE-ISO-Name** den Pfad zum freigegebenen Ordner mit dem aktualisierten WinPE-Dateinamen an. Informationen zum Aktualisieren der WinPE-Datei finden Sie unter WinPE-Aktualisierung.
   b. Geben Sie für **Netzwerk-WinPE-ISO-Name** den Pfad zum freigegebenen Ordner mit dem aktualisierten WinPE-Dateinamen an. Informationen zum Aktualisieren der WinPE-Datei finden Sie im Abschnitt WinPE-Aktualisierung des einheitlichen Benutzerhandbuchs *OpenManage Integration for Microsoft System Center für Configuration Manager und Virtual Machine Manager*.
   c. Wählen Sie für **Zugangsdatenprofil** die Zugangsdaten aus, die Zugriff auf den Freigabeordner mit der WinPE-Datei haben.
   d. (Optional) Um ein neues Windows-Zugangsdatenprofil zu erstellen, klicken Sie auf **Neu erstellen**. Weitere Informationen zum Erstellen eines Zugangsdatenprofils finden Sie unter Zugangsdatenprofil erstellen.
   e. (Optional) Um ein neues Windows-Zugangsdatenprofil zu erstellen, klicken Sie auf **Neu erstellen**. Informationen zum Erstellen eines Zugangsdatenprofils finden Sie im entsprechenden Abschnitt des Benutzerhandbuchs *OpenManage Integration for Microsoft System Center für Configuration Manager und Virtual Machine Manager*.
6. (Optional) Führen Sie die folgenden Schritte aus, um die LC-Treiber-Injektion zu aktivieren:

   ANMERKUNG: Stellen Sie sicher, dass Sie das Kontrollkästchen **Dell Lifecycle Controller Treiberinjektion aktivieren** aktivieren, da die neuesten Betriebssystemtreiberpakete für NIC-Karten in den neuesten Betriebssystemtreibern verfügbar sind.

   a. Wählen Sie **Dell Lifecycle Controller Treiberinjektion aktivieren**.
   b. Wählen Sie das Betriebssystem aus, das Sie bereitstellen möchten, damit die entsprechenden Treiber ausgewählt werden.
7. Klicken Sie unter **Zusammenfassung** auf **Fertigstellen**.

Aktualisieren Sie die Seite **Hypervisor-Profil**, um die vorgenommenen Änderungen anzuzeigen.

Ändern eines Hypervisor-Profils

Berücksichtigen Sie Folgendes, wenn Sie ein Hypervisor-Profil modifizieren möchten:

- Sie können Hostprofile, Hostgruppen und Treiber vom Lifecycle Controller her ändern.
- Sie können den WinPE ISO-Namen ändern. Sie können das ISO-Image jedoch nicht ändern.

1. Wählen Sie das Profil aus, das Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.
2. Geben Sie die Details ein und klicken Sie dann auf **Fertig stellen**.

Aktualisieren Sie die Seite **Hypervisor-Profil**, um die vorgenommenen Änderungen anzuzeigen.

Löschen eines Hypervisor-Profils

Wählen Sie das Hypervisor-Profil aus, das Sie löschen möchten, und klicken Sie dann auf **Löschen**.

Aktualisieren Sie die Seite **Hypervisor-Profil**, um die vorgenommenen Änderungen anzuzeigen.

12

Ermitteln von Geräten und Synchronisieren von Servern mit der OMIMSSC-Konsole

Bei der Ermittlung werden unterstützte modulare Systeme und Bare-Metal-Server von PowerEdge oder Hostserver oder Knoten zu OMIMSSC hinzugefügt.

Bei der Synchronisierung mit der MSSC-Konsole werden Hostserver von der registrierten Microsoft-Konsole (MECM oder SCVMM) zu OMIMSSC hinzugefügt. Daher können Sie mit einem der Prozesse Geräte zu OMIMSSC hinzufügen. Erst nachdem Sie die Geräte ermittelt haben, können Sie sie in OMIMSSC verwalten.

Themen:

Ermitteln von Geräten in OMIMSSC

Ermitteln Sie MX7000-Modularsysteme, Hosts und nicht zugewiesene Server in OMIMSSC. Informationen zu ermittelten Geräten werden im OMIMSSC-Gerät gespeichert.

Mit den folgenden Methoden können Sie Dell EMC-Server anhand ihrer iDRAC-IP-Adresse ermitteln:

- Ermitteln von Servern über die automatische Ermittlung
- Ermitteln von Servern über die manuelle Ermittlung

ANMERKUNG: Das ermittelte Gerät wird als "hardwarekompatibel" markiert, wenn es unterstützte Versionen von LC-Firmware, iDRAC und BIOS enthält, die für die Verwendung mit OMIMSSC erforderlich sind. Informationen zu unterstützten Versionen finden Sie in den Versionshinweisen OpenManage Integration for Microsoft System Center.

Ermitteln Sie modulare Systeme mit der Geräte-IP-Adresse mithilfe von Ermitteln modularer Systeme mit der Methode "manuelle Ermittlung".

Geräteerkennung in der OMIMSSC-Konsolenerweiterung für MECM

Ermitteln Sie Geräte in der OMIMSSC-Konsolenerweiterung für MECM. Nach dem Ermitteln eines Servers wird der Server zu einer vordefinierten Gruppe in OMIMSSC und einer der folgenden vordefinierten MECM-Gruppen oder -Sammlungen hinzugefügt: **Sammlung "Alle Dell Lifecycle Controller-Server"** und **Sammlung "Dell-Server importieren"**, die unter den **Gerätesammlungen** erstellt werden.

Wenn der ermittelte Server nicht in MECM vorhanden ist oder wenn in MECM keine vordefinierten Gruppen oder Sammlungen vorhanden sind, werden die vordefinierten Sammlungen erstellt und der ermittelte Server wird der entsprechenden Gruppe hinzugefügt.

Geräteerkennung in der OMIMSSC-Konsolenerweiterung für SCVMM

Ermitteln Sie Modularsysteme, Hyper-V-Hosts und nicht zugewiesene Server in der OMIMSSC-Konsolenerweiterung für SCVMM. Nach der Ermittlung werden die Geräte den jeweiligen vordefinierten Aktualisierungsgruppen hinzugefügt.

Voraussetzungen für die Ermittlung von Geräten

Verwaltete Systeme sind die von OMIMSSC verwalteten Geräte. Die Systemanforderungen für die Ermittlung von Servern mit OMIMSSC-Konsolenerweiterungen lauten wie folgt:

- OMIMSSC Konsolenerweiterung für MECM unterstützt modulare, monolithische und Tower-Server-Modelle für Server ab der 12. Generation.
- OMIMSSC Konsolenerweiterung für SCVMM unterstützt modulare und monolithische Servermodelle ab der 12. Servergeneration.
- Verwenden Sie für die Quell- und Zielkonfiguration denselben Festplattentyp: Nur Solid-State (SSD), SAS oder nur Serial ATA (SATA).
- Für ein erfolgreiches Cloning des Hardwareprofil-RAID für Zielsystemfestplatten verwenden Sie die gleiche oder eine größere Größe und Anzahl von Festplatten, die in der Quelle vorhanden sind.
- RAID-aufgeteilte virtuelle Festplatten werden nicht unterstützt.
- iDRAC mit freigegebenem LOM wird nicht unterstützt.
- Die RAID-Konfiguration auf externen Controllern wird nicht unterstützt.
- Aktivieren Sie die Erfassung des Systembestands beim Neustart (CSIOR) in verwalteten Systemen. Nähere Informationen erhalten Sie in der iDRAC-Dokumentation.

Ermitteln von Servern über die automatische Ermittlung

Um Server automatisch zu ermitteln, verbinden Sie die Server mit dem Netzwerk und schalten Sie die Server ein. OMIMSSC erkennt automatisch die nicht zugewiesenen Server mithilfe der Remote-Aktivierungsfunktion von iDRAC. OMIMSSC fungiert als Bereitstellungsserver und verwendet die iDRAC-Referenz zur automatischen Ermittlung von Servern.

1. Erstellen Sie in OMIMSSC ein Gerätetyp-Zugangsdatenprofil, indem Sie die iDRAC-Zugangsdaten angeben, und legen Sie sie als Standard für Server fest. Weitere Informationen zum Erstellen eines Zugangsdatenprofils finden Sie unter Zugangsdatenprofil erstellen.
2. Deaktivieren Sie das vorhandene Administratorkonto in den iDRAC-Einstellungen des verwalteten Geräts.

   ANMERKUNG: Es wird empfohlen, dass Sie über ein Gastnutzerkonto mit Benutzerberechtigungen verfügen, um sich bei iDRAC anzumelden, falls die automatische Ermittlung fehlschlägt, und ein sicheres Kennwort zu wählen.

3. Aktivieren Sie die automatische Ermittlungsfunktion in den iDRAC-Einstellungen des verwalteten Geräts. Nähere Informationen erhalten Sie in der iDRAC-Dokumentation.
4. Geben Sie in verwalteten Geräten in den iDRAC-Einstellungen die IP-Adresse der OMIMSSC-Appliance unter **Bereitstellungsserver-IP** an und starten Sie den Server neu.

Ermitteln von Servern über die manuelle Ermittlung

So ermitteln Sie PowerEdge-Server mithilfe einer IP-Adresse oder eines IP-Bereichs manuell. Geben Sie zum Ermitteln von Servern die iDRAC-IP-Adresse und die Gerätetyp-Zugangsdaten eines Servers an. Wenn Sie Server mithilfe eines IP-Bereichs ermitteln, geben Sie einen IP-Bereich (IPv4) in einem Subnetz an, indem Sie den Start- und Endbereich sowie die Zugangsdaten des Gerätetyps eines Servers angeben.

Stellen Sie sicher, dass ein Standardprofil für Zugangsdaten verfügbar ist.

1. Führen Sie in der OMIMSSC-Konsole einen der folgenden Schritte aus:
   - Klicken Sie im Dashboard auf **Server ermitteln**.
   - Klicken Sie im Navigationsbereich auf **Konfiguration und Bereitstellung**, klicken Sie auf **Serveransicht** und dann auf **Ermitteln**.
2. Klicken Sie auf **Ermitteln**.
3. Wählen Sie auf der Seite **Ermitteln** die erforderliche Option aus:
   - **Ermitteln mit einer IP-Adresse**: Ermitteln Sie einen Server anhand einer IP-Adresse.
   - **Ermitteln mit einem IP-Bereich**: Ermitteln Sie alle Server innerhalb eines IP-Bereichs.
4. Wählen Sie das Gerätetyp-Zugangsdatenprofil aus oder klicken Sie auf **Neu erstellen**, um ein Gerätetyp-Zugangsdatenprofil zu erstellen.

   Das ausgewählte Profil wird auf allen Servern angewendet.
5. Geben Sie in der **iDRAC-IP-Adresse** die IP-Adresse des Servers an, den Sie ermitteln möchten.
6. Führen Sie unter **Über eine IP-Adresse oder einen IP-Adressbereich ermitteln** einen der folgenden Schritte aus:
   - Geben Sie im **Startbereich der IP-Adresse** und im **Endbereich der IP-Adresse** den gewünschten IP-Adressbereich an, also den Start- und Endbereich.
   - Wählen Sie **Ausschlussbereich aktivieren**, wenn Sie einen IP-Adressbereich ausschließen möchten, und geben Sie unter **Startbereich der IP-Adresse** und **Endbereich der IP-Adresse** den Bereich an, den Sie ausschließen möchten.
7. Geben Sie einen eindeutigen Jobnamen und eine Beschreibung für den Job an und klicken Sie auf **Fertig stellen**.

Um diesen Job zu verfolgen, ist standardmäßig die Option **Zur Jobliste wechseln** ausgewählt.

Die Seite **Job- und Protokollcenter** wird angezeigt. Erweitern Sie den Ermittlungsjob, um den Fortschritt des Jobs auf der Registerkarte **Ausführen** anzuzeigen.

Nach dem Ermitteln eines Servers wird der Server der Registerkarte **Hosts** oder der Registerkarte **Nicht zugewiesen** auf der Seite **Serveransicht** des Abschnitts **Konfiguration und Bereitstellung** hinzugefügt.

- Wenn Sie einen Server mit einem bereitgestellten Betriebssystem ermitteln und der Server bereits in der MECM- oder SCVMM-Konsole vorhanden ist, wird der Server als Host-Server auf der Registerkarte **Hosts** aufgeführt.
- Wenn Sie einen PowerEdge-Server ermitteln, der nicht in MECM oder SCVMM aufgeführt ist, wird der Server in allen OMIMSSC-Konsolenerweiterungen auf der Registerkarte **Nicht zugewiesen** als nicht zugewiesener Server aufgeführt, wenn mehrere Microsoft-Konsolen bei einer einzelnen OMIMSSC-Appliance angemeldet sind.

Nach dem Ermitteln eines Servers wird der Server als hardwarekompatibel gekennzeichnet, wenn er unterstützte Versionen von LC-Firmware, iDRAC und BIOS enthält, die mit OMIMSSC zusammenarbeiten. Um die Firmwareversionen der Serverkomponenten anzuzeigen, bewegen Sie den Mauszeiger über die Spalte **Hardwarekompatibilität** in die Serverzeile. Informationen zu den unterstützten Versionen finden Sie in den Versionshinweisen OpenManage Integration for Microsoft System Center.

Für jeden ermittelten Server wird eine Lizenz verbraucht. Die Anzahl der **lizenzierten Knoten** im **Lizenzcenter** verringert sich mit der Anzahl der Server.

ANMERKUNG: Um die Server verwenden zu können, die mit einer früheren Version der OMIMSSC-Appliance ermittelt wurden, ermitteln Sie die Server erneut.

ANMERKUNG: Wenn Sie sich als delegierter Administrator bei OMIMSSC anmelden, können Sie alle Host- und nicht zugewiesenen Server anzeigen, die nicht für den angemeldeten Benutzer spezifisch sind. Daher können Sie keine Operationen auf solchen Servern ausführen. Stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen verfügen, bevor Sie Vorgänge auf solchen Servern ausführen.

Ermitteln von MX7000-Modularsystemen mithilfe der manuellen Ermittlung

Um das PowerEdge MX7000 Modularsystem mithilfe einer IP-Adresse oder eines IP-Bereichs manuell zu ermitteln, geben Sie die IP-Adresse und die Gerätetyp-Zugangsdaten des modularen Systems an. Wenn Sie modulare Systeme mithilfe eines IP-Bereichs ermitteln, geben Sie einen IP-Bereich (IPv4) in einem Subnetz an, indem Sie den Start- und Endbereich sowie die Gerätetyp-Zugangsdaten des modularen Systems angeben.

Stellen Sie sicher, dass das Standard-Zugangsdatenprofil eines Modularsystems, das Sie ermitteln möchten, verfügbar ist.

Führen Sie zur Ermittlung modularer Server folgende Schritte durch:

1. Klicken Sie in OMIMSSC auf **Konfiguration und Bereitstellung**, klicken Sie auf **Modularsystemansicht** und klicken Sie dann auf **Ermitteln**.
2. Klicken Sie auf **Ermitteln**.
3. Wählen Sie auf der Seite **Ermitteln** die erforderliche Option aus:
   - **Ermitteln mit einer IP-Adresse**: Ermitteln Sie ein modulares System mithilfe einer IP-Adresse.
   - **Ermitteln mit einem IP-Bereich**: Ermitteln Sie alle modularen Systeme innerhalb eines IP-Bereichs.
4. Wählen Sie das Gerätetyp-Zugangsdatenprofil aus oder klicken Sie auf **Neu erstellen**, um ein Gerätetyp-Zugangsdatenprofil zu erstellen.

   Das ausgewählte Profil wird auf allen Servern angewendet.
5. Geben Sie unter **IP-Adresse** die IP-Adresse des modularen Systems an, das Sie ermitteln möchten.
6. Führen Sie unter **Über eine IP-Adresse oder einen IP-Adressbereich ermitteln** einen der folgenden Schritte aus:
   - Geben Sie im **Startbereich der IP-Adresse** und im **Endbereich der IP-Adresse** den gewünschten IP-Adressbereich an, also den Start- und Endbereich.
   - Wählen Sie **Ausschlussbereich aktivieren**, wenn Sie einen IP-Adressbereich ausschließen möchten, und geben Sie unter **Startbereich der IP-Adresse** und **Endbereich der IP-Adresse** den Bereich an, den Sie ausschließen möchten.
7. Wählen Sie unter **Ermittlungsmethoden für modulare Systeme** eine der folgenden Optionen aus:
   - **Einfache Ermittlung**: Ermittelt modulare Systeme und auch die Anzahl der Server im modularen System.
   - **Umfassende Ermittelung**: Erkennt modulare Systeme und Geräte, die im modularen System vorhanden sind, wie Eingabe/Ausgabe-Modulen (IOM) und Speichergeräten.

ANMERKUNG: Stellen Sie für eine umfassende Ermittlung des MX7000 und seiner Komponenten sicher, dass der PowerEdge MX7000 und alle seine Komponenten mit IPv4-Adresse aktiviert sind.

8. Geben Sie einen eindeutigen Jobnamen an und klicken Sie auf **Fertig stellen**.

   Um diesen Job zu verfolgen, ist standardmäßig die Option **Zur Jobliste wechseln** ausgewählt.

   Erweitern Sie den Ermittlungsjob in **Job- und Protokollcenter**, um den Fortschritt des Jobs auf der Registerkarte **Ausführen** anzuzeigen.

Synchronisieren der OMIMSSC-Konsolenerweiterung mit registriertem MECM

Sie können alle Server (Hosts und nicht zugewiesene) von registrierten MECM zu OMIMSSC synchronisieren. Außerdem erhalten Sie nach der Synchronisierung die neuesten Firmware-Bestandsinformationen zu den Servern.

Stellen Sie vor dem Synchronisieren von OMIMSSC und der registrierten MECM-Konsole sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Informationen zum Standard-iDRAC-Zugangsdatenprofil für Server enthalten.
- Aktualisieren Sie die **Dell Default Collection**, bevor Sie OMIMSSC mit MECM synchronisieren. Wenn jedoch ein nicht zugewiesener Server in MECM ermittelt wird, wird er der **Von Dell importierte Server-Sammlung** hinzugefügt. Fügen Sie zum Hinzufügen dieses Servers zur **Dell Default Collection** die iDRAC-IP-Adresse des Servers auf der **OOB**-Seite hinzu.
- Stellen Sie sicher, dass in MECM keine doppelten Einträge von Geräten vorhanden sind.

Nach der Synchronisierung von OMIMSSC mit MECM wird, wenn das Gerät nicht in MECM vorhanden ist, die Sammlung **Alle Dell Lifecycle Controller-Server** und die Sammlung **Dell-Server importieren** unter **Gerätesammlungen** erstellt, und der Server wird der entsprechenden Gruppe hinzugefügt.

Synchronisieren der OMIMSSC-Konsolenerweiterung mit registriertem SCVMM

Sie können alle Hyper-V-Hosts, Hyper-V-Host-Cluster, modulare Hyper-V-Hosts und nicht zugewiesene Server von SCVMM-Konsolen mit der OMIMSSC-Konsolenerweiterung für SCVMM synchronisieren. Außerdem erhalten Sie nach der Synchronisierung die neuesten Firmware-Bestandsinformationen zu den Servern.

Berücksichtigen Sie Folgendes, bevor Sie OMIMSSC mit SCVMM synchronisieren:

- Informationen zum Standard-iDRAC-Zugangsdatenprofil für Server enthalten.
- Wenn der Baseboard Management Controller (BMC) des Hostservers nicht mit der iDRAC-IP-Adresse konfiguriert ist, können Sie den Hostserver nicht mit OMIMSSC synchronisieren. Konfigurieren Sie daher BMC in SCVMM (weitere Informationen finden Sie im MSDN-Artikel unter `technet.microsoft.com`) und synchronisieren Sie dann OMIMSSC mit SCVMM.
- Da SCVMM sehr viele Hosts in der Umgebung unterstützt, ist die Synchronisierung ein zeitintensiver Vorgang.

Synchronisieren mit der registrierten Microsoft-Konsole

Führen Sie den folgenden Schritt aus, um in der Microsoft-Konsole verwaltete Server zu OMIMSSC hinzuzufügen:

1. Klicken Sie in OMIMSSC auf **Konfiguration und Bereitstellung**, klicken Sie auf **Serveransicht** und klicken Sie dann auf **Mit OMIMSSC synchronisieren**, um alle Hosts zu synchronisieren, die im registrierten MSSC des OMIMSSC-Geräts aufgelistet sind.
2. Um alle Hosts zu synchronisieren, die im registrierten MSSC des Geräts aufgelistet sind, klicken Sie auf **Mit OMIMSSC synchronisieren**.

   Die Synchronisierung ist ein relativ zeitintensiver Vorgang. Zeigen Sie den Jobstatus auf der Seite **Jobs und Protokolle** an.

Beheben von Synchronisierungsfehlern

Die Server, die nicht mit OMIMSSC synchronisiert sind, werden mit ihrer iDRAC-IP-Adresse und ihrem Host-Namen aufgeführt.

ANMERKUNG: Stellen Sie sicher, dass Sie für alle Server, die aufgrund von Problemen wie ungültigen Zugangsdaten oder der iDRAC-IP-Adresse oder Konnektivität oder anderen Problemen nicht synchronisiert werden, die Probleme zuerst beheben, und anschließend synchronisieren.

ANMERKUNG: Während der Neusynchronisierung werden Hostserver, die aus der registrierten MSSC-Umgebung gelöscht werden, auf die Registerkarte **Nicht zugewiesene Server** in den OMIMSSC-Konsolenerweiterungen verschoben. Wenn ein Server außer Betrieb gesetzt wird, entfernen Sie diesen Server dann aus der Liste der nicht zugewiesenen Server.

So synchronisieren Sie Server mit Problemen mit Zugangsdatenprofilen erneut:

1. Klicken Sie in OMIMSSC auf **Konfiguration und Bereitstellung**, klicken Sie auf **Serveransicht** und dann auf **Synchronisierungsfehler beheben**.
2. Klicken Sie auf **Synchronisierungsfehler beheben**.
3. Wählen Sie die Server für die Neusynchronisierung aus und wählen Sie das Zugangsdatenprofil aus. Um ein Zugangsdatenprofil zu erstellen, klicken Sie auf **Neu erstellen**.
4. Geben Sie einen Jobnamen an und wählen Sie ggf. die Option **Zur Jobliste wechseln** aus, um den Jobstatus nach dem Senden des Jobs automatisch anzuzeigen.
5. Klicken Sie auf **Fertig stellen**, um den Job zu senden.

Anzeigen des Systemsperrmodus

Die Einstellung für den Systemsperrmodus ist in iDRAC ab der 14. Servergeneration verfügbar. Aktiviert sperrt die Einstellung die Systemkonfiguration, einschließlich Firmwareupdates. Wenn der Sperrmodus des Systems aktiviert ist, können Benutzer keine Konfigurationseinstellungen mehr ändern. Diese Einstellung dient ausschließlich zum Schutz des Systems vor unbeabsichtigten Änderungen. Um Vorgänge auf den verwalteten Servern auszuführen, stellen Sie sicher, dass Sie die Einstellung auf der iDRAC-Konsole deaktivieren. In der OMIMSSC-Konsole wird der Status des Systemsperrmodus mit einem Schlossbild vor der iDRAC-IP-Adresse des Servers dargestellt.

1. Ein Schlossbild wird zusammen mit der iDRAC-IP der Server angezeigt, wenn die Einstellung auf diesem System aktiviert ist.
2. Ein Bild eines offenen Schlosses wird zusammen mit der iDRAC-IP-Adresse der Server angezeigt, wenn die Einstellung auf diesem System deaktiviert ist.

ANMERKUNG: Überprüfen Sie vor dem Starten der OMIMSSC-Konsolenerweiterungen die Einstellung des iDRAC-Systemsperrmodus auf den verwalteten Servern.

Weitere Informationen zum iDRAC-Systemsperrmodus finden Sie in der iDRAC-Dokumentation unter `dell.com/support`.

13

Entfernen von Geräten aus OMIMSSC

Wenn einer der aufgelisteten Server nicht mehr verwaltet werden muss, kann er aus der Liste der verwalteten Server entfernt werden. Wenn der Server aus dem System Center aus der Verwaltung entfernt wurde, kann dieser von der OMIMSSC-Appliance entfernt werden.

Führen Sie die folgenden Schritte aus, um einen Server zu entfernen:

Berücksichtigen Sie die folgenden Punkte, bevor Sie einen Server entfernen:

- Nachdem Sie einen Server entfernt haben, wird die verbrauchte Lizenz aufgegeben.
- Sie können einen in OMIMSSC aufgelisteten Server basierend auf den folgenden Kriterien löschen:
  - Ein nicht zugewiesener Server, der auf der Registerkarte **Nicht zugewiesene Server** aufgeführt ist.
  - Wenn Sie einen Hostserver entfernen, der in registrierten MECM oder SCVMM bereitgestellt ist und in OMIMSSC auf der Registerkarte **Hosts** vorhanden ist, entfernen Sie zuerst den Server in MECM oder SCVMM und anschließend den Server in OMIMSSC.

1. Klicken Sie in der OMIMSSC-Konsole auf **Konfiguration und Bereitstellung** und klicken Sie dann auf **Serveransicht**:
   - So löschen Sie nicht zugewiesene Server: Wählen Sie auf der Registerkarte **Nicht zugewiesene Server** den Server aus und klicken Sie auf **Löschen**.
   - So löschen Sie Host-Server: Wählen Sie auf der Registerkarte **Hostserver** den Server aus und klicken Sie auf **Löschen**.
2. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.

Themen:

Entfernen modularer Systeme aus OMIMSSC

Führen Sie zum Löschen eines modularen Systems die folgenden Schritte durch:

1. Klicken Sie in der OMIMSSC-Konsole auf **Konfiguration und Bereitstellung** und klicken Sie dann auf **Modularsystemansicht**.
2. Wählen Sie das modulare System aus und klicken Sie auf **Löschen**.

14

Ansichten in OMIMSSC

Zeigen Sie alle in OMIMSSC auf der Seite **Konfiguration und Bereitstellung** ermittelten Geräte sowie deren Hardware- und Firmware-Bestandsinformationen an. Zeigen Sie auch alle Jobs mit Status auf der Seite **Job- und Protokollcenter** an.

Themen:

Serveransicht.

Auf der Seite **Serveransicht** werden alle nicht zugewiesenen Hostserver aufgelistet, die in OMIMSSC auf den Registerkarten **Nicht zugewiesene Server** und **Hosts** ermittelt werden.

Zeigen Sie auf der Registerkarte **Nicht zugewiesene Server** die iDRAC-IP-Adresse, die Service-Tag-Nummer, das Modell, die Generation, die Prozessorgeschwindigkeit, den Arbeitsspeicher des Servers, den Kompatibilitätsstatus mit der zugewiesenen Betriebsvorlage, die Service-Tag-Nummer des modularen Systems (falls ein modularer Server vorhanden ist) und Informationen zur Hardwarekompatibilität an. Wenn Sie den Mauszeiger über die Spalte **Hardware-Kompatibilität** bewegen, können Sie die Versionen von BIOS, iDRAC, LC und Treiberpaketen des Geräts anzeigen. Weitere Informationen zur Hardwarekompatibilität finden Sie unter Informationen zum Firmwareupdate.

Zeigen Sie auf der Registerkarte **Hosts** den Hostnamen, die iDRAC-IP-Adresse, die Service-Tag-Nummer, das Modell, die Generation, die Prozessorgeschwindigkeit, den Arbeitsspeicher des Servers und die Service-Tag-Nummer des modularen Systems an, falls es sich um einen modularen Server handelt, den Vollqualifizierten Domainnamen (FQDN) des Clusters, falls der Server Teil eines Clusters ist, den Kompatibilitätsstatus mit der zugewiesenen Betriebsvorlage und Informationen zur Hardwarekompatibilität. Wenn Sie den Mauszeiger über die Spalte **Hardware-Kompatibilität** bewegen, können Sie die Versionen von BIOS, iDRAC, LC und Treiberpaketen des Geräts anzeigen. Weitere Informationen zur Hardwarekompatibilität finden Sie unter Informationen zum Firmwareupdate.

Auf der Seite **Serveransicht** können Sie folgende Tasks ausführen:

- Server ermitteln
- Zeigen Sie aktualisierte Informationen an, indem Sie die Seite aktualisieren.
- Server löschen aus OMIMSSC.
- Synchronisieren mit der registrierten Microsoft-Konsole.
- Beheben von Synchronisierungsfehlern.
- Betriebsvorlage zuweisen und Kompatibilitätsprüfung der Betriebsvorlage durchführen.
- Bereitstellen der Betriebsvorlage
- Server mit Cluster-Gruppe korrelieren und dem modularen System, dem der Server angehört
- iDRAC-Konsole starten

So zeigen Sie Server an:

1. Klicken Sie in der Konsolenerweiterung OMIMSSC auf **Konfiguration und Bereitstellung** und klicken Sie dann auf **Serveransicht**.
2. Erweitern Sie **Konfiguration und Bereitstellung** und klicken Sie auf **Serveransicht**.
3. Klicken Sie zum Anzeigen von Bare-Metal-Servern auf die Registerkarte **Nicht zugewiesene Server**.
4. Klicken Sie zum Anzeigen von Hostservern auf die Registerkarte **Hosts**.
   a. Um Hostgruppen in verschachteltem Format anzuzeigen, wie in MECM oder SCVMM gruppiert, klicken Sie auf das Dropdownmenü **Konsolen-Hosts auswählen**.

   Im Dropdownmenü **Konsolen-Hosts auswählen** werden alle in MECM vorhandenen Hostgruppen sowie ein interner Gruppenname aufgeführt. Wenn Sie den internen Gruppennamen auswählen, werden alle in MECM und OMIMSSC ermittelten und verwalteten Hosts angezeigt.

Berücksichtigen Sie nach dem Ermitteln von Servern die folgenden Punkte:

- Die Spalte **Betriebsvorlage** wird nach der Ermittlung der Server als **Nicht zugewiesen** angezeigt. Um die Firmware zu aktualisieren und das Betriebssystem auf diesen Servern bereitzustellen, weisen Sie Betriebsvorlage zu und stellen Sie sie bereit. Weitere Informationen finden Sie unter Betriebsvorlage.
- Die Spalte **Betriebsvorlage** wird nach der Ermittlung der Server als **Nicht zugewiesen** angezeigt. Um die Firmware zu aktualisieren und das Betriebssystem auf diesen Servern bereitzustellen, weisen Sie Betriebsvorlage zu und stellen Sie sie bereit. Weitere Informationen finden Sie unter Zuweisen von Betriebsvorlage für Server und Bereitstellen von Betriebsvorlage für Server.
- Die ermittelten Server werden vordefinierten Gruppen in OMIMSSC hinzugefügt. Sie können nutzerdefinierte Aktualisierungsgruppen basierend auf funktionalen Anforderungen erstellen. Weitere Informationen finden Sie unter Informationen zu Aktualisierungsgruppen.
- Die ermittelten Server werden vordefinierten Gruppen in OMIMSSC hinzugefügt. Sie können nutzerdefinierte Aktualisierungsgruppen basierend auf funktionalen Anforderungen erstellen. Weitere Informationen finden Sie unter Aktualisierungsgruppen.
- Wenn Sie sich als delegierter Administrator bei OMIMSSC anmelden, können Sie alle Host- und nicht zugewiesenen Server anzeigen, die nicht für diesen Benutzer spezifisch sind. Stellen Sie daher sicher, dass Sie über die erforderlichen Berechtigungen verfügen, bevor Sie Vorgänge auf den Servern ausführen.
- Wenn mehrere Microsoft-Konsolen bei OMIMSSC registriert sind, gelten Hostserver speziell für die Microsoft-Konsole, in der sie verwaltet werden. Die nicht zugewiesenen Server gelten für alle Konsolen.

iDRAC-Konsole

Führen Sie den folgenden Schritt aus, um die iDRAC-Konsole zu starten:

Erweitern Sie in OMIMSSC den Punkt **Konfiguration und Bereitstellung** und wählen Sie eine der folgenden Optionen aus:Erweitern Sie **Konfiguration und Bereitstellung** und wählen Sie eine der folgenden Optionen aus:

- Klicken Sie auf **Serveransicht**. Klicken Sie basierend auf dem Server (wenn es sich um einen Host oder einen nicht zugewiesenen Server handelt) auf die Registerkarte **Nicht zugewiesene Server** oder **Hosts** und klicken Sie auf die **iDRAC-IP**-Adresse des Servers.

  Die Registerkarte **Nicht zugewiesene Server** wird standardmäßig angezeigt.

  Klicken Sie auf **Hosts**, um die Registerkarte "Hosts" anzuzeigen.

- Klicken Sie auf **Clusteransicht**. Erweitern Sie den Clustertyp und erweitern Sie die Clustergruppe auf Serverebene.

  Die Registerkarte **Server** wird angezeigt.

Modularsystemansicht

Auf der Seite **Modularsystemansicht** werden alle in OMIMSSC erkannten modularen Systeme aufgeführt.

Zeigen Sie die CMC-IP-Adresse, die Service-Tag-Nummer, das Modell, die Firmwareversion, den Kompatibilitätsstatus der Vorlage des Modularsystems für eine zugewiesene Betriebsvorlage, die Anzahl der Server, die E/A-Module und die auf diesem Modularsystem vorhandenen Speichergeräte an. Konfigurieren Sie die Hardware und aktualisieren Sie die Firmware des modularen Systems, indem Sie die Betriebsvorlage bereitstellen.

Auf der Seite **Modularsystemansicht** können Sie folgende Tasks ausführen:

- Ermitteln modularer Systeme mithilfe der manuellen Ermittlung
- Modulares System löschen
- Aktualisieren Sie die Seite, um die neuesten Inventarinformationen anzuzeigen.
- Betriebsvorlage dem Modularsystem zuweisen
- Bereitstellen der Betriebsvorlage für das modulare System
- Anzeigen von E/A-Modulen
- E/A-Module starten

So zeigen Sie das in OMIMSSC erkannte Modularsystem an:

1. Klicken Sie in OMIMSSC auf **Konfiguration und Bereitstellung** und klicken Sie dann auf **Modularsystemansicht**.
   Alle erkannten Modellnamen der Modularsysteme werden angezeigt.
2. Um ein bestimmtes modulares System anzuzeigen, klicken Sie unter **Modularsystemansicht** auf einen Modellnamen.

   Alle modularen Systeme dieses Modells werden mit ihrer Service-Tag-Nummer angezeigt.
3. Um alle in diesem Modularsystem vorhandenen Geräte anzuzeigen, klicken Sie auf "Service-Tag-Nummer".

   Alle Server, Eingabe-/Ausgabe-Module und Speichergeräte werden zusammen mit ihren Details angezeigt.

ANMERKUNG: Erst nach einer umfassenden Erkennung eines modularen Systems werden alle Geräte im modularen System und ihre Informationen angezeigt.

- Standardmäßig wird die Registerkarte **Server** angezeigt.

  Alle Server, die in diesem modularen System erkannt werden, werden angezeigt.

- Klicken Sie auf die Registerkarte **E/A-Module**, um alle in einem modularen System vorhandenen Eingabe-/Ausgabe-Module anzuzeigen.
- Um alle im modularen System vorhandenen Speichergeräte anzuzeigen, klicken Sie auf die Registerkarte **Speichergeräte**.

Berücksichtigen Sie nach dem Erkennen modularer Systeme die folgenden Punkte:

- Die Spalte **Betriebsvorlage** wird nach der Erkennung der modularen Systeme als **Nicht zugewiesen** angezeigt. Um die Firmware zu aktualisieren und das Betriebssystem auf diesen modularen Systemen bereitzustellen, weisen Sie Betriebsvorlage zu und stellen Sie sie bereit. Weitere Informationen finden Sie unter Verwalten von Betriebsvorlage.
- Die Spalte **Betriebsvorlage** wird nach der Ermittlung der Server als **Nicht zugewiesen** angezeigt. Um die Firmware zu aktualisieren und das Betriebssystem auf diesen modularen Systemen bereitzustellen, weisen Sie Betriebsvorlage zu und stellen Sie sie bereit. Weitere Informationen finden Sie unter Zuweisen von Betriebsvorlage für modulare Systeme und Bereitstellen von Betriebsvorlage für modulare Systeme.
- Zeigen Sie die Anzahl der Eingabe-/Ausgabe-Module, Speichergeräte und Server an, die in Modularsystemen nach einer einfachen Erkennung vorhanden sind. Führen Sie eine erweiterte Erkennung durch, um weitere Details zu den Komponenten in einem modularen System anzuzeigen.

Modulare OpenManage Enterprise-Konsole

Führen Sie die folgenden Schritte aus, um die OpenManage Enterprise Modular-Konsole zu starten:

1. Erweitern Sie in OMIMSSC **Konfiguration und Bereitstellung** und klicken Sie auf **Modulare Systeme**.1
2. Klicken Sie auf **Geräte-IP** des modularen Systems.

Eingabe/Ausgabe-Module

Alle Netzwerk-E/A-Module werden mit IP-Adresse, Service-Tag-Nummer, E/A-Typ, Modell, Firmwareversion und Steckplatzinformationen angezeigt.

Starten Sie die E/A-Modul-Konsole von der Seite Eingabe/Ausgabe-Module.

Führen Sie die folgenden Schritte aus, um Informationen zu Eingabe-/Ausgabe-Modulen anzuzeigen:

1. Klicken Sie in OMIMSSC auf **Konfiguration und Bereitstellung**, und klicken Sie dann auf **Modularsystemansicht**. Erweitern Sie die **Modularsystemansicht** und klicken Sie auf Service-Tag-Nummer.

   Alle Service-Tag-Nummern dieses Modells werden angezeigt.
2. Klicken Sie auf ein Modellsystem, um die darunter aufgelisteten Geräte zu erweitern. Klicken Sie auf die Service-Tag-Nummer, um ein bestimmtes Modulares System anzuzeigen.
3. Klicken Sie auf die Registerkarte **E/A-Module**, um das E/A-Modul anzuzeigen.

I/O-Module der Konsole

Führen Sie die folgenden Schritte aus, um die Eingabe-/Ausgabemodul-Konsole zu starten:

1. Erweitern Sie in OMIMSSC den Punkt **Konfiguration und Bereitstellung** und klicken Sie auf **Modularsystemansicht**. Erweitern Sie das Modell auf die Ebene einzelner Geräte.

   Alle Geräte unter diesem Modell werden angezeigt.
2. Klicken Sie auf die Registerkarte **E/A-Module**.
3. Klicken Sie auf die **IP-Adresse** des Geräts.

Clusteransicht

Auf der Seite **Clusteransicht** werden alle in OMIMSSC ermittelten Cluster aufgeführt. Zeigen Sie den vollqualifizierten Namen (FQDN), die Service-Tag-Nummer und die Anzahl der Server in diesem Cluster an. Erstellen Sie außerdem einen logischen Switch für Cluster und anschließend einen Windows Server HCI-Cluster mithilfe der vordefinierten Betriebsvorlage.

Auf der Seite **Clusteransicht** können Sie folgende Tasks ausführen:

- Logischen Switch erstellen (nur für SCVMM 2016- und 2019-Nutzer)
- Erstellen von Windows server HCI-Clustern (nur für SCVMM 2016- und 2019-Nutzer)
- iDRAC-Konsole starten
- Aktualisieren Sie die Seite, um die neuesten ermittelten Cluster anzuzeigen.

So zeigen Sie in OMIMSSC ermittelte Clustergruppen an:

1. Klicken Sie in OMIMSSC auf **Konfiguration und Bereitstellung** und klicken Sie dann auf **Clusteransicht**.
   Alle verschiedenen Clustertypen werden gruppiert und aufgelistet.
2. Erweitern Sie den Clustertyp, um Informationen zu bestimmten Clustertypen anzuzeigen.
   Alle Cluster dieses Typs werden im linken Bereich aufgelistet.
3. Um die in einem Cluster vorhandenen Server anzuzeigen, klicken Sie auf einen Clusternamen.

Ansicht Wartungscenter

Auf der Seite **Wartungscenter** werden alle ermittelten Geräte in Gruppen und die Ressourcen aufgeführt, die zum Verwalten von Geräten in OMIMSSC erforderlich sind. Um die Server HCI-Clustergruppen auf der Seite **Wartungscenter** anzuzeigen, stellen Sie sicher, dass Sie **Alle Aktualisierungsgruppen** im Drop-Down-Menü **Aktualisierungsgruppe** ausgewählt haben. Hier können Sie den Firmware-Bestand des Geräts anzeigen, die Geräte verwalten, indem Sie ihre Firmware gemäß den Empfehlungen auf dem neuesten Stand halten, den Server auf einen früheren Zustand zurücksetzen, falls er ausgefallen ist, eine ersetzte Komponente mit derselben Konfiguration wie bei der alten Komponente ausstatten und Serverprotokolle zur Behebung von Problemen exportieren. Auf der Seite **Aktualisierungs-Einstellungen** werden alle Aktualisierungsquellen, Abfragen und Benachrichtigungen für die neuesten Aktualisierungen aus der Standard-Aktualisierungsquelle, Aktualisierungsgruppen von Geräten, für die eine ähnliche Verwaltung erforderlich ist, sowie alle für Serverkonfigurationen erforderlichen Schutz-Vaults angezeigt.

ANMERKUNG: Standardmäßig enthält OMIMSSC eine Katalogdatei, in der eine frühere Version des Vergleichsberichts für vordefinierte HTTPS-Aktualisierungsquellen angezeigt wird. Laden Sie daher den neuesten Katalog herunter, um den neuesten Vergleichsbericht anzuzeigen. Um den neuesten Katalog herunterzuladen, bearbeiten und speichern Sie die HTTPS-Aktualisierungsquellen.

ANMERKUNG: Die Baseline-Version einer bestimmten Komponente eines Geräts wird als nicht verfügbar markiert, wenn die Aktualisierung nicht im ausgewählten Katalog für Aktualisierunsgquellen vorhanden ist.

Auf der Seite **Wartungscenter** können Sie folgende Tasks ausführen:

- Eine Aktualisierungsquelle erstellen
- Abfragehäufigkeit einstellen
- Wählen Sie vordefinierte Aktualisierungsgruppen oder Nutzerdefinierte Aktualisierungsgruppen erstellen aus.
- Anzeigen und Aktualisieren der Firmware-Bestandsaufnahme
- Aktualisieren und Herabstufen der Firmwareversionen mithilfe der Methode "Aktualisierung ausführen"
- Erstellen von Schutz-Vaults
- Exportieren von Serverprofilen
- Importieren von Serverprofilen
- Exportieren der Bestandsaufnahme

So zeigen Sie die **Wartungscenter**-Seite an:

Klicken Sie in OMIMSSC auf **Wartungscenter**.
Die Seite **Wartungscenter** wird angezeigt.

Jobs und Protokollcenter

Anzeigen von Informationen zu Jobs, die in OMIMSSC initiiert wurden, sowie den Status des Jobs und dessen Teilvorgängen. Sie können auch Jobs einer bestimmten Jobkategorie filtern und anzeigen.

Sie können Aufträge anzeigen, die von OMIMSSC, im OMIMSSC-Verwaltungsportal und aus der OMIMSSC-Konsolenerweiterung initiiert wurden.

- OMIMSSC Verwaltungsportal: Zeigt Jobs an, die von allen OMIMSSC-Konsolen und Benutzern initiiert wurden
- OMIMSSC Konsole: Zeigt für einen Benutzer und eine Konsole spezifische Jobs an

Jobnamen werden entweder vom System generiert oder von Benutzern bereitgestellt, und die Teilvorgänge werden nach der IP-Adresse oder dem Hostnamen der verwalteten Systeme benannt. Erweitern Sie die Teilvorgänge, um die Aktivitätsprotokolle für diesen Job anzuzeigen. Jobs werden in vier Gruppen eingeteilt:

- **Ausführen**: Zeigt alle Jobs an, die gerade ausgeführt werden, bzw. deren Fortschrittstatus.
- **Verlauf**: Zeigt alle Jobs mit deren Jobstatus an, die in der Vergangenheit ausgeführt wurden.
- **Geplant**: Zeigt alle Jobs an, die für ein zukünftiges Datum und eine zukünftige Uhrzeit geplant sind. Sie können diese geplanten Jobs auch abbrechen.
- **Allgemeine Protokolle**: Zeigt die für die OMIMSSC-Appliance spezifischen, gemeinsamen Protokollmeldungen an, die nicht spezifisch für einen Teilvorgang und andere Aktivitäten sind. Jeder Job wird mit einem Nutzernamen und einem Konsolen-FQDN angezeigt, von dem aus er initiiert wurde.
  - **Gerät-Protokollnachrichten**: Zeigt alle für die OMIMSSC-Appliance spezifischen Protokollnachrichten an, z. B. den Neustart der OMIMSSC-Appliance. Sie können diese Nachrichtenkategorie nur im OMIMSSC-Verwaltungsportal anzeigen.
  - **Allgemeine Protokollmeldungen**: Zeigt Protokollmeldungen an, die den Jobs gemeinsam sind, die in verschiedenen Jobkategorien auf den Registerkarten **Ausführen**, **Verlauf** und **Geplant** aufgeführt sind. Diese Protokolle sind spezifisch für eine Konsole und einen Nutzer.

    Wenn beispielsweise ein Firmwareaktualisierungsjob für eine Gruppe von Servern ausgeführt wird, werden auf der Registerkarte Protokollmeldungen angezeigt, die zur Erstellung des SUU-Repositorys (Server Update Utility) für diesen Auftrag gehören.

Die verschiedenen Status eines Jobs, die in OMIMSSC definiert sind, lauten wie folgt:

- **Abgebrochen**: Der Job wird manuell oder nach dem Neustart der OMIMSSC-Appliance abgebrochen.
- **Erfolgreich**: Der Job wurde erfolgreich abgeschlossen.
- **Fehlgeschlagen**: Der Job war nicht erfolgreich.
- **In Bearbeitung**: Der Job wird gerade ausgeführt.
- **Geplant**: Der Job wurde für einen späteren Zeitpunkt geplant.

  ANMERKUNG: Wenn mehrere Jobs gleichzeitig an dasselbe Gerät gesendet werden, schlagen sie fehl. Stellen Sie daher sicher, dass Sie Jobs für dasselbe Gerät zu unterschiedlichen Zeiten planen.
- **Warten**: Der Job befindet sich in einer Warteschlange.
- **Wiederkehrender Zeitplan**: Der Job wird in regelmäßigen Abständen ausgeführt.

1. Klicken Sie in OMIMSSC auf **Jobs und Protokollcenter**.
2. Klicken Sie auf die gewünschte Registerkarte, um eine bestimmte Kategorie von Jobs anzuzeigen, z. B. **Geplant**, **Verlauf** oder **Allgemein**.

   Erweitern Sie einen Job, um alle in diesem Job enthaltenen Geräte anzuzeigen. Erweitern Sie weiter, um die Protokollnachrichten für diesen Job anzuzeigen.

   ANMERKUNG: Alle jobbezogenen allgemeinen Protokollmeldungen sind unter der Registerkarte **Allgemeine** und nicht unter der Registerkarte **Ausführen** oder **Verlauf** aufgeführt.
3. (Optional) Wenden Sie Filter an, um verschiedene Jobgruppen und Jobstatus in der Spalte **Status** anzuzeigen.

15

Verwalten von Betriebsvorlage

Betriebsvorlage enthalten die vollständige Device-Konfiguration und werden zur Bereitstellung von Betriebssystemen und Aktualisierung der Firmware auf PowerEdge-Servern und modularen Systemen in einer Microsoft-Umgebung verwendet.

Die Betriebsvorlage repliziert Hardware und Firmware eines Referenzservers (goldener Server) während der Betriebssystembereitstellung auf viele andere Server. Sie enthält Firmware-, Hardware- und Betriebssystemkomponenten, deren Attribut auf den aktuellen Wert des Referenzservers festgelegt ist. Diese Werte können geändert werden, bevor diese Vorlage auf Geräte angewendet wird. Sie können auch den Kompatibilitätsstatus anhand einer zugewiesenen Betriebsvorlage überprüfen und den Kompatibilitätsbericht auf einer Zusammenfassungsseite anzeigen.

Nur Komponenten, die auf dem Referenzserver verfügbar sind, werden als Betriebsvorlage-Komponenten dynamisch abgerufen und angezeigt. Beispiel: Wenn der Server nicht über eine FC-Komponente verfügt, wird diese in der Betriebsvorlage nicht angezeigt.

Informationen zu Referenzservern und Referenzsystemen finden Sie unter Informationen zur Referenzserverkonfiguration und Informationen zur Referenzkonfiguration modularer Systeme.

In der folgenden Tabelle werden die Komponenten beschrieben, die in der Betriebsvorlage aufgeführt sind sowie die Anzeige- und Bereitstellungsfunktionen der einzelnen Komponenten:

Tabelle 9. Funktionsweise der Betriebsvorlage

Komponente	Konfiguration bereitstellen	Firmwareupdate	Konfiguration anzeigen	Kompatibilitätsstatus für Betriebsvorlagen
BIOS	Ja	Ja	Ja	Ja
iDRAC	Ja	Ja	Ja	Ja
NIC/CNA	Ja	Ja	Ja	Ja
RAID	Ja	Ja	Ja	Ja
FC	Ja	Ja	Ja	Ja
Windows	Ja	—	Nein	—
RHEL	Ja	—	Nein	—
ESXI	Ja	—	Nein	—
Managementmodul	Ja	Ja	Ja	Ja

Themen:

Vordefinierte Betriebsvorlage

Vordefinierte Vorlagen verfügen über alle Konfigurationen, die erforderlich sind, um Windows Server HCI-Cluster oder Windows Server Software Defined (WSSD) zu erstellen. OMIMSSC unterstützt das Erstellen von Clustern auf AX-6515, AX-740XD, AX-640, RN740XD, RN740XD2 und RN640 sowie Windows Server HCI Ready-Node-Modellen zusammen mit ihren spezifischen Netzwerkadaptern.

Tabelle 10. Liste der vordefinierten Betriebsvorlage

Name der Betriebsvorlage	Beschreibung
AX-6515_QLogic	Diese Betriebsvorlage ist für Dell EMC HCI-Lösungen für Microsoft Windows Server für die Modelle AX-6515
AX-6515_Mellanox	Diese Betriebsvorlage ist für Dell EMC HCI-Lösungen für Microsoft Windows Server für die Modelle AX-6515
AX-740xd_RN740xd_QLogic	Diese Betriebsvorlage ist für Dell EMC HCI-Lösungen für Microsoft Windows Server für die Modelle AX-740xd und RN740xd.
AX-740xd_RN740xd_Mellanox	Diese Betriebsvorlage ist für Dell EMC HCI-Lösungen für Microsoft Windows Server für die Modelle AX-740xd und RN740xd.
AX-640_RN640_Mellanox	Diese Betriebsvorlage ist für Dell EMC HCI-Lösungen für Microsoft Windows Server für die Modelle AX-640 und RN640
AX-640_RN640_QLogic	Diese Betriebsvorlage ist für Dell EMC HCI-Lösungen für Microsoft Windows Server für die Modelle AX-640 und RN640
RN440_QLogic	Diese Betriebsvorlage ist für Dell EMC HCI-Lösungen für Microsoft Windows Server für die Modelle RN440
RN740xd2_Mellanox	Diese Betriebsvorlage ist für Dell EMC HCI-Lösungen für Microsoft Windows Server für die Modelle RN740xd2
RN740xd2_QLogic	Diese Betriebsvorlage ist für Dell EMC HCI-Lösungen für Microsoft Windows Server für die Modelle RN740xd2

Berücksichtigen Sie die folgenden Punkte, bevor Sie eine Betriebsvorlage bereitstellen:

- Die vordefinierten Vorlagen sind nur für Verwaltungssysteme verfügbar, auf denen SCVMM 2016 und 2019 ausgeführt wird.
- Die vordefinierte Windows Server HCI-Vorlage zeigt die NIC Karte in Steckplatz 1. Während der Bereitstellung der Betriebsvorlage wird die NIC-Konfiguration jedoch auf den rechten Steckplatz angewendet. Wenn sich auf dem Gerät mehrere NIC-Karten befinden, werden alle NIC-Karten mit derselben Konfiguration konfiguriert, die in der Betriebsvorlage angegeben ist.

Informationen zur Konfiguration des Referenzservers

Eine Serverkonfiguration mit einer bevorzugten Startsequenz, BIOS, RAID-Einstellungen, Hardwarekonfiguration, Attributen der Firmware-Aktualisierung und Betriebssystemparametern, die ideal für eine Organisation geeignet ist, wird als Referenzserverkonfiguration bezeichnet.

Ermitteln Sie einen Referenzserver, erfassen Sie die Referenzservereinstellungen in einer Betriebsvorlage und replizieren Sie sie auf verschiedenen Servern mit derselben Hardwarekonfiguration.

Informationen zur Konfiguration des modularen Systems

Eine modulare Systemkonfiguration mit einer bevorzugten Netzwerkkonfiguration, einem Benutzerkonto, Sicherheitsfunktionen und Alerts, die ideal für eine Organisation geeignet ist, wird als Referenz für die modulare Systemkonfiguration oder Referenzgehäuse bezeichnet.

Ermitteln Sie ein modulares Referenzsystem und erfassen Sie die Einstellungen des modularen Referenzsystems in einer Betriebsvorlage und replizieren Sie sie auf verschiedene modulare Systeme derselben Modelle.

Erstellen einer Betriebsvorlage von Referenzservern

Stellen Sie vor dem Erstellen der Betriebsvorlage sicher, dass Sie die folgenden Tasks ausführen:

- Ermitteln Sie einen Referenzserver mithilfe der Ermittlungsfunktion. Informationen zum Ermitteln von Servern finden Sie unter Ermitteln von Servern mithilfe der manuellen Ermittlung.
- Für MECM-Benutzer:
  - Erstellen Sie eine Tasksequenz. Weitere Informationen finden Sie unter Erstellen einer Tasksequenz.
  - Erstellen Sie eine Tasksequenz. Weitere Informationen finden Sie im einheitlichen Benutzerhandbuch zu OpenManage Integration für Microsoft System Center.
  - Für die Bereitstellung eines Betriebssystems, das nicht Windows ist, benötigen Sie ein Gerätetyp-Zugangsdatenprofil. Weitere Informationen finden Sie unter Erstellen eines Zugangsdatenprofils.
- Für SCVMM-Benutzer:
  - Erstellen Sie ein Hypervisor-Profil. Weitere Informationen zum Erstellen eines Hypervisor-Profils finden Sie unter Erstellen eines Hypervisor-Profils.
  - Verwenden Sie für die Windows-Bereitstellung ein Gerätetyp-Zugangsdatenprofil. Weitere Informationen finden Sie unter Erstellen eines Zugangsdatenprofils.
- Wenn Sie nicht die Standard-Aktualisierungsquelle verwenden, erstellen Sie eine Aktualisierungsquelle. Weitere Informationen finden Sie unter Erstellen einer Aktualisierungsquelle.

Sie können eine Betriebsvorlage erstellen, indem Sie die Konfiguration des Referenzservers erfassen. Nach dem Erfassen der Konfiguration können Sie die Vorlage direkt speichern oder die Attribute für Aktualisierungsquelle, Hardwarekonfiguration und Windows-Komponente gemäß Ihren Anforderungen bearbeiten. Jetzt können Sie die Vorlage speichern, die auf homogenen PowerEdge-Servern verwendet werden kann.

1. Führen Sie in OMIMSSC einen der folgenden Schritte aus, um eine Betriebsvorlage zu öffnen:
   - Klicken Sie auf dem OMIMSSC-Dashboard auf **Betriebsvorlage erstellen**.
   - Klicken Sie im Navigationsbereich auf **Profile** > **Betriebsvorlage** und klicken Sie dann auf **Erstellen**.

   Es wird der Assistent **Betriebsvorlage** angezeigt.
2. Klicken Sie auf **Erstellen**.
   Es wird der Assistent **Betriebsvorlage** angezeigt.
3. Geben Sie einen Namen und eine Beschreibung für die Vorlage ein.
4. Wählen Sie den Gerätetyp aus, geben Sie die IP-Adresse des Referenzgeräts ein und klicken Sie auf Weiter.

   ANMERKUNG: Sie können die Konfiguration des Referenzservers mit iDRAC 2.0 und höher erfassen.

5. Klicken Sie unter Gerätekomponenten auf eine Komponente, um die verfügbaren Attribute und ihre Werte anzuzeigen.
   Dies sind die Komponenten:
   - Firmwareupdate
   - Hardwarekomponenten, darunter RAID, NIC und BIOS

     ANMERKUNG: In der Komponente iDRAC Embedded 1 werden die Privilegien und ihre Werte für das Attribut **Benutzer-Administratorrechte** angegeben.

Value	Berechtigung
1	Anmelden
2	Konfigurieren
4	Benutzer konfigurieren
8	Protokolle
16	Systemsteuerung
32	Auf die virtuelle Konsole zugreifen
64	Auf virtuelle Datenträger zugreifen
128	Systemvorgänge

256	Debug
499	Operatorrechte

- Betriebssystem: Wählen Sie entweder Windows oder ESXi oder RHEL aus.

6. Verwenden Sie die horizontale Bildlaufleiste, um eine Komponente zu finden. Wählen Sie die Komponente aus, erweitern Sie eine Gruppe und bearbeiten Sie dann die Attributwerte. Verwenden Sie die vertikale Bildlaufleiste, um Gruppen und Attribute einer Komponente zu bearbeiten.
7. Aktivieren Sie das Kontrollkästchen für jede Komponente, da die Konfigurationen der ausgewählten Komponenten auf das verwaltete Gerät angewendet werden, wenn die Betriebsvorlage angewendet wird. Alle Konfigurationen vom Referenzgerät werden jedoch erfasst und in der Vorlage gespeichert.

   ANMERKUNG: Unabhängig von der Auswahl im Kontrollkästchen für jede Komponente werden alle Konfigurationen in der Vorlage erfasst.

   ANMERKUNG: Die Betriebsvorlage erfasst das Kennwort beim Abrufen vom Referenzserver nicht. Stellen Sie vor der Bereitstellung sicher, dass Sie die Kennwortwerte für ausgewählte Attribute festlegen.

   Führen Sie in der Komponente Betriebssystem die Schritte je nach Anforderung in einer der folgenden Optionen aus:

   - Informationen zur Bereitstellung des Windows-Betriebssystems auf MECM finden Sie unter Windows-Komponente für die OMIMSSC-Konsolenerweiterung für MECM.
   - Informationen zur Bereitstellung des Windows-Betriebssystems auf SCCM finden Sie unter Windows-Komponente für die OMIMSSC-Konsolenerweiterung für SCVMM.
   - OMIMSSC
   - Informationen zur Bereitstellung eines Betriebssystems, das kein Windows-Betriebssystem ist, finden Sie unter Nicht-Windows-Komponente für die OMIMSSC-Konsolenerweiterungen.
8. Um das Profil zu speichern, klicken Sie auf **Fertig stellen**.

Empfehlung: Wenn Ihr Referenz-iDRAC-Server über eine Enterprise-Lizenz verfügt und Sie die SCEP-Attribute sehen, stellen Sie sicher, dass Sie diese Attribute aufheben, da Sie nur mit einer Rechenzentrums-Lizenz unterstützt werden.

Windows-Betriebssystemkomponente für die OMIMSSC-Konsolenerweiterung für MECM

Führen Sie beim Erstellen oder Bearbeiten der Betriebsvorlage für den Server die folgenden Schritte für die Windows-Komponente aus:

1. Wählen Sie eine Tasksequenz und Bereitstellungsmethode aus.

   ANMERKUNG: Im Dropdownmenü werden nur die Tasksequenzen aufgelistet, die für Sammlungen bereitgestellt werden.

   Informationen zur Tasksequenz finden Sie unter Tasksequenz.

   Informationen zur Tasksequenz finden Sie im einheitlichen Benutzerhandbuch OpenManage Integration for Microsoft System Center.

2. Wählen Sie eine der folgenden Optionen als **Bereitstellungsmethode** aus:
   - **Start mit Netzwerk-ISO**: Führt einen Neustart mit einem angegebenen ISO-Image durch.
   - **Stufenweise Bereitstellung von ISO in vFlash und Neustart**: Lädt das ISO in vFlash herunter und führt einen Neustart durch.
   - **Neustart in vFlash**: führt einen Neustart in vFlash durch. Stellen Sie sicher, dass das ISO-Image auf vFlash vorhanden ist.

     ANMERKUNG: Um die Option **Neustart in vFlash** zu verwenden, muss die Bezeichnung für die Partition, die auf vFlash erstellt wurde, **ISOIMG** sein.
3. (Optional) Um das in der Netzwerkfreigabe vorhandene Image zu verwenden, wählen Sie die Option **Netzwerk-ISO als Fallback verwenden**.
4. Geben Sie eine LC-Startmedien-Abbilddatei ein.
5. Wählen Sie die für das Betriebssystem erforderlichen Treiber.

ANMERKUNG: Die Bereitstellung des Betriebssystems Windows Server 2016 auf AMD-Plattformen bietet keine Unterstützung für x2apic. Stellen Sie sicher, dass Sie die BIOS-x2apic und die logischen Prozessoreinstellungen deaktivieren, bevor Sie das Betriebssystem installieren.

Windows-Betriebssystemkomponente für die OMIMSSC-Konsolenerweiterung für SCVMM

Führen Sie beim Erstellen oder Bearbeiten der Betriebsvorlage für den Server die folgenden Schritte für die Windows-Komponente aus:

Wählen Sie unter **Hypervisor-Profil**, **Zugangsdatenprofil** und **Server-IP** aus.

ANMERKUNG: Hostname und **Serververwaltungs-NIC** sind immer Poolwerte. Geben Sie für die Serververwaltung-NIC die MAC-Adresse des Netzwerkports an, über den das Betriebssystem mit SCVMM kommunizieren soll.

Wenn Sie für **Server-IP aus** die Option **Statisch** auswählen und sicherstellen, dass Sie das logische Netzwerk in SCVMM konfiguriert haben und die folgenden Felder Poolwerte sind:

- **Logisches Netzwerk der Konsole**
- **IP-Subnetz**
- **Statische IP-Adresse**

ANMERKUNG: Die Bereitstellung des Betriebssystems Windows Server 2016 auf AMD-Plattformen bietet keine Unterstützung für x2apic. Stellen Sie sicher, dass Sie die BIOS-x2apic und die logischen Prozessoreinstellungen deaktivieren, bevor Sie das Betriebssystem installieren.

Nicht-Windows-Komponente für OMIMSSC-Konsolenerweiterungen

Führen Sie beim Erstellen oder Bearbeiten der Betriebsvorlage für den Server die folgenden Schritte für eine Nicht-Windows-Komponente aus:

Wählen Sie ein anderes Betriebssystem als Windows, die Version des Betriebssystems, den Typ des Freigabeordners, den ISO-Dateinamen, den Ort der ISO-Datei und das Kennwort für das Root-Konto des Betriebssystems aus.

(Optional) Wählen Sie ein Windows-Zugangsdatenprofil für den Zugriff auf die CIFS-Freigabe aus.

Der **Hostname** ist ein Poolwert und wenn Sie die DHCP-Option deaktivieren, sind die folgenden Felder Poolwerte:

- **IP-Adresse**
- **Subnetzmaske**
- **Standard-Gateway**
- **Primärer DNS-Server**
- **Sekundärer DNS-Server**

ANMERKUNG: Die Freigabetypen NFS (Network File System) und CIFS (Common Internet File System) werden für die Bereitstellung von anderen Betriebssystemen als Windows unterstützt.

Erstellen einer Betriebsvorlage aus Referenzmodularsystemen

Stellen Sie vor dem Erstellen der Betriebsvorlage sicher, dass Sie die folgenden Tasks ausführen:

- Ermitteln Sie ein modulares System mithilfe der **Ermittlungsfunktion**. Informationen zum Ermitteln modularer Systeme finden Sie unter Ermitteln eines modularen Systems mithilfe der manuellen Ermittlung.
- Wenn Sie nicht die Standard-Aktualisierungsquelle verwenden, erstellen Sie eine Aktualisierungsquelle. Weitere Informationen finden Sie unter Erstellen einer Aktualisierungsquelle.

Sie können eine Betriebsvorlage erstellen, indem Sie die Konfiguration der Referenzmodularsysteme erfassen. Nach dem Erfassen der Konfiguration können Sie die Vorlage direkt speichern oder die Attribute für die Aktualisierungsquelle und die Hardwarekonfiguration gemäß Ihren Anforderungen bearbeiten. Jetzt können Sie die Vorlage speichern, mit der andere modulare Systeme desselben Modells konfiguriert werden können.

ANMERKUNG: Wenn Sie Active Directory-Benutzer (AD-Benutzer) auf anderen MX7000-Geräten konfigurieren möchten, müssen Sie sicherstellen, dass Sie eine Betriebsvorlage aus einem MX7000-Modularsystem erstellen, in dem alle AD-Benutzer konfiguriert sind.

ANMERKUNG: Die Kennwörter des Nutzerkontos werden aus Sicherheitsgründen nicht in der Betriebsvorlage des Referenzmodularsystems erfasst. Bearbeiten Sie die Betriebsvorlage, um ein neues Nutzerkonto und ein neues Kennwort

hinzuzufügen, und wenden Sie dann die Betriebsvorlage auf die verwalteten modularen Systeme an. Andernfalls können Sie die Betriebsvorlage ohne Änderungen an den Benutzerkonten anwenden. Dieselben Kennwörter, die im Referenzmodulsystem verwendet werden, werden auf das verwaltete Modulsystem angewendet.

1. Führen Sie in OMIMSSC einen der folgenden Schritte aus, um eine Betriebsvorlage zu öffnen:
   - Klicken Sie auf dem OMIMSSC-Dashboard auf **Betriebsvorlage erstellen**.
   - Klicken Sie im Navigationsbereich auf **Profile** > **Betriebsvorlage** und klicken Sie dann auf **Erstellen**.

   Es wird der Assistent **Betriebsvorlage** angezeigt.
2. Klicken Sie auf **Erstellen**.
   Es wird der Assistent **Betriebsvorlage** angezeigt.
3. Geben Sie einen Namen und eine Beschreibung für die Vorlage ein.
4. Klicken Sie unter **Gerätekomponenten** auf eine Komponente, um die verfügbaren Attribute und ihre Werte anzuzeigen.
   Dies sind die Komponenten:
   - Firmwareupdate
   - Eingebettetes Managementmodul

   ANMERKUNG: Stellen Sie sicher, dass das Attribut **Web-Server** aktiviert ist. Wenn diese Komponente nicht aktiviert ist, kann nach der Bereitstellung der Betriebsvorlage nicht über OMIMSSC auf die MX7000 Modularsysteme zugegriffen werden.

   ANMERKUNG: Stellen Sie für **SNMP-Konfiguration** und **Syslog-Konfiguration** sicher, dass Sie alle vier für jedes Attribut verfügbaren Konfigurationen auswählen, um sie auf verwaltete Geräte anzuwenden.
5. Verwenden Sie die horizontale Bildlaufleiste, um eine Komponente zu finden. Wählen Sie die Komponente aus, erweitern Sie eine Gruppe und bearbeiten Sie dann die Attributwerte. Verwenden Sie die vertikale Bildlaufleiste, um Gruppen und Attribute einer Komponente zu bearbeiten.
6. Aktivieren Sie das Kontrollkästchen für jede Komponente, da die Konfigurationen der ausgewählten Komponenten auf das verwaltete Gerät angewendet werden, wenn die Betriebsvorlage angewendet wird. Alle Konfigurationen vom Referenzgerät werden jedoch erfasst und in der Vorlage gespeichert.
7. Um das Profil zu speichern, klicken Sie auf **Fertig stellen**.

Erstellen von Clustern mithilfe der Betriebsvorlage

In diesem Kapitel werden Informationen zum Erstellen des Windows Server HCI-Clusters beschrieben.

Erstellen eine logischen Switches für Windows Server HCI-Cluster

Erstellen Sie einen logischen Switch über OMIMSSC in SCVMM.

ANMERKUNG: Die im Abschnitt **Konfiguration für Verwaltung** eingegebene IP-Adresse überschreibt die IP-Adresse, die in der Betriebssystemkomponente der vordefinierten Betriebsvorlage von Windows Server HCI angegeben ist.

1. Erweitern Sie in OMIMSSC den Punkt **Konfiguration und Bereitstellung**, klicken Sie auf **Clusteransicht** und klicken Sie dann auf **Logischen Switch erstellen** für Cluster.
2. Klicken Sie auf **Logischen Switch für Cluster erstellen**.
3. Geben Sie einen Namen für den logischen Switch an und wählen Sie die in SCVMM vorhandene Hostgruppe für die Zuweisung des logischen Switches aus.
4. Geben Sie die folgenden Details ein und klicken Sie dann auf **Erstellen**.
   a. Geben Sie in **Konfiguration für Verwaltung** die Details zu **Subnetz**, **Start-IP**, **End-IP**, **DNS-Server**, **DNS-Suffix** und **Gateway** an.

      ANMERKUNG: Geben Sie die Subnetzinformationen in CIDR-Notation (Classless InterDomain Routing) an.

   b. Geben Sie in **Konfiguration für Speicher** die Details zu **VLAN**, **Subnetz**, **Start-IP** und **End-IP** an.
5. Geben Sie einen eindeutigen Jobnamen und eine Beschreibung für den Job ein und klicken Sie auf **Erstellen**.
   Um diesen Job zu verfolgen, ist standardmäßig die Option **Zur Jobliste wechseln** ausgewählt.

Um zu überprüfen, ob der logische Switch erfolgreich erstellt wurde, suchen Sie im Dropdownmenü auf der Seite **Cluster erstellen** nach dem Namen des logischen Switches.

Um die Details des logischen Switches anzuzeigen, führen Sie die folgenden Schritte in SCVMM aus:

1. Um den Namen des logischen Switches anzuzeigen, klicken Sie auf **Fabric** und klicken Sie unter **Netzwerk** auf **Logische Switches**.
2. Um das Uplink Port Profile (UPP) des logischen Switches anzuzeigen, klicken Sie auf **Fabric** und klicken Sie unter **Netzwerk** auf **Logische Switches**.
3. Klicken Sie zum Anzeigen des Netzwerks des logischen Switches auf **Fabric**, und klicken Sie unter **Netzwerk** auf **Logische Netzwerke**.

Erstellen von Windows Server HCI-Clustern

- Stellen Sie sicher, dass Sie ein logisches Netzwerk erstellen, indem Sie die Funktion **Logischen Switch erstellen** für Cluster verwenden.
- Stellen Sie sicher, dass Sie SCVMM 2016 oder 2019 verwenden.
- Stellen Sie sicher, dass Sie die Windows Server 2016 oder 2019 Datacenter Edition verwenden.
- Stellen Sie sicher, dass die Konfigurationen der verwalteten Server den Anforderungen der Firmware- und Treiberversion der Windows Server HCI-Lösung entsprechen. Weitere Informationen finden Sie in der *Supportmatrix zu für Windows Server HCI vorbereiteten Knoten von Dell EMC, PowerEdge R740XD, R740XD2 und PowerEdge R640*.
- Informationen zu Infrastruktur-und Verwaltungsdetails von Windows Server HCI finden Sie im *Bereitstellungshandbuch zu Dell EMC Microsoft Windows Server HCI Ready Node für eine skalierbare hyperkonvergente Infrastruktur mit RN740xd, RN740XD2, RN640, RN440 und AX6515 Windows Server HCI Ready Nodes.*

Berücksichtigen Sie Folgendes, bevor Sie Windows Server HCI-Cluster erstellen:

- Sie können einen Windows Server HCI-Cluster in OMIMSSC erstellen, indem Sie nur eine statische IP-Adresse angeben.
- Die Größe des virtuellen Laufwerks wird in der vordefinierten Betriebsvorlage von Windows Server HCI als Null angezeigt. Nach dem Anwenden der vordefinierten Betriebsvorlage für Windows Server HCI wird das virtuelle Laufwerk jedoch nur in der Größe erstellt, die der vollen Größe des physischen M.2-Speichermediums entspricht. Weitere Informationen zum virtuellen Laufwerk finden Sie im iDRAC-Benutzerhandbuch unter dell.com/support.
- Stellen Sie sicher, dass die IP-Adresse in der Betriebsvorlage konfiguriert ist, wenn die Option Betriebssystem-zu-iDRAC-Passthrough aktiviert ist.

Führen Sie die folgenden Schritte aus, um Windows Server HCI-Cluster zu erstellen:

1. Klicken Sie in OMIMSSC auf **Konfiguration und Bereitstellung** und klicken Sie dann auf **Clusteransicht**.
   Die Seite **Clusteransicht** wird angezeigt.
2. Um einen Cluster zu erstellen, klicken Sie auf **Erstellen**.
   Es wird die Seite **Cluster erstellen** angezeigt.
3. Geben Sie einen Clusternamen an und wählen Sie die vordefinierte Betriebsvorlage zum Erstellen von Windows Server HCI-Clustern aus.
   - Nicht zugewiesene Server, die nur zu einem bestimmten Servermodell und einer NIC-Karte gehören, werden basierend auf der Betriebsvorlage angezeigt, die Sie im Dropdownmenü **Betriebsvorlage** auswählen.
4. Um Server zu einem Cluster hinzuzufügen, wählen Sie die Server mithilfe des Kontrollkästchens aus.
5. Klicken Sie zum Hinzufügen systemspezifischer Poolwerte auf **Attributwertpool exportieren**.

   Bearbeiten und speichern Sie die Datei, damit Sie die systemspezifischen Poolwerte angeben können. Weitere Informationen finden Sie unter Ausfüllen der Poolwert-CSV-Datei.
6. (Optional) Wenn Sie systemspezifische Werte festlegen müssen, klicken Sie im **Attributwertepool** auf **Durchsuchen** und wählen Sie die bearbeitete CSV-Datei aus.
7. Geben Sie einen eindeutigen Jobnamen an und klicken Sie auf **Erstellen**.

   Um diesen Job zu verfolgen, ist standardmäßig die Option **Zur Jobliste wechseln** ausgewählt.

   ANMERKUNG: Wenn die Betriebssystembereitstellung durchgeführt wird, sehen Sie ein Hostprofil/physische Computerprofile, die in SCVMM geklont werden (Name des Servers mit GUID versehen). Diese Profile werden für einzelne Server-OSD verbraucht.

So überprüfen Sie, ob die Cluster erfolgreich erstellt wurden:
1. Überprüfen Sie anhand des Status des Clusterjobs, ob dieser erfolgreich erstellt wurde.
2. Zeigen Sie den Cluster in der Seite **Clusteransicht** an.
3. Zeigen Sie den Cluster in SCVMM an.

Weitere Informationen finden Sie unter Erstellen eines Profils für einen physischen Computer im Abschnitt Voraussetzungen der Dokumentation von Microsoft zur Bereitstellung eines Hyper-V-Hosts oder -Clusters von Bare-Metal-Computern.

ANMERKUNG: Es wird empfohlen, dass Cluster Witness für einen Cluster mit zwei Knoten konfiguriert werden muss. Die Cluster Witness-Konfiguration trägt dazu bei, ein Cluster oder Speicherquorum aufrechtzuerhalten, wenn ein Knoten oder eine Netzwerkkommunikation ausfällt. Weitere Informationen finden Sie im Leitfaden zur Bereitstellung von Windows Server HCI.

Anzeigen der Betriebsvorlage

So zeigen Sie erstellte Betriebsvorlage an:

Klicken Sie in der OMIMSSC-Konsole auf **Profile und Vorlagen** und klicken Sie dann auf **Betriebsvorlage**. Hier werden alle erstellten Vorlagen aufgelistet.

Bearbeiten der Betriebsvorlage

Sie können die Aktualisierungsquelle, die Hardwarekonfigurationen und das Betriebssystem einer Betriebsvorlage ändern.

Berücksichtigen Sie Folgendes, bevor Sie eine Betriebsvorlage ändern:

- Die Werte einiger Attribute hängen von den Werten anderer Attribute ab. Wenn Sie Attributwerte manuell ändern, stellen Sie sicher, dass Sie auch die jeweils abhängigen Attribute ändern. Wenn diese voneinander abhängigen Werte nicht ordnungsgemäß geändert werden, schlägt die Anwendung der Hardwarekonfigurationen möglicherweise fehl.
- Die Erstellung einer Betriebsvorlage ruft alle Hardwarekonfigurationen vom angegebenen Referenzserver ab, die möglicherweise systemspezifische Attribute enthalten. Beispiel: statische IPv4-Adresse, Bestands-Tag. Informationen zur Konfiguration von systemspezifischen Attributen finden Sie unter Konfigurieren von systemspezifischen Werten mit der Betriebsvorlage
- Attributen in der Betriebsvorlage werden die aktuellen Werte des Referenzservers zugewiesen. In der Betriebsvorlage sind außerdem andere anwendbare Werte für die Attribute aufgeführt.
- Um vordefinierte Betriebsvorlage und nutzerdefinierte Betriebsvorlage zu ändern, führen Sie folgende Schritte durch:

ANMERKUNG: (Nur für SCVMM-Nutzer und -Server) Alle verbindlichen Attribute. (Obligatorische Attribute, die in der Betriebsvorlage erfasst werden, sind die von Dell EMC empfohlenen Attribute für Windows Server HCI-Cluster), die für Windows Server HCI die schreibgeschützten Attribute in der vordefinierten Windows-Server HCI-Vorlage sind. Sie können jedoch den Namen der Vorlage, der Betriebssystemkomponenten und der Hardwarekonfigurationsattribute bearbeiten.

1. Wählen Sie die Vorlage aus, die Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.
   Die Seite Betriebsvorlage wird angezeigt.
2. (Optional) Bearbeiten Sie den Namen und die Beschreibung für die Vorlage, und klicken Sie auf **Weiter**.
3. Klicken Sie auf eine Komponente, um die verfügbaren Attribute und ihre Werte in **Gerätekomponenten** anzuzeigen.
4. Ändern Sie die Werte der verfügbaren Attribute.

   ANMERKUNG: Aktivieren Sie das Kontrollkästchen für jede Komponente, da nur die Konfigurationen der ausgewählten Komponenten auf das verwaltete System angewendet werden, wenn die Betriebsvorlage angewendet wird.

   ANMERKUNG: Bei der Bearbeitung der Betriebsvorlage werden einige wenige schreibgeschützte Komponentenattribute der Advanced Host Controller Interface (AHCI) als bearbeitbar aufgeführt. Wenn diese schreibgeschützten Attribute festgelegt werden und die Betriebsvorlage bereitgestellt wird, werden jedoch keine Änderungen an dem Gerät vorgenommen.

   - Für MX7000 Modulare Systeme:
     - Konfigurationen werden nur angewendet, wenn alle Attribute für eine Gruppe ausgewählt sind. Stellen Sie daher sicher, dass Sie alle Attribute in einer Gruppe auswählen, auch wenn Sie nur eines der Attribute in der Gruppe ändern möchten.
     - Um einen neuen Benutzer über eine Betriebsvorlage hinzuzufügen, wählen Sie alle Attribute vorhandener Benutzer aus, die beim Erfassen der Betriebsvorlage exportiert wurden, wählen Sie die kürzlich hinzugefügten Benutzergruppen aus und speichern Sie die Betriebsvorlage.
     - Informationen zur Angabe der Zeitzonenwerte finden Sie im Anhang.
5. Führen Sie für die Betriebssystemkomponente je nach Anforderung einen der folgenden Tasks aus:
   - Informationen zur Bereitstellung des Windows-Betriebssystems auf MECM finden Sie unter Windows-Komponente für die OMIMSSC-Konsolenerweiterung für MECM.
   - Informationen zur Bereitstellung des Windows-Betriebssystems auf SCCM finden Sie unter Windows-Komponente für die OMIMSSC-Konsolenerweiterung für SCVMM.
   - OMIMSSC
   - Informationen zur Bereitstellung eines Betriebssystems, das kein Windows-Betriebssystem ist, finden Sie unter Nicht-Windows-Komponente für die OMIMSSC-Konsolenerweiterungen.

6. Um das Profil zu speichern, klicken Sie auf **Fertig stellen**.

Empfehlung: Bei der Bearbeitung der Betriebsvorlage werden einige wenige schreibgeschützte Komponentenattribute der Advanced Host Controller Interface (AHCI) als bearbeitbar aufgeführt. Wenn diese schreibgeschützten Attribute festgelegt werden und die Betriebsvorlage bereitgestellt wird, werden jedoch keine Änderungen an dem Gerät vorgenommen.

Konfigurieren von systemspezifischen Werten (Pool-Werte) unter Verwendung der Betriebsvorlage auf mehreren Servern

OMIMSSC ruft die bestehende Konfiguration des Geräts ab. Systemspezifische Attribute wie z. B. die statische IPv4-Adresse für iDRAC werden als Poolwert in der Betriebsvorlage angezeigt. Pool-Wert-Attribute, die abhängige Attribute sind, werden standardmäßig zusammen mit anderen Attributen ausgewählt.

1. Wählen Sie die Vorlage aus, die Sie bearbeiten möchten, und klicken Sie auf Bearbeiten.
   Die Seite Betriebsvorlage wird angezeigt.
2. (Optional) Bearbeiten Sie den Namen und die Beschreibung für die Vorlage, und klicken Sie auf **Weiter**.
3. Klicken Sie auf eine Komponente, um die verfügbaren Attribute und ihre Werte in Gerätekomponenten anzuzeigen.
4. Erweitern Sie die **Attributgruppe**. Wenn der Wert des Attributs ein **Pool-Wert** ist, wird das Attribut als systemspezifisches Attribut identifiziert. Informationen über die Attributgruppe und die Komponente für alle systemspezifischen Attribute finden Sie in Tabelle 13 im Abschnitt Systemspezifische Attribute in der Betriebsvorlage.
5. Wenn Sie diese systemspezifischen Attribute nicht anwenden möchten, identifizieren Sie diese Attribute (wie in Schritt 4 beschrieben) und heben Sie die Auswahl auf, während Sie die Betriebsvorlage bearbeiten.
6. Die Eingabe zu diesen systemspezifischen Attributen kann für mehrere Server über eine .CSV-Datei durch **Pool-Attribute exportieren** während der Bereitstellung der Betriebsvorlage erfolgen, siehe Bereitstellung von Betriebsvorlagen auf Servern.

ANMERKUNG: Weitere Informationen zum Auffüllen von Pool-Werten in einer CSV Datei finden Sie unter Auffüllen der Pool-Wert-CSV-Datei-und systemspezifischen Attribute in der Betriebsvorlage.

Empfehlung: Wenn Sie beim Erstellen einer Betriebsvorlage das Kontrollkästchen eines abhängigen Attributs mit einem Poolwert wählen und deaktivieren, können Sie die Betriebsvorlage mit der folgenden Fehlermeldung nicht speichern: `Select at least one attribute, under the selected components, before creating the Operational Template` Wählen Sie ein anderes abhängiges Attribut mit einem Poolwert oder das gleiche abhängige Attribut aus und speichern Sie die Betriebsvorlage. Erstellen Sie dann eine neue Betriebsvorlage.

Zuweisen der Betriebsvorlage und Durchführen der Kompatibilitätsprüfung für Server

Weisen Sie einem Server eine Betriebsvorlage zu und führen Sie die Kompatibilität der Betriebsvorlage aus. Erst nachdem Sie einem Server eine Betriebsvorlage zugewiesen haben, können Sie den Kompatibilitätstatus der Betriebsvorlage anzeigen. Sie können die Konfiguration eines Servers mit einer Betriebsvorlage vergleichen, indem Sie die Vorlage einem Server zuweisen. Nachdem Sie eine Betriebsvorlage zugewiesen haben, wird der Kompatibilitätsjob ausgeführt und der Status der Betriebsvorlage wird nach Abschluss angezeigt.

Führen Sie zum Zuweisen einer Betriebsvorlage die folgenden Schritte durch:

1. Klicken Sie in OMIMSSC auf **Konfiguration und Bereitstellung** und klicken Sie dann auf **Serveransicht**. Wählen Sie die erforderlichen Server aus und klicken Sie auf **Betriebsvorlage zuweisen und Kompatibilität ausführen**.

   Die Seite Betriebsvorlage **zuweisen** und Kompatibilität ausführen wird angezeigt.
2. Wählen Sie die erforderlichen Server aus und klicken Sie auf **Betriebsvorlage zuweisen und Kompatibilität ausführen**.
3. Wählen Sie die Vorlage aus dem Dropdownmenü Betriebsvorlage aus, geben Sie einen Auftragsnamen ein und klicken Sie auf **Zuweisen**.

   In der Dropdown-Liste Betriebsvorlage werden Vorlagen des gleichen Typs angezeigt wie für die im vorherigen Schritt ausgewählten Geräte.

   Wenn das Gerät mit der Vorlage kompatibel ist, wird ein **grünes** Feld mit einem Häkchen angezeigt.

Wenn die Betriebsvorlage nicht erfolgreich auf dem Gerät angewendet wird oder die Hardwarekomponente in der Betriebsvorlage nicht ausgewählt ist, wird ein Symbolfeld **Information** angezeigt.

Wenn das Gerät der Vorlage nicht entspricht, wird ein Symbolfeld **Warnung** angezeigt. Nur wenn das Gerät nicht mit der zugewiesenen Betriebsvorlage kompatibel ist, können Sie einen zusammenfassenden Bericht anzeigen, indem Sie auf die Verknüpfung mit dem Namen der Vorlage klicken. Auf der Seite **Kompatibilitätszusammenfassungsbericht** für Betriebsvorlage wird ein zusammenfassender Bericht der Unterschiede zwischen der Vorlage und dem Gerät angezeigt.

Führen Sie die folgenden Schritte aus, um einen ausführlichen Bericht anzuzeigen:

a. Klicken Sie auf **Kompatibilitätsdetails anzeigen**. Hier werden die Komponenten angezeigt, deren Attributwerte sich von denen der zugewiesenen Vorlage unterscheiden. Die Farben zeigen die verschiedenen Zustände der Kompatibilität der Betriebsvorlage an.
   - Warnsymbol für gelbe Farbe: Inkompatibilität. Bedeutet, dass die Konfiguration des Geräts nicht mit den Vorlagenwerten übereinstimmt.
   - Rotes Farbfeld: Gibt an, dass die Komponente nicht auf dem Gerät vorhanden ist.

Zuweisen der Betriebsvorlage für Modularsysteme

Weisen Sie eine Betriebsvorlage einem modularen System zu und führen Sie die Kompatibilität der Betriebsvorlage aus. Dieser Vorgang vergleicht die Konfiguration eines Modularsystems mit einer Betriebsvorlage, indem die ausgewählte Vorlage einem Modularsystem zugewiesen wird. Nachdem Sie eine Betriebsvorlage zugewiesen haben, wird der Kompatibilitätsjob ausgeführt und der Kompatibilitätsstatus wird nach Abschluss angezeigt.

Führen Sie die folgenden Schritte aus, um eine Betriebsvorlage für modulare Systeme zuzuweisen:

1. Klicken Sie in OMIMSSC auf **Konfiguration und Bereitstellung**, und klicken Sie dann auf **Modularsystemansicht**. Wählen Sie das gewünschte modulare System aus und klicken Sie auf **Betriebsvorlage zuweisen**.

   Die Seite Betriebsvorlage **zuweisen** wird angezeigt.
2. Wählen Sie die erforderlichen modularen Systeme aus und klicken Sie auf **Betriebsvorlage zuweisen und Kompatibilität ausführen**.

   Die Seite Betriebsvorlage **zuweisen** wird angezeigt.
3. Wählen Sie die Vorlage aus dem Dropdownmenü Betriebsvorlage aus, geben Sie einen Auftragsnamen ein und klicken Sie auf **Zuweisen**.

   Wenn das Gerät mit der Vorlage kompatibel ist, wird ein **grünes** Feld mit einem Häkchen angezeigt.

   Wenn die Betriebsvorlage nicht erfolgreich auf dem Gerät angewendet wird oder die Hardwarekomponente in der Betriebsvorlage nicht ausgewählt ist, wird ein Symbolfeld **Information** angezeigt.

   ANMERKUNG: Der Kompatibilitätsstatus der Betriebsvorlage schließt alle Änderungen aus, die an Benutzerattributen vorgenommen werden.

   Wenn das Gerät der Vorlage nicht entspricht, wird ein Symbolfeld **Warnung** angezeigt. Nur wenn das Gerät nicht mit der zugewiesenen Betriebsvorlage kompatibel ist, können Sie einen zusammenfassenden Bericht anzeigen, indem Sie auf die Verknüpfung mit dem Namen der Vorlage klicken. Auf der Seite **Kompatibilitätszusammenfassungsbericht** für Betriebsvorlage wird ein zusammenfassender Bericht der Unterschiede zwischen der Vorlage und dem Gerät angezeigt.

   Führen Sie die folgenden Schritte aus, um einen ausführlichen Bericht anzuzeigen:

   a. Klicken Sie auf **Kompatibilitätsdetails anzeigen**. Hier werden die Komponenten angezeigt, deren Attributwerte sich von denen der zugewiesenen Vorlage unterscheiden. Die Farben zeigen die verschiedenen Zustände der Kompatibilität der Betriebsvorlage an.
      - Warnsymbol für gelbe Farbe: Inkompatibilität. Bedeutet, dass die Konfiguration des Geräts nicht mit den Vorlagenwerten übereinstimmt.
      - Rotes Farbfeld: Gibt an, dass die Komponente nicht auf dem Gerät vorhanden ist.

Bereitstellen von Betriebsvorlagen

ANMERKUNG: Stellen Sie sicher, dass Sie keine Attribute aktivieren, die die Zugangsdaten ändern, um sich nach der Bereitstellung der Betriebsvorlage beim Gerät anmelden zu können.

1. Klicken Sie in OMIMSSC auf Konfiguration und Bereitstellung und klicken Sie auf **Serveransicht**. Wählen Sie die Server aus, auf die Sie die Vorlage angewendet haben, und klicken Sie dann auf **Betriebsvorlage bereitstellen**.
   Die Seite **Betriebsvorlage bereitstellen** wird angezeigt.

2. Klicken Sie in OMIMSSC auf **Konfiguration und Bereitstellung** und klicken Sie auf **Modularsystemansicht**. Wählen Sie das modulare System aus, dem Sie die Vorlage zugewiesen haben, und klicken Sie dann auf **Betriebsvorlage bereitstellen**.
   Die Seite **Betriebsvorlage bereitstellen** wird angezeigt.
3. (Optional) Um alle Attribute, die in der ausgewählten Vorlage als Poolwerte markiert sind, in eine CSV-Datei zu exportieren, klicken Sie auf **Poolattribute exportieren**. Andernfalls fahren Sie mit Schritt 4 fort.

   ANMERKUNG: Fügen Sie vor dem Exportieren der Poolwerte die IP-Adresse des OMIMSSC-Geräts, auf dem die OMIMSSC-Konsolenerweiterung installiert ist, zur lokalen Intranetsite hinzu. Weitere Informationen zum Hinzufügen der IP-Adresse im IE-Browser finden Sie im Abschnitt *Browsereinstellungen* im *Benutzerhandbuch zur Dell EMC OpenManage Integration für Version 7.2.1 von Microsoft System Center für Configuration Manager und System Center Virtual Machine Manager*.

4. Wenn Sie die Poolwerte exportiert haben, geben Sie Werte für alle Attribute ein, die in der CSV-Datei als Poolwerte markiert sind, und speichern Sie die Datei. Wählen Sie im **Attributwertpool** diese Datei aus, um sie zu importieren.

   Das Format einer .CSV Datei ist `attribute-value-pool.csv`

   ANMERKUNG: Stellen Sie sicher, dass Sie eine .CSV-Datei auswählen, die alle richtigen Attribute enthält. Die iDRAC-IP- oder iDRAC-Zugangsdaten ändern sich aufgrund der Vorlage nicht, da der Job nach den Änderungen der iDRAC-IP- oder iDRAC-Zugangsdaten nicht von OMIMSSC aufgezeichnet und als fehlgeschlagen markiert wird, obwohl der Job in iDRAC erfolgreich sein kann.

5. Geben Sie einen eindeutigen Jobnamen und eine Beschreibung für den Job ein und klicken Sie auf **Bereitstellen**.

   Um diesen Job zu verfolgen, ist standardmäßig die Option **Zur Jobliste wechseln** ausgewählt.

Bereitstellen der Betriebsvorlage auf Servern

Stellen Sie für die Bereitstellung des Betriebssystems auf verwalteten Servern sicher, dass auf Ihrem Verwaltungssystem und dem für die Bereitstellung verwendeten Betriebssystemabbild der KB-Artikel 4093492 oder höher installiert ist.

Sie können Windows und Nicht-Windows-Betriebssysteme (ESXi und RHEL) bereitstellen, indem Sie die Betriebsvorlage bereitstellen, die Servern zugewiesen ist.

ANMERKUNG: Laden Sie die entsprechenden Treiber von `Dell.com/support` herunter und installieren Sie sie, wenn nach der Bereitstellung des Windows 2016 oder Windows 2019 Betriebssystems auf der 12. Generation der Server unter „Gerätemanager“ ein gelbes Warnsymbol angezeigt wird.

ANMERKUNG: Die Bereitstellung von Betriebsvorlagen auf Servern wird blockiert, wenn der Sperrmodus auf den Servern aktiviert ist.

ANMERKUNG: Wenn Sie Windows auf einem UEFI-basierten Gerät bereitstellen, formatieren Sie die Festplatte, die die Windows-Partition enthält, mit einem GPT-Dateisystem (GUID Partition Table). Weitere Informationen finden Sie im Abschnitt UEFIGPT-basierte Festplatten-Partitionen in der Dokumentation von Microsoft.

1. Klicken Sie in OMIMSSC auf Konfiguration und Bereitstellung und klicken Sie auf **Serveransicht**. Wählen Sie die Server aus, auf denen Sie eine Vorlage bereitstellen möchten, und klicken Sie dann auf **Betriebsvorlage bereitstellen**.
   Die Seite **Betriebsvorlage bereitstellen** wird angezeigt.

   ANMERKUNG: Wenn die Eingabeaufforderung *`Press any key to boot to CD \ DVD .....`* beim Starten des Tasksequenz-Datenträgers angezeigt wird. Informationen zum Entfernen der Eingabeaufforderung und zum automatischen Starten des Tasksequenz-Datenträgers finden Sie im Abschnitt Installieren von Windows auf einem EFI-basierten Computer der Dokumentation von Microsoft.

2. Wählen Sie die Server aus, auf denen Sie eine Vorlage bereitstellen möchten, und klicken Sie dann auf **Betriebsvorlage bereitstellen**.
   Die Seite **Betriebsvorlage bereitstellen** wird angezeigt.
3. Um alle Attribute, die in der ausgewählten Vorlage als Pool-Werte markiert sind, in eine CSV-Datei zu exportieren, klicken Sie auf **Poolattribute exportieren**.

   Fügen Sie vor dem Exportieren der Poolwerte die IP-Adresse des OMIMSSC-Geräts, auf dem die OMIMSSC-Konsolenerweiterung installiert ist, zur lokalen Intranetsite hinzu.
4. Wenn Sie die Poolwerte exportiert haben, geben Sie Werte für alle Attribute ein, die in der CSV-Datei als Poolwerte markiert sind, und speichern Sie die Datei. Wählen Sie im **Attributwertpool** diese Datei aus, um sie zu importieren.

   Das Format einer .CSV Datei ist `attribute-value-pool.csv`

ANMERKUNG: Stellen Sie sicher, dass Sie eine .CSV-Datei auswählen, die alle richtigen Attribute enthält. Die iDRAC-IP- oder iDRAC-Zugangsdaten ändern sich aufgrund der Vorlage nicht, da der Job nach den Änderungen der iDRAC-IP- oder iDRAC-Zugangsdaten nicht von OMIMSSC aufgezeichnet und als fehlgeschlagen markiert wird, obwohl der Job in iDRAC erfolgreich sein kann.

5. Geben Sie einen eindeutigen Jobnamen und eine Beschreibung für den Job ein und klicken Sie auf **Bereitstellen**.

   Um diesen Job zu verfolgen, ist standardmäßig die Option **Zur Jobliste wechseln** ausgewählt.

Bereitstellen der Betriebsvorlage für das modulare System

Sie können Modularsystem-Komponenten konfigurieren und die Firmwareversionen des modularen Systems aktualisieren, indem Sie die zugewiesene Betriebsvorlage bereitstellen.

ANMERKUNG: Wenn in einem Multi-Gehäuse-Management (MCM) das Hauptgehäuse mit **Weiterleiten an Mitgliedsgehäuse** konfiguriert ist und die Konfiguration und Aktualisierung von Hauptgehäuse und Mitgliedsgehäuse von OMIMSSC aus vorgenommen wird, werden die durch die Verteilung vorgenommenen Änderungen überschrieben.

1. Klicken Sie in OMIMSSC auf **Konfiguration und Bereitstellung** und klicken Sie auf **Modularsystemansicht**. Wählen Sie das modulare System aus, dem Sie die Vorlage zugewiesen haben, und klicken Sie dann auf **Betriebsvorlage bereitstellen**.
   Die Seite Betriebsvorlage **bereitstellen** wird angezeigt.
2. (Optional) Um alle Attribute, die in der ausgewählten Vorlage als Poolwerte markiert sind, in eine CSV-Datei zu exportieren, klicken Sie auf **Poolattribute exportieren**. Andernfalls fahren Sie mit Schritt 4 fort.
3. Wenn Sie die Poolwerte exportiert haben, geben Sie Werte für alle Attribute ein, die in der CSV-Datei als Poolwerte markiert sind, und speichern Sie die Datei. Wählen Sie im **Attributwertpool** diese Datei aus, um sie zu importieren.

   Das Format einer .CSV Datei ist `attribute-value-pool.csv`

   ANMERKUNG: Stellen Sie sicher, dass Sie eine .CSV-Datei auswählen, die alle richtigen Attribute enthält, und dass sich die CMC-IP- oder CMC-Zugangsdaten aufgrund der Vorlage nicht ändern, da der Job nach der Änderung der CMC-IP- oder CMC-Zugangsdaten nicht von OMIMSSC verfolgt wird.

4. Geben Sie einen eindeutigen Jobnamen und eine Beschreibung für den Job ein und klicken Sie auf **Bereitstellen**.

   ANMERKUNG: Es werden keine systemspezifischen Poolwertattribute für das modulare System unterstützt. Daher sind keine Poolwerte zum Exportieren vorhanden.

   Um diesen Job zu verfolgen, ist standardmäßig die Option **Zur Jobliste wechseln** ausgewählt.

Aufheben der Zuweisung der Betriebsvorlage

1. Führen Sie in OMIMSSC einen der folgenden Tasks aus:
   - Klicken Sie auf **Konfiguration und Bereitstellung** und klicken Sie auf **Serveransicht**.
   - Klicken Sie auf **Konfiguration und Bereitstellung** und klicken Sie auf **Modularsystemansicht**.

   Wählen Sie die Geräte aus und klicken Sie auf **Betriebsvorlage zuweisen und Kompatibilität ausführen**.

   Die Seite **Betriebsvorlage zuweisen und Kompatibilität ausführen** wird angezeigt.
2. Wählen Sie die Geräte aus und klicken Sie auf **Betriebsvorlage und Kompatibilität ausführen**.
   Die **Seite Betriebsvorlage und Kompatibilität ausführen** wird angezeigt.
3. Wählen Sie **Zuweisung aufheben** im Dropdown-Menü **Betriebsvorlage** und klicken Sie auf **Zuweisen**.
   Die Betriebsvorlage ist den ausgewählten Geräten nicht zugewiesen.

Betriebsvorlage löschen

Führen Sie zum Löschen einer Betriebsvorlage die folgenden Schritte durch:

Stellen Sie vor dem Löschen einer Betriebsvorlage Folgendes sicher:

- Die ausgewählte Betriebsvorlage ist keinem Server oder modularem System zugewiesen. Wenn sie einem Gerät zugewiesen ist, heben Sie die Zuweisung der Vorlage auf und löschen Sie die Vorlage.
- Es werden keine Jobs ausgeführt, die der Betriebsvorlage zugeordnet sind.
- Sie haben keine vordefinierte Betriebsvorlage ausgewählt, da Sie keine vordefinierte Vorlage löschen können.
- Die Schritte zum Löschen eines beliebigen Typs von Betriebsvorlage sind identisch.

Wählen Sie die Vorlage aus, das Sie löschen möchten, und klicken Sie auf **Löschen**. Um zu bestätigen, klicken Sie auf **Ja**.

16

Bereitstellen des Betriebssystem mittels OMIMSSC

Aktualisieren Sie vor der Bereitstellung des Windows-Betriebssystems auf den verwalteten Servern das WinPE-Image, erstellen Sie eine Tasksequenz, eine LC-Boot-Mediendatei und eine startfähige ISO-Datei für Tasksequenzmedien. Die Schritte variieren fürMECM- und SCVMM-Konsolenbenutzer. Weitere Informationen erhalten Sie im folgenden Abschnitt. Beachten Sie bei der Bereitstellung eines Betriebssystems, das kein Windows-Betriebssystem ist, die im Abschnitt Vorbereiten der Bereitstellung eines anderen Betriebssystems als Windows beschriebenen Punkte.

Themen:

Informationen zum WinPE-Image-Aktualisierung

Das Image der Windows-Vorinstallationsumgebung (WinPE) wird zum Bereitstellen des Betriebssystems verwendet. Verwenden Sie ein aktualisiertes WinPE-Image zum Bereitstellen des Betriebssystems, da das von MECM oder SCVMM verfügbare WinPE-Image möglicherweise nicht die neuesten Treiber enthält. Um ein WinPE-Image mit allen erforderlichen Treibern zu erstellen, aktualisieren Sie das Image mit dem Dell EMC OpenManage-Treiberpaket. Stellen Sie sicher, dass die relevanten, auf das Betriebssystem bezogenen Treiberpakete im Lifecycle Controller installiert sind.

1. Um ein WinPE-Image mit allen erforderlichen Treibern zu erstellen, aktualisieren Sie das Image mit dem Dell EMC OpenManage-Treiberpaket.
2. Stellen Sie sicher, dass die relevanten, auf das Betriebssystem bezogenen Treiberpakete im Lifecycle Controller installiert sind.

ANMERKUNG: Ändern Sie nicht den Dateinamen der Datei boot.wim.

Bereitstellen der WIM-Datei für MECM

Kopieren Sie die Datei `boot.wim` vom folgenden Speicherort `\\shareip\sms_sitecode\OSD\boot\x64\boot.wim`, und fügen Sie sie dann in einen Freigabeordner ein, auf den OMIMSSC zugreifen kann.
Zum Beispiel Speicherort des freigegebenen Pfades: `\\shareip\sharefolder\boot.wim`

Bereitstellen der WIM-Datei für SCVMM

Das WinPE-Basis-Image ist für das Injizieren von startkritischen Dell Treibern aus OpenManage Server-Treiberpaket erforderlich. Dieses Image wird durch die Installation von PXE-Servern in SCVMM erzeugt. Weitere Informationen zur Installation von PXE-Servern in SCVMM finden Sie in der Microsoft-Dokumentation.

1. Installieren und konfigurieren Sie die Windows Deployment Server-Rolle (WDS) auf einem Server und fügen Sie den PXE-Server dann zu SCVMM hinzu.

   Informationen zum Hinzufügen der WDS-Rolle auf einem Server und zum Hinzufügen eines PXE-Servers zu SCVMM finden Sie im Abschnitt Bereitstellen eines Hyper-V-Hosts oder -Clusters von Bare-Metal-Computern in der Microsoft-Dokumentation.
2. Kopieren Sie die Datei `boot.wim` vom PXE-Server an folgenden Speicherort:
   `C:\RemoteInstall\DCMgr\Boot\Windows\Images` und fügen Sie sie in einen Freigabeordner ein, auf den OMIMSSC zugreifen kann.
   Zum Beispiel Speicherort des freigegebenen Pfades: `\\shareip\sharefolder\boot.wim`

Der WDS-und PXE-Server ist nur für die Generierung des WinPE-basierten Boot.in-Images erforderlich und darf nicht in Bereitstellungsszenarien verwendet werden.

Extrahieren von Treibern aus OpenManage Server-Treiberpaket

Die Dell EMC OpenManage Server Driver Pack DVD ist ein öffentlich eingeführtes Paket von Dell EMC, das die Betriebssystemtreiber für alle Plattformen einrichtet. Ab der aktuellen Version unterstützt OMIMSC Administratoren bei der Erstellung des WinPE-Images unter Verwendung des OpenManage-Treiberpakets.

`To download OpenManage driver pack, launch` **https://www.dell.com/support**`/ -> Search for the keyword` **Dell EMC OpenMange server Driver Pack DVD** `and download the corresponding openManage server driver pack based on the supported platforms.`

1. Laden Sie das ISO als Laufwerk auf einem beliebigen lokalen Windows-Rechner.

   ANMERKUNG: Stellen Sie sicher, dass Sie die richtige WinPE-Version verwenden.
2. Verwenden Sie die Eingabeaufforderung und navigieren Sie zum Pfad `<MountedDrive>:\server_assistant\driver_tool\bin`.
3. Befehl ausführen `make_driver_dir.exe -i <MountedDrive> -d <ExtractedWinPEPath> -o <filter option> --extract`

   Nehmen wir an, das geladene Laufwerk befindet sich in F und der extrahierte Ausgabepfad `C:\om_server_diver_pack` verwendet folgende Beispiele zum Extrahieren von Treibern für alle unterstützten Plattformen:

   a. Zum Extrahieren von Windows 2016- und 2019-Treibern für alle unterstützten Plattformen `make_driver_dir.exe -i F:\ -d c:\om_server_driver_pack -o WINPE10 --extract`
   b. Zum Extrahieren von Windows 2012 R2-Treibern für alle unterstützten Plattformen `make_driver_dir.exe -i F:\ -d c:\om_server_driver_pack -o WINPE5 --extract`

ANMERKUNG: Entfernen Sie nach Abschluss der Extraktion die Treiber aus dem folgenden Verzeichnis `<ExtractedWinPEPath>\WINPE5\chipset\9D99N\SBDrv`.

Aktualisieren eines WinPE-Image

Jedem WinPE-Aktualisierungsjob wird ein eindeutiger Auftragsname zugewiesen.

1. Wählen Sie in OMIMSSC die Option **WinPE-Aktualisierung** aus.
   Die Seite **WinPE-Aktualisierung** wird angezeigt.
2. Geben Sie unter **Image-Quelle** für **Nutzerdefinierter WinPE-Image-Pfad** den WinPE-Image-Pfad zusammen mit dem Dateinamen ein, unter dem das Image vorhanden ist.
   Zum Beispiel `\\Shareip\sharefolder\WIM\boot.wim`.
3. Geben Sie unter **OM-Treiber-DVD-Pfad** für **OM-Treiber-Pfad** den Speicherort der Dell EMC OpenManage-Treiber ein.
   Beispiel: `\\Shareip\sharefolder\<extracted share folder>`
4. Geben Sie unter **Ausgabedatei** für **ISO- oder WIM-Dateiname** einen Namen für die Datei zusammen mit dem gemeinsamen Dateipfad ein, in dem das WinPE-Abbild erzeugt wird.

   Geben Sie einen der Ausgabedateitypen ein:

   - WIM-Datei für MECM
   - ISO-Datei für SCVMM
5. Geben Sie unter **Zugangsdatenprofil** für **Zugangsdatenprofil** die Zugangsdaten ein, die Zugriff auf den Freigabeordner haben, in dem das WinPE-Image gespeichert ist.
6. (Optional) Um die Job-Liste anzuzeigen, wählen Sie **Zur Job-Liste wechseln** aus.
   - WIM-Datei für MECM
   - ISO-Datei für SCVMM
   - WIM-Datei für MECM
   - ISO-Datei für SCVMM

   Daraufhin wird den einzelnen Updates für die Windows Preinstallation Environment (WinPE) ein eindeutiger Job-Name zugewiesen.
7. Klicken Sie auf **Aktualisieren**.
   Das WinPE-Image mit dem Dateinamen, der im vorherigen Schritt angegeben wurde, wird unter \\Shareip\sharefolder\WIM erstellt.

Vorbereiten der Betriebssystembereitstellung auf der MECM-Konsole

Erstellen Sie vor der Bereitstellung des Betriebssystems auf verwalteten Servern, die mit OMIMSSC in der MECM-Konsole ermittelt wurden, eine für Dell EMC spezifische oder eine nutzerdefinierte Tasksequenz, eine LC-Startmediendatei und eine startfähige ISO-Datei für Tasksequenzmedien.

Aufgabenreihenfolge – MECM

Die Tasksequenz ist eine Reihe von Befehlen, die zum Bereitstellen des Betriebssystems auf dem verwalteten System mithilfe von MECM verwendet werden.

Bevor Sie eine Betriebsvorlage erstellen, empfiehlt Dell EMC, dass Sie die folgenden Voraussetzungen erfüllen.

1. Stellen Sie im Configuration Manager sicher, dass das System ermittelt wurde und unter **Bestand und Übereinstimmung** > **Geräte-Sammlungen** > **Alle Dell Lifecycle Controller-Server** vorhanden ist. Weitere Informationen finden Sie unter Ermittlung von Servern.
2. Installieren Sie die neueste BIOS-Version auf dem System.
3. Installieren Sie die neueste Version des Lifecycle Controllers auf dem System.
4. Installieren Sie die neueste Version der iDRAC-Firmware auf dem System.

ANMERKUNG: Starten Sie die Configuration Manager-Konsole immer mit Administratorrechten.

Arten von Tasksequenzen

Es gibt zwei Möglichkeiten, eine Tasksequenz zu erstellen:

- Sie können eine Dell-spezifische Tasksequenz mit der OMIMSSC-Bereitstellungsvorlage erstellen.
- Sie können eine benutzerdefinierte Tasksequenz erstellen.

Die Tasksequenz geht zum nächsten Tasksequenz-Schritt weiter, unabhängig davon, ob der Befehl erfolgreich war oder fehlgeschlagen ist.

Erstellen einer für Dell spezifischen Tasksequenz

So erstellen Sie eine für Dell spezifische Tasksequenz mit der Option **OMIMSSC-Serverbereitstellungsvorlage** in MECM:

1. Starten Sie den Configuration Manager.
   Es wird der Configuration Managerkonsolen-Bildschirm angezeigt.
2. Wählen Sie im linken Bereich **Software-Bibliothek** > **Übersicht** > **Betriebssysteme** > **Tasksequenz** aus.
3. Klicken Sie mit der rechten Maustaste auf **Tasksequenzen** und klicken Sie dann auf **OMIMSSC-Serverbereitstellung** > **OMIMSSC-Serverbereitstellungsvorlage erstellen**.
   Der **OMIMSSC-Serverbereitstellungs-Tasksequenz-Assistent** wird angezeigt.
4. Geben Sie den Namen der Tasksequenz in das Feld **Name der Tasksequenz** ein.
5. Wählen Sie das zu verwendende Startabbild aus der Dropdown-Liste aus.

   ANMERKUNG: Es wird empfohlen, dass Sie das von Ihnen erstellte nutzerdefinierte Dell-Startabbild verwenden.

6. Wählen Sie unter **Betriebssysteminstallation** den Betriebssysteminstallationstyp aus. Dies sind die Optionen:
   - **BS WIM-Abbild verwenden**
   - **BS-Installation per Skript**
7. Wählen Sie ein Betriebssystempaket im Drop-Down-Menü **Zu verwendendes Betriebssystempaket** aus.
8. Wenn Sie über ein Paket mit **unattend.xml** verfügen, dann wählen Sie es im Menü **Paket mit unattend.xml Info** aus. Wählen Sie anderenfalls **<jetzt nicht auswählen>** aus.
9. Klicken Sie auf **Erstellen**.
   Das Fenster **Tasksequenz erstellt** wird mit dem Namen der von Ihnen erstellten Tasksequenz angezeigt.
10. Klicken Sie im angezeigten Feld für die Bestätigungsmeldung auf **Schließen**.

Erstellen Sie eine nutzerdefinierte Tasksequenz.

1. Starten Sie den Configuration Manager.
   Es wird die Configuration Managerkonsole angezeigt.
2. Wählen Sie im linken Bereich die Option **Software-Bibliothek** > **Übersicht** > **Betriebssysteme** > **Tasksequenzen** aus.
3. Klicken Sie mit der rechten Maustaste auf **Tasksequenzen** und dann auf **Tasksequenz erstellen**.
   Daraufhin wird der **Assistent zum Erstellen einer Tasksequenz** angezeigt.
4. Wählen Sie **Neue nutzerdefinierte Tasksequenz erstellen** aus und klicken Sie dann auf **Weiter.**
5. Geben Sie einen Namen für die Tasksequenz in das Textfeld **Tasksequenzname** ein.
6. Suchen Sie das von Ihnen erstellte Dell-Startabbild heraus und klicken Sie auf **Weiter**.
   Daraufhin wird der Bildschirm **Einstellungen bestätigen** angezeigt.
7. Überprüfen Sie die Einstellungen, und klicken Sie dann auf **Weiter**.
8. Klicken Sie im angezeigten Feld für die Bestätigungsmeldung auf **Schließen**.

Bearbeiten einer Tasksequenz

ANMERKUNG: Beim Bearbeiten der Tasksequenz auf MECM 2016 und 2019 werden in den Referenzmeldungen zu fehlenden Objekten das Paket **Setup-Fenster und ConfigMgr** nicht aufgeführt. Fügen Sie das Paket hinzu und speichern Sie dann die Tasksequenz.

1. Starten Sie den Configuration Manager.
   Es wird der Bildschirm Configuration Manager angezeigt.
2. Wählen Sie im linken Bereich die Option **Software-Bibliothek** > **Betriebssysteme** > **Task-Sequenzen**.
3. Klicken Sie mit der rechten Maustaste auf die Tasksequenz, die Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.
   Daraufhin wird das Fenster **Tasksequenz-Editor** angezeigt.
4. Klicken Sie auf **Hinzufügen** > **Dell Deployment** > **Treiber von Dell Lifecycle-Controller anwenden.**
   Die nutzerdefinierte Aktion für Ihre Dell Serverbereitstellung wird geladen. Sie können jetzt Änderungen an der Tasksequenz vornehmen.

   ANMERKUNG: Wenn Sie eine Tasksequenz zum ersten Mal bearbeiten, wird die Fehlermeldung **Windows und Configuration Manager-Setup** angezeigt. Um den Fehler zu beheben, erstellen Sie das Configuration Manager Client-Aktualisierungspaket und wählen Sie es aus. Weitere Informationen zur Paketerstellung finden Sie in der Configuration Manager-Dokumentation unter **technet.microsoft.com**.

   ANMERKUNG: Bei der Bearbeitung einer Tasksequenz in MECM 2016 und 2019 listen die Nachrichten für fehlende Objektverweise das Paket Windows und ConfigMgr einrichten nicht auf. Daher müssen Sie das Paket hinzufügen und dann die Tasksequenz speichern.

Einstellen eines freigegebenen Standard-Speicherorts für den Lifecycle Controller-Startdatenträger

So legen Sie einen freigegebenen Standard-Speicherort für den Lifecycle Controller-Startdatenträger fest:

1. Wählen Sie im **Configuration Manager** die Option **Verwaltung** > **Standortverwaltung** > **Standorte**
2. Klicken Sie mit der rechten Maustaste auf **<Name des Standortservers>**, wählen Sie **Standortkomponenten konfigurieren** aus und wählen Sie **Out-of-Band-Management** aus.
   Das Fenster **Bandexterne Verwaltungskomponenten – Eigenschaften** wird angezeigt.
3. Klicken Sie auf die Registerkarte **Lifecycle Controller**.
4. Klicken Sie unter **Standardfreigabeort für Startdatenträger des nutzerdefinierten Lifecycle Controllers** auf **Modifizieren**, um den Standardfreigabeort des nutzerdefinierten Lifecycle Controller-Startdatenträgers zu modifizieren.
5. Geben Sie im Fenster **Freigabeinformationen ändern** einen neuen Freigabenamen und Freigabepfad ein.
6. Klicken Sie auf **OK**.

Tasksequenz-Datenträger erstellen (Startfähiges ISO-Image)

1. Klicken Sie im Configuration Manager unter **Softwarebibliothek** mit der rechten Maustaste auf **Tasksequenzen** und wählen Sie **Tasksequenzmedien erstellen** aus.

   ANMERKUNG: Stellen Sie sicher, dass Sie das Boot Image über alle Verteilungspunkte hinweg verwalten und aktualisieren, bevor Sie diesen Assistenten starten.

   ANMERKUNG: OMIMSSC bietet keine Unterstützung für das Standalone-Media-Verfahren zum Erstellen eines Tasksequenz-Datenträgers.

2. Wählen Sie im **Tasksequenz-Datenträgerassistenten** die Option **Startfähige Datenträger** aus, aktivieren Sie die Option **Unbeaufsichtigte Bereitstellung des Betriebssystems zulassen** und klicken Sie auf **Weiter**.
3. Wählen Sie **CD/DVD Set** aus, klicken Sie auf **Durchsuchen** und wählen Sie den Speicherort für das ISO-Image aus.
4. Klicken Sie auf **Weiter**.
5. Heben Sie die Markierung des Kontrollkästchens **Datenträger mit einem Kennwort schützen** auf und klicken Sie auf **Weiter**.
6. Suchen Sie nach dem Start-Image **PowerEdge Server Deployment Boot Image** und wählen Sie es aus.

   ANMERKUNG: Verwenden Sie nur das mit DTK erstellte Start-Image.

7. Wählen Sie aus dem Drop-Down-Menü den Verteilungspunkt aus und wählen Sie das Kontrollkästchen**Verteilungspunkte untergeordneter Sites anzeigen**.
8. Klicken Sie auf **Weiter**.
   Der **Zusammenfassung**sbildschirm mit den Informationen zum Tasksequenz-Datenträger wird angezeigt.
9. Klicken Sie auf **Weiter**.
   Der Fortschrittsbalken wird angezeigt.
10. Schließen Sie den Assistenten nach Abschluss der Erstellung des Images.

Vorbereiten der Bereitstellung eines Betriebssystems, das kein Windows ist

Stellen Sie sicher, dass Sie die folgenden Punkte für die Bereitstellung von Nicht-Windows-Betriebssystemen auf verwalteten Systemen berücksichtigen:

- Die ISO-Datei ist entweder in der NFS-Datei (Network File System Version) oder in der CIFS-Freigabe (Common Internet File System) mit Lese- und Schreibzugriff verfügbar.
- Bestätigen Sie, dass das virtuelle Laufwerk auf dem verwalteten System verfügbar ist.
- Nach der Bereitstellung des ESXi-Betriebssystems wird der Server in die Sammlung **Managed Lifecycle Controller (ESXi)** in MECM verschoben.
- Nach der Bereitstellung eines beliebigen Betriebssystems, das kein Windows-Betriebssystem ist, werden die Server in die **Standard-Host-Aktualisierungsgruppe (nicht Windows)** verschoben.
- Es wird empfohlen, dass der Netzwerkadapter an der Netzwerkschnittstelle am Server angeschlossen ist, auf dem das Betriebssystem bereitgestellt wird.

17

Bereitstellen von Geräten mithilfe von OMIMSSC

Dieses Kapitel enthält allgemeine Informationen zum Ermitteln, Bereitstellen des Betriebssystems, zum Erstellen von Clustern und zum Verwalten von Dell EMC Geräten mit OMIMSSC.

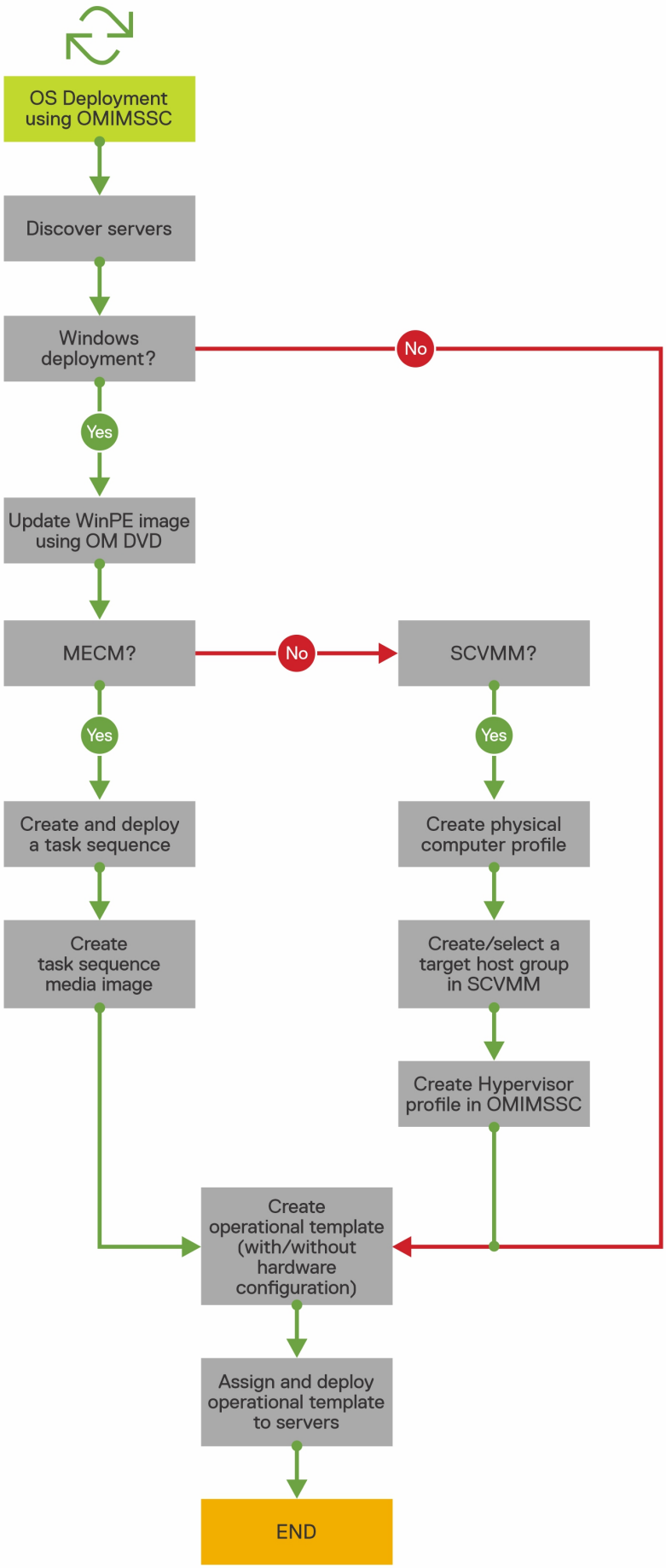
Themen:

Workflow für Bereitstellungsszenarien

Verwenden Sie OMIMSSC zum Bereitstellen von Windows- und Nicht-Windows-Betriebssystemen in MECM- oder SCVMM-Umgebungen mit Betriebsvorlage.

ANMERKUNG: Stellen Sie sicher, dass Sie die Firmwareversionen der Geräte auf die neuesten Versionen aktualisieren, die unter oder `downloads.dell.com` verfügbar sind, bevor Sie das Betriebssystem bereitstellen.

Hier ist eine bildliche Darstellung der Anwendungsfälle für die Betriebssystembereitstellung in OMIMSSC.


OS Deployment using OMIMSSC
Discover servers
Windows deployment?
No
Yes
Update WinPE image using OM DVD
MECM?
No
SCVMM?
Yes
Yes
Create and deploy a task sequence
Create physical computer profile
Create task sequence media image
Create/select a target host group in SCVMM
Create Hypervisor profile in OMIMSSC
Create operational template (with/without hardware configuration)
Assign and deploy operational template to servers
END

Bereitstellen des Windows-Betriebssystems mithilfe der OMIMSSC-Konsolenerweiterung für MECM

Führen Sie die folgenden Schritte aus, um das Windows-Betriebssystem über die MECM-Konsole mit OMIMSSC bereitzustellen:

ANMERKUNG: Stellen Sie vor der Bereitstellung des Betriebssystems auf einem Hostserver sicher, dass in MECM der Status **Client** des Servers **Nein** lautet.

1. Laden Sie das neueste Dell EMC OpenManage server-Treiberpaket herunter und erstellen Sie ein WIM-Startabbild für die Windows-Vorinstallationsumgebung (WinPE). Weitere Informationen dazu finden Sie unter WinPE-Aktualisierung.
2. Importieren Sie dieses .WIN-Abbild in die MECM-Konsole und erstellen Sie ein Startabbild in MECM. Weitere Informationen finden Sie in der *Microsoft-Dokumentation*.
3. Erstellen Sie eine Tasksequenz über MECM. Weitere Informationen finden Sie unter Erstellen einer Tasksequenz.
4. Erstellen Sie ein Tasksequenz-Datenträger-Image in MECM. Weitere Informationen finden Sie in der *Microsoft-Dokumentation*.

   ANMERKUNG: Um die unbeaufsichtigte Betriebssystembereitstellung beim Erstellen von Tasksequenzmedien zu aktivieren, aktivieren Sie unter **Datenträgertyp auswählen** die Option **Unbeaufsichtigte Bereitstellung des Betriebssystems zulassen**.

5. Ermitteln Sie den Referenzserver auf der Seite **Ermitteln**. Weitere Informationen finden Sie unter Ermitteln von Servern mithilfe der manuellen Ermittlung.
6. Erstellen Sie eine Betriebsvorlage, indem Sie alle Details des ermittelten Servers erfassen. Weitere Informationen finden Sie unter Erstellen von Betriebsvorlagen von Referenzservern.
7. Weisen Sie auf verwalteten Geräten eine Betriebsvorlage zu und überprüfen Sie die Kompatibilität der Vorlage. Weitere Informationen finden Sie unter Zuweisen von Betriebsvorlagen und Ausführen der Kompatibilität von Betriebsvorlagen.
8. Stellen Sie eine Betriebsvorlage bereit, um die Gerätevorlage kompatibel zu machen. Weitere Informationen finden Sie unter Bereitstellen einer Betriebsvorlage.
9. Zeigen Sie den Jobstatus für die Betriebssystembereitstellung auf der Seite **Job- und Protokollcenter** an. Weitere Informationen finden Sie unter Job- und Protokollcenter starten.

Bereitstellen des Hypervisor-Betriebssystems mit der OMIMSSC-Konsolenerweiterung für SCVMM

Die verschiedenen Szenarien für die Hypervisor-Bereitstellung lauten wie folgt:

Tabelle 11. Hypervisor-Bereitstellungsszenarien

Zustand	Aktion
Wenn Sie die neuesten werkseitigen Treiber benötigen.	Aktivieren Sie beim Erstellen eines Hypervisor-Profils die LC-Treiberinjektion (Lifecycle Controller).
Wenn Sie die vorhandene Hardwarekonfiguration beibehalten möchten.	Deaktivieren Sie beim Erstellen der Betriebsvorlage das Kontrollkästchen für alle Komponenten, für die keine Änderungen erforderlich sind.

Führen Sie die folgenden Schritte aus, um das Windows-Betriebssystem über den Hypervisor über die SCVMM-Konsole mit OMIMSSC bereitzustellen:

1. Laden Sie das neueste Dell EMC OpenManage-Treiberpaket herunter und erstellen Sie ein ISO-Image für die Windows-Vorinstallationsumgebung (WinPE). Weitere Informationen dazu finden Sie im Abschnitt WinPE-Aktualisierung.
2. Erstellen Sie ein physisches Computerprofil und eine Hostgruppe in SCVMM. Weitere Informationen finden Sie in der SCVMM-Dokumentation.
3. Erstellen Sie in der OMIMSSC-Konsolenerweiterung für SCVMM ein Hypervisor-Profil. Weitere Informationen finden Sie unter Erstellen eines Hypervisor-Profils.
4. Ermitteln Sie den Referenzserver auf der Seite Ermitteln. Weitere Informationen finden Sie unter Ermitteln von Servern mithilfe der manuellen Ermittlung.
5. Erstellen Sie eine Betriebsvorlage, indem Sie alle Details des ermittelten Servers erfassen. Weitere Informationen finden Sie unter Erstellen von Betriebsvorlagen von Referenzservern.

6. Weisen Sie auf verwalteten Geräten eine Betriebsvorlage zu und überprüfen Sie die Kompatibilität der Vorlage. Weitere Informationen finden Sie unter Zuweisen von Betriebsvorlagen und Ausführen der Kompatibilität von Betriebsvorlagen.
7. Stellen Sie eine Betriebsvorlage bereit, um die Gerätevorlage kompatibel zu machen. Weitere Informationen finden Sie unter Bereitstellen einer Betriebsvorlage.
8. Zeigen Sie den Jobstatus für die Betriebssystembereitstellung auf der Seite Job- und Protokollcenter an. Weitere Informationen finden Sie unter Job- und Protokollcenter starten.

Erneutes Bereitstellen von Windows-Betriebssystemen unter Verwendung von OMIMSSC

Führen Sie die folgenden Schritte aus, um das Windows-Betriebssystem auf einem Server mithilfe der OMIMSSC-Konsolenerweiterung für MECM oder der OMIMSSC-Konsolenerweiterung für SCVMM erneut bereitzustellen.

1. Löschen Sie den Server von der Microsoft-Konsole. Weitere Informationen finden Sie in der Microsoft-Dokumentation.
2. Ermitteln Sie den Server erneut oder synchronisieren Sie OMIMSSC mit der registrierten Microsoft-Konsole. Der Server wird in OMIMSSC als nicht zugewiesener Server hinzugefügt. Weitere Informationen zur Ermittlung finden Sie unter Ermitteln von Servern mithilfe der manuellen Ermittlung. Weitere Informationen zur Synchronisierung finden Sie unter Synchronisieren mit der registrierten Microsoft-Konsole.
3. Erstellen Sie eine Betriebsvorlage, indem Sie alle Details des ermittelten Servers erfassen. Weitere Informationen finden Sie unter Erstellen von Betriebsvorlagen von Referenzservern.
4. Weisen Sie auf verwalteten Geräten eine Betriebsvorlage zu und überprüfen Sie die Kompatibilität der Vorlage. Weitere Informationen finden Sie unter Zuweisen von Betriebsvorlagen und Ausführen der Kompatibilität von Betriebsvorlagen.
5. Stellen Sie eine Betriebsvorlage bereit, um die Gerätevorlage kompatibel zu machen. Weitere Informationen finden Sie unter Bereitstellen einer Betriebsvorlage.
6. Zeigen Sie den Jobstatus für die Betriebssystembereitstellung auf der Seite **Job- und Protokollcenter** an. Weitere Informationen finden Sie unter Job- und Protokollcenter starten.

Bereitstellen eines anderen Betriebssystems als Windows mit OMIMSSC-Konsolenerweiterungen

Führen Sie die folgenden Schritte aus, um ein Nicht-Windows-Betriebssystem mit OMIMSSC bereitzustellen:

ANMERKUNG: Die Schritte zur Bereitstellung von anderen Betriebssystemen als Windows über OMIMSSC sind in beiden Microsoft-Konsolen gleich.

1. Ermitteln Sie den Referenzserver auf der Seite **Ermitteln**. Weitere Informationen finden Sie unter Ermitteln von Servern mithilfe der manuellen Ermittlung.
2. Erstellen Sie eine Betriebsvorlage, indem Sie alle Details des ermittelten Servers erfassen. Weitere Informationen finden Sie unter Erstellen von Betriebsvorlagen von Referenzservern.
3. Weisen Sie auf verwalteten Geräten eine Betriebsvorlage zu und überprüfen Sie die Kompatibilität der Vorlage. Weitere Informationen finden Sie unter Zuweisen von Betriebsvorlagen und Ausführen der Kompatibilität von Betriebsvorlagen.
4. Stellen Sie eine Betriebsvorlage bereit, um die Gerätevorlage kompatibel zu machen. Weitere Informationen finden Sie unter Bereitstellen einer Betriebsvorlage.

   ANMERKUNG: Wenn die DHCP-Suche während der Bereitstellung fehlschlägt, kommt es zu einer Zeitüberschreitung für den Server, und der Server wird nicht in die Sammlung **Verwaltete Lifecycle Controller Lifecycle Controller (ESXi)** in MECM verschoben.

Erstellen von Windows Server HCI-Clustern mithilfe von vordefinierten Betriebsvorlage

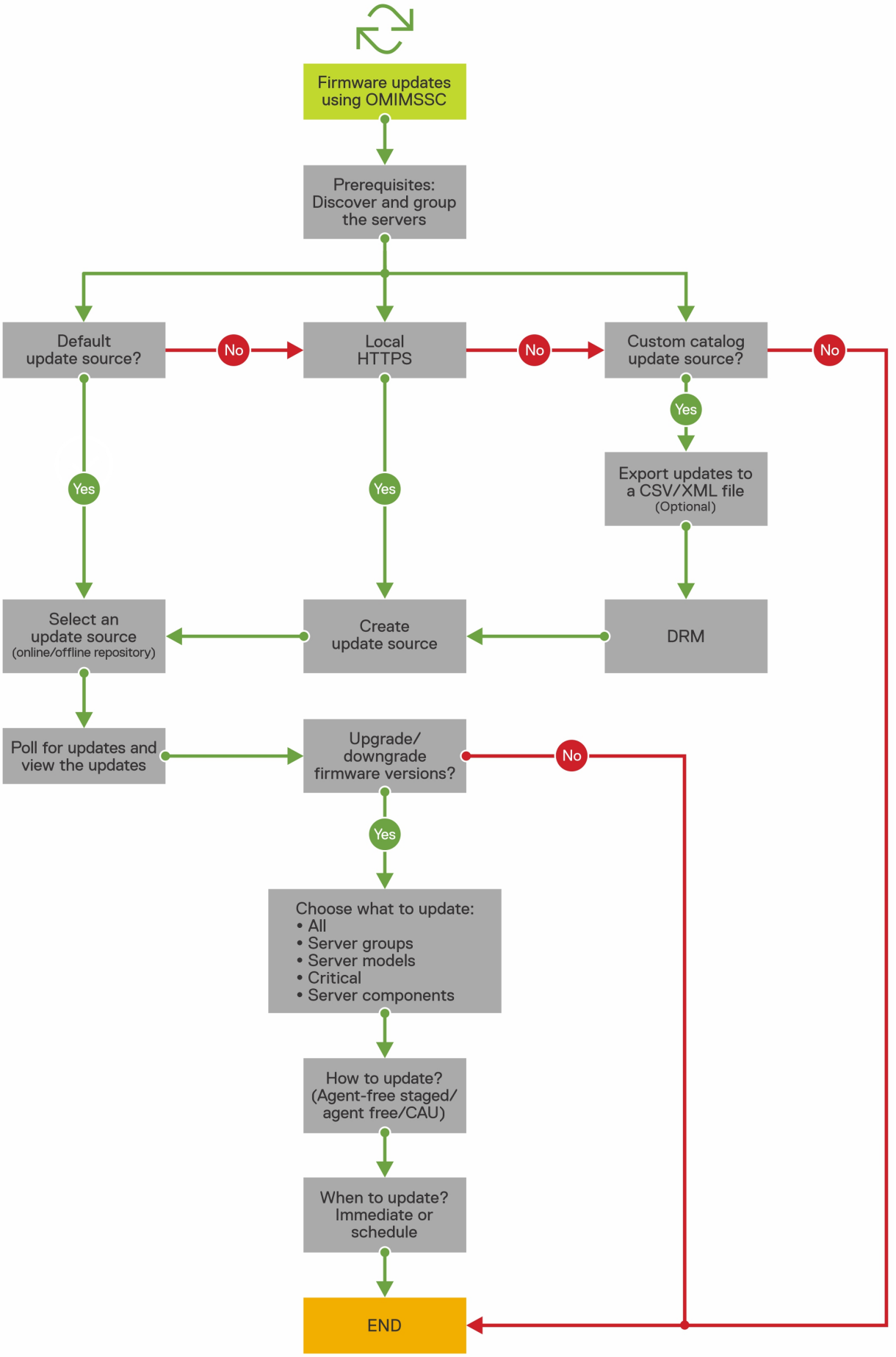
Führen Sie die folgenden Schritte aus, um Cluster mithilfe von OMIMSSC zu erstellen:

1. Ermitteln Sie den Referenzserver auf der Seite **Ermitteln**. Weitere Informationen finden Sie unter Ermitteln von Servern mithilfe der manuellen Ermittlung.
2. Bearbeiten Sie die vordefinierte Betriebsvorlage. Weitere Informationen finden Sie unter Betriebsvorlage ändern.

3. Erstellen Sie einen logischen Switch. Weitere Informationen finden Sie unter Logischen Switch erstellen.
4. Erstellen Sie ein Windows Server HCI-Cluster. Weitere Informationen finden Sie unter Erstellen von Windows Server-HCI-Clustern.

Aktualisieren der Firmware von Servern und MX7000-Geräten

Hier ist eine bildliche Darstellung des Firmwareaktualisierung-Workflows.


Firmware updates using OMIMSSC
Prerequisites: Discover and group the servers
Default update source?
No
Local HTTPS
No
Custom catalog update source?
No
Yes
Export updates to a CSV/XML file (Optional)
Yes
Yes
Select an update source (online/offline repository)
Create update source
DRM
Poll for updates and view the updates
Upgrade/ downgrade firmware versions?
No
Yes
Choose what to update:
• All
• Server groups
• Server models
• Critical
• Server components
How to update? (Agent-free staged/ agent free/CAU)
When to update? Immediate or schedule
END

Sie können die ausgewählten Geräte mithilfe von Online-Quellen oder lokalen Quellen (DRM/HTTPS) aktualisieren.

1. Erstellen oder wählen Sie eine Standardaktualisierungsquelle. Weitere Informationen zur Aktualisierungsquelle finden Sie unter Aktualisierungsquelle.

   ANMERKUNG: Stellen Sie sicher, dass Sie die Aktualisierungsquelle mit dem neuesten Katalog aktualisieren, indem Sie die Abruf- und Benachrichtigungsfunktion verwenden. Weitere Informationen zu Abfragen und Benachrichtigungen finden Sie unter Abfragen und Benachrichtigungen.

   Wenn Sie Windows Server HCI-Cluster aktualisieren, wählen Sie eine vordefinierte Aktualisierungsquelle aus, die für Windows Server HCI-Cluster spezifisch ist. Diese Aktualisierungsquellen werden nur auf der Seite **Wartungscenter** angezeigt.

   Wenn Sie MX7000-Geräte aktualisieren, wählen Sie eine vordefinierte Aktualisierungsquelle aus, die für modulare Systeme spezifisch ist. Diese Aktualisierungsquellen werden nur auf der Seite **Wartungscenter** angezeigt.

2. Erstellen oder wählen Sie die Standardaktualisierungsgruppen. Weitere Informationen über Aktualisierungsgruppen finden Sie unter Aktualisierungsgruppen.
3. Ermitteln oder synchronisieren Sie die Geräte mit einer registrierten Microsoft-Konsole und stellen Sie sicher, dass der Gerätebestand auf dem neuesten Stand ist. Weitere Informationen zur Ermittlung und Synchronisierung finden Sie unter Geräteermittlung und -synchronisierung. Weitere Informationen zum Server-Inventar finden Sie unter Starten der Serveransicht.
4. Aktualisieren Sie das Gerät mithilfe einer der folgenden Optionen:
   - Wählen Sie die erforderlichen Geräte aus und klicken Sie auf **Aktualisierung ausführen**. Weitere Informationen finden Sie unter Aktualisieren oder Zurückstufen von Firmwareversionen mithilfe der Methode "Aktualisierung ausführen".

     ANMERKUNG: Aktivieren Sie zum Zurückstufen der Firmware der Gerätekomponenten das Kontrollkästchen **Herabstufen zulassen**. Wenn diese Option nicht ausgewählt ist, gibt es keine Aktion für die Komponente, für die ein Firmware-Zurückstufen erforderlich ist.
   - Wählen Sie die Firmwareaktualisierungskomponente in der Betriebsvorlage aus und stellen Sie diese Vorlage bereit. Weitere Informationen zur Betriebsvorlage finden Sie unter Betriebsvorlage.

Konfigurieren von ersetzten Komponenten

Informationen zum Anpassen der Firmware-Version oder der Konfigurationseinstellungen der ersetzten Komponente entsprechend der alten Komponente finden Sie unter Anwenden von Firmware- und Konfigurationseinstellungen.

Exportieren und Importieren des Serverprofils

Exportieren Sie das Serverprofil einer bestimmten Instanz und importieren Sie anschließend das Profil, um den Server wiederherzustellen:

1. Erstellen Sie einen Schutz-Vault. Weitere Informationen zum Erstellen eines Schutz-Vaults finden Sie unter Erstellen eines Schutz-Vaults.
2. Exportieren Sie ein Serverprofil. Weitere Informationen zum Exportieren eines Serverprofils finden Sie unter Serverprofil exportieren.
3. Importieren Sie das Serverprofil auf den Server, von dem es exportiert wurde. Weitere Informationen zum Importieren eines Serverprofils finden Sie unter Serverprofil importieren.

   ANMERKUNG: Sie können das Serverprofil einschließlich der RAID-Konfiguration nur importieren, wenn die RAID-Konfiguration in das Profil exportiert wird.

Die Funktion zum Exportieren und Importieren von Server-Profilen wird auf

- Server mit iDRAC-Version 4.40.00.00 und höher nicht unterstützt.
- iDRAC 9-basierte PowerEdge-Server.

  Verwenden Sie die Betriebsvorlage, wenn Sie die Server-Hardwarekonfiguration, die Firmware und die Betriebssystem-Baseline sichern möchten.

18

Aktualisieren von Firmware OMIMSSC

Halten Sie Dell EMC-Geräte auf dem neuesten Stand, indem Sie mit OMIMSSC eine Aktualisierung auf die neueste Firmware durchführen, um Sicherheitsoptionen zu verwenden sowie Korrekturen und Verbesserungen vorzunehmen. Aktualisieren Sie die Firmware der Geräte mithilfe von Dell EMC-Aktualisierungs-Repositorys.

Das Aktualisieren der Firmware wird nur auf hardwarekompatiblen Geräten unterstützt. Für die Verwendung der in OMIMSSC verfügbaren Funktionen auf den verwalteten Geräten müssen die verwalteten Geräte über die mindestens erforderlichen Firmware-Versionen von iDRAC, Lifecycle Controller (LC) und BIOS verfügen. Geräte mit den erforderlichen Firmware-Versionen sind hardwarekompatibel.

Themen:

Infos zu Aktualisierungsgruppen

Aktualisierungsgruppen sind eine Gruppe von Geräten, für die eine ähnliche Aktualisierungsverwaltung erforderlich ist. In OMIMSSC werden zwei Arten von Aktualisierungsgruppen unterstützt:

- Vordefinierte Aktualisierungsgruppen: Sie können vordefinierte Aktualisierungsgruppen nicht manuell erstellen, ändern oder löschen.
- Nutzerdefinierte Aktualisierungsgruppen: In diesen Gruppen können Sie Geräte erstellen und ändern.

ANMERKUNG: Alle in SCVMM vorhandene Servergruppen werden in OMIMSSC aufgelistet. Die Liste der Server in OMIMSSC ist jedoch nicht benutzerspezifisch. Stellen Sie daher sicher, dass Sie Zugriff auf diese Geräte haben.

Vordefinierte Aktualisierungsgruppen

Nach dem Ermitteln eines Geräts wird das ermittelte Gerät einer der folgenden vordefinierten Gruppen hinzugefügt.

- **Standardhostgruppen**: Diese Gruppe besteht aus Servern, die mit dem Windows-Betriebssystem bereitgestellt oder mit einer registrierten Microsoft-Konsole synchronisiert werden.
- **Nicht zugewiesene Standardgruppen**: Diese Gruppe besteht aus ermittelten nicht zugewiesenen oder Bare-Metal-Servern.
- **Nicht-Windows-Host-Standardgruppen**: Diese Gruppe besteht aus Servern, die mit Nicht-Windows-Betriebssystemen bereitgestellt werden.
- **Gehäuse-Aktualisierungsgruppen**: Diese Gruppe besteht aus modularen Servern und Gehäusen oder modularen Systemen. Server der 12. Generation und höher werden zusammen mit ihren Gehäuseinformationen ermittelt. Standardmäßig wird eine Gruppe mit dem folgenden Namensformat erstellt: `Chassis-Service-tag-of-Chassis-Group-` Zum Beispiel `Chassis-GJDC4BS-Group`. Wenn ein modularer Server aus einer Cluster-Aktualisierungsgruppe gelöscht wird, wird der Server zusammen mit seinen CMC-Informationen der Gehäuse-Aktualisierungsgruppe hinzugefügt. Auch wenn keine modularen Server in der entsprechenden Gehäuse-Aktualisierungsgruppe vorhanden sind, bleibt die Gehäuse-Aktualisierungsgruppe weiterhin bestehen, da sich alle modularen Server im Gehäuse in einer Cluster-Aktualisierungsgruppe befinden. Es werden jedoch nur die CMC-Informationen angezeigt.
- **Cluster-Aktualisierungsgruppen**: Diese Gruppe besteht aus **Windows Server-Failover-Clustern**. Wenn ein modularer Server der 12. Generation und später Teil eines Clusters ist, werden die CMC-Informationen ebenfalls in der Bestandsliste auf der Seite **Wartungscenter** hinzugefügt.

Nutzerdefinierte Aktualisierungsgruppen

Erstellen Sie nutzerdefinierte Aktualisierungsgruppen des Typs **Allgemeine Aktualisierungsgruppen**, indem Sie die ermittelten Geräte zu Gruppen hinzufügen, für die eine ähnliche Verwaltung erforderlich ist. Sie können ein Gerät jedoch nur zu einer nutzerdefinierten

Aktualisierungsgruppe aus **nicht zugewiesenen Standardaktualisierungsgruppen** und **Standard-Hostaktualisierungsgruppen** hinzufügen. Um die Server in einer nutzerdefinierten Aktualisierungsgruppe hinzuzufügen, suchen Sie das entsprechende Gerät mithilfe der Service-Tag-Nummer. Nachdem Sie ein Gerät zu einer nutzerdefinierten Aktualisierungsgruppe hinzugefügt haben, wird das Gerät aus der vordefinierten Aktualisierungsgruppe entfernt und ist nur in der nutzerdefinierten Aktualisierungsgruppe verfügbar.

Anzeigen von Updategruppen

So zeigen Sie Aktualisierungsgruppen an:

1. Klicken Sie in **OMIMSSC** auf **Wartungscenter** und dann auf **Wartungseinstellungen**.
2. Klicken Sie bei den **Wartungseinstellungen** auf **Aktualisierungsgruppen**.
   Alle nutzerdefinierten Gruppen, die erstellt werden, werden mit Name, Gruppentyp und Anzahl der Server in der Gruppe angezeigt.

Erstellen von nutzerdefinierten Updategruppen

1. Klicken Sie in der OMIMSSC-Konsole auf **Wartungscenter** und dann auf **Wartungseinstellungen**.
2. Klicken Sie bei den **Wartungseinstellungen** auf **Aktualisierungsgruppen** und dann auf **Erstellen**.
   Die Seite **Firmwareaktualisierungsgruppe** wird angezeigt.
3. Geben Sie einen Gruppennamen und eine Beschreibung an und wählen Sie den Typ der zu erstellenden Aktualisierungsgruppe aus.

   In nutzerdefinierten Aktualisierungsgruppen können nur Server der folgenden Aktualisierungsgruppentypen enthalten sein:
   - Allgemeine Aktualisierungsgruppe – Diese Gruppe besteht aus Servern aus standardmäßigen, nicht zugewiesenen Aktualisierungsgruppen und standardmäßigen Host-Aktualisierungsgruppen.
   - Host-Aktualisierungsgruppe – Diese Gruppe besteht aus Servern aus Standard-Host-Aktualisierungsgruppen.

   Sie können auch eine Kombination von Servern aus zwei Arten von Servergruppen verwenden.
4. Um Server zu der Aktualisierungsgruppe hinzuzufügen, suchen Sie die Server mithilfe ihrer Service-Tag-Nummer, und klicken Sie auf den Rechtspfeil, um Server zu der Liste der **Server in der Aktualisierungsgruppe** hinzuzufügen.
5. Klicken Sie zum Erstellen der nutzerdefinierten Aktualisierungsgruppe auf **Speichern**.

   ANMERKUNG: Nutzerdefinierte Aktualisierungsgruppen sind System Center-spezifisch und werden anderen Nutzern desselben System Centers angezeigt.

Bearbeiten von nutzerdefinierten Updategruppen

Berücksichtigen Sie die folgenden Punkte, wenn Sie eine nutzerdefinierte Aktualisierungsquelle modifizieren möchten:

- Der Typ einer Aktualisierungsgruppe kann nach der Erstellung nicht mehr geändert werden.
- Um Server zwischen zwei nutzerdefinierten Aktualisierungsgruppen zu verschieben, können Sie:
  1. Den Server aus einer bestehenden nutzerdefinierten Aktualisierungsgruppe entfernen. Dieser wird dann automatisch zu der vordefinierten Aktualisierungsgruppe hinzugefügt.
  2. Die nutzerdefinierte Gruppe, zu der der Server hinzugefügt wird, bearbeiten und anschließend anhand der Service-Tag-Nummer nach dem Server suchen.

1. Klicken Sie in **OMIMSSC** auf **Wartungscenter** und dann auf **Wartungseinstellungen**.
2. Klicken Sie bei den **Wartungseinstellungen** auf **Aktualisierungsgruppen**, wählen Sie die gewünschte Gruppe aus, und klicken Sie anschließend auf **Bearbeiten**, um die Aktualisierungsgruppe zu ändern.

Nutzerdefinierte Updategruppen entfernen

Beachten Sie Folgendes, wenn Sie eine nutzerdefinierte Aktualisierungsgruppe löschen möchten:

- Sie können eine Aktualisierungsgruppe nicht löschen, wenn mit ihr ein Job verknüpft ist, der geplant oder in Bearbeitung ist oder sich in der Warteposition befindet. Löschen Sie daher die geplanten Jobs, die einer nutzerdefinierten Aktualisierungsgruppe zugewiesen sind, bevor Sie die Servergruppe löschen.
- Sie können eine Aktualisierungsgruppe auch löschen, wenn Server in dieser Aktualisierungsgruppe vorhanden sind. Nach dem Löschen einer solchen Aktualisierungsgruppe werden die Server jedoch in ihre jeweiligen vordefinierten Aktualisierungsgruppen verschoben.
- Wenn ein Gerät aus der nutzerdefinierten Aktualisierungsgruppe aus MSSC gelöscht wird und Sie OMIMSSC mit dem registrierten MSSC synchronisieren, wird das Gerät aus der nutzerdefinierten Aktualisierungsgruppe entfernt und in die entsprechende vordefinierte Gruppe verschoben.

1. Klicken Sie in **OMIMSSC** auf **Wartungscenter** und dann auf **Wartungseinstellungen**.
2. Klicken Sie bei den **Wartungseinstellungen** auf **Aktualisierungsgruppen**, wählen Sie die gewünschte Gruppe aus, und klicken Sie anschließend auf **Löschen**, um die Aktualisierungsgruppe zu löschen.

Info zu Aktualisierungsquellen

Aktualisierungsquellen beziehen sich auf Katalogdateien, die Dell EMC Aktualisierungen (BIOS, Treiberpakete wie Verwaltungskomponenten, Netzwerkkarten) und die eigenständige ausführbare DUP-Datei enthalten (Dell Update Packages).

Sie können eine Aktualisierungsquelle oder ein Repository erstellen und als Standardupdatequelle festlegen, um einen Vergleichsbericht zu erstellen und Benachrichtigungen zu erhalten, wenn neue Katalogdateien im Repository verfügbar sind.

Mit OMIMSSC können Sie die Firmware der Geräte mithilfe von Online- oder Offline-Aktualisierungsquellen auf dem neuesten Stand halten.

Online-Aktualisierungsquellen sind Repositorys, die von Dell EMC verwaltet werden.

Offline-Aktualisierungsquellen sind lokale Repositorys und werden verwendet, wenn keine Internetverbindung besteht.

Es wird empfohlen, dass Sie nutzerdefinierte Repositorys erstellen und die Netzwerkfreigabe im lokalen Intranet der OMIMSSC-Appliance ablegen. Dadurch können Sie Internet-Traffic einsparen und außerdem ein sicheres internes Repository bereitstellen.

Aktualisieren Sie die Firmware mithilfe einer der folgenden Aktualisierungsquellen:

- **DRM-Repository** ist ein Offline-Repository. Exportieren Sie die Bestandsinformationen der ermittelten Geräte aus der OMIMSSC-Appliance, um ein Repository in DRM vorzubereiten. Informationen zur Integration mit DRM und zum Erstellen einer Aktualisierungsquelle über DRM finden Sie unter Integration mit DRM. Wählen Sie nach dem Erstellen eines Repositorys in DRM in OMIMSSC die durch DRM erstellte Aktualisierungsquelle und die relevanten Geräte aus und initiieren Sie eine Aktualisierung auf den Geräten. Informationen zu DRM finden Sie in den Dokumenten zu Dell Repository Manager unter `dell.com\support`.
- **HTTPS** – kann ein Online-oder Offline-Repository sein. Aktualisieren Sie bestimmte Komponenten von Geräten in Bezug auf die neueste Aktualisierung, die auf der HTTPS-Site bereitgestellt wird. Dell EMC erstellt alle zwei Monate ein Repository und veröffentlicht die folgenden Aktualisierungen über PDK-Kataloge:
  - Server-BIOS und Firmware
  - Von Dell EMC zertifizierte Betriebssystemtreiberpakete für die Bereitstellung des Betriebssystems

  ANMERKUNG: Wenn Sie beim Bereitstellen der Betriebsvorlage eine Online-Aktualisierungsquelle auswählen, werden die neuesten Firmware-Versionen heruntergeladen und auf die verwalteten Geräte angewendet. Daher können sich die Firmwareversionen zwischen Referenzgerät und bereitgestelltem Gerät unterscheiden.
- **Referenz-Firmwarebestand und Vergleich**: Kann über DRM in ein Offline-Repository konvertiert werden. Erstellen Sie eine Referenzbestandsdatei, die den Firmwarebestand der ausgewählten Geräte enthält. Die Referenzbestandsdatei kann Bestandsinformationen eines Geräts desselben Typs oder Modells enthalten oder mehrere Geräte unterschiedlichen Typs oder Modells haben. Sie können die Bestandsinformationen der in OMIMSSC vorhandenen Geräte mit der gespeicherten Referenzbestandsdatei vergleichen. Informationen zum Übergeben der exportierten Datei an DRM und zum Erstellen eines Repositorys finden Sie in den Dokumenten zu *Dell Repository Manager* unter `dell.com\support`.

Vordefinierte Aktualisierungsquellen und Standard-Aktualisierungsquellen

OMIMSSC enthält die vordefinierte Aktualisierungsquelle, die nach einer Neuinstallation oder einem Upgrade verfügbar ist. **Dell EMC Enterprise Katalog** ist eine vordefinierte standardmäßige Aktualisierungsquelle vom Typ HTTPS. Sie können jedoch eine andere Aktualisierungsquelle erstellen und diese als Standardaktualisierungsquelle markieren.

ANMERKUNG: Wenn Sie einen Proxyserver verwenden, können Sie zum Zugriff auf das Repository die Aktualisierungsquelle bearbeiten, um die Proxy-Details hinzuzufügen und die Änderungen zu speichern.

Vordefinierte und standardmäßige Aktualisierungsquellen für Windows Server HCI-Cluster

OMIMSSC unterstützt das Aktualisieren von Windows Server HCI-Clustern über bestimmte vordefinierte Aktualisierungsquellen. Diese Aktualisierungsquellen beziehen sich auf Katalogdateien, die die neuesten und empfohlenen Firmwareversionen von Komponenten für Windows Server HCI-Cluster enthalten. Sie werden nur auf der **Wartungscenter**-Seite aufgelistet.

AKTUALISIERUNGSKATALOG FÜR MICROSOFT HCI-LÖSUNGEN ist eine vordefinierte Aktualisierungsquelle vom Typ HTTPS und gehört zum **DELL EMC ENTERPRISE-KATALOG**.

Vordefinierte und standardmäßige Aktualisierungsquellen für modulare Systeme

OMIMSSC unterstützt die Aktualisierung modularer Systeme durch bestimmte vordefinierte Aktualisierungsquellen. Diese Aktualisierungsquellen beziehen sich auf Katalogdateien, die die neuesten und empfohlenen Firmwareversionen von Komponenten für modulare Systeme enthalten. Sie werden nur auf der **Wartungscenter**-Seite aufgelistet.

DELL EMC MX LÖSUNGSKATALOG ist eine vordefinierte Aktualisierungsquelle vom Typ HTTPS und gehört zum **DELL EMC ENTERPRISE-KATALOG**.

Validierung der Daten mithilfe der Testverbindung

Verwenden Sie **Testverbindung**, um zu überprüfen, ob der Speicherort der Aktualisierungsquelle mithilfe der Zugangsdaten, die beim Erstellen der Aktualisierungsquelle angegeben wurden, erreichbar ist. Erst wenn die Verbindung erfolgreich ist, können Sie eine Aktualisierungsquelle erstellen.

Einrichten lokaler HTTPS

So richten Sie Ihr lokales HTTPS ein:

1. Erstellen Sie eine Ordnerstruktur in Ihrem lokalen HTTPS, die ein exaktes Replikat von `downloads.dell.com` darstellt.
2. Laden Sie die Datei `catalog.gz` von der Online-HTTPS herunter, die sich an folgendem Speicherort befindet: `https://downloads.dell.com/catalog/catalog.xml.gz`. Extrahieren Sie dann die Dateien.
3. Extrahieren Sie die Datei `catalog.xml` und ändern Sie den Eintrag **baseLocation** in Ihre lokale HTTPS-URL. Komprimieren Sie dann die Datei mit der `.gz`-Erweiterung.
   Ändern Sie beispielsweise die **baseLocation** von `downloads.dell.com` in den Hostnamen oder die IP-Adresse, z. B. `hostname.com`.
4. Legen Sie die Katalogdatei mit der modifizierten Katalogdatei und den DUP-Dateien in Ihrem lokalen HTTPS-Ordner ab, dessen Struktur der von `downloads.dell.com` entspricht.

Anzeigen der Aktualisierungsquelle

1. Klicken Sie in **OMIMSSC** auf **Wartungscenter**.
2. Klicken Sie im **Wartungscenter** auf **Wartungseinstellungen** und dann auf **Aktualisierungsquelle**.
   Alle erstellten Aktualisierungsquellen werden zusammen mit ihrer Beschreibung, dem Quelltyp, dem Speicherort und dem Namen des Zugangsdatenprofils angezeigt.

Eine Aktualisierungsquelle erstellen

- Stellen Sie basierend auf dem Aktualisierungsquelltyp sicher, dass das Zugangsdatenprofil für Windows verfügbar ist.
- Stellen Sie sicher, dass Sie DRM mit Administratorrollen installieren und konfigurieren, wenn Sie eine DRM-Aktualisierungsquelle erstellen.

1. Klicken Sie in der OMIMSSC-Konsole auf **Wartungscenter** und dann auf **Wartungseinstellungen**.
2. Klicken Sie auf **Aktualisierungsquelle**.
3. Klicken Sie auf der Seite **Aktualisierungsquelle** auf **Neu erstellen** und geben Sie den Namen und die Beschreibung der Aktualisierungsquelle ein.
4. Wählen Sie im Dropdownmenü **Quelltyp** einen der folgenden Typen von Aktualisierungsquellen aus:
   - HTTPS-Quellen: Wählen Sie diese Option aus, um eine Online-HTTPS-Aktualisierungsquelle zu erstellen.
     ANMERKUNG: Wenn Sie eine Aktualisierungsquelle vom Typ HTTPS erstellen möchten, geben Sie den vollständigen Pfad zum Katalog mit dem Namen des Katalogs sowie Ihre Proxy-Zugangsdaten für den Zugriff auf die Aktualisierungsquelle an.

     DRM-Repository: Wählen Sie diese Option aus, um eine lokale Repository-Aktualisierungsquelle zu erstellen. Stellen Sie sicher, dass DRM installiert ist.

ANMERKUNG: Wenn Sie eine DRM-Quelle erstellen, geben Sie Ihre Windows-Zugangsdaten ein und stellen Sie sicher, dass auf den freigegebenen Windows-Speicherort zugegriffen werden kann. Geben Sie im Feld "Ort" den vollständigen Pfad der Katalogdatei mit dem Dateinamen an.

- Inventarausgabedateien: Wählen Sie diese Option aus, um den Firmware-Bestand anhand der Konfiguration des Referenzservers anzuzeigen.

  ANMERKUNG: Sie können einen Vergleichsbericht anzeigen, indem Sie **Inventarausgabedateien** als Aktualisierungsquelle verwenden. Die Bestandsinformationen des Referenzservers werden mit allen anderen Servern verglichen, die in OMIMSSC ermittelt werden.

5. Geben Sie unter **Ort** die URL der Aktualisierungsquelle einer HTTPS-Quelle und den gemeinsam genutzten Windows-Speicherort für DRM an.
6. Um auf die Aktualisierungsquelle zuzugreifen, wählen Sie das gewünschte Zugangsdatenprofil unter **Zugangsdaten** aus.
7. Wählen Sie unter **Proxy-Zugangsdaten** die entsprechenden Proxy-Zugangsdaten aus, wenn ein Proxy für den Zugriff auf die HTTPS-Quelle erforderlich ist.
8. (Optional) Um die erstellte Aktualisierungsquelle als Standardquelle zu verwenden, wählen Sie die Option **Als Standardquelle festlegen** aus.
9. Klicken Sie auf **Verbindung testen** und klicken Sie dann auf **Speichern**, um zu überprüfen, ob der Speicherort der Aktualisierungsquelle mit den angegebenen Zugangsdaten erreichbar ist.

   ANMERKUNG: Sie können die Aktualisierungsquelle nur erstellen, wenn die Testverbindung erfolgreich ist.

Bearbeiten von Aktualisierungsquellen

Berücksichtigen Sie Folgendes, wenn Sie eine Aktualisierungsquelle ändern möchten:

- Zur Bearbeitung der Aktualisierungsquelle **AKTUALISIERUNGSKATALOG FÜR MICROSOFT HCI-LÖSUNGEN** müssen Sie die entsprechende vordefinierte Aktualisierungsquelle bearbeiten und die Änderungen speichern. Diese Aktualisierung zeigt die Aktualisierungsquelle **Aktualisierungskatalog für Microsoft HCI-Lösungen**.
- Nach Erstellung einer Aktualisierungsquelle können Typ und Speicherort nicht mehr geändert werden.
- Sie können eine Aktualisierungsquelle auch dann ändern, wenn die Aktualisierungsquelle von einem laufenden oder geplanten Auftrag verwendet wird oder in einer Bereitstellungsvorlage verwendet wird. Beim Ändern der verwendeten Aktualisierungsquelle wird eine Warnmeldung angezeigt. Klicken Sie auf **Bestätigen**, um zu den Änderungen zu gelangen.
- Wenn eine Katalogdatei in der Aktualisierungsquelle aktualisiert wird, wird die lokal zwischengespeicherte Katalogdatei nicht automatisch aktualisiert. Um die im Cache gespeicherte Katalogdatei zu aktualisieren, bearbeiten Sie die Aktualisierungsquelle oder löschen und erstellen Sie die Aktualisierungsquelle erneut.

Wählen Sie die Aktualisierungsquelle aus, die Sie ändern möchten, klicken Sie auf **Bearbeiten** und aktualisieren Sie die Quelle nach Bedarf.

Aktualisierungsquelle entfernen

Berücksichtigen Sie Folgendes, wenn Sie eine Aktualisierungsquelle löschen möchten:

- Sie können keine vordefinierte Aktualisierungsquelle löschen.
- Sie können eine Aktualisierungsquelle nicht löschen, wenn sie in einem laufenden oder geplanten Job verwendet wird.
- Sie können eine Aktualisierungsquelle nicht löschen, wenn es sich um eine Standard-Aktualisierungsquelle handelt.

Wählen Sie die Aktualisierungsquelle aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.

Integration mit dem Dell EMC Repository Manager (DRM)

OMIMSSC OMIMSSC ist in DRM integriert, um nutzerdefinierte Aktualisierungsquellen in OMIMSSC zu erstellen. Die Integration ist ab DRM-Version 2.2 verfügbar. Stellen Sie die ermittelten Geräteinformationen vom OMIMSSC-Gerät für DRM bereit. Mithilfe der verfügbaren Bestandsinformationen können Sie ein nutzerdefiniertes Repository in DRM erstellen und als Aktualisierungsquelle in OMIMSSC festlegen, um Firmwareupdates durchzuführen und Cluster auf verwalteten Geräten zu erstellen. Weitere Informationen zum Erstellen eines Repositorys in DRM finden Sie in den Dell EMC Repository Manager-Dokumenten unter `Dell.com/support/home`.

Integrieren von DRM in OMIMSSC

Dieser Abschnitt beschreibt das Verfahren zur Repository-Erstellung mit Integration.

ANMERKUNG: Berücksichtigen Sie Faktoren wie das Testen der Testumgebung, Sicherheitsaktualisierungen, Anwendungsempfehlungen und Hinweise von Dell EMC, um die erforderlichen Aktualisierungen vorzubereiten.

ANMERKUNG: Wenn Sie nach der Aktualisierung von OMIMSSC die neuesten Bestandsinformationen zu den ermittelten Geräten anzeigen möchten, integrieren Sie DRM erneut mit dem OMIMSSC-Gerät.

1. Klicken Sie auf der Startseite auf **Neues Repository hinzufügen**. Die Option **Neues Repository hinzufügen** wird angezeigt.
2. Wählen Sie die Registerkarte **Integration** aus, geben Sie den **Repository**-Namen und seine **Beschreibung** ein.
3. Wählen Sie **Nutzerdefiniert** aus und klicken Sie auf **Systeme auswählen**, um ein bestimmtes System auszuwählen.
4. Wählen Sie aus dem Drop-Down-Menü **Integrationstyp** das Produkt aus, das Sie integrieren möchten. Je nach ausgewähltem Produkt werden die folgenden Optionen angezeigt: Folgende Optionen stehen zur Verfügung:
   a. Dell OpenManage Integration für Microsoft System Center – geben Sie den Hostnamen oder die IP-Adresse, den Nutzernamen, das Kennwort und den Proxyserver an.

      ANMERKUNG: Stellen Sie sicher, dass das Kennwort keine Sonderzeichen enthält, wie `<, >, ',", &`.

   b. Dell Konsolen Integration – geben Sie die URL https://<IP>/genericconsolerepository, Admin als Nutzername, Kennwort und Proxyserver an.

   ANMERKUNG: Die Integration der Dell Konsole ist auf Konsolen anwendbar, die die Webservices, wie z. B. OpenManage Integration für System Center Virtual Machine Manager (SCVMM), integriert haben.
5. Nachdem Sie die erforderliche Option ausgewählt haben, klicken Sie auf **Verbinden**. Die verfügbaren Systeme und Modelle werden im Abschnitt **Integrationstyp** angezeigt.
6. Klicken Sie auf **Hinzufügen**, um das Repository zu erstellen. Das Repository wird im Repository-Dashboard auf der Startseite angezeigt.

   ANMERKUNG: Achten Sie bei der Auswahl von Bundle-Typen oder DUP-Formaten darauf, Windows 64-Bit und Betriebssystem unabhängig auszuwählen, wenn Dell PowerEdge MX7000-Gehäuse Bestandteil des OMIMSSC ist.

Nach der Integration von DRM in OMIMSSC finden Sie im Abschnitt *Abrufen des Firmware-Katalogs für HCI Lösungen für Microsoft Windows Server Ready Nodes mithilfe von Dell Repository-Manager* des Betriebshandbuchs für *Dell EMC Microsoft HCI-Lösungen für Microsoft Windows Server Ready Node-Betrieb zur Verwaltung und Überwachung des Lebenszyklus der Ready Nodes* unter `dell.com/support`

Abfragehäufigkeit einstellen

Konfigurieren Sie Abfragen und Benachrichtigungen, um Alerts zu erhalten, wenn in der Aktualisierungsquelle eine neue Katalogdatei verfügbar ist, die als Standard ausgewählt ist. Die OMIMSSC-Appliance speichert einen lokalen Cache der Aktualisierungsquelle. Die Farbe der Benachrichtigungsglocke wird orange, wenn eine neue Katalogdatei in der Aktualisierungsquelle verfügbar ist. Um den im OMIMSSC-Gerät verfügbaren lokal zwischengespeicherten Katalog zu ersetzen, klicken Sie auf das Glockensymbol. Nachdem Sie die alte Katalogdatei durch die neueste Katalogdatei ersetzt haben, wird die Farbe der Glocke grün.

So stellen Sie die Abfragehäufigkeit ein:

1. Klicken Sie in OMIMSSC auf **Wartungscenter** und dann auf **Abfrage und Benachrichtigung**.
2. Klicken Sie auf **Abfrage und Benachrichtigung**.
3. Wählen Sie aus, wie häufig die Abfrage stattfinden soll:
   - **Nie** – Diese Option ist standardmäßig ausgewählt. Wählen Sie sie, um niemals Aktualisierungen zu erhalten.
   - **Einmal pro Woche** – Wählen Sie diese Option aus, um einmal pro Woche Aktualisierungen für neue Kataloge, die an der Aktualisierungsquelle verfügbar sind, zu erhalten.
   - **Einmal alle 2 Wochen** – Wählen Sie diese Option aus, um alle zwei Wochen Aktualisierungen für neue Kataloge, die an der Aktualisierungsquelle verfügbar sind, zu erhalten.
   - **Einmal pro Monat** – Wählen Sie diese Option aus, um einmal pro Monat Aktualisierungen für neue Kataloge, die an der Aktualisierungsquelle verfügbar sind, zu erhalten.

Anzeigen und Aktualisieren der Firmware-Bestandsaufnahme

Zeigen Sie den Vergleichsbericht für Geräte anhand einer Aktualisierungsquelle auf der Seite **Wartungscenter** an. Wenn Sie eine Aktualisierungsquelle auswählen, wird ein Bericht angezeigt, in dem die vorhandene Firmware mit der in der ausgewählten Aktualisierungsquelle vorhandenen Firmware verglichen wird. Der Bericht wird beim Ändern der Aktualisierungsquelle dynamisch generiert. Der Serverbestand wird mit der Aktualisierungsquelle verglichen und die vorgeschlagenen Aktionen werden aufgelistet. Diese Aktivität nimmt aufgrund der Anzahl der vorhandenen Geräte und Gerätekomponenten viel Zeit in Anspruch. Sie können während dieses Vorgangs keine anderen Tasks ausführen. Durch das Aktualisieren des Bestands wird der gesamte Bestand des Geräts aktualisiert, auch wenn Sie eine einzelne Komponente auf diesem Gerät auswählen.

Manchmal wird der Bestand des Geräts aktualisiert, auf der Seite wird jedoch nicht der neueste Bestand angezeigt. Verwenden Sie daher die Aktualisierungsoption, um die neuesten Bestandsinformationen der ermittelten Geräte anzuzeigen.

ANMERKUNG: Wenn nach dem Aktualisieren auf die neueste Version von OMIMSSC die Verbindung zu `downloads.dell.com` fehlschlägt, kann die standardmäßige Dell Online-DELL EMC ENTERPRISE-KATALOG-Aktualisierungsquelle nicht herunterladen. Daher ist der Vergleichsbericht nicht verfügbar. Um einen Vergleichsbericht für die standardmäßige Aktualisierungsquelle anzuzeigen, bearbeiten Sie die DELL EMC ENTERPRISE-KATALOG-Aktualisierungsquelle, erstellen Sie Proxy-Zugangsdaten und wählen Sie dann die Aktualisierungsquelle aus dem Dropdownmenü **Aktualisierungsquelle auswählen** aus. Weitere Informationen zum Bearbeiten einer Aktualisierungsquelle finden Sie unter Aktualisierungsquelle ändern.

ANMERKUNG: Eine lokale Kopie der Katalogdatei befindet sich in OMIMSSC, wenn das Produkt geliefert wird. Daher ist der aktuellste Vergleichsbericht nicht verfügbar. Aktualisieren Sie die Katalogdatei, um den neuesten Vergleichsbericht anzuzeigen. Um die Katalogdatei zu aktualisieren, bearbeiten Sie die Aktualisierungsquelle und speichern Sie sie, oder löschen Sie eine Aktualisierungsquelle und erstellen Sie sie erneut.

ANMERKUNG: In MECM werden Serverdetails wie **Treiberpaketversion** und Verfügbare Treiber für das Betriebssystem auch nach dem Aktualisieren der Bestandsinformationen nicht auf der Eigenschaftenseite **Bandexterne Controller von Dell** (OOB) aktualisiert. Um die OOB-Eigenschaften zu aktualisieren, synchronisieren Sie OMIMSSC mit dem registrierten MECM.

ANMERKUNG: Bei einer Aktualisierung von OMIMSSC werden Informationen zu Servern, die in früheren Versionen ermittelt wurden, nicht angezeigt. Die neuesten Serverinformationen und den korrekten Vergleichsbericht finden Sie, wenn Sie die Server erneut ermitteln.

So aktualisieren und zeigen Sie den Firmwarebestand der ermittelten Geräte an:

1. Klicken Sie in **OMIMSSC** auf **Wartungscenter**.
   Die Seite **Wartungscenter** wird mit einem Vergleichsbericht für alle Geräte angezeigt, die in OMIMSSC anhand der ausgewählten Aktualisierungsquelle ermittelt wurden.
2. (Optional) Um einen Vergleichsbericht nur für eine bestimmte Gerätegruppe anzuzeigen, wählen Sie nur die erforderlichen Geräte aus.
3. (Optional) Um einen Vergleichsbericht für eine andere Aktualisierungsquelle anzuzeigen, ändern Sie die Aktualisierungsquelle, indem Sie sie in der Dropdownliste **Aktualisierungsquelle auswählen** auswählen.
4. Um Firmware-Informationen zu Gerätekomponenten wie der aktuellen Version, der Baseline-Version und den von Dell EMC empfohlenen Aktualisierungsaktionen anzuzeigen, erweitern Sie die Servergruppe von **Gerätegruppe/Server** auf die Serverebene und dann auf die Komponentenebene. Zeigen Sie auch die Anzahl der empfohlenen Aktualisierungen für Geräte an. Bewegen Sie den Mauszeiger auf das Symbol für verfügbare Aktualisierungen, um die entsprechenden Details der Aktualisierungen anzuzeigen, z. B. Anzahl der wichtigen und empfohlenen Aktualisierungen.

   Die Anzeigefarbe für das Symbol für verfügbare Aktualisierungen basiert auf der allgemeinen Wichtigkeit der Aktualisierungen. Nachfolgend sind die kritischen Aktualisierungskategorien aufgeführt:

   - Die Farbe ist auch dann rot, wenn der Server oder die Servergruppe eine einzige kritische Aktualisierung enthält.
   - Die Farbe ist gelb, wenn keine wichtigen Aktualisierungen vorhanden sind.
   - Die Farbe ist grün, wenn die Firmwareversionen auf dem neuesten Stand sind.

   Nach dem Ausfüllen des Vergleichsberichts werden folgende Aktualisierungsaktionen vorgeschlagen:

   - Zurückstufen: Eine frühere Version ist verfügbar und Sie können die vorhandene Firmware auf diese Version zurückstufen.
   - Keine Aktion erforderlich: Die vorhandene Firmware entspricht der in der Aktualisierungsquelle.
   - Keine Aktualisierung verfügbar: Für diese Komponente sind keine Aktualisierungen verfügbar.

     ANMERKUNG: Es sind keine Aktualisierungen für Komponenten der Stromversorgungseinheiten (PSU) für MX7000 Modularsysteme und Server in Online-Katalogen verfügbar. Wenn Sie die Netzteilkomponente für das MX7000

Modularsystem aktualisieren möchten, finden Sie weitere Informationen unter Aktualisieren der Netzteilkomponente für Dell EMC PowerEdge MX7000-Geräte. Wenden Sie sich an den Dell EMC Support, um die PSU-Komponente für Server zu aktualisieren.

- Aktualisierung – Optional: Aktualisierungen sind optional und bestehen aus neuen Funktionen oder bestimmten Konfigurationsaktualisierungen.
- Aktualisierung – Dringend: Es sind kritische Aktualisierungen verfügbar, die der Behebung von Sicherheits-, Leistungs- oder anderer Probleme in Komponenten, wie beispielsweise dem BIOS, dienen.
- Aktualisierung – Empfohlen: Aktualisierungen mit Problembehebungen oder Funktionserweiterungen für Komponenten. Außerdem sind Kompatibilitätspatches mit anderen Firmwareupdates enthalten.

Anwendung eines Filters

Sie können Filter anwenden, um nur bestimmte Informationen im Vergleichsreport anzuzeigen.

Filtern Sie den Vergleichsbericht basierend auf verfügbaren Serverkomponenten. OMIMSSC unterstützt drei Kategorien von Filtern:

- **Aktualisierungsart** – Wählen Sie diesen Filter aus, um nur den ausgewählten Aktualisierungstyp auf Servern anzuzeigen.
- **Komponententyp** – Wählen Sie diesen Filter aus, um nur die ausgewählten Komponenten auf Servern anzuzeigen.
- **Servermodell** – Wählen Sie diesen Filter aus, um nur die ausgewählten Servermodelle anzuzeigen.

ANMERKUNG: Sie können keine Serverprofile exportieren und importieren, wenn die Filter angewendet werden.

So wenden Sie die Filter an:

Klicken Sie in OMIMSSC auf **Wartungscenter**, klicken Sie auf das Dropdownmenü für Filter, und wählen Sie anschließend die Filter aus.

Entfernen von Filtern

So entfernen Sie Filter:

Klicken Sie in OMIMSSC auf **Wartungscenter** und klicken Sie anschließend auf **Filter löschen**, oder deaktivieren Sie die betreffenden Kontrollkästchen.

Aktualisieren und Herabstufen der Firmwareversionen mithilfe der Methode "Aktualisierung ausführen"

Bevor Sie Aktualisierungen auf Geräten anwenden, vergewissern Sie sich, dass die folgenden Bedingungen erfüllt sind:

- Eine Aktualisierungsquelle ist verfügbar.

  ANMERKUNG: Wählen Sie die Aktualisierungsquelle der UPDATE-KATALOG FÜR MICROSOFT HCI-LÖSUNGEN oder die Aktualisierungsquellen des KATALOGS FÜR DELL EMC MX-LÖSUNGEN, um Firmwareaktualisierungen auf Windows Server HCI-Clustern oder MX7000 Modularsystemen anzuwenden, da diese Aktualisierungsquellen eine modifizierte Referenz zum Katalog sind, der empfohlene Firmware-Versionen von Komponenten für Windows Server HCI-Cluster und Modularsystemen enthält.
- Die Job-Warteschlange von iDRAC oder Management Module (MM) wird vor dem Anwenden der Aktualisierung auf den verwalteten Geräten gelöscht.

Wenden Sie Aktualisierungen auf ausgewählte Gerätegruppen an, die mit OMIMSSC hardwarekompatibel sind. Aktualisierungen können sofort angewendet oder geplant werden. Die für Firmwareupdates erstellten Jobs werden auf der Seite **Job- und Protokollcenter** aufgelistet.

Berücksichtigen Sie die folgenden Punkte, bevor Sie die Firmware aktualisieren oder ein Zurückstufen durchführen:

- Wenn Sie diesen Task starten, dauert der Task aufgrund der Anzahl der vorhandenen Geräte und Gerätekomponenten sehr lange.
- Sie können Firmwareupdates auf eine einzelne Komponente eines Geräts anwenden oder auf die gesamte Umgebung.
- Wenn für ein Gerät keine anwendbaren Aktualisierungen oder Zurückstufungen vorhanden sind, bewirkt das Durchführen eines Firmwareupdates auf den Geräten keine Aktionen.
- Informationen zum Aktualisieren des Gehäuses finden Sie im Abschnitt Aktualisieren der CMC-Firmware im Benutzerhandbuch der Dell PowerEdge M1000e Chassis Management Controller-Firmware.
  - Informationen zum Aktualisieren der Gehäuse-Firmware in VRTX finden Sie im Abschnitt Aktualisieren der Firmware im Benutzerhandbuch des Dell Chassis Management Controllers für Dell PowerEdge VRTX.

- Informationen zum Aktualisieren der Gehäuse-Firmware in FX2 finden Sie im Abschnitt Aktualisieren der Firmware im Benutzerhandbuch des Dell Chassis Management Controllers für Dell PowerEdge FX2.

1. Klicken Sie in OMIMSSC auf **Wartungscenter**, wählen Sie den Server oder die Servergruppe sowie eine Aktualisierungsquelle aus, und klicken Sie anschließend auf **Aktualisierung ausführen**.
2. Wählen Sie die Server oder Gruppen des modularen Systems und eine Aktualisierungsquelle aus und klicken Sie dann auf **Aktualisierung ausführen**.
3. Geben Sie unter **Aktualisierungsdetails** den Job-Namen und die Beschreibung des Firmwareupdates an.
4. Um das Zurückstufen der Firmwareversionen zu aktivieren, aktivieren Sie das Kontrollkästchen **Zurückstufen zulassen**.

   Wenn diese Option nicht ausgewählt ist, gibt es keine Aktion für die Komponente, für die ein Firmware-Zurückstufen erforderlich ist.
5. Wählen Sie unter **Aktualisierung planen** eine der folgenden Optionen aus:
   - **Jetzt ausführen**: Wählen Sie diese Option, um die Aktualisierungen sofort anzuwenden.
   - Wählen Sie das Datum und die Uhrzeit für die Planung eines künftigen Firmwareupdates aus.
6. Wählen Sie eine der folgenden Methoden und klicken Sie auf **Fertig stellen**.
   - **Agent-freie stufenweise Aktualisierungen**: Aktualisierungen, die ohne Neustart des Systems anwendbar sind, werden sofort angewendet, und die Aktualisierungen, die einen Neustart erfordern, werden beim Neustart des Systems angewendet. Aktualisieren Sie den Bestand, um zu prüfen, ob alle Aktualisierungen angewendet wurden. Der gesamte Aktualisierungsauftrag schlägt fehl, wenn die Operation auch nur auf einem Gerät fehlschlägt.
   - **Agent-freie Aktualisierungen** werden angewendet und das System wird sofort neu gestartet.

     ANMERKUNG: OMIMSSC unterstützt nur **agent-freie Aktualisierungen** für MX7000 Modularsysteme.

   ANMERKUNG: **Clusterfähiges Aktualisieren (CAU**): automatisiert den Aktualisierungsvorgang mithilfe der Windows-CAU-Funktion für Cluster-Aktualisierungsgruppen, um die Verfügbarkeit des Servers zu gewährleisten. Aktualisierungen werden an den Cluster-Aktualisierung-Koordinator weitergeleitet, der sich auf demselben System befindet, auf dem der SCVMM-Server installiert ist. Der Aktualisierungsprozess ist automatisiert, um die Verfügbarkeit des Servers zu gewährleisten. Der Aktualisierungsjob wird unabhängig von der im Dropdownmenü für die **Aktualisierungsmethode** getroffenen Auswahl an die CAU-Funktion (clusterfähiges Aktualisieren) von Microsoft übermittelt. Weitere Informationen finden Sie unter Aktualisierungen mit CAU.

   ANMERKUNG: Nach dem Senden eines Firmwareupdatejobs an iDRAC interagiert OMIMSSC mit iDRAC, um den Status des Jobs abzurufen, und zeigt ihn auf der Seite **Jobs und Protokolle** im OMIMSSC-Verwaltungsportal an. Wenn iDRAC längere Zeit keine Antwort auf die Abfrage des Jobstatus gibt, wird der Status des Jobs als "fehlgeschlagen" markiert.

Aktualisierungen unter Verwendung von CAU

Aktualisierungen auf Servern (die Teil eines Clusters sind) erfolgen über den Cluster-Aktualisierungskoordinator, der auf demselben System vorhanden ist, auf dem der SCVMM-Server installiert ist. Die Aktualisierungen werden nicht stufenweise bereitgestellt und sofort angewendet. Mit Cluster Aware Update (CAU) können Sie Unterbrechungen oder Serverausfälle minimieren und eine kontinuierliche Verfügbarkeit der Arbeitslast gewährleisten. Daher hat dies keine Auswirkungen auf den von der Clustergruppe bereitgestellten Dienst. Weitere Informationen zu CAU finden Sie im Abschnitt „Übersicht zum clusterfähigen Aktualisieren“ unter `technet.microsoft.com`.

Überprüfen Sie vor dem Anwenden der Aktualisierungen auf Cluster-Aktualisierungsgruppen Folgendes:

- Stellen Sie sicher, dass der registrierte Benutzer über Administratorrechte zum Aktualisieren von Clustern über die CAU-Funktion verfügt.
- Es besteht Konnektivität zur gewählten Aktualisierungsquelle.
- Die Failover-Cluster sind verfügbar.
- Überprüfen Sie die Verfügbarkeit der Clusteraktualisierung und stellen Sie sicher, dass im Clusterbereitschaftsbericht keine wesentlichen Fehler und Warnungen für die Anwendung der CAU-Methode enthalten sind. Weitere Informationen zu CAU finden Sie im Abschnitt mit den Voraussetzungen und bewährten Verfahren für clusterfähiges Aktualisieren unter `Technet.microsoft.com`.
- Stellen Sie sicher, dass entweder Windows Server 2012 R2 oder ein Windows 2016- oder Windows 2019-Betriebssystem auf allen Failover Cluster-Knoten installiert ist, damit die CAU-Funktion unterstützt wird.
- Die Konfiguration für automatische Aktualisierungen ist so festgelegt, dass Aktualisierungen auf Failover-Cluster-Knoten nicht automatisch installiert werden.
- Aktivieren Sie eine Firewallregel, die das Remote-Herunterfahren jedes Knotens im Failovercluster erlaubt.
- Stellen Sie sicher, dass die Clustergruppe mindestens zwei Knoten hat.

ANMERKUNG:

- Informationen zum Anwenden der Aktualisierungen finden Sie unter Aktualisieren und Zurückstufen von Firmwareversionen mithilfe der Methode "Aktualisierung ausführen". Informationen zu Dell EMC Repository Manager zum Herunterladen von Firmware-und

Treiberaktualisierungen finden Sie auf der Seite Firmware- und Treiber-Update-Katalog für Dell EMC Lösungen für Microsoft Azure Stack HCI unter `dell.com\support`, wo Sie die Katalogdatei herunterladen.

19

Verwalten von Geräten mithilfe von OMIMSSC

Halten Sie Server und modulare Systeme auf dem neuesten Stand, indem Sie Jobs für das Aktualisieren der Firmware für Server- und modulare Systemkomponenten planen. Verwalten Sie Server, indem Sie Server in einem früheren Zustand wiederherstellen. Exportieren Sie dazu ihre frühere Konfiguration, wenden Sie die Konfigurationen der alten Komponente auf die ersetzte Komponente an und exportieren Sie LC-Protokolle zur Problembehandlung.

Themen:

Server-Wiederherstellung

Speichern Sie die Konfigurationen eines Servers im Schutz-Vault, indem Sie die Konfigurationen eines Servers in ein Profil exportieren und das Profil auf demselben Server importieren, um ihn in einen früheren Zustand zurückzusetzen.

Schutz-Vaults

Der Schutz-Vault ist ein sicherer Ort, an dem Sie Serverprofile speichern können. Exportieren Sie das Serverprofil von einem Server oder einer Gruppe von Servern und importieren Sie es auf denselben Server oder dieselbe Servergruppe. Sie können dieses Serverprofil an einem freigegebenen Speicherort im Netzwerk speichern, indem Sie einen externen Vault oder einen internen Vault auf einer vFlash-SD-Karte (Secure Digital Card) erstellen. Sie können einen Server oder eine Gruppe von Servern nur einem Schutz-Vault zuweisen. Sie können jedoch einen Schutz-Vault mit vielen Servern oder Servergruppen verknüpfen. Sie können ein Serverprofil nur in einem Schutz-Vault speichern. Sie können jedoch eine beliebige Anzahl von Serverprofilen in einem einzigen Schutz-Vault speichern.

Erstellen eines Schutz-Vaults

Stellen Sie sicher, dass der Schutz-Vault zugreifbar ist.

1. Klicken Sie in **OMIMSSC** auf **Wartungscenter** und dann auf **Wartungseinstellungen**.
2. Klicken Sie im **Wartungscenter** auf **Schutz-Vault** und dann auf **Erstellen**.
3. Wählen Sie den gewünschten Schutz-Vault-Typ aus und geben Sie die Details an.
   - Wenn Sie einen Schutz-Vault vom Typ **Netzwerkfreigabe** erstellen, geben Sie einen Speicherort an, an dem die Profile gespeichert werden sollen, Anmeldedaten für den Zugriff auf diesen Speicherort und eine Passphrase zur Sicherung des Profils.
     ANMERKUNG: Diese Art von Schutz-Vault bietet die Unterstützung von Dateifreigaben vom Typ Common Internet File System (CIFS).
   - Wenn Sie einen Schutz-Vault vom Typ **vFlash** erstellen möchten, geben Sie die Passphrase an, um für die Sicherheit des Profils zu sorgen.

Bearbeiten des Schutz-Vaults

Name, Beschreibung und Schutz-Vault-Typ sowie die Passphrase können nicht geändert werden.

1. Klicken Sie in **OMIMSSC** auf **Wartungs Center** > **Wartungseinstellungen** > **Schutz-Vault**.
2. Um die Vault zu ändern, wählen Sie sie aus und klicken Sie auf **Bearbeiten**.

ANMERKUNG: Wenn die Schutz-Vault geändert wird, während die Jobs zum Serverprofilexport oder -import laufen, werden die bearbeiteten Informationen für die ausstehenden Unteraufgaben im Job berücksichtigt.

Schutz-Vault entfernen

In den folgenden Fällen kann ein Schutz-Vault nicht gelöscht werden:

- Der Schutz-Vault ist einem Server oder einer Gruppe von Servern zugeordnet.

  Um einen solchen Schutz-Vault zu löschen, löschen Sie den Server oder die Servergruppe und löschen Sie dann den Schutz-Vault.

- Dem Schutz-Vault ist ein geplanter Job zugeordnet. Um einen solchen Schutz-Vault zu löschen, löschen Sie den geplanten Job und löschen Sie dann den Schutz-Vault.

1. Klicken Sie in **OMIMSSC** auf **Wartungs Center** > **Wartungseinstellungen** > **Schutz-Vault**.
2. Wählen Sie den zu löschenden Vault aus und klicken Sie auf **Löschen**.

Exportieren von Serverprofilen

Exportieren Sie ein Serverprofil einschließlich der installierten Firmware-Images auf verschiedenen Komponenten wie BIOS, RAID, NIC, iDRAC, Lifecycle Controller und der Konfiguration dieser Komponenten. Die OMIMSSC-Appliance erstellt eine Datei mit allen Konfigurationen, die Sie auf einer vFlash-SD-Karte oder einer Netzwerkfreigabe speichern können. Wählen Sie einen Schutz-Vault Ihrer Wahl aus, um diese Datei zu speichern. Sie können die Konfigurationsprofile eines Servers oder einer Gruppe von Servern sofort exportieren oder den Export für einen späteren Zeitpunkt planen. Sie können auch eine entsprechende Wiederholungsoption auswählen, wie oft die Serverprofile exportiert werden müssen.

Deaktivieren Sie die Option **Bei Fehler F1/F2-Eingabeaufforderung** in den **BIOS-Einstellungen**.

Berücksichtigen Sie Folgendes, bevor Sie Serverprofile exportieren:

- In einer Instanz können Sie nur einen Job zum Exportieren der Konfiguration für eine Gruppe von Servern planen.
- Sie können keine anderen Aktivitäten auf diesem Server oder dieser Gruppe von Servern ausführen, deren Konfigurationsprofile exportiert werden.
- Stellen Sie sicher, dass der Job **Automatische Sicherung** in iDRAC nicht zur gleichen Zeit geplant ist.
- Sie können keine Serverprofile exportieren, wenn die Filter angewendet werden. Deaktivieren Sie zum Exportieren von Serverprofilen alle angewendeten Filter.
- Stellen Sie zum Exportieren von Serverprofilen sicher, dass Sie über die iDRAC Enterprise-Lizenz verfügen.
- Stellen Sie vor dem Exportieren des Serverprofils sicher, dass die IP-Adresse des Servers nicht geändert wird. Wenn sich die Server-IP aufgrund eines anderen Vorgangs geändert hat, ermitteln Sie diesen Server in OMIMSSC erneut und planen Sie den Job zum Exportieren des Serverprofils.

1. Klicken Sie in OMIMSSC auf **Wartungscenter**. Wählen Sie die Server aus, deren Profile Sie exportieren möchten, und klicken Sie im Dropdownmenü **Geräteprofil** auf **Exportieren**.
   Die Seite **Serverprofil exportieren** wird angezeigt.
2. Wählen Sie die Server aus, deren Profile Sie exportieren möchten, und klicken Sie im Dropdownmenü **Geräteprofil** auf **Exportieren**.
   Die Seite **Serverprofil exportieren** wird angezeigt.
3. Geben Sie auf der Seite **Serverprofil exportieren** die Jobdetails an und wählen Sie einen Schutz-Vault aus.

   Weitere Informationen zu Schutz-Vaults finden Sie unter Erstellen eines Schutz-Vaults.

   Wählen Sie unter **Export des Serverprofils planen** eine der folgenden Optionen aus:
   - **Jetzt ausführen**: Bei Auswahl dieser Option wird die Serverkonfiguration der ausgewählten Server oder Gruppe von Servern sofort exportiert.
   - Planen: Legen Sie einen Zeitplan für das Exportieren der Serverkonfiguration der ausgewählten Gruppe von Servern fest.
     - **Nie**: Wählen Sie diese Option aus, um das Serverprofil nur einmal zur geplanten Zeit zu exportieren.
     - **Einmal pro Woche**: Wählen Sie diese Option aus, um das Serverprofil einmal pro Woche zu exportieren.
     - **Einmal alle 2 Wochen**: Wählen Sie diese Option aus, um das Serverprofil alle zwei Wochen zu exportieren.
     - **Einmal alle 4 Wochen**: Wählen Sie diese Option aus, um das Serverprofil alle vier Wochen zu exportieren.

Serverprofil importieren

Sie können ein Serverprofil importieren, das zuvor für denselben Server oder dieselbe Servergruppe exportiert wurde. Das Importieren eines Serverprofils ist hilfreich, um die Konfiguration und Firmware eines Servers in einem im Profil gespeicherten Zustand wiederherzustellen.

Es gibt zwei Möglichkeiten, Serverprofile zu importieren:

- Serverprofil schnell importieren: Mit dieser Option können Sie das zuletzt exportierte Serverprofil für diesen Server automatisch importieren. Für diesen Vorgang müssen Sie nicht für jeden Server einzelne Serverprofile auswählen.
- Nutzerdefiniertes Serverprofil importieren: Mit dieser Option können Sie Serverprofile für jeden der einzeln ausgewählten Server importieren. Beispiel: Wenn der Export von Serverprofilen geplant ist und einmal täglich durchgeführt wird, können Sie mithilfe dieser Funktion ein bestimmtes Serverprofil für den Import auswählen, das in der Liste der verfügbaren Serverprofile am Schutz-Vault für diesen Server enthalten ist.

Hinweise zum Importieren von Serverprofilen:

- Sie können ein Serverprofil nur aus einer Liste der exportierten Serverprofile für diesen Server importieren. Sie können nicht dieselben Serverprofile für verschiedene Server oder Servergruppen importieren. Wenn Sie versuchen, das Serverprofil eines anderen Servers oder einer anderen Servergruppe zu importieren, schlägt der Import des Serverprofils fehl.
- Falls für einen bestimmten Server oder eine Gruppe von Servern kein Serverprofil-Image verfügbar ist und für diesen Server bzw. diese Servergruppe ein Job zum Importieren eines Serverprofils initiiert wird, schlägt dieser Job fehl. Zu den Aktivitätsprotokollen wird eine Protokollnachricht mit den Details des Fehlers hinzugefügt.
- Wenn nach dem Export eines Serverprofils eine Komponente vom Server entfernt und anschließend ein Job zum Importieren eines Profils gestartet wird, werden alle Komponenteninformationen wiederhergestellt, nur die fehlenden Komponenteninformationen werden übersprungen. Diese Informationen sind nicht im Aktivitätsprotokoll von OMIMSSC verfügbar. Weitere Informationen zu den fehlenden Komponenten finden Sie im **LifeCycle-Protokoll** des iDRAC.
- Sie können kein Serverprofil importieren, nachdem Sie die Filter angewendet haben. Deaktivieren Sie zum Importieren von Serverprofilen alle angewendeten Filter.
- Um Serverprofile zu importieren, müssen Sie über die iDRAC Enterprise-Lizenz verfügen.

1. Wählen Sie in OMIMSSC unter **Wartungscenter** die Server aus, deren Profile Sie importieren möchten, und klicken Sie auf **Importieren** im Dropdown-Menü **Geräteprofil**.
   Die Seite **Serverprofil importieren** wird angezeigt.
2. Wählen Sie die Server aus, deren Profile Sie importieren möchten, und klicken Sie im Dropdownmenü **Geräteprofil** auf **Importieren**.
   Die Seite **Serverprofil importieren** wird angezeigt.
3. Geben Sie die Details an und wählen Sie den gewünschten **Server-Import-Profiltyp** aus.

   ANMERKUNG: Ein Serverprofil wird zusammen mit der vorhandenen RAID-Konfiguration exportiert. Sie können das Serverprofil jedoch einschließlich der RAID-Konfiguration auf dem Server oder der Servergruppe importieren. **Daten beibehalten** ist standardmäßig ausgewählt und behält die vorhandene RAID-Konfiguration im Server bei. Deaktivieren Sie das Kontrollkästchen, wenn Sie die im Serverprofil gespeicherten RAID-Einstellungen anwenden möchten.

4. Um das Serverprofil zu importieren, klicken Sie auf **Fertig stellen**.

Anwenden von Firmware- und Konfigurationseinstellungen auf ersetzte Teile

Die Funktion zum Ersetzen von Teilen aktualisiert eine ausgetauschte Serverkomponente automatisch auf die erforderliche Firmwareversion oder die Konfiguration der alten Komponente oder auf beides. Die Aktualisierung erfolgt automatisch, wenn Sie den Server nach dem Ersetzen der Komponente neu starten.

So legen Sie die Konfiguration für die Teilersetzung fest:

1. Wählen Sie in OMIMSSC unter **Wartungscenter** die Server oder Servergruppe aus und klicken Sie dann auf **Teilersetzung**.

   ANMERKUNG: Der Optionsname wird zu **Teilersetzung konfigurieren** erweitert, wenn Sie zu **Teilersetzung** wechseln.

   Die Seite **Teilersetzungskonfiguration** wird angezeigt.
2. Wählen Sie die Server aus, deren Komponente Sie konfigurieren möchten, und klicken Sie dann auf **Teilersetzung**.

ANMERKUNG: Der Optionsname wird zu **Teilersetzung konfigurieren** erweitert, wenn Sie zu **Teilersetzung** wechseln.

Die Seite **Teilersetzungskonfiguration** wird angezeigt.

3. Sie können für **CSIOR**, **Teile-Firmwareaktualisierung** und **Teilekonfigurationsaktualisierung** eine der folgenden Optionen festlegen und dann auf **Fertig stellen** klicken:
   - Systembestandsaufnahme bei Neustart durchführen (CSIOR) - Erfasst alle Komponenteninformationen bei jedem Neustart des Systems.
     - **Aktiviert** - Die Bestandsaufnahmeinformationen für die Software und Hardware der Serverkomponenten werden automatisch bei jedem Neustart des Systems aktualisiert.
     - **Deaktiviert** - Die Bestandsaufnahmeinformationen für die Software und Hardware der Serverkomponenten werden nicht aktualisiert.
     - **Ändern Sie nicht den Wert auf dem Server** - Die vorhandene Serverkonfiguration wird beibehalten.
   - Teile-Firmwareaktualisierung: Wiederherstellung oder Aktualisierung oder Zurückstufen der Firmware-Version der Komponente je nach getroffener Auswahl.
     - **Deaktiviert**:- Die Teile-Firmwareaktualisierung ist deaktiviert und das Gleiche gilt für die ersetzte Komponente.
     - **Nur Versionsaktualisierung zulassen**: Aktualisierte Firmware-Versionen werden auf die ersetzte Komponente angewendet, wenn die Firmware-Version der neuen Komponente älter als die vorhandene Version ist.
     - **Firmware des ersetzten Teils anpassen**: Die Firmware-Version der neuen Komponente wird der Firmware-Version der ursprünglichen Komponente angepasst.
     - **Ändern Sie nicht den Wert auf dem Server** - Die vorhandene Komponentenkonfiguration wird beibehalten.
   - Teilekonfigurationsaktualisierung: Wiederherstellung oder Aktualisierung der Komponentenkonfiguration je nach getroffener Auswahl.
     - **Deaktiviert**: Die Teilekonfigurationsaktualisierung ist deaktiviert und die gespeicherte Konfiguration der alten Komponente wird nicht auf die ersetzte Komponente angewendet.
     - **Immer anwenden**: Die Teilekonfigurationsaktualisierung ist aktiviert und die gespeicherte Konfiguration der alten Komponente wird auf die ersetzte Komponente angewendet.
     - **Nur bei übereinstimmender Firmware anwenden**: Die gespeicherte Konfiguration der alten Komponente wird nur dann auf die ersetzte Komponente angewendet, wenn deren Firmware-Versionen übereinstimmen.
     - **Ändern Sie nicht den Wert auf dem Server** - Die vorhandene Konfiguration wird beibehalten.

Erfassen von LC-Protokollen für Server

LC-Protokolle stellen Aufzeichnungen vergangener Aktivitäten auf einem verwalteten Server bereit. Diese Protokolldateien sind für die Serveradministratoren nützlich, da sie detaillierte Informationen zu empfohlenen Maßnahmen und andere technische Informationen enthalten, die für die Fehlerbehebung nützlich sind. Die verschiedenen Arten von Informationen in LC-Protokollen sind Alerts, Konfigurationsänderungen an den System-Hardwarekomponenten, Firmware-Änderungen aufgrund einer Aktualisierung oder Zurückstufung, Ersatzteile, Temperaturwarnungen, detaillierte Zeitstempel über den Beginn der Aktivität, Schweregrad der Aktivität und so weiter. Die exportierte LC-Protokolldatei wird in einem Ordner gespeichert und der Ordner wird nach der Service-Tag-Nummer des Servers benannt. LC-Protokolle werden im folgenden Format gespeichert: `<YYYYMMDDHHMMSSSSS>.<file format>`. So ist beispielsweise `20160720103001O597.xml.gz` der Name der LC-Datei, der das Datum und die Uhrzeit der Dateierstellung enthält. Es gibt zwei Möglichkeiten, LC-Protokolle zu erfassen:

- Vollständige LC-Protokolle: Exportiert aktive und archivierte LC-Protokolldateien. Sie sind groß und werden daher im Format `.gz` komprimiert und an den angegebenen Speicherort auf einer CIFS-Netzwerkfreigabe exportiert.
- Aktive LC-Protokolle: Exportiert aktuelle LC-Protokolldateien sofort oder plant einen Job, um die Protokolldateien in regelmäßigen Abständen zu exportieren. Diese Protokolldateien können Sie anzeigen, durchsuchen und in die OMIMSSC Appliance exportieren. Darüber hinaus können Sie eine Sicherung der Protokolldateien in einer Netzwerkfreigabe speichern.

Um ein LC-Protokoll zu erfassen, führen Sie die folgenden Schritte aus:

1. Klicken Sie in OMIMSSC auf **Wartungscenter**. Wählen Sie einen Server oder eine Gruppe von Servern aus, klicken Sie auf das Dropdownmenü **LC-Protokolle** und dann auf **LC-Protokolle erfassen**.
2. Wählen Sie die Server aus, deren Protokolle Sie exportieren möchten, klicken Sie dann auf das Dropdownmenü **LC-Protokolle** und klicken Sie dann auf **LC-Protokolle erfassen**.
3. Wählen Sie in **LC-Protokollerfassung** eine der folgenden Optionen aus und klicken Sie auf **Fertig stellen**.
   - **Vollständige LC-Protokolle (.gz) exportieren** – Wählen Sie diese Option aus, um die vollständigen LC-Protokolle nach Angabe der Windows-Zugangsdaten in eine CIFS-Netzwerkfreigabe zu exportieren.
   - **Aktive Protokolle exportieren (Jetzt ausführen)** – Wählen Sie diese Option aus, um die aktiven Protokolle sofort in das OMIMSSC-Gerät zu exportieren.

- (Optional) Wählen Sie das Kontrollkästchen **LC-Protokolle auf der Netzwerkfreigabe sichern**, um eine Sicherungskopie der LC-Protokolle nach Angabe der Windows-Zugangsdaten auf der CIFS-Netzwerkfreigabe zu speichern.

- **LC-Protokollsammlung planen** – Wählen Sie diese Option aus, um die aktiven Protokolle in regelmäßigen Abständen zu exportieren.

  Wählen Sie unter **LC-Protokollsammlung planen** ein Datum und eine Uhrzeit zum Exportieren der Protokolldateien aus.

  Wählen Sie ein Optionsfeld aus, je nachdem, wie oft die Dateien exportiert werden müssen. Die verfügbaren Optionen für die Planung der Häufigkeit, um festzulegen, wie oft die LC-Protokolle erfasst werden sollen, sind:

  - **Nie** – Diese Option ist standardmäßig ausgewählt. Wählen Sie diese Option aus, um die LC-Protokolle nur einmal zur geplanten Zeit zu exportieren.
  - **Täglich** – Wählen Sie diese Option aus, um die LC-Protokolle täglich zur geplanten Zeit zu exportieren.
  - **Einmal pro Woche** – Wählen Sie diese Option aus, um die LC-Protokolle einmal pro Woche zur geplanten Zeit zu exportieren.
  - **Einmal alle 4 Wochen** – Wählen Sie diese Option aus, um die LC-Protokolle alle vier Wochen zur geplanten Zeit zu exportieren.
  - (Optional) Wählen Sie das Kontrollkästchen **LC-Protokolle auf der Netzwerkfreigabe sichern**, um eine Sicherungskopie der LC-Protokolle nach Angabe der Windows-Zugangsdaten auf der CIFS-Netzwerkfreigabe zu speichern.

  ANMERKUNG: Stellen Sie einen Freigabeordner mit ausreichend Speicherplatz zur Verfügung, da die exportierten Dateien groß sind.

Um diesen Job zu verfolgen, ist standardmäßig die Option **Zur Jobliste wechseln** ausgewählt.

Anzeigen von LC-Protokollen

Zeigen Sie alle aktiven LC-Protokolle an, suchen Sie nach einer detaillierten Beschreibung und laden Sie die Protokolle im CSV-Format herunter.

So fügen Sie die OMIMSSC-Appliance auf der **Lokalen Intranet-Seite** hinzu:

1. Klicken Sie in OMIMSSC auf **Wartungscenter**. Wählen Sie einen Server oder eine Gruppe von Servern aus, klicken Sie auf das Dropdownmenü **LC-Protokolle** und dann auf **LC-Protokolle anzeigen**.
2. Wählen Sie die Server aus, deren Protokolle Sie anzeigen möchten, klicken Sie auf das Dropdownmenü **LC-Protokolle** und klicken Sie dann auf **LC-Protokolle anzeigen**.
3. Alle Server in der ausgewählten Gruppe und die Server, für welche LC-Protokolle erfasst werden, werden mit ihren LC-Protokolldateien aufgelistet. Klicken Sie auf den Dateinamen, um alle Protokolleinträge in der LC-Protokolldatei speziell für diesen Server anzuzeigen. Weitere Informationen finden Sie unter Dateibeschreibung.
4. (Optional) Verwenden Sie das Suchfeld, um die Beschreibung in allen Protokolldateien zu suchen und die Datei im CSV-Format zu exportieren.

   Für die Suche der Meldungsbeschreibung in der LC-Datei gibt es zwei Möglichkeiten:
   - Klicken Sie auf den Dateinamen, öffnen Sie die LC-Protokolldatei und suchen Sie eine Beschreibung im Suchfeld.
   - Geben Sie einen Beschreibungstext in das Suchfeld ein und lassen Sie dann alle LC-Dateien an, in denen dieser Text vorkommt, anzeigen.

   ANMERKUNG: Wenn die Beschreibung der LC-Protokollmeldung lang ist, wird die Meldung auf 80 Zeichen gekürzt.

   ANMERKUNG: Die neben der LC-Protokollmeldung angezeigte Zeit folgt der iDRAC-Zeitzone.

Dateibeschreibung

Auf dieser Seite können Sie detaillierte Informationen zu empfohlenen Aktionen sowie einige andere technische Informationen anzeigen, die für das Nachverfolgen oder Alerts eines bestimmten Servers nützlich sind.

Um den Inhalt einer Datei anzuzeigen, klicken Sie auf einen Dateinamen:

- Sie können nach bestimmten Nachrichtenbeschreibungen suchen.
- Sie können entweder die Protokolldateien im Fenster anzeigen oder die Datei herunterladen, um zusätzliche Protokollnachrichten anzuzeigen.
- Sie können alle von einem Benutzer für eine Aktivität bereitgestellten Kommentare anzeigen.

ANMERKUNG: Bei Verwendung der Suchoption werden nur die Suchergebnisse in eine CSV-Datei exportiert.

ANMERKUNG: Wenn die Meldung lang ist, wird sie auf 80 Zeichen gekürzt.

ANMERKUNG: Klicken Sie auf **Meldungs-ID** zum Anzeigen weiterer Informationen zu der Meldung.

Bestand exportieren

Exportieren Sie die Bestandsliste ausgewählter Server oder einer Gruppe von Servern in eine XML- oder CSV-Datei. Sie können diese Informationen in einem freigegebenen Windows-Verzeichnis oder auf einem Verwaltungssystem speichern. Verwenden Sie diese Bestandsinformationen, um eine Referenzbestandsdatei in einer Aktualisierungsquelle zu erstellen.

ANMERKUNG: Sie können die XML-Datei in DRM importieren und basierend auf der Inventardatei ein Repository erstellen.

ANMERKUNG: Obwohl Sie nur die Komponenteninformationen eines Servers auswählen und exportieren, werden die vollständigen Bestandsaufnahmedaten des Servers exportiert.

1. Klicken Sie in **OMIMSSC** auf **Wartungscenter**.
2. Wählen Sie die Server aus, für welche Sie die Bestandsaufnahme exportieren möchten, und wählen Sie das Format im Drop-Down-Menü **Bestandsaufnahme exportieren** aus.

   Die Datei wird je nach Auswahl im CSV- oder XML-Format exportiert. Die Datei enthält Details wie Servergruppen, Service-Tag-Nummer des Servers, Hostname oder IP-Adresse, Gerätemodell, Komponentenname, aktuelle Firmware-Version dieser Komponente, Firmware-Version von der Aktualisierungsquelle und Aktualisierungsaktion für diese Komponente.

Verwalten von Jobs

Stellen Sie sicher, dass sich der Job im Status **Geplant** befindet.

1. Führen Sie in OMIMSSC Folgendes aus:
   - Klicken Sie im Navigationsbereich auf **Wartungscenter** und dann auf **Jobs verwalten**.
   - Klicken Sie im Navigationsbereich auf **Jobs und Protokollcenter** und dann auf die Registerkarte **Geplant**.
2. Wählen Sie die Jobs aus, die Sie abbrechen möchten, klicken Sie auf **Abbrechen** und anschließend zum Bestätigen auf **Ja**.

20

Bereitstellung von Azure Stack HCI-Cluster

Im folgenden sind die Schritte zur Bereitstellung von Azure Stack HCI-Cluster beschrieben:

1. Erstellen Sie die erforderlichen Windows- und Geräte-Zugangsdatenprofile.
2. WinPE-Image erstellen
   a. Installieren Sie die WDS-Funktion auf SCVMM, und konfigurieren Sie sie dann.
   b. Hinzufügen eines PXE-Servers im SCVMM-Server unter Verwendung von Ressourcen hinzufügen und Angabe desselben Servernamens (SCVVM-Hostname) PXE-Server.
   c. Erstellen Sie den freigegebenen Ordner innerhalb des SCVMM-Servers und kopieren Sie dann Boot.wim aus C:\RemoteInstall\DCMgr\Boot\Windows\Images in einen freigegebenen Ordner.
   d. Extrahieren der Treiber vom Dell EMC OpenManage-Treiberpaket.
   e. Erstellen Sie ein WinPE-Image.
   f. Stellen Sie sicher, dass das WinPE-Bild in einem freigegebenen Ordner in SCVMM platziert wird.
3. Fügen Sie Windows Server 2016 und 2019 VM-Vorlage zur in SCVMM-Bibliothek hinzu. Weitere Informationen finden Sie in der Microsoft-Dokumentation.
   a. Ändern Sie die folgenden Eigenschaften:
   - Betriebssystem: Windows Server 2016 und 2019 Datacenter
   - Virtualisierungsplattform: Microsoft Hyper-V

   ANMERKUNG: Zum Erstellen einer virtuellen Windows Server 2019-Festplatte (.vhdx) unter Verwendung einer .iso-Datei für die Betriebssystembereitstellung siehe https://gallery.technet.microsoft.com/scriptcenter/Convert-WindowsImageps1-0fe23a8f
4. Erstellen Sie ein physisches Computerprofil (PCP) in SCVMM. Wählen Sie in der Hardwarekonfiguration > Festplatte und Partitionen das Partitionsschema als **GUID-Partitionstabelle** aus. Weitere Informationen finden Sie unter Erstellen eines Profils für physische Computer im Abschnitt Voraussetzungen der Microsoft-Dokumentation zur Bereitstellung eines Hyper-V-Hosts oder -Clusters von Bare-Metal-Computern.
5. Erstellen Sie eine Hostgruppe in SCVMM, um Azure Stack HCI-Cluster zu hosten. Informationen zum Erstellen von Hostgruppen in SCVMM finden Sie in der Microsoft-Dokumentation.
6. Erstellen eines Hypervisor-Profils
7. Ermitteln Sie die Geräte in Dell EMC OpenManage Enterprise.
8. Konfigurieren Sie mithilfe von vordefinierten Betriebsvorlagen.
9. (Optional) Überprüfen Sie die Compliance (Konfiguration und Bereitstellung > Serveransicht > Wählen Sie den Server aus und weisen Sie eine Betriebsvorlage zu).
10. Logischen Switch erstellen.
11. Stellen Sie Azure Stack HCI-Cluster bereit.
    Um die erfolgreiche Clusterbereitstellung zu überprüfen, gehen Sie zu **Cluster-Ansicht**, um zu überprüfen, ob das Cluster mit der entsprechenden Kategorie aufgeführt wird.

21

Troubleshooting

Themen:

Ressourcen für die Verwaltung von OMIMSSC

Verwenden Sie dieses Handbuch, um die erforderlichen Berechtigungen zu prüfen und alle in OMIMSSC aufgetretenen Probleme zu lösen.

Stellen Sie zur Behebung von Problemen in OMIMSSC sicher, dass Sie über die folgenden Ressourcen verfügen:

- Kontodetails des Benutzers mit Lesezugriff, um sich beim OMIMSSC-Gerät anzumelden und verschiedene Vorgänge auszuführen.

  Um sich als Nur-Lese-Benutzer von der OMIMSSC Appliance-VM aus anzumelden, geben Sie den Nutzernamen als `readonly` mit demselben Kennwort ein, das für die Anmeldung bei der OMIMSSC Appliance-VM verwendet wurde.

- Protokolldateien mit einer Gesamtübersicht und vollständigen Details der Fehler:
  - Aktivitätsprotokolle: Enthalten benutzerspezifische und allgemeine Informationen zu den in OMIMSSC initiierten Jobs und dem Status der in OMIMSSC ausgeführten Jobs. Um Aktivitätsprotokolle anzuzeigen, rufen Sie die Seite **Jobs und Protokolle** in der OMIMSSC-Konsolenerweiterung auf.
  - Vollständige Protokolle: Enthalten administratorbezogene Protokolle und mehrere detaillierte Protokolle, die sich auf Szenarien in OMIMSSC beziehen. Um die vollständigen Protokolle anzuzeigen, öffnen Sie die Seite **Jobs und Protokolle** im **OMIMSSC-Admin-Portal**, **Einstellungen** und dann **Protokolle**.
  - LC-Protokolle: Enthalten Informationen auf Serverebene sowie detaillierte Fehlermeldungen zu Vorgängen, die in OMIMSSC ausgeführt werden. Informationen zum Herunterladen und Anzeigen der LC-Protokolle finden Sie im *Benutzerhandbuch für Dell EMC OpenManage Integration für Microsoft System Center für System Center Configuration Manager und für System Center Virtual Machine Manager*.

    ANMERKUNG: Starten Sie zur Problembehandlung einzelner Geräte von der Seite iDRAC oder OpenManage Enterprise Module (OME-Modular) aus OMIMSSC, klicken Sie auf die Seite **Konfiguration und Bereitstellung**, öffnen Sie die entsprechende Ansicht und klicken Sie auf die IP-Adresse des Geräts.

ANMERKUNG: Beim Administrator-Benutzer des SCVMM-Servers sollte es sich nicht um ein SCVMM-Dienstkonto handeln.

ANMERKUNG: Wenn Sie ein Upgrade von SC2012 VMM SP1 auf SC2012 VMM R2 ausführen, dann führen Sie auch ein Upgrade auf Windows PowerShell 4.0 aus.

Überprüfen der Berechtigungen für die Verwendung der OMIMSSC-Konsolenerweiterung für MECM

Stellen Sie nach der Installation von OMIMSSC sicher, dass der registrierte Benutzer über die folgenden Berechtigungen verfügt:

1. Geben Sie auf dem System, auf dem OMIMSSC installiert ist, die **Schreibberechtigungen** für den Ordner *<Configuration Manager Admin Console-Installationsverzeichnis>\XmlStorage\Extensions\DLCPlugin* mithilfe von PowerShell-Befehlen an.

   Vervollständigen Sie die folgenden Voraussetzungen auf dem Standortserver und SMS-Anbieterserver, bevor Sie die OMIMSSC-Komponente installieren:

   a. Führen Sie in PowerShell den Befehl aus: `PSRemoting`.

      Wenn der Befehl `PSRemoting` deaktiviert ist, aktivieren und führen Sie den Befehl `PSRemoting` unter Verwendung der folgenden Befehle aus.

      i. Führen Sie den folgenden Befehl aus: `Enable-PSRemoting`
      ii. Geben Sie in die Bestätigungsmeldung `Y` ein.

   b. Führen Sie in PowerShell den Befehl aus: `Get-ExecutionPolicy`.

      Wenn die Richtlinie nicht auf `RemoteSigned` festgelegt ist, legen Sie sie mit den folgenden Befehlen auf `RemoteSigned` fest.

      i. Führen Sie den folgenden Befehl aus: `Set-ExecutionPolicy RemoteSigned`.
      ii. Geben Sie in die Bestätigungsmeldung `Y` ein.

2. Konfigurieren Sie den Benutzerzugriff auf die Windows Management Instrumentation (WMI). Weitere Informationen finden Sie unter Konfigurieren des Benutzerzugriffs auf WMI.
3. Erteilen Sie Freigabe- und Ordnerberechtigungen zum Schreiben von Dateien in die Posteingangsordner.

   So erteilen Sie Freigabe- und Ordnerberechtigungen für Schreibdateien der DDR-Inbox:

   a. Erteilen Sie an der Configuration Manager-Konsole unter **Verwaltung** dem Nutzer die Berechtigung, auf die **SMS_<Sitecode>**-Freigabe zu schreiben.
   b. Gehen Sie mit **File Explorer** zum freigegebenen Speicherort der **SMS_<sitecode>**-Freigabe, und dann zum Verzeichnis `ddm.box`. Gewähren Sie dem Domänennutzer den Vollzugriff für die folgenden Ordner:
      - **SMS_<sitecode>**
      - Posteingänge
      - `ddm.box`

Konfigurieren des Nutzerzugriffs auf WMI

So konfigurieren Sie den Benutzerzugriff auf WMI im Remote-Modus:

ANMERKUNG: Stellen Sie sicher, dass die Firewall des Systems die WMI-Verbindung nicht blockiert.

1. Geben Sie für den Remote-Zugriff auf das Distributed Component Object Model (DCOM) Berechtigungen für den registrierten MECM-Benutzer an.

   So erteilen Sie DCOM Benutzerberechtigungen:

   a. Starten Sie `dcomcnfg.exe`.
   b. Erweitern Sie im linken Bereich in der **Komponentendienste**-Konsole die Option **Computer**, klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und wählen Sie **Eigenschaften** aus.
   c. Auf **COM-Sicherheit**:
      - Klicken Sie unter **Zugriffsberechtigungen** auf **Limits bearbeiten** und wählen Sie **Remotezugriff** aus.
      - Klicken Sie unter **Start- und Aktivierungsberechtigungen** auf **Limits bearbeiten** und wählen Sie **Lokaler Start**, **Remote-Start** und **Remote-Aktivierung** aus.

2. Um auf die WMI-Komponenten (Windows Management and Instrumentation) von DCOM Config zuzugreifen, müssen Sie dem registrierten Benutzer Benutzerberechtigungen erteilen.

   So erteilen Sie Benutzerberechtigungen für DCOM Config WMI:

   a. Starten Sie `dcomcnfg.exe`.
   b. Erweitern Sie **Arbeitsplatz** > **DCOM Config**.
   c. Klicken Sie mit der rechten Maustaste auf **Windows Management and Instrumentation** und wählen Sie **Eigenschaften** aus.
   d. Klicken Sie auf der Registerkarte **Sicherheit** unter **Start- und Aktivierungsberechtigungen** auf **Bearbeiten** und wählen Sie die Berechtigungen **Remote-Start** und **Remote-Aktivierung** aus.

3. Legen Sie die Namespace-Sicherheit fest und erteilen Sie Berechtigungen.

   So legen Sie die Namespace-Sicherheit fest und erteilen Berechtigungen.

   a. Starten Sie `wmimgmt.msc`
   b. Klicken Sie im Fensterbereich **WMI-Steuerung** mit der rechten Maustaste auf **WMI-Steuerung**, wählen Sie **Eigenschaften** und anschließend die Registerkarte **Sicherheit** aus.

c. Navigieren Sie zu `ROOT\SMS Namespace`.
d. Wählen Sie die Berechtigungen **Methoden ausführen**, **Anbieter-Schreibzugriff**, **Konto aktivieren** und **Remote-Aktivierungsberechtigungen** aus.
e. Navigieren Sie zu `Root\cimv2\OMIMSSC`.
f. Wählen Sie die Berechtigungen **Methoden ausführen**, **Anbieter-Schreibzugriff**, **Konto aktivieren** und **Remote-Aktivierung** aus.
Alternativ dazu wird der Configuration Manager-Benutzer Mitglied der Gruppe **SMS_Admin** und Sie können den bereits vorhandenen Berechtigungen der Gruppe **Remote-Aktivierung** hinzufügen.

Überprüfen der PowerShell-Berechtigungen für die Verwendung der OMIMSSC-Konsolenerweiterung für SCVMM

Überprüfen Sie, ob der **`PSRemoting`**-Status aktiviert ist und **`ExecutionPolicy`** auf **`RemoteSigned`** gesetzt ist. Wenn der Status abweicht, führen Sie die folgenden Schritte in PowerShell aus:

a. Führen Sie in PowerShell den Befehl aus: `PSRemoting`.
Wenn der Befehl `PSRemoting` deaktiviert ist, aktivieren und führen Sie den Befehl `PSRemoting` unter Verwendung der folgenden Befehle aus.
   i. Führen Sie den folgenden Befehl aus: `Enable-PSRemoting`
   ii. Geben Sie in die Bestätigungsmeldung `Y` ein.
b. Führen Sie in PowerShell den Befehl aus: `Get-ExecutionPolicy`.
Wenn die Richtlinie nicht auf `RemoteSigned` festgelegt ist, legen Sie sie mit den folgenden Befehlen auf `RemoteSigned` fest.
   i. Führen Sie den folgenden Befehl aus: `Set-ExecutionPolicy RemoteSigned`.
   ii. Geben Sie in die Bestätigungsmeldung `Y` ein.

Installations- und Aktualisierungsszenarien in OMIMSSC

In diesem Abschnitt finden Sie alle Informationen zur Fehlerbehebung, die sich auf die Installation und Aktualisierung von OMIMSSC beziehen.

Überprüfen der OMIMSSC Appliance-VM-Konfiguration

Um zu überprüfen, ob die OMIMSSC Appliance-VM entsprechend konfiguriert ist, wählen Sie OMIMSSC Appliance-VM aus und klicken Sie mit der rechten Maustaste darauf. Klicken Sie anschließend auf **Einstellungen** und führen Sie dann die folgenden Aufgaben durch:

1. Überprüfen Sie, ob die Zuordnung von Speicher für die OMIMSSC-Appliance der Anforderung entspricht, die in Allgemeine Systemanforderungen für OMIMSSC erwähnt wird. Stellen Sie den entsprechenden Speicher alternativ in **Startwert des RAM** zur Verfügung und klicken Sie auf **Anwenden**.
2. Überprüfen Sie, ob die Prozessoranzahl der Anforderung entspricht, die in Systemanforderungen für OMIMSSC erwähnt wird. Stellen Sie Prozessoranzahl alternativ in **Startwert des RAM** zur Verfügung und klicken Sie auf **Anwenden**.
3. Überprüfen Sie, ob im Feld **Virtuelle Festplatte** unter IDE Controller: **IDE Controller 0** > **Festplatte** die **virtuelle Festplatte** auf die **OMIMSSC-v7-Datei** verweist. Andernfalls klicken Sie auf **Durchsuchen**, navigieren Sie zu dem Speicherort, an dem die VHD-Datei entpackt wurde, wählen Sie die **OMIMSSC-v7-Datei** aus und klicken Sie auf **Anwenden**.
4. Überprüfen Sie, ob **Netzwerkkarte** > **Virtueller Switch** an eine physische NIC-Karte angeschlossen ist, andernfalls konfigurieren Sie die NIC-Karte, und wählen Sie die entsprechende NIC-Karte aus dem Dropdownmenü **Virtueller Switch** aus und klicken Sie auf **Anwenden**.

Wenn die neu erstellte virtuelle Maschine mit der ausgewählten virtuellen Festplatte der OMIMSSC-Appliance nicht mit einer Kernel-Panic-Ausnahme starten kann, bearbeiten Sie die Einstellungen der virtuellen Maschine und aktivieren Sie die Option für den dynamischen Arbeitsspeicher für diese virtuelle Maschine. Führen Sie dazu die folgenden Tasks aus:

1. Klicken Sie mit der rechten Maustaste auf die OMIMSSC Appliance-VM, klicken Sie auf **Einstellungen** und dann auf **Arbeitsspeicher**.

2. Aktivieren Sie unter **Dynamischer Arbeitsspeicher** das Kontrollkästchen **Dynamischen Arbeitsspeicher aktivieren** und geben Sie die Details an.

Registrierungsfehler

Wenn die Testverbindung oder die Registrierung fehlschlägt, wird eine Fehlermeldung angezeigt.

Führen Sie die folgenden Schritte aus, um das Problem zu umgehen:

- Ein Ping von der OMIMSSC-Appliance an den registrierten FQDN des MECM- oder SCVMM-Servers durch Anmelden an der OMIMSSC-Appliance-VM als Benutzer mit Lesezugriff. Wenn es eine Antwort gibt, warten Sie einige Zeit und fahren Sie dann mit der Registrierung fort.

  Um die OMIMSSC-Appliance-VM als Benutzer mit Lesezugriff zu starten, geben Sie den Nutzernamen `readonly` mit demselben Kennwort ein, mit dem Sie sich an der OMIMSSC Appliance-VM anmelden.

- Stellen Sie sicher, dass der MECM- oder SCVMM-Server ausgeführt wird.
- Das zur Registrierung der Konsole verwendete Microsoft-Konto muss ein delegierter Administrator oder ein Administrator in System Center und ein lokaler Administrator für den System Center-Server sein.
- Speziell für SCVMM-Benutzer:
  - Stellen Sie sicher, dass der SCVMM-Server nicht bei einer anderen OMIMSSC-Appliance registriert ist. Wenn Sie denselben SCVMM-Server bei der OMIMSSC-Appliance registrieren möchten, löschen Sie das **OMIMSSC-Registrationsprofil**-Anwendungsprofil des SCVMM-Servers.
  - Wenn Sie das SCVMM-Rollupupdate angewendet haben, überprüfen Sie die Indigo-TCP-Portnummer der SCVMM-Konsole in der Registrierung (`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft System Center Virtual Machine Manager AdministratorConsole\Settings`). Verwenden Sie dieselbe Portnummer, die zum Registrieren der SCVMM-Konsole verwendet wurde. Standardmäßig ist es 8100.

Fehler bei der Testverbindung

Wenn die Benutzernamen gleich sind und die Kennwörter für das Domainbenutzerkonto und das lokale Benutzerkonto unterschiedlich sind, schlägt die Testverbindung zwischen der Microsoft-Konsole und dem OMIMSSC-Gerät fehl.

Das Domainbenutzerkonto lautet beispielsweise: `domain\user1` und das Kennwort ist `pwd1`. Das lokale Benutzerkonto ist `user1` und das Kennwort `Pwd2`. Wenn Sie versuchen, sich mit dem obigen Domainbenutzerkonto zu registrieren, schlägt die Testverbindung fehl.

Verwenden Sie als Problemumgehung unterschiedliche Benutzernamen für die Domainbenutzer und lokalen Benutzerkonten, oder verwenden Sie ein einzelnes Benutzerkonto als lokaler Benutzer und während der Microsoft-Konsolenregistrierung im OMIMSSC-Gerät.

Fehler beim Starten von OMIMSSC nach der Installation der MECM-Konsolenerweiterung

Seit den von MECM 2103 installierten Setups ist der OMIMSSC-Konsolen-Startpunkt in der MECM-Konsole nicht standardmäßig verfügbar.

Deaktivieren Sie als Problemumgehung die Option **Nur Konsolenerweiterungen zulassen, die für die Hierarchie genehmigt wurden** in den Eigenschaften der **Hierarchie-Einstellungen**. *Weitere Informationen finden Sie im Abschnitt zur Configuration Manager-Konsole in der* Microsoft-Dokumentation.

Fehler beim Herstellen der Verbindung zur OMIMSSC-Konsolenerweiterung für SCVMM

Wenn Sie versuchen, OMIMSSC zu starten, nachdem Sie die OMIMSSC-Konsolenerweiterung in der SCVMM-Umgebung registriert und installiert haben, wird der folgende Fehler angezeigt: `Connection to server failed`.

Führen Sie die folgenden Schritte aus, um das Problem zu umgehen:

1. Fügen Sie die IP-Adresse und den vollqualifizierten Domainnamen der OMIMSSC-Appliance in der SCVMM-Konsole ins lokale Intranet hinzu, wenn Sie OMIMSSC starten.
2. Fügen Sie die OMIMSSC-Appliance-IP und den FQDN im DNS bei den Zonen für Vorwärtsauflösung und **Zonen für Rückwärtsauflösung** hinzu.

3. Um weitere Details zu erhalten, überprüfen Sie, ob Fehlermeldungen in der Datei `C:\ProgramData\VMMLogs\AdminConsole` vorhanden sind.

Fehler beim Zugriff auf die Konsolenerweiterung nach der Aktualisierung von SCVMM R2

Wenn Sie nach dem Anwenden des Update Rollups für SC2012 R2 VMM versuchen, die bereits installierte OMIMSSC-Konsole zu öffnen, zeigt SCVMM aus Sicherheitsgründen eine Fehlermeldung an und Sie können nicht auf die OMIMSSC-Konsole zugreifen.

Um dieses Problem zu umgehen, gehen Sie wie folgt vor:

1. Löschen Sie den Ordner am Standardpfad: `C:\Program Files\Microsoft System Center 2012 R2\Virtual Machine Manager\Bin\AddInPipeline\AddIns\<username>`
2. Starten Sie SCVMM neu.
3. Entfernen Sie die Konsolenerweiterung und importieren Sie die Konsolenerweiterung wie im Abschnitt *Importieren der OMIMSSC-Konsolenerweiterung für SCVMM* des *Installationshandbuchs zu Dell EMC OpenManage Integration für Microsoft System Center für System Center Configuration Manager und System Center Virtual Machine Manager* beschrieben.

IP-Adresse nicht dem OMIMSSC-Gerät zugewiesen

Nach dem Erstellen und Starten der OMIMSSC-Geräte-VM wird die IP-Adresse dem OMIMSSC-Gerät nicht zugewiesen oder angezeigt.

Überprüfen Sie als Problemumgehung, ob der virtuelle Switch einem physischen Switch zugeordnet ist, ob der Switch ordnungsgemäß konfiguriert ist, und stellen Sie dann eine Verbindung zum OMIMSSC-Gerät her.

SCVMM stürzt während des Importierens der OMIMSSC-Konsolenerweiterung ab

Die Administratorkonsole von SC2016 VMM RTM Build 4.0.1662.0 kann beim Importieren der OMIMSSC-Konsolenerweiterung abstürzen.

Aktualisieren Sie als Problemumgehung SCVMM gemäß dem KB-Artikel 4094925, der unter `support.microsoft.com/kb/4094925` verfügbar ist, und importieren Sie anschließend die OMIMSSC-Konsolenerweiterung.

Fehler bei der Anmeldung an OMIMSSC-Konsolenerweiterungen

Die Anmeldung der OMIMSSC-Konsolenerweiterung schlägt mit der folgenden Fehlermeldung fehl: `Failed to login. Ensure to use correct credentials or check if account is locked in Active Directory.`

Um dieses Problem zu umgehen, stellen Sie sicher, dass Sie die korrekten Zugangsdaten verwenden, und stellen Sie sicher, dass das Konto nicht in Active Directory gesperrt ist. Wenn ein Konto in Active Directory gesperrt war, versuchen Sie es nach einigen Minuten erneut, basierend auf der Richtlinie zur Active Directory-Kontosperrung. Weitere Informationen zu Active Directory-Kontosperrungsrichtlinien finden Sie in der Microsoft-Dokumentation.

SC2012 VMM SP1 stürzt während der Aktualisierung ab

Nach dem Upgrade auf SC2012 VMM SP1 stürzt beim Import der OMIMSSC-Konsolenerweiterung in SC2012 VMM UR5 oder höher die SCVMM-Konsole ab.

Informationen zu diesem Problem und zur Behebung des Problems finden Sie unter Problem 5 der Knowledge Base-URL: `support.microsoft.com/kb/2785682`.

Aktualisieren Sie als Problemumgehung SCVMM unabhängig von der Version des installierten Updaterollups.

OMIMSSC Admin-Portal-Szenarien

Dieser Abschnitt enthält alle Informationen zur Fehlerbehebung im Zusammenhang mit dem OMIMSSC-Admin-Portal

Fehlermeldung beim Zugriff auf das OMIMSSC-Admin-Portal über den Mozilla Firefox-Browser

Wenn Sie mit dem Mozilla Firefox-Browser auf das OMIMSSC-Admin-Portal zugreifen, wird die folgende Warnmeldung angezeigt: "`Secure Connection Failed`".

Um dieses Problem zu umgehen, löschen Sie das Zertifikat, das von einem vorherigen Eintrag des Verwaltungsportals im Browser erstellt wurde. Weitere Informationen zum Löschen eines Zertifikats aus dem Mozilla Firefox-Browser finden Sie unter `support.mozilla.org`

Fehler beim Anzeigen des Dell EMC Logos im OMIMSSC-Verwaltungsportal

Wenn das OMIMSSC-Verwaltungsportal mit einem Standard-IE-Browser von Windows 2016 gestartet wird, wird das Verwaltungsportal nicht mit dem Dell EMC Logo angezeigt.

Um dieses Problem zu umgehen, gehen Sie wie folgt vor:

- Aktualisieren Sie den IE-Browser auf die neueste Version.
- Löschen Sie den Browserverlauf und fügen Sie die URL des OMIMSSC-Verwaltungsportals zur Favoritenliste des Browsers hinzu.

Szenarien für Ermittlung, Synchronisierung und Inventarisierung in OMIMSSC

In diesem Abschnitt finden Sie alle Informationen zur Problembehandlung im Zusammenhang mit Anmeldeinformationen, zum Erkennen von Servern, zum Gruppieren von Servern und zum Synchronisieren der registrierten Microsoft-Konsole in OMIMSSC bei Verwendung von OMIMSSC.

Fehler beim Ermitteln der Server

Wenn mehrere Microsoft-Konsolen bei einer OMIMSSC-Appliance registriert sind und Sie versuchen, einen Server zu ermitteln, auch wenn eine der SCCM-Konsolen nicht erreichbar ist, schlägt der Job zur Serverermittlung fehl.

Deaktivieren Sie als Problemumgehung die MECM-Konsole, die nicht erreichbar ist, oder beheben Sie die Fehler und stellen Sie sicher, dass die MECM-Konsole über das OMIMSSC-Gerät erreichbar ist.

Fehler beim automatischen Erkennen von iDRAC-Servern

Die automatische Ermittlung von iDRAC-Servern schlägt fehl, wenn das festgelegte Kennwort der standardmäßigen Geräte-Zugangsdaten nicht stark genug ist.

Um dieses Problem zu umgehen, stellen Sie sicher, dass Sie ein sicheres Kennwort festlegen. Weitere Informationen zu den Anforderungen an die Passwortrichtlinie finden Sie im iDRAC-Benutzerhandbuch.

Ermittelte Server werden nicht der Sammlung "Alle Dell Lifecycle Controller Server" hinzugefügt

Nach dem Ermitteln der Server in der OMIMSSC-Konsolenerweiterung für MECM wird der Server möglicherweise nicht der Sammlung **Alle Dell Lifecycle Controller-Server** hinzugefügt.

Löschen Sie als Problemumgehung die Sammlung **Alle Dell Lifecycle Controller-Server** und ermitteln Sie den Server. Die Sammlung wird automatisch in MECM erstellt und der Server wird dieser Gruppe hinzugefügt.

Fehler beim Ermitteln der Server aufgrund falscher Zugangsdaten

Wenn Sie während der Erkennung falsche Anmeldeinformationsdaten angeben, sind basierend auf der iDRAC-Version die folgenden Auflösungen verfügbar:

- Wenn Sie bei der Ermittlung von PowerEdge-Servern der 12. Generation mit einer iDRAC-Version ab 2.10.10.10 falsche Details im Zugangsdatenprofil angeben, schlägt die Serverermittlung mit dem folgenden Verhalten fehl:
  - Beim ersten Fehlversuch wird die Server-IP-Adresse nicht blockiert.
  - Beim zweiten Fehlversuch wird die Server-IP-Adresse 30 Sekunden lang blockiert.
  - Ab dem dritten Fehlversuch wird die Server-IP-Adresse 60 Sekunden lang blockiert.

  Sie können die Serverermittlung mit den richtigen Zugangsdatenprofildetails erneut versuchen, nachdem die IP-Adresse entsperrt ist.
- Wenn das Standard-iDRAC-Zugangsdatenprofil geändert wird, nachdem ein Server im Gerät erkannt und hinzugefügt wurde, kann auf dem Server keine Aktivität ausgeführt werden. Um mit dem Server zu arbeiten, ermitteln Sie den Server mit dem neuen Zugangsdatenprofil erneut.

Erstellung einer falschen VRTX-Gehäusegruppe nach der Servererkennung

Wenn modulare Server, die sich zuvor in einem anderen Gehäuse befanden, einem VRTX-Gehäuse hinzugefügt und in OMIMSSC erkannt werden, enthalten die modularen Server die vorherigen Gehäuse-Service-Tag-Informationen. Daher wird im Gerät eine VRTX-Gehäusegruppe mit alten Gehäuseinformationen anstelle der neuesten Gehäuseinformationen erstellt.

Um dieses Problem zu umgehen, gehen Sie wie folgt vor:

1. Aktivieren Sie CSIOR und setzen Sie den iDRAC auf dem neu hinzugefügten modularen Server zurück.
2. Löschen Sie manuell alle Server der VRTX-Gehäusegruppe, und ermitteln Sie die Server anschließend erneut.

Synchronisieren von Hostservern mit registriertem MECM nicht möglich

Während der Synchronisierung der OMIMSSC-Konsolenerweiterung mit registriertem MECM werden die Server nicht als Unteraufgaben im Synchronisations-Job aufgeführt und daher nicht synchronisiert.

Um dieses Problem zu umgehen, starten Sie die MECM-Konsole mit der Berechtigung „als Administrator ausführen“ und aktualisieren Sie die Out-of-band-Konfiguration für einen Server. Synchronisieren Sie dann die OMIMSSC-Konsolenerweiterung mit registriertem MECM.

Weitere Informationen finden Sie im Thema „Synchronisieren mit der registrierten Microsoft-Konsole“ im *Einheitlichen Benutzerhandbuch zu OpenManage Integration für Microsoft System Center Version 7.3 für Microsoft Endpoint Configuration Manager and System Center Virtual Machine Manager*.

Leere Cluster-Aktualisierungsgruppe wird bei automatischer Ermittlung oder Synchronisierung nicht gelöscht

Wenn ein Cluster in OMIMSSC erkannt wird, wird im **Wartungscenter** eine Clusteraktualisierungsgruppe mit allen in der Clusteraktualisierungsgruppe aufgeführten Servern erstellt. Wenn später alle Server über SCVMM aus diesem Cluster entfernt werden und eine automatische Erkennung oder Synchronisierung mit SCVMM durchgeführt wird, wird die leere Clusteraktualisierungsgruppe nicht im **Wartungscenter** gelöscht.

Um dieses Problem zu umgehen, löschen Sie die leere Servergruppe, und ermitteln Sie die Server erneut.

Fehler beim Erstellen des Clusters während der Anwendung von Clusterfunktionen

Wenn die Clustererstellung auf Knoten während der Anwendung von Clusterfunktionen fehlschlägt und die Bereitstellung des Betriebssystems erfolgreich ist. Während der Clustererstellung wird die Fehlermeldung `Failed to install the features on`

`hosts that are required for creating clusters` angezeigt und die Protokolle werden angezeigt, `Failed to run Pre Cluster Creation Scripts on Host Create Cluster`.

Um dieses Problem zu umgehen, stellen Sie sicher, dass die **Zugangsdaten für den Computer-Zugang**, die im **physischen Computer-Profil** ausgewählt sind und für die Clustererstellung verwendet werden, mit dem registrierten Benutzer identisch sind. Der registrierte Benutzer sollte entweder ein Domänenadministrator oder ein Domänennutzer mit Berechtigungen zum Hinzufügen von Systemen zur Domäne sein.

Status des Cluster-fähigen Aktualisierungsjobs kann nicht abgerufen werden

Wenn der Status des Cluster-fähigen Aktualisierungsjobs die Fertigstellung des Aktualisierungsjobs veröffentlicht.

Um dieses Problem zu umgehen, überprüfen Sie den Job-Status mit Microsoft Failover Cluster-Verwaltungstool und stellen Sie sicher, dass Sie mit OMIMSSC erstellte Dateien in SCVMM-Server nach Abschluss des Jobs löschen.

Fehler beim Ausführen von auf Wartungstasks bezogenen Tasks auf neu erkannten Servern

Wenn Sie einen Server oder alle Server in einer Aktualisierungsgruppe aus OMIMSSC löschen und diese erneut ermitteln, können Sie keine anderen Vorgänge auf diesen Servern ausführen, wie Firmware-Aktualisierung, Exportieren und Importieren von LC-Protokollen, Exportieren und Importieren von Serverprofilen.

Um dieses Problem zu umgehen, führen Sie nach der erneuten Ermittlung des oder der gelöschten Server die Firmwareupdates mithilfe der Funktion **Betriebsvorlage bereitstellen** in der **Serveransicht** aus. Für andere Wartungsszenarien verwenden Sie iDRAC.

Generische Szenarien in OMIMSSC

Dieser Abschnitt enthält Informationen zur Behebung von Fehlern, die unabhängig von den Workflows in OMIMSSC sind.

Fehler beim Zugriff auf die CIFS-Freigabe über den Hostnamen

Die modularen Server können nicht über den Hostnamen auf die CIFS-Freigabe zugreifen, um einen Job in OMIMSSC auszuführen.

Geben Sie als Problemumgehung die IP-Adresse des Servers mit der CIFS-Freigabe anstelle des Hostnamens an.

Fehler beim Anzeigen der Seite "Jobs und Protokolle" in der Konsolenerweiterung

Die Seite **Jobs- und Protokollcenter** wird in OMIMSSC-Konsolenerweiterungen nicht angezeigt.

Registrieren Sie als Problemumgehung die Konsole erneut, und starten Sie die Seite **Jobs und Protokolle**.

Fehlgeschlagene Vorgänge auf verwalteten Systemen

Aufgrund einer TLS-Version (Transport Layer Security) funktionieren auf den verwalteten Systemen alle Funktionen von OMIMSSC nicht wie erwartet.

Wenn Sie die iDRAC-Firmware Version 2.40.40.40 oder höher verwenden, ist TLS (Transport Layer Security)-Versionen 1.1 oder später standardmäßig aktiviert. Installieren Sie vor der Installation der Konsolenerweiterung die Aktualisierung, um TLS 1.1 oder höher zu aktivieren, wie im folgenden KB-Artikel beschrieben: `Support.microsoft.com/de-de/kb/3140245`. Es wird empfohlen, die Unterstützung für TLS 1.1 oder höher auf Ihrem SCVMM-Server und der SCVMM-Konsole zu aktivieren, um sicherzustellen, dass OMIMSSC wie erwartet funktioniert. Weitere Informationen zu iDRAC finden Sie unter Dell.com/idracmanuals.

Fehler beim Starten der Online-Hilfe für OMIMSSC

Bei Verwendung des Betriebssystems Windows 2012 R2 wird der Inhalt der kontextabhängigen Online-Hilfe mit einer Fehlermeldung angezeigt.

Aktualisieren Sie als Lösung das Betriebssystem mit den neuesten KB-Artikeln und zeigen Sie dann die Online-Hilfe an.

OMIMSSC Fehlschlagen von Jobs aufgrund eines nicht unterstützten Kennworts für die Netzwerkfreigabe

Einige OMIMSSC-Jobs schlagen fehl, da einige der Sonderzeichen im Netzwerkfreigabe-Kennwort nicht von iDRAC unterstützt werden.

Im folgenden finden Sie eine Liste der fehlgeschlagenen Jobs und die Fehlermeldungen im Zusammenhang mit dem jeweiligen Job:

- LC-Protokolle konnten nicht exportiert werden - `Failed to Export Complete LC Logs from iDRAC IP <IP address> Cannot access network share`
- Fehler bei der Bereitstellung von RHEL- und ESXi-Betriebssystemen: `Inaccessible network share`
- Fehler beim Aktualisieren der Firmware mithilfe von DRM -`Firmware update failed on server with iDRAC IP <IP address> for <Component>`
- Fehler beim Bereitstellen des Windows-Betriebssystems – `Inaccessible network share for iDRAC <IP address>`
- Fehler beim Export und Import des Serverprofils – `Failed to invoke Export Server Profile on iDRAC IP: <iDRAC_IP> with error Cannot Access Network Share`

Um dieses Problem zu umgehen, stellen Sie sicher, dass Sie ein für iDRAC empfohlenes Kennwort für die Netzwerkfreigabe verwenden. Nähere Informationen erhalten Sie in der iDRAC-Dokumentation.

Firmwareupdateszenarien in OMIMSSC

Dieser Abschnitt enthält alle Informationen zur Fehlerbehebung im Zusammenhang mit Aktualisierungsquellen, dem Aktualisieren von Gruppen, Repositories und Bestandsaufnahmen nach Aktualisierungen.

Fehler bei der Testverbindung für lokale Aktualisierungsquelle

Nachdem Sie die Details einer lokalen Aktualisierungsquelle überprüft haben, schlägt die Testverbindung möglicherweise fehl, da eventuell nicht auf die erforderlichen Dateien zugegriffen werden kann.

Stellen Sie als Problemumgehung sicher, dass die Datei `catalog.gz` in der folgenden Ordnerstruktur vorhanden ist.

- Für lokale DRM-Aktualisierungsquelle: `\\IP address\\catalog\<catalogfile>.gz`

Fehler beim Erstellen der DRM-Aktualisierungsquelle

Das Erstellen einer DRM-Aktualisierungsquelle auf einem Verwaltungsserver, der unter Windows 10 ausgeführt wird, schlägt möglicherweise fehl und es wird die folgende Fehlermeldung angezeigt: `Failed to reach location of update source. Please try again with correct location and/or credentials.`

Weitere Informationen finden Sie im Protokoll **omimsscappliance_main** im OMIMSSC-Verwaltungsportal, wenn folgende Fehlermeldung angezeigt wird: *`Unix command failed SmbException: com.dell.pg.tetris.business.samba.smbclient.SmbException: session setup failed: NT_STATUS_IO_TIMEOUTwhere EnableSMB1Protocol = false.`*

Um dieses Problem zu umgehen, lesen Sie den folgenden KB-Artikel: *support.microsoft.com/de-de/help/4034314*

Fehler beim Erstellen des Repositorys während der Firmware-Aktualisierung

Die Erstellung eines Repositorys kann während einer Firmware-Aktualisierung aufgrund falscher Anmeldeinformationen fehlschlagen, die beim Erstellen einer Aktualisierungsquelle angegeben wurden, oder das OMIMSSC-Gerät kann keine Aktualisierungsquelle aufrufen.

Stellen Sie als Problemumgehung sicher, dass die Aktualisierungsquelle von dort aus erreichbar ist, wo das OMIMSSC-Gerät gehostet wird, und geben Sie beim Erstellen einer Aktualisierungsquelle die korrekten Anmeldeinformationen an.

Fehler beim Aktualisieren der Firmware von Clustern

Nachdem in OMIMSSC ein Job zum Aktualisieren der Firmware von Clustern übergeben wurde, werden die Cluster aus bestimmten Gründen nicht aktualisiert. In den **Aktivitätsprotokollen** werden die folgenden Fehlermeldungen angezeigt.

```
Cluster Aware Update failed for cluster group <cluster group name>.
```

```
Failed to perform Cluster Aware Update for cluster group <cluster group name>.
```

ANMERKUNG: Die Aktionen des Cluster Aware Updates werden an folgenden Speicherorten protokolliert: \ \ < SCVMM CIFS-Freigabe > \OMIMSSC_UPDATE\reports Ordner, in dem der Cluster-Aware-Update-Bericht gespeichert wird. Der \\SCVMM-CIFS-share\OMIMSSC_UPDATE\reports\log Ordner enthält außerdem die Dell EMC System Update (DSU) Plug-in-Protokolle für jeden Knoten. Erweiterte Skript-Protokolle sind unter C:\Window\Temp verfügbar, der aus precau.log- und postcau.log-Dateien in jedem Cluster-Knoten für das Windows Server HCI-Cluster besteht.

Ursachen für eine fehlgeschlagene Firmwareaktualisierung auf Clustern mit der folgenden Problemumgehung:

- Wenn die erforderlichen DUPs und Katalogdateien nicht in der ausgewählten lokalen Aktualisierungsquelle vorhanden sind.

  Als Problemumgehung können Sie sicherstellen, dass alle erforderlichen DUPs und Katalogdateien im Repository verfügbar sind und anschließend die Firmware der Cluster aktualisieren.

- Die Clustergruppe reagiert nicht mehr oder der Firmwareaktualisierungsjob wurde in CAU aufgrund eines laufenden Jobs abgebrochen. Anschließend werden die DUPs heruntergeladen und in jeden zur Clustergruppe gehörenden Serverclusterknoten platziert.

  Löschen Sie als Problemumgehung alle Dateien im Ordner Dell und aktualisieren Sie anschließend die Firmware der Cluster.

- Wenn der Lifecycle Controller (LC) mit anderen Vorgängen beschäftigt ist, schlägt der Firmwareaktualisierungstask auf einem Cluster-Knoten fehl. Um zu überprüfen, ob die Aktualisierung fehlgeschlagen ist, weil der LC-Server beschäftigt ist, überprüfen Sie die folgenden Fehlermeldungen in jedem Knoten des Clusters unter folgendem Pfad: `C:\dell\suu\invcolError.log`

  ```
  Inventory Failure: IPMI driver is disabled. Please enable or load the driver and then
  reboot the system.
  ```

  Fahren Sie als Problemumgehung den Server herunter, entfernen Sie die Stromkabel und starten Sie den Server neu. Aktualisieren Sie nach dem Neustart die Firmware der Cluster.

ANMERKUNG: Um weitere Informationen zu einem CAU-Fehler zu erhalten, überprüfen Sie den Status der Funktion im Verwaltungstool von Windows-Failover-Cluster und lesen Sie den Abschnitt der Microsoft-Dokumentation mit den Best Practices für clusterfähige Aktualisierungen.

Fehler bei der Firmware-Aktualisierung wegen belegter Job-Warteschlange

Ein von OMIMSSC an iDRAC übermittelter Firmware-Aktualisierungsjob schlägt fehl und das OMIMSSC-Hauptprotokoll zeigt den folgenden Fehler an: `JobQueue Exceeds the size limit. Delete unwanted JobID(s).`

Löschen Sie als Problemumgehung manuell die abgeschlossenen Jobs in iDRAC und wiederholen Sie den Firmware-Aktualisierungsjob. Weitere Informationen zum Löschen von Jobs in iDRAC finden Sie in der iDRAC-Dokumentation unter **dell.com/support/home**.

Fehler bei der Firmwareaktualisierung unter Verwendung der DRM-Aktualisierungsquelle

Der Firmwareaktualisierungsjob schlägt möglicherweise fehl, wenn Sie eine DRM-Aktualisierungsquelle mit unzureichendem Zugriff auf die Freigabeordner verwenden. Wenn das beim Erstellen der DRM-Aktualisierungsquelle bereitgestellte Windows-Zugangsdatenprofil nicht Teil der Domainadministratorgruppe oder der lokalen Administratorgruppe ist, wird die folgende Fehlermeldung angezeigt: `Local cache creation failure`.

Um dieses Problem zu umgehen, gehen Sie wie folgt vor:

1. Klicken Sie nach der Erstellung des Repositorys im DRM mit der rechten Maustaste auf den Ordner; klicken Sie anschließend auf die Registerkarte **Sicherheit** und dann auf **Erweitert**.
2. Klicken Sie auf **Vererbung aktivieren** und wählen Sie die Option **Alle untergeordneten Objektberechtigungseinträge durch vererbbare Berechtigungseinträge aus diesem Objekt ersetzen** und geben Sie dann den Ordner mit Lese- und Schreibzugriff für **Jeden** frei.

Firmwareaktualisierung für Komponenten unabhängig von der Auswahl

Dieselben Komponenten auf identischen Servern werden während einer Firmwareaktualisierung unabhängig von der Auswahl der Komponenten auf diesen einzelnen Servern aktualisiert. Dieses Verhalten wird bei der 12. und 13. Generation von PowerEdge-Servern mit Enterprise-Lizenz von iDRAC beobachtet.

Um dieses Problem zu umgehen, gehen Sie wie folgt vor:

- Wenden Sie zunächst Aktualisierungen für gemeinsame Komponenten auf identischen Servern an und wenden Sie dann Aktualisierungen für bestimmte Komponenten auf einzelnen Servern an.
- Führen Sie stufenweise Aktualisierungen mit geplanten Ausfallzeiten durch, um die erforderliche Firmwareaktualisierung umzusetzen.

Benutzerdefinierte Aktualisierungsgruppe kann nicht gelöscht werden

Wenn nach dem Planen eines Jobs auf einem Server, der zu einer benutzerdefinierten Aktualisierungsgruppe gehört, der Server von der Microsoft-Konsole gelöscht wird und Sie die registrierte Microsoft-Konsole mit OMIMSSC synchronisieren, wird der Server aus der benutzerdefinierten Aktualisierungsgruppe entfernt und in eine vordefinierte Aktualisierungsgruppe verschoben. Sie können eine solche benutzerdefinierte Aktualisierungsgruppe nicht löschen, da sie einem geplanten Job zugeordnet ist.

Löschen Sie als Problemumgehung den geplanten Job von der Seite **Jobs und Protokolle** und löschen Sie dann die benutzerdefinierte Aktualisierungsgruppe.

Fehler beim Aktualisieren des WinPE-Images

Wenn Sie versuchen, das WinPE-Abbild zu aktualisieren, schlägt der Aktualisierungsauftrag möglicherweise mit der folgenden Fehlermeldung fehl: `Remote connection to console failed.`

Führen Sie als Problemumgehung den Befehl **DISM** aus, um alle zuvor bereitgestellten Abbilder in der Microsoft-Konsole zu bereinigen, und versuchen Sie dann erneut, das WinPE-Abbild zu aktualisieren.

Ändern der Glockenfarbe der Statusabfragen und Benachrichtigungen nach der Aktualisierung der Häufigkeit

Wenn ein verwalteter Server in OMIMSSC nicht erkannt wird und Sie die Häufigkeit der Abruf- und Benachrichtigungsoption ändern, wird die Farbe der Glocke nach einiger Zeit gelb, auch wenn der Katalog keine Änderungen enthält.

Ermitteln Sie als Problemumgehung verwaltete Server und ändern Sie dann die Häufigkeit der Abfrage- und Benachrichtigungsoption.

Betriebssystembereitstellungsszenarien in OMIMSSC

Dieser Abschnitt enthält alle Informationen zur Fehlerbehebung im Zusammenhang mit der Betriebssystem- oder (für SCVMM) Hypervisor-Bereitstellung mit der Betriebsvorlage in OMIMSSC.

Allgemeine Szenarien für die Betriebssystembereitstellung

Dieser Abschnitt enthält alle allgemeinen Informationen zur Problembehandlung, die sich auf die Betriebssystembereitstellung beziehen.

Fehler beim Bereitstellen der Betriebsvorlage

Nach der Bereitstellung der Betriebsvorlage auf den ausgewählten Servern sind die Attribute oder Attributwerte nicht für die ausgewählte CSV-Datei geeignet oder die iDRAC-IP- oder iDRAC-Berechtigungsnachweise werden aufgrund der Konfigurationen in der Vorlage geändert. Der Job in iDRAC ist erfolgreich. Der Status dieses Jobs in OMIMSSC wird jedoch aufgrund einer ungültigen CSV-Datei als "nicht erfolgreich" oder als "fehlgeschlagen" angezeigt oder der Job kann aufgrund der iDRAC-Änderungen auf dem Zielserver nicht verfolgt werden.

Stellen Sie als Problemumgehung sicher, dass die ausgewählte CSV-Datei über die richtigen Attribute und Attributwerte verfügt, und dass sich die IP-Adresse oder die Anmeldeinformationen von iDRAC nicht aufgrund der Konfigurationen in der Vorlage ändern.

Fehler beim Speichern einer Betriebsvorlage

Wenn Sie beim Erstellen einer Betriebsvorlage das Kontrollkästchen eines abhängigen Attributs mit einem Poolwert wählen und deaktivieren, können Sie die Betriebsvorlage mit der folgenden Fehlermeldung nicht speichern:

```
Select atleast one attribte, under the selected components, before creating the Operational
Template.
```

Führen Sie als Problemumgehung eine der folgenden Aktionen aus:

- Wählen Sie ein anderes abhängiges Attribut mit einem Poolwert oder das gleiche abhängige Attribut aus und speichern Sie die Betriebsvorlage.
- Erstellen Sie eine neue Betriebsvorlage.

Fehler bei der Bereitstellung des Betriebssystems Windows Servers 2016 auf AMD-Servern

Die Bereitstellung des Betriebssystems Windows Server 2016 auf AMD-Plattformen bietet keine Unterstützung für x2apic. Die Bereitstellung des Betriebssystems schlägt daher fehl.

Um dieses Problem zu umgehen, bearbeiten Sie die Betriebsvorlage, die für die Bereitstellung verwendet wird, wählen Sie die BIOS-Komponente aus und deaktivieren Sie BIOS-x2apic und die logischen Prozessoreinstellungen. Wiederholen Sie die Bereitstellung mithilfe dieser Vorlage. Weitere Informationen finden Sie im KB-Artikel Dell EMC AMD Server bleibt bei Anzeige des Windows-Logos während der Installation von Windows Server 2016 hängen.

Szenarien zur Betriebssystembereitstellung für MECM-Benutzer

In diesem Abschnitt finden Sie alle Informationen zur Problembehandlung, die sich auf die Betriebssystembereitstellung mit OMIMSSC in der MECM-Konsole beziehen.

Bereitstellungsoption in Tasksequenz nicht sichtbar

Die Option **Bereitstellen** wird in einer vorhandenen Tasksequenz nicht angezeigt, nachdem die OMIMSSC-Konsolenerweiterung für MECM deinstalliert und erneut installiert wurde.

Öffnen Sie als Problemumgehung die Tasksequenz zur Bearbeitung, aktivieren Sie die Option **Anwenden** erneut und klicken Sie auf **OK**. Die Option **Bereitstellen** wird erneut angezeigt.

So aktivieren Sie erneut die Option **Anwenden**:

1. Klicken Sie mit der rechten Maustaste auf die Tasksequenz und wählen Sie **Bearbeiten** aus.
2. Wählen Sie **Neustart mit Windows PE ausführen**. Geben Sie im Abschnitt **Beschreibung** ein beliebiges Zeichen ein und löschen Sie es, damit die Änderung nicht gespeichert wird.
3. Klicken Sie auf **OK**.

   Hierdurch wird die Option **Anwenden** erneut aktiviert.

Fehler beim Hinzufügen von Servern zur Sammlung "Managed Lifecycle Controller Lifecycle Controller (ESXi)" in MECM

Wenn die DHCP-Suche während der Bereitstellung des Betriebssystems fehlschlägt, kommt es zu einer Zeitüberschreitung für den Server, und der Server wird nicht in die Sammlung "Managed Lifecycle Controller Lifecycle Controller (ESXi)" in MECM verschoben.

Installieren Sie als Problemumgehung den MECM-Clientserver und führen Sie dann eine Synchronisierung durch, um die Server der Sammlung "Managed Lifecycle Controller Lifecycle Controller (ESXi)" hinzuzufügen.

Fehler bei der Bereitstellung des Windows Betriebssystems auf iDRAC 9-basierten PowerEdge-Servern

Die Bereitstellung des Windows-Betriebssystems schlägt auf iDRAC 9-basierten PowerEdge-Servern fehl, die sich im UEFI-Startmodus befinden.

Um dieses Problem zu umgehen, fügen Sie eine Verzögerung in der Datei Winpeshl.ini hinzu, die im Verzeichnis C:\Program Files\Microsoft Configuration Manager\OSD\bin\x64 gefunden werden kann. Weitere Informationen finden Sie unter dem Link des Microsoft-Forums *Betriebssystem-Bereitstellung – Tasksequenz kann nicht gelesen werden. Wpelnit.exe wird nicht automatisch gestartet*.

Szenarien zur Betriebssystembereitstellung für SCVMM-Benutzer

In diesem Abschnitt finden Sie alle Informationen zur Problembehandlung im Zusammenhang mit der Hypervisor-Bereitstellung in OMIMSSC über die SCVMM-Konsole.

Hypervisor-Bereitstellungsfehler aufgrund von LC oder Firewall-Schutz

Die Hypervisor-Bereitstellung schlägt fehlt und zeigt die folgende Fehlermeldung im Aktivitätsprotokoll an: `Error New-SCVMHost failed with following error : An out of band operation (SMASH) for the BMC <IP ADDRESS> failed on IDRAC IP : <IP ADDRESS>.`

Dieser Fehler kann aus einem der folgenden Gründe auftreten:

- Dell Lifecycle Controller-Status ist ungültig

  Melden Sie sich zur Lösung des Problems an der iDRAC-Benutzeroberfläche an, und setzen Sie Lifecycle Controller zurück.

  Wenn das Problem nach dem Zurücksetzen des Lifecycle Controllers weiterhin auftritt, versuchen Sie, das Problem mit den folgenden Schritten zu lösen:

- Virenschutz oder Firewall verhindern möglicherweise die erfolgreiche Ausführung des `WINRM`-Befehls.

  Weitere Informationen finden Sie im folgenden KB-Artikel. `support.microsoft.com/kb/961804`

Hypervisor-Bereitstellungsfehler aufgrund von weiterhin vorhandenen Treiberdateien in der Bibliotheksfreigabe

Die Hypervisor-Bereitstellung schlägt fehlt und zeigt die folgende Fehlermeldung im Aktivitätsprotokoll an:

- **Error**: `Error while applying Hypervisor Profile to host <IP Address>. Failed with error : For input string: ""`
- **Information**: `Successfully deleted drivers from library share sttig.<MicrosoftConsoleName>.com for <server uuid>`
- **Error**: `Deleting staging share (drivers) for <server uuid> failed.`

Diese Fehler können aufgrund von Ausnahmebedingungen des VMM-Befehls `GET-SCJOB status` auftreten und die Treiberdateien bleiben in der Bibliotheksfreigabe erhalten. Bevor Sie es erneut versuchen oder eine andere Hypervisor-Bereitstellung durchführen, müssen Sie diese Dateien aus der Bibliotheksfreigabe entfernen.

So entfernen Sie Dateien aus der Bibliotheksfreigabe: Anschließend können Sie die Hypervisors bereitstellen.

1. Wählen Sie in der SCVMM-Konsole die Option **Bibliothek** > **Bibliotheksserver** aus, und wählen Sie dann den IG-Server aus, der als Bibliotheksserver hinzugefügt wurde.
2. Wählen Sie im Bibliotheksserver die Bibliotheksfreigabe aus, und löschen Sie sie.
3. Nachdem die Bibliotheksfreigabe gelöscht wurde, stellen Sie eine Verbindung mit der IG-Freigabe über `\\<Integration Gateway server>\LCDriver\` her.
4. Löschen Sie den Ordner mit den Treiberdateien.

SCVMM-Fehler 21119 beim Hinzufügen von Servern zu Active Directory

Beim Hinzufügen von Servern zu Active Directory wird der SCVMM-Fehler 21119 angezeigt. `Error 21119: The physical computer with <SMBIOS GUID> did not join Active Directory in time. The comptuer was expected to join Active Directory using the computer name <host.domain>.`

Um dieses Problem zu umgehen, gehen Sie wie folgt vor:

1. Warten Sie einige Zeit, um zu sehen, ob der Server zu Active Directory hinzugefügt wird.
2. Wenn der Server nicht zu Active Directory hinzugefügt wird, fügen Sie den Server manuell zu Active Directory hinzu.
3. Fügen Sie den Server zu SCVMM hinzu.
4. Nachdem der Server zu SCVMM hinzugefügt wurde, führen Sie eine Neuermittlung des Servers in OMIMSSC durch.

   Der Server wird jetzt auf der Registerkarte **Host** aufgelistet.

Erstellungsszenario zu Windows Server HCI-Cluster für SCVMM-Benutzer

In diesem Abschnitt finden Sie alle Informationen zur Problembehandlung, die sich auf das Erstellen von Windows Server HCI in OMIMSSC in der SCVMM-Konsole beziehen.

Der Funktionszustand des Windows Servers HCI-Clusters ist unbekannt.

Wenn Sie einen Windows Server HCI-Cluster auf Knoten erstellen, die Teil eines vorhandenen Clusters waren, weisen der Storage-Pool und die Festplattenkonfigurationen die Konfigurationen des vorhandenen Clusters auf. Daher wird der Cluster-Storage-Pool möglicherweise nicht erstellt. Wenn der Cluster-Storage-Pool erstellt wird, wird der Integritätsstatus möglicherweise als unbekannt angezeigt.

Löschen Sie als Problemumgehung den Storage-Pool und die Festplattenkonfiguration mit den vorhandenen Clusterdetails, und erstellen Sie dann den Windows Server HCI-Cluster. Weitere Informationen zum Löschen des Storage-Pools finden Sie in der Microsoft-Dokumentation im Abschnitt *Fehlerbehebung Windows Server HCI-Funktionsstatus und Betriebsstatus*.

Serverprofilszenarien in OMIMSSC

In diesem Abschnitt finden Sie alle Informationen zur Fehlerbehebung, die sich auf das Exportieren und Importieren der Serverprofile in OMIMSSC beziehen.

Serverprofile werden nicht exportiert

Nachdem Sie einen Job zum Exportieren eines Serverprofils geplant haben, wird das Serverprofil nicht exportiert und die Fehlermeldung `The selectors for the resource are not valid` angezeigt.

Um dieses Problem zu umgehen, setzen Sie iDRAC zurück und planen Sie den Job zum Exportieren eines Serverprofils. Nähere Informationen erhalten Sie in der iDRAC-Dokumentation unter `dell.com/support`.

Zeitüberschreitung beim Importieren des Serverprofils nach zwei Stunden

Nach dem Senden eines Jobs zum Serverprofil-Import in OMIMSSC tritt nach Ablauf von zwei Stunden eine Zeitüberschreitung ein.

Führen Sie die folgenden Schritte aus, um das Problem zu umgehen:

1. Starten Sie den Server, drücken Sie F2 und gehen Sie dann zu den **BIOS-Einstellungen**.
2. Klicken Sie auf **System-Setup** und wählen Sie **Verschiedene Einstellungen** aus.
3. Deaktivieren Sie **Bei Fehler F1/F2-Eingabeaufforderung**.

Nachdem Sie die folgenden Schritte ausführen, exportieren Sie das Serverprofil erneut und verwenden Sie das gleiche Serverprofil für den Import auf diesen Server.

LC-Protokollszenarien in OMIMSSC

In diesem Abschnitt finden Sie alle Informationen zur Behebung von Fehlern, die sich auf das Exportieren und Anzeigen von LC-Protokollen beziehen.

Fehler beim Exportieren von LC-Protokollen im CSV-Format

Wenn Sie versuchen, die LC-Protokolldateien in das CSV-Format herunterzuladen, schlägt der Downloadvorgang fehl.

Um dieses Problem zu umgehen, fügen Sie den FQDN des OMIMSSC-Geräts im Browser unter der lokalen Intranetsite hinzu. Informationen zum Hinzufügen der OMIMSSC-Appliance im lokalen Intranet finden Sie im Abschnitt *Anzeigen von LC-Protokollen* im *einheitlichen Benutzerhandbuch zu Dell EMC OpenManage Integration für Microsoft System Center Version 7.3 für Microsoft Endpoint Configuration Manager und System Center Virtual Machine Manager*.

Fehler beim Öffnen der LC-Protokolldateien

Wenn Sie nach dem Erfassen der LC-Protokolle versuchen, die LC-Protokolldatei für einen Server anzuzeigen, wird folgende Fehlermeldung angezeigt: "`Failed to perform the requested action. For more information see the activity log`".

Um dieses Problem zu umgehen, setzen Sie den iDRAC zurück. Erfassen Sie dann die LC-Protokolle und lassen Sie sie anzeigen. Informationen zum Zurücksetzen des iDRAC finden Sie in der iDRAC-Dokumentation unter `Dell.com/support`.

Fehler bei der Testverbindung

Wenn die Benutzernamen gleich sind und die Kennwörter für das Domainbenutzerkonto und das lokale Benutzerkonto unterschiedlich sind, schlägt die Testverbindung zwischen der Microsoft-Konsole und dem OMIMSSC-Gerät fehl.

Das Domainbenutzerkonto lautet beispielsweise: `domain\user1` und das Kennwort ist `pwd1`. Das lokale Benutzerkonto ist `user1` und das Kennwort `Pwd2`. Wenn Sie versuchen, sich mit dem obigen Domainbenutzerkonto zu registrieren, schlägt die Testverbindung fehl.

Verwenden Sie als Problemumgehung unterschiedliche Benutzernamen für die Domainbenutzer und lokalen Benutzerkonten, oder verwenden Sie ein einzelnes Benutzerkonto als lokaler Benutzer und während der Microsoft-Konsolenregistrierung im OMIMSSC-Gerät.

22

Anhang I: Werte der Zeitzonenattribute

Geben Sie die Zeitzonenattributwerte manuell in MX7000-Geräten an, indem Sie die folgende Tabelle verwenden:

Tabelle 12. Zeitzonendetails

Zeitzonen-ID	Zeitzonenunterschied
TZ_ID_1	(GMT-12:00) Internationale Datumsgrenze West
TZ_ID_2	(GMT+14:00) Samoa
TZ_ID_3	(GMT-10:00) Hawaii
TZ_ID_4	(GMT-09:00) Alaska
TZ_ID_5	(GMT-08:00) Pacific Time (USA und Kanada)
TZ_ID_6	(GMT-08:00) Baja California
TZ_ID_7	(GMT-07:00) Arizona
TZ_ID_8	(GMT-07:00) Chihuahua, La Paz, Mazatlan
TZ_ID_9	(GMT-07:00) Mountain (USA und Kanada)
TZ_ID_10	(GMT-06:00) Mittelamerika
TZ_ID_11	(GMT-06:00) Central Standard Time (USA und Kanada)
TZ_ID_12	(GMT-06:00) Guadalajara, Mexiko Stadt, Monterrey
TZ_ID_13	(GMT-06:00) Saskatchewan
TZ_ID_14	(GMT-05:00) Bogota, Lima, Quito
TZ_ID_15	(GMT-05:00) Eastern Standard Time (USA und Kanada)
TZ_ID_16	(GMT-05:00) Indiana (Ost)
TZ_ID_17	(GMT-04:30) Caracas
TZ_ID_18	(GMT-04:00) Asunción
TZ_ID_19	(GMT-04:00) Atlantic Time (Kanada)
TZ_ID_20	(GMT-04:00) Cuiaba
TZ_ID_21	(GMT-04:00) Georgetown, La Paz, Manaus, San Juan
TZ_ID_22	(GMT-04:00) Santiago
TZ_ID_23	(GMT-03:30) Neufundland
TZ_ID_24	(GMT-03:00) Brasilia
TZ_ID_25	(GMT-03:00) Buenos Aires
TZ_ID_26	(GMT-03:00) Cayenne, Fortaleza
TZ_ID_27	(GMT-03:00) Grönland
TZ_ID_28	(GMT-03:00) Montevideo
TZ_ID_29	(GMT-02:00) Mid-Atlantic
TZ_ID_30	(GMT-01:00) Azoren
TZ_ID_31	(GMT-01:00) Cape Verde Is

Tabelle 12. Zeitzonendetails (fortgesetzt)

Zeitzonen-ID	Zeitzonenunterschied
TZ_ID_32	(GMT+00:00) Casablanca
TZ_ID_33	(GMT+00:00) Coordinated Universal Time
TZ_ID_34	(GMT+00:00) Dublin, Edinburgh, Lissabon, London
TZ_ID_35	(GMT+00:00) Monrovia, Reykjavik
TZ_ID_36	(GMT+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien
TZ_ID_37	(GMT+01:00) Belgrad, Bratislava, Budapest, Laibach, Prag
TZ_ID_38	(GMT+01:00) Brüssel, Kopenhagen, Madrid, Paris
TZ_ID_39	(GMT+01:00) Sarajevo, Skopje, Warschau, Zagreb
TZ_ID_40	(GMT+01:00) West Zentralafrika
TZ_ID_41	(GMT+02:00) Windhoek
TZ_ID_42	(GMT+02:00) Amman
TZ_ID_43	(GMT+03:00) Istanbul
TZ_ID_44	(GMT+02:00) Beirut
TZ_ID_45	(GMT+02:00) Kairo
TZ_ID_46	(GMT+02:00) Damaskus
TZ_ID_47	(GMT+02:00) Harare, Prätoria
TZ_ID_48	(GMT+02:00) Helsinki, Kiew, Riga, Sofia, Tallinn, Vilnius
TZ_ID_49	(GMT+02:00) Jerusalem
TZ_ID_50	(GMT+02:00) Minsk
TZ_ID_51	(GMT+03:00) Bagdad
TZ_ID_52	(GMT+03:00) Kuwait, Riad
TZ_ID_53	(GMT+03:00) Moskau, St. Petersburg, Wolgograd
TZ_ID_54	(GMT+03:00) Nairobi
TZ_ID_55	(GMT+03:30) Teheran
TZ_ID_56	(GMT+04:00) Abu Dhabi, Muskat
TZ_ID_57	(GMT+04:00) Baku
TZ_ID_58	(GMT+04:00) Port Louis
TZ_ID_59	(GMT+04:00) Tiflis
TZ_ID_60	(GMT+04:00) Eriwan
TZ_ID_61	(GMT+04:30) Kabul
TZ_ID_62	(GMT+05:00) Jekaterinburg
TZ_ID_63	(GMT+05:00) Islamabad, Karachi
TZ_ID_64	(GMT+05:00) Taschkent
TZ_ID_65	(GMT+05:30) Chennai, Kolkata, Mumbai, Neu-Delhi
TZ_ID_66	(GMT+05:30) Sri Jayawardenepura
TZ_ID_67	(GMT+05:45) Kathmandu
TZ_ID_68	(GMT+06:00) Astana

Tabelle 12. Zeitzonendetails (fortgesetzt)

Zeitzonen-ID	Zeitzonenunterschied
TZ_ID_69	(GMT+06:00) Dhaka
TZ_ID_70	(GMT+06:00) Novosibirsk
TZ_ID_71	(GMT+06:30) Yangon (Rangoon)
TZ_ID_72	(GMT+07:00) Bangkok, Hanoi, Jakarta
TZ_ID_73	(GMT+07:00) Krasnojarsk
TZ_ID_74	(GMT+08:00) Peking, Chongqing, Hongkong, Ürümqi
TZ_ID_75	(GMT+08:00) Irkutsk
TZ_ID_76	(GMT+08:00) Kuala Lumpur, Singapur
TZ_ID_77	(GMT+08:00) Perth
TZ_ID_78	(GMT+08:00) Taipei
TZ_ID_79	(GMT+08:00) Ulaanbaatar
TZ_ID_80	(GMT+08:30) Pjöngjang
TZ_ID_81	(GMT+09:00) Osaka, Sapporo, Tokio
TZ_ID_82	(GMT+09:00) Seoul
TZ_ID_83	(GMT+09:00) Jakutsk
TZ_ID_84	(GMT+09:30) Adelaide
TZ_ID_85	(GMT+09:30) Darwin
TZ_ID_86	(GMT+10:00) Brisbane
TZ_ID_87	(GMT+10:00) Canberra, Melbourne, Sydney
TZ_ID_88	(GMT+10:00) Guam, Port Moresby
TZ_ID_89	(GMT+10:00) Hobart
TZ_ID_90	(GMT+10:00) Wladiwostok
TZ_ID_91	(GMT+11:00) Magadan, Salomonen, Neukaledonien
TZ_ID_92	(GMT+12:00) Auckland, Wellington
TZ_ID_93	(GMT+12:00) Fidschi
TZ_ID_94	(GMT+13:00) Nuku'alofa
TZ_ID_95	(GMT+14:00) Kiritimati
TZ_ID_96	(GMT+02:00) Athen, Bukarest

23

Anhang II: Füllen von Pool-Werten

CSV-Datei mit Pool-Wert füllen

Tabelle 13. Dateiformat des Pool-Werts

serviceTag (automatisch ausgefüllt)	FQDD (automatisch ausgefüllt)	poolAttributeName	poolAtrributeValue
Service-Tag-Nummer des Geräts, von dem die systemspezifischen Attribute exportiert werden	Identifiziert die Komponente, die dem systemspezifischen Attribut zugeordnet ist	Identifiziert das systemspezifische Attribut, das konfiguriert werden soll	Festlegen des Werts für das angegebene systemspezifische Attribut

Tabelle 14. Systemspezifische Werte für die Hardware-Komponente

Komponente	Gruppenname	Attributname
BIOS	Verschiedene Einstellungen	Bestands-Tag
BIOS	Einstellungen für Verbindung 1	Initiator-Gateway
BIOS	Einstellungen für Verbindung 1	Initiator IP Address (Initiator-IP-Adresse)
BIOS	Einstellungen für Verbindung 1	Initiator-Subnetzmaske
BIOS	Einstellungen für Verbindung 1	Ziel-IP-Adresse
BIOS	Einstellungen für Verbindung 1	Zielname
BIOS	Einstellungen für Verbindung 2	Initiator-Gateway
BIOS	Einstellungen für Verbindung 2	Initiator IP Address (Initiator-IP-Adresse)
BIOS	Einstellungen für Verbindung 2	Initiator-Subnetzmaske
BIOS	Einstellungen für Verbindung 2	Ziel-IP-Adresse
BIOS	Einstellungen für Verbindung 2	Zielname
BIOS	Netzwerkeinstellungen	iSCSI Initiatorname
BIOS	Integrierte Geräte	PCIe-Link 1 für integrierte Netzwerkkarte 1
BIOS	Integrierte Geräte	PCIe-Link 2 für integrierte Netzwerkkarte 1
BIOS	Integrierte Geräte	PCIe-Link 3 für integrierte Netzwerkkarte 1
iDRAC	NIC-Informationen	DNS-RAC-Name
iDRAC	NIC-Informationen	VLAN aktivieren
iDRAC	NIC-Informationen	VLAN-ID
iDRAC	IPv4-Informationen	IPv4 aktivieren
iDRAC	IPv4-Informationen	IPv4 DHCP aktivieren
iDRAC	IPv6-Information	IPV6 aktivieren
iDRAC	IPv6-Information	IPv6 AutoConfig
iDRAC	Server-Topologie	Name des Rechenzentrums
iDRAC	Server-Topologie	Name des Gangs

Tabelle 14. Systemspezifische Werte für die Hardware-Komponente (fortgesetzt)

Komponente	Gruppenname	Attributname
iDRAC	Server-Topologie	Rack-Name
iDRAC	Server-Topologie	Rack-Steckplatz
iDRAC	Active Directory	Active Directory-RAC-Name
iDRAC	Statische NIC-Informationen	DNS-Domänenname
iDRAC	Statische IPv4-Informationen	IPv4-Adresse
iDRAC	Statische IPv4-Informationen	Netzwerkmaske
iDRAC	Statische IPv4-Informationen	Gateway
iDRAC	Statische IPv4-Informationen	DNS-Server 1
iDRAC	Statische IPv4-Informationen	DNS-Server 2
iDRAC	Statische IPv6-Informationen	IPv6-Adresse 1
iDRAC	Statische IPv6-Informationen	IPv6-Gateway
iDRAC	Statische IPv6-Informationen	IPV6-Link-Local-Präfixlänge
iDRAC	Statische IPv6-Informationen	IPV6-DNS-Server 1
iDRAC	Statische IPv6-Informationen	IPv6-DNS-Server 2
iDRAC	Serverbetriebssystem	Server-Hostname
iDRAC	Server-Topologie	Zimmername
iDRAC	NIC-Informationen	DNS-RAC-Name
iDRAC	NIC-Informationen	DNS-RAC-Name
iDRAC	IPv4-Informationen	IPv4 DHCP aktivieren
iDRAC	Statische IPv4-Informationen	IPv4-Adresse
iDRAC	Statische IPv4-Informationen	Netzwerkmaske
iDRAC	Statische IPv4-Informationen	Gateway
iDRAC	Statische IPv4-Informationen	DNS-Server 1
iDRAC	Statische IPv4-Informationen	DNS-Server 2
iDRAC	Statische IPv6-Informationen	IPv6-Gateway
iDRAC	Statische IPv6-Informationen	IPV6-Link-Local-Präfixlänge
iDRAC	Statische IPv6-Informationen	DNS-Server 1
iDRAC	Statische IPv6-Informationen	DNS-Server 2
Netzwerk	Allgemeine iSCSI-Parameter	Gegenseitige CHAP-Authentifizierung
Netzwerk	Parameter für erstes iSCSI-Ziel	Verbinden
Netzwerk	Parameter für zweites iSCSI-Ziel	Verbinden
Netzwerk	Parameter für erstes iSCSI-Ziel	Start-LUN
Netzwerk	Parameter für erstes iSCSI-Ziel	CHAP-ID
Netzwerk	Parameter für erstes iSCSI-Ziel	CHAP Secret (CHAP-Geheimschlüssel)
Netzwerk	Parameter für erstes iSCSI-Ziel	IP-Adresse
Netzwerk	Parameter für erstes iSCSI-Ziel	iSCSI-Name
Netzwerk	Parameter für erstes iSCSI-Ziel	TCP-Anschluss

Tabelle 14. Systemspezifische Werte für die Hardware-Komponente (fortgesetzt)

Komponente	Gruppenname	Attributname
Netzwerk	iSCSI Initiator-Parameter	CHAP-ID
Netzwerk	iSCSI Initiator-Parameter	CHAP Secret (CHAP-Geheimschlüssel)
Netzwerk	iSCSI Initiator-Parameter	Standard-Gateway
Netzwerk	iSCSI Initiator-Parameter	IP-Adresse
Netzwerk	iSCSI Initiator-Parameter	IPv4-Adresse
Netzwerk	iSCSI Initiator-Parameter	IPv4-Standard-Gateway
Netzwerk	iSCSI Initiator-Parameter	IPv4 primäre DNS
Netzwerk	iSCSI Initiator-Parameter	IPv4 sekundäre DNS
Netzwerk	iSCSI Initiator-Parameter	IPv6-Adresse
Netzwerk	iSCSI Initiator-Parameter	IPv6-Standard-Gateway
Netzwerk	iSCSI Initiator-Parameter	IPv6 primäre DNS
Netzwerk	iSCSI Initiator-Parameter	IPv6 sekundäre DNS
Netzwerk	iSCSI Initiator-Parameter	iSCSI-Name
Netzwerk	iSCSI Initiator-Parameter	Primärer DNS-Server
Netzwerk	iSCSI Initiator-Parameter	Sekundärer DNS-Server
Netzwerk	iSCSI Initiator-Parameter	Subnetzmaske
Netzwerk	iSCSI Initiator-Parameter	Subnetzmasken-Präfix
Netzwerk	Parameter für sekundäres iSCSI-Gerät	MAC-Adresse des sekundären Geräts
Netzwerk	Parameter für zweites iSCSI-Ziel	Start-LUN
Netzwerk	Parameter für zweites iSCSI-Ziel	CHAP Secret (CHAP-Geheimschlüssel)
Netzwerk	Parameter für zweites iSCSI-Ziel	CHAP-ID
Netzwerk	Parameter für zweites iSCSI-Ziel	IP-Adresse
Netzwerk	Parameter für zweites iSCSI-Ziel	iSCSI-Name
Netzwerk	Parameter für zweites iSCSI-Ziel	TCP-Anschluss
Netzwerk	Parameter für sekundäres iSCSI-Gerät	Unabhängigen Zielnamen verwenden
Netzwerk	Parameter für sekundäres iSCSI-Gerät	Unabhängiges Zielportal verwenden
Netzwerk	Haupt-Konfigurationsseite	Virtuelle FIP-MAC-Adresse
Netzwerk	Haupt-Konfigurationsseite	Virtuelle iSCSI Offload MAC-Adresse
Netzwerk	Haupt-Konfigurationsseite	Virtuelle MAC-Adresse
Netzwerk	Konfiguration der Partition n	Virtuelle MAC-Adresse
Netzwerk	Haupt-Konfigurationsseite	GUID für virtuelle Anschlüsse
Netzwerk	Haupt-Konfigurationsseite	Virtueller World Wide Knotenname
Netzwerk	Konfiguration der Partition n	Virtueller World Wide Knotenname
Netzwerk	Haupt-Konfigurationsseite	Virtueller World Wide Schnittstellenname
Netzwerk	Konfiguration der Partition n	Virtueller World Wide Schnittstellenname
Netzwerk	Haupt-Konfigurationsseite	Weltweiter Knotenname
Netzwerk	Konfiguration der Partition n	Weltweiter Knotenname

Tabelle 14. Systemspezifische Werte für die Hardware-Komponente (fortgesetzt)

Komponente	Gruppenname	Attributname
FC	Fibre Channel-Zielkonfiguration	Startscanauswahl
FC	Fibre Channel-Zielkonfiguration	Erste FC-Ziel-LUN
FC	Fibre Channel-Zielkonfiguration	Erstes FC-Ziel für World Wide Port Name
FC	Fibre Channel-Zielkonfiguration	Zweite FC-Ziel-LUN
FC	Fibre Channel-Zielkonfiguration	Zweites FC-Ziel für World Wide Port Name
FC	Port-Konfigurationsseite	Virtueller World Wide Knotenname
FC	Port-Konfigurationsseite	Virtueller World Wide Schnittstellenname
Management-Modul für MX Chasis	ChassisLocation	Rechenzentrum
Management-Modul für MX Chasis	ChassisLocation	Raum
Management-Modul für MX Chasis	ChassisLocation	Gang
Management-Modul für MX Chasis	ChassisLocation	Rack
Management-Modul für MX Chasis	ChassisLocation	Rack-Steckplatz
Management-Modul für MX Chasis	ChassisLocation	Speicherort

Tabelle 15. Systemspezifische Werte für Windows-Komponente

serviceTag (automatisch ausgefüllt)	FQDD (automatisch ausgefüllt)	poolAttributeName	poolAtrributeValue	Einzelheiten über das Attribut und das Ausfüllen
xxxxxxx	WINDOWS	HOSTNAME	WIN19SRVDTA	Was: Dies ist der Hostname, der auf dem eingesetzten/bereitstellten Server eingestellt werden soll.
xxxxxxx	WINDOWS	ServerMngNIC	<MAC-Adressen>	Was: Dies ist die MAC-Adresse des Netzwerkanschlusses, der mit System Center und OMMISSC Appliance kommunizieren kann. Wie: Rufen Sie die MAC-Adresse von iDRAC ab, indem Sie zu einem bestimmten Port navigieren.
xxxxxxx	WINDOWS	LOGICALNETWORK	OSD MIT STATISCHER IP	Was: Dies ist das Netzwerkprofil, das in SCVMM erstellt wird und über einen statischen IP-Pool, Subnetz und andere Netzwerkdetails verfügt, die auf MN angewendet werden sollen. Wie: Erstellen Sie das logische Netzwerkprofil in SCVMM und geben Sie den Namen der erstellten Vorlage an. Weitere Informationen finden Sie unter Planen der VMM-Netzwerkstruktur in der Dokumentation von Microsoft.
xxxxxxx	WINDOWS	IP-SUBNET	100.100.28.0/22	Was: Dies ist die Subnetzmaske für die statische IP-Pool-Eingabe im obigen logischen Netzwerkprofil.
xxxxxxx	WINDOWS	IP-ADRESSE	100.100.31.145	Was: Dies ist die statische IP, die auf den bereitgestellten verwalteten Knoten anzuwenden ist.

Tabelle 16. Systemspezifische Werte für Nicht-Windows-Komponenten

serviceTag (automatisch ausgefüllt)	FQDD (automatisch ausgefüllt)	poolAttributeName	poolAtrributeValue	Einzelheiten über das Attribut und das Ausfüllen
xxxxxxx	LINUX	HOSTNAME	<Hostname>	Was: Dies ist der Hostname, der auf dem eingesetzten/bereitstellten Server eingestellt werden soll.
xxxxxxx	LINUX	IP-ADRESSE	<Statische IP-Adresse>	Was: Dies ist die statische IP, die auf den bereitgestellten verwalteten Knoten anzuwenden ist.
xxxxxxx	LINUX	SUBNETZMASKE	<Subnetzmaske>	Was: Dies ist die Subnetzmaske für den statischen IP-Pool
xxxxxxx	LINUX	DEFAULTGATEWAY	<Standard-Gateway>	Was: Dies ist das Standard-Gateway
xxxxxxx	LINUX	PRIMARYDNSSERVER	<Primärer DNS-Server>	Was: Dies ist der primäre DNS Server
xxxxxxx	LINUX	SECONDARYDNSSERVER	<Sekundärer DNS-Server>	Was: Dies ist ein sekundärer DNS-Server

24

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

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

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

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