




# OpenManage Integration for Microsoft System Center Version 7.0

Benutzerhandbuch

## Anmerkungen, Vorsichtshinweise und Warnungen

-  **ANMERKUNG:** Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie Ihr Produkt besser einsetzen können.
-  **VORSICHT:** Ein VORSICHTSHINWEIS macht darauf aufmerksam, dass bei Nichtbefolgung von Anweisungen eine Beschädigung der Hardware oder ein Verlust von Daten droht, und zeigt auf, wie derartige Probleme vermieden werden können.
-  **WARNUNG:** Durch eine WARNUNG werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

**Copyright © 2009 - 2017 Dell Inc. oder dessen Tochtergesellschaften. Alle Rechte vorbehalten.** Dell, EMC und andere Marken sind Marken von Dell Inc. oder deren Tochtergesellschaften. Andere Marken können Marken ihrer jeweiligen Inhaber sein.

# Inhaltsverzeichnis

<b>1 Einführung</b> .....	<b>7</b>
OMIMSSC-Funktionen.....	7
<b>2 Informationen zu OMIMSSC-Komponenten</b> .....	<b>9</b>
<b>3 Admin-Portal</b> .....	<b>10</b>
Ändern von IG- und SCCM- oder SCVMM-Konten.....	10
Ändern der Anmeldeinformationen im OMIMSSC-Verwaltungsportal .....	10
Reparieren der OMIMSSC-Konsolenerweiterung für SCCM.....	11
Reparieren der OMIMSSC-Konsolenerweiterung für SCVMM.....	11
Reparieren von OMIMSSC IG.....	11
<b>4 Starten von OMIMSSC über eine registrierte MSSC-Konsole</b> .....	<b>12</b>
Browsereinstellungen.....	12
Starten der OMIMSSC-Konsolenerweiterung für SCCM.....	12
Starten der OMIMSSC-Konsolenerweiterung für SCVMM.....	13
<b>5 Anwendungsfälle</b> .....	<b>14</b>
Bereitstellen von Betriebssystemen mit der OMIMSSC-Konsolenerweiterung für SCCM.....	14
Betriebssystembereitstellung mit der OMIMSSC-Konsolenerweiterung für SCVMM.....	15
Nicht-Windows-Betriebssystembereitstellungen mit OMIMSSC-Konsolenerweiterungen.....	15
Anwenden von Aktualisierungen auf Server.....	15
Konfigurieren von ersetzten Komponenten.....	16
Exportieren und Importieren von Serverprofilen.....	16
<b>6 Profile</b> .....	<b>17</b>
Info zu Anmeldeprofilen.....	17
Vordefinierte Anmeldeprofile.....	17
Erstellen eines Anmeldeprofils.....	18
Ändern eines Anmeldeprofils.....	18
Löschen eines Anmeldeprofils.....	19
Hypervisor-Profile.....	19
Erstellen eines Hypervisor-Profiles.....	19
Ändern eines Hypervisor-Profiles.....	20
Löschen eines Hypervisor-Profiles.....	20
<b>7 Beginnen mit der Konfiguration und Bereitstellung</b> .....	<b>21</b>
<b>8 Ermitteln von Servern und Synchronisieren mit der MSSC-Konsole</b> .....	<b>23</b>
Referenzserverkonfigurationen.....	23
Ermitteln von Servern in OMIMSSC.....	23
Ermitteln von Servern in der OMIMSSC-Konsolenerweiterung für SCCM.....	24

Ermitteln von Servern in der OMIMSSC-Konsolenerweiterung für SCVMM.....	24
Systemanforderungen für verwaltete Systeme .....	24
Ermitteln von Servern über die automatische Ermittlung.....	25
Ermitteln von Servern über die manuelle Ermittlung.....	25
Synchronisieren von OMIMSSC-Konsolenerweiterungen mit einer registrierten SCCM-Umgebung.....	26
Synchronisieren der OMIMSSC-Konsolenerweiterung mit einer registrierten SCVMM-Umgebung.....	26
Synchronisieren mit registriertem MSSC.....	27
Beheben von Synchronisierungsfehlern.....	27
Löschen von Servern aus OMIMSSC.....	27
Starten der iDRAC-Konsole.....	28
<b>9 OMIMSSC-Lizenzierung.....</b>	<b>29</b>
Optionen nach dem Hochladen von Lizenzen.....	29
Lizenzdatei für neue Einkäufe.....	29
Stacking-Lizenzen.....	30
Ersatz von Lizenzen .....	30
Erneutes Importieren von Lizenzen.....	30
Importieren mehrerer Lizenzen.....	30
Erzwingung.....	30
Aktualisieren von Lizenzen.....	30
Testlizenz.....	30
Lizenznutzung in OMIMSSC nach Serverermittlung.....	30
Importieren einer Lizenz in OMIMSSC.....	31
Anzeigen von Lizenzdetails.....	31
<b>10 Betriebsvorlage.....</b>	<b>32</b>
Vorbereitung auf die Bereitstellung.....	32
Erstellen von WinPE-ISO-Images .....	32
Tasksequenz.....	33
Bearbeiten einer Tasksequenz.....	35
Erstellen eines Lifecycle Controller-Startdatenträgers.....	35
Einstellen eines freigegebenen Standard-Speicherorts für den Lifecycle Controller-Startdatenträger.....	36
Tasksequenz-Datenträger erstellen (Startfähiges ISO-Image).....	36
Bereitstellen von nicht Windows-basierten Betriebssystemen .....	36
Verwalten einer Betriebsvorlage.....	37
Erstellen einer Betriebsvorlage.....	37
Anzeigen von Betriebsvorlage.....	39
Bearbeiten von Betriebsvorlage.....	39
Löschen einer Betriebsvorlage.....	40
Zuweisen einer Betriebsvorlage und Prüfen der Betriebsvorlage-Compliance.....	41
Bereitstellen einer Betriebsvorlage.....	41
<b>11 Integration mit Dell Repository Manager (DRM).....</b>	<b>43</b>
<b>12 Maintenance.....</b>	<b>44</b>
Allgemeines zu Firmware-Aktualisierungen .....	44

Anwenden von Aktualisierungen auf Server.....	45
Wiederherstellung.....	54
Schutz-Vaults.....	54
Exportieren von Serverprofilen.....	55
Importieren von Serverprofilen.....	56
Anwenden von Firmware- und Konfigurationseinstellungen.....	57
Erfassen von LC-Protokollen.....	58
Anzeigen von LC-Protokollen.....	59
Dateibeschreibung.....	59
Exportieren von Bestandsdaten.....	60
<b>13 Anzeigen von Informationen in OMIMSSC.....</b>	<b>61</b>
Anzeigen von Jobs.....	62
Verwalten von Jobs.....	62
<b>14 Fehlerbehebung.....</b>	<b>63</b>
Bereitstellungsoption wird in Tasksequenz nicht angezeigt.....	63
VRTX-Gehäusegruppen werden doppelt erstellt .....	64
Leere Cluster-Aktualisierungsgruppe wird bei automatischer Ermittlung oder Synchronisierung nicht gelöscht.....	64
Aktualisierungsquelle kann nicht erstellt werden.....	64
Fehler bei der Firmware-Aktualisierung wegen belegter Job-Warteschlange.....	64
Firmware-Aktualisierung auf Cluster-Aktualisierungsgruppe schlägt fehl.....	65
Fehler bei der Firmware-Aktualisierung auf Servern der 11. Generation.....	65
Fehler bei der Firmware-Aktualisierung während der Verwendung der DRM-Aktualisierungsquelle .....	65
Fehler bei einem geplanten Job für eine Aktualisierungsgruppe.....	65
Fehler bei der Anwendung einer Betriebsvorlage .....	66
Fehler beim Zugriff auf CIFS-Freigabe unter Verwendung des Hostnamens.....	66
Fehler bei der FTP-Verbindung bei Verwendung der Standard-Aktualisierungsquelle des Systems.....	66
Fehler beim Erstellen eines Repositorys während einer Firmware-Aktualisierung.....	66
Benutzerdefinierte Aktualisierungsgruppe kann nicht gelöscht werden.....	66
Fehler beim Anzeigen von Jobs und Protokollen.....	67
Fehler beim Exportieren von LC-Protokollen im CSV-Format.....	67
Serverprofile werden nicht exportiert .....	67
Fehler beim Anzeigen des Dell EMC Logos im Admin-Portal von OMIMSSC.....	67
Fehler beim Anzeigen von LC-Protokollen .....	67
Firmware-Aktualisierung auf einigen Komponenten, unabhängig von der Auswahl.....	67
Fehler bei der Hypervisor-Bereitstellung.....	68
Hypervisor-Bereitstellungsfehler aufgrund von weiterhin vorhandenen Treiberdateien in der Bibliotheksfreigabe.....	68
Fehler bei der Hypervisor-Bereitstellung mit Active Directory für die 11. Generation von PowerEdge-Blade-Servern.....	69
Falsche Anmeldeinformationen während der Ermittlung.....	69
IG-Installationsproblem während der Ausführung mehrerer Instanzen des Installationsprogramms auf dem gleichen Server .....	69
Zeitüberschreitung beim Importieren des Serverprofils nach zwei Stunden.....	69

Aktuelle Bestandsaufnahmeinformationen werden auch nach erfolgter Firmware-Aktualisierung nicht angezeigt.....	70
SCVMM-Fehler 21119 beim Hinzufügen von Servern zu Active Directory.....	70
<b>15 Anhang.....</b>	<b>71</b>
<b>16 Zugriff auf Dokumente von der Dell EMC Support-Website.....</b>	<b>72</b>
Kontaktaufnahme mit Dell.....	72

# Einführung

OpenManage Integration for Microsoft System Center (OMIMSSC) bietet Integrationen in die System Center-Produktsuite, die über den gesamten Lebenszyklus das Management von Dell EMC-Servern mithilfe von iDRAC (integrated Dell Remote Access Controller) mit Lifecycle Controller (LC) ermöglicht.

OMIMSSC bietet Betriebssystembereitstellung, Hardware-Patching, Firmware-Aktualisierung und Serverwartung. Mit OMIMSSC können Sie entweder die Integration in Microsoft System Center Configuration Manager (SCCM) zum Verwalten der Dell EMC-Server in herkömmlichen Rechenzentren oder die Integration in Microsoft System Center Virtual Machine Manager (SCVMM) zum Verwalten der Dell EMC-Server in virtualisierten und Cloud-Umgebungen verwenden.

Dieses Handbuch enthält Informationen über die Verwendung des Produkts und alle Anwendungsfälle für das Produkt.

Weitere Informationen zu SCCM und SCVMM finden Sie in der Microsoft-Dokumentation.

## OMIMSSC-Funktionen

**Tabelle 1. Funktionen in dieser Version**

Funktion	Beschreibung
Bereitstellung von nicht Windows-basierten Betriebssystemen	Unterstützung für die Bereitstellung nicht Windows-basierter Betriebssysteme (ESXi und RHEL)
PowerEdge-Server der 14. Generation	Unterstützung für die Ermittlung und Verwaltung von Dell EMC PowerEdge-Servern der 14. Generation
iDRAC-Sperrmodus	Unterstützung für den iDRAC-Sperrmodus auf PowerEdge-Servern der 14. Generation
Multi-Konsolen-Unterstützung	Unterstützung für die Integration mehrerer SCCM- und SCVMM-Konsolen mit einer einzigen OMIMSSC-Appliance
Ermittlung	Ermittlung von PowerEdge-Servern ab Generation 11 sowie Bereitstellung der Server in Microsoft System Center (MSSC)-Umgebungen
Synchronisierung mit MSSC	Synchronisierung aller in der registrierten SCCM- oder SCVMM-Umgebung vorhandenen Dell EMC Host-Systeme mit OMIMSSC
Lizenzcenter	Verwaltung von OMIMSSC-Lizenzen über das Admin-Portal
Bestandsaufnahme	Abrufen der wichtigsten Bestandsinformationen zu Dell EMC Servern
Hardwarekonfiguration	Unterstützung für die Konfiguration der Netzwerkkadpater sowie der Fibre Channel-, PCIe- und SSD-Komponenten von PowerEdge-Servern
Erstellung von Startmedien	Unterstützung für die Erstellung von Startmedien für unbeaufsichtigte Bereitstellungen aus Tasksequenzmedien

Betriebsvorlagen	Verwendung einer einheitlichen Vorlage für Firmware-Aktualisierungen, Hardwarekonfiguration und Betriebssystembereitstellungen
Konformität mit Betriebsvorlagen	Überprüfung von Hardwarekonfigurationen auf Konformität mit Betriebsvorlagen
Microsoft CAU (Cluster-Aware Updating, clusterfähiges Aktualisieren)	Automatisierung der Firmware-Aktualisierung mithilfe der CAU-Funktion von Microsoft
Export von Bestandinformationen	Export des nach dem Abgleich des Serverbestands mit der Aktualisierungsquelle erstellten Vergleichsberichts als CSV- oder XML-Datei
Serverprofil exportieren	Export von Serverprofilen an interne oder externe Speicherorte, inklusive Firmware-Abbildern auf Komponenten wie BIOS (Basic Input Output System), RAID (Redundant Array of Independent Disks), NIC (Network Interface Controller), iDRAC, LC usw.
Serverprofil importieren	Import von Serverprofilen mit Beibehaltung oder Ausschluss der aktuellen RAID-Einstellungen
Erfassen und Anzeigen von Lifecycle Controller (LC)-Protokollnachrichten	Möglichkeit, LC-Protokollnachrichten zu exportieren, anzuzeigen, als CSV-Datei herunterzuladen und zu durchsuchen
Abfrage und Benachrichtigungen	Konfiguration von Benachrichtigungen, um sich über neue Kataloge in der Aktualisierungsquelle informieren zu lassen

# Informationen zu OMIMSSC-Komponenten

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

- Die OpenManage Integration for Microsoft System Center-Appliance-VM, auch als „Appliance“ bezeichnet, wird auf einem Hyper-V als virtuelle Maschine basierend auf CentOS gehostet und führt folgende Aufgaben aus:
  - Interagiert mit den Dell EMC-Servern über iDRAC unter Verwendung von Web Services-Management (WSMAN)-Befehlen.
  - Ermöglicht die Verwaltung der OMIMSSC-Appliance über das Verwaltungsportal.
- Bei OMIMSSC Integration Gateway, auch bezeichnet als Integration Gateway (IG), handelt es sich um Webservices, die auf dem Windows Server installiert sind und folgende Aufgaben ausführen:
  - Führt SCCM- oder SCVMM-PowerShell-Befehle aus und fungiert als intermediäres Gateway zwischen SCCM oder SCVMM und der Appliance.
  - Passt WinPE benutzerspezifisch für die Appliance an.
- OpenManage Integration for Microsoft System Center-Konsole, auch bekannt als OMIMSSC-Konsole
  - OMIMSSC-Konsolen-Plug-in für SCCM, auch bekannt als OMIMSSC-Konsolenerweiterung für SCCM
  - OMIMSSC-Konsolen-Add-in für SCVMM, auch bekannt als OMIMSSC-Konsolenerweiterung für SCVMM

## Admin-Portal

Im Admin-Portal können Sie sich als Administrator bei OMIMSSC anmelden und alle Jobs sehen, die von den unterschiedlichen Benutzern in OMIMSSC angestoßen wurden. Außerdem können Sie hier die Lizenzdetails sehen, erforderliche Komponenten herunterladen und OMIMSSC aktualisieren. Unten sehen Sie eine Liste der Anwendungsfälle für das Admin-Portal, die auch das Thema Lizenzierung berücksichtigen.

Themen:

- [Ändern von IG- und SCCM- oder SCVMM-Konten](#)
- [Reparieren der OMIMSSC-Konsolenerweiterung für SCCM](#)
- [Reparieren der OMIMSSC-Konsolenerweiterung für SCVMM](#)
- [Reparieren von OMIMSSC IG](#)

### Ändern von IG- und SCCM- oder SCVMM-Konten

Mithilfe dieser Option können Sie die Kennwörter von SCCM-, SCVMM- und IG-Konten in der OMIMSSC-Konsole ändern.

#### Info über diese Aufgabe

Sie können die SCCM- und SCVMM-Administratoranmeldeinformationen sowie die IG-Anmeldeinformationen über das Verwaltungsportal ändern. Bei diesem Prozess handelt es sich um eine sequenzielle Aktivität.

- Schaffen Sie für das IG-Konto die folgenden Voraussetzungen vor dem Ändern des Kontos in OMIMSSC:
  - Ändern Sie die Anmeldeinformationen in Active Directory.
  - Ändern Sie die Anmeldeinformationen im IG-Installationsprogramm.
- Ändern Sie für das SCCM- oder SCVMM-Konto die Anmeldeinformationen in Active Directory vor dem Ändern des Kontos in OMIMSSC.

So ändern Sie das OMIMSSC IG-Konto über das Installationsprogramm:

#### Schritte

- 1 Führen Sie das IG-Installationsprogramm aus.
- 2 Wählen Sie unter **Programmwartung** die Option **Reparieren** aus und klicken Sie auf **Weiter**.
- 3 Ändern Sie das Kennwort und klicken Sie dann auf **Weiter**.
- 4 Klicken Sie in **Modifizierung des Programms** auf **Installieren**.
- 5 Klicken Sie nach Abschluss der Änderung auf **Finish (Fertig stellen)**.

### Ändern der Anmeldeinformationen im OMIMSSC-Verwaltungsportal

- 1 Klicken Sie im OMIMSSC-Verwaltungsportal auf **Settings (Einstellungen)** und dann auf **Console Enrolment (Konsolenregistrierung)**. Die registrierten Konsolen werden angezeigt.
- 2 Wählen Sie eine Konsole zur Bearbeitung aus und klicken Sie auf **Edit (Bearbeiten)**.
- 3 Geben Sie die neuen Details ein und klicken Sie auf **Finish (Fertig stellen)**, um die Änderungen zu speichern.

# Reparieren der OMIMSSC-Konsolenerweiterung für SCCM

Um die OMIMSSC-Dateien im Falle einer Beschädigung zu reparieren, führen Sie folgende Schritte durch:

- 1 Führen Sie das Installationsprogramm für die OMIMSSC-Konsolenerweiterung für SCCM aus.  
Der **Welcome-Bildschirm (Startbildschirm)** wird angezeigt.
- 2 Klicken Sie auf **Next** (Weiter).
- 3 Wählen Sie unter **Program Maintenance (Programmwartung)** die Option **Repair (Reparieren)** aus und klicken Sie auf **Next (Weiter)**.  
Das Fenster **Ready to Repair the Program (Bereit zur Reparatur des Programms)** wird angezeigt.
- 4 Klicken Sie auf **Install (Installieren)**.  
Ein Verlaufs bildschirm zeigt den Fortschritt der Installation an. Wenn die Installation abgeschlossen ist, wird das Fenster **InstallShield Wizard Completed (InstallShield-Assistent abgeschlossen)** angezeigt.
- 5 Klicken Sie auf **Fertigstellen**.

# Reparieren der OMIMSSC-Konsolenerweiterung für SCVMM

Um die OMIMSSC-Dateien im Falle einer Beschädigung zu reparieren, führen Sie folgende Schritte durch:

- 1 Führen Sie das Installationsprogramm für die OMIMSSC-Konsolenerweiterung für SCVMM aus.
- 2 Wählen Sie unter **Program Maintenance (Programmwartung)** die Option **Repair (Reparieren)** aus und klicken Sie auf **Next (Weiter)**.
- 3 Klicken Sie unter **Ready to Repair or Remove the program (Bereit zum Reparieren oder Entfernen des Programms)** auf **Repair (Reparieren)**.
- 4 Wenn die Reparatur abgeschlossen ist, klicken Sie auf **Finish (Fertigstellen)**.

# Reparieren von OMIMSSC IG

## Info über diese Aufgabe

Mithilfe dieser Option können Sie gelöschte oder beschädigt Dateien neu installieren oder die für OMIMSSC IG erforderlichen Ordner neu erstellen.

## Schritte

- 1 Führen Sie das OMIMSSC IG-Installationsprogramm aus.
- 2 Wählen Sie unter **Program Maintenance (Programmwartung)** die Option **Repair (Reparieren)** aus und klicken Sie auf **Next (Weiter)**.
- 3 Geben Sie unter **Bereit zum Reparieren** das Kennwort für das IG-Benutzerkonto an, und klicken Sie dann auf **Installieren**.
- 4 Klicken Sie auf **Finish (Fertig stellen)**, sobald die Reparatur abgeschlossen ist.

# Starten von OMIMSSC über eine registrierte MSSC-Konsole

In diesem Kapitel erfahren Sie, wie Sie OMIMSSC über eine registrierte SCCM-Konsole oder SCVMM-Konsole starten.

Themen:

- [Browsereinstellungen](#)
- [Starten der OMIMSSC-Konsolenerweiterung für SCCM](#)
- [Starten der OMIMSSC-Konsolenerweiterung für SCVMM](#)

## Browsereinstellungen

### Info über diese Aufgabe

Fügen Sie vor dem Starten von OMIMSSC die IP-Adresse von OMIMSSC zur Site-Liste des **lokalen Intranets** hinzu, um die folgenden Vorgänge ausführen zu können:

- Export und Anzeige des Firmware-Bestands
- Anzeigen von LC-Protokollen
- Export von Pool-Werten in der Betriebsvorlage

Führen Sie vor dem Herunterladen von CSV-Dateien die folgenden Schritte aus:

### Schritte

- 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 SCCM

### Voraussetzung

Melden Sie sich beim Windows-Betriebssystem mit den gleichen Anmeldeinformationen an, die für die Anmeldung bei der OMIMSSC-Konsolenerweiterung für SCCM verwendet werden.

### Schritt

Klicken Sie in der SCCM-Konsole auf **Assets and Compliance (Bestand und Kompatibilität)**, klicken Sie auf **Overview (Übersicht)** und klicken Sie anschließend auf **OMIMSSC console extension for SCCM (OMIMSSC-Konsolenerweiterung für SCCM)**.

① **ANMERKUNG:** Wenn Sie eine Verbindung mit der SCCM-Konsole über RDP (Remote Desktop Protocol) herstellen, wird die OMIMSSC-Sitzung möglicherweise abgemeldet, wenn RDP geschlossen wird. Melden Sie sich also wieder an, nachdem Sie die RDP-Sitzung erneut geöffnet haben.

## Starten der OMIMSSC-Konsolenerweiterung für SCVMM

1 Wählen Sie in der SCVMM-Konsole **Fabric** und dann die Servergruppen **All Hosts (Alle Hosts)** aus.

① **ANMERKUNG:** Um OMIMSSC zu starten, können Sie eine beliebige Host-Gruppe auswählen, für die Sie Zugriffsberechtigungen haben.

2 Wählen Sie in der Multifunktionsleiste **Home (Start) OMIMSSC** aus.

# Anwendungsfälle

Eine Betriebssystembereitstellung ist nur auf Servern möglich, deren Hardwarekonfiguration mit OMIMSSC kompatibel ist. Aktualisieren Sie vor der Betriebssystembereitstellung die Firmware auf die jeweils neueste Version (verfügbar unter [ftp.dell.com](http://ftp.dell.com) oder [downloads.dell.com](http://downloads.dell.com)) und fahren Sie anschließend mit der Betriebssystembereitstellung fort. Unten sehen Sie einige Anwendungsfälle für die OMIMSSC-Konsolenerweiterungen.

Themen:

- Bereitstellen von Betriebssystemen mit der OMIMSSC-Konsolenerweiterung für SCCM
- Betriebssystembereitstellung mit der OMIMSSC-Konsolenerweiterung für SCVMM
- Nicht-Windows-Betriebssystembereitstellungen mit OMIMSSC-Konsolenerweiterungen
- Anwenden von Aktualisierungen auf Server
- Konfigurieren von ersetzten Komponenten
- Exportieren und Importieren von Serverprofilen

## Bereitstellen von Betriebssystemen mit der OMIMSSC-Konsolenerweiterung für SCCM

### Info über diese Aufgabe

Gehen Sie wie folgt vor, um das Betriebssystem auf den gewünschten Servern bereitzustellen:

### Schritte

- 1 Laden Sie das neueste Dell Deployment Toolkit (DTK) herunter und erstellen Sie ein WinPE (Windows Preinstallation Environment)-Start-ISO-Abbild. Weitere Informationen finden Sie im Abschnitt zum Thema [WinPE-Aktualisierung](#).
- 2 Importieren Sie dieses WIM-Abbild in die SCCM-Konsole und erstellen Sie in SCCM ein Startabbild. Weitere Informationen finden Sie in der *Microsoft-Dokumentation*.
- 3 Erstellen Sie in SCCM eine Tasksequenz. Weitere Informationen finden Sie unter [Creating task sequence](#) (Erstellen einer Tasksequenz).
- 4 Erstellen Sie in SCCM ein Tasksequenzmedien-Abbild. Weitere Informationen finden Sie in der *Microsoft-Dokumentation*.
- 5 Erzeugen Sie ein ISO-Abbild für eine unbeaufsichtigte Bereitstellung. Weitere Informationen finden Sie im Kapitel zum Thema [Erstellen von LC-Startmedien](#).
- 6 Ermitteln Sie über die Seite **Discovery** (Ermittlung) einen Referenzserver. Weitere Informationen finden Sie unter [Discovering servers using manual discovery](#) (Ermitteln von Servern über die manuelle Ermittlung).
- 7 Erstellen Sie eine Betriebsvorlage. Weitere Informationen finden Sie unter [Creating Operational Template](#) (Erstellen einer Betriebsvorlage).
- 8 Weisen Sie eine Betriebsvorlage zu. Weitere Informationen finden Sie unter [Assigning Operational Template](#) (Zuweisen einer Betriebsvorlage).
- 9 Stellen Sie eine Betriebsvorlage bereit. Weitere Informationen finden Sie unter [Deploying Operational Template](#) (Bereitstellen einer Betriebsvorlage).

**ANMERKUNG:** Bevor Sie ein Betriebssystem auf einem Host-Server bereitstellen, müssen Sie sich vergewissern, dass der Client-Status des Servers in SCCM auf Nein gesetzt ist.

**ANMERKUNG:** Nach einer erfolgreichen Bereitstellung des Windows-Betriebssystems in der SCCM-Umgebung wird der Server in OMIMSSC nicht als Host aufgeführt. Damit der Server auf der Host-Registerkarte aufgeführt wird, müssen Sie sich zunächst vergewissern, dass der Client-Status des Servers in SCCM auf Ja gesetzt ist, und anschließend OMIMSSC mit SCCM synchronisieren.

- 10 Den Status von Jobs zur Firmware-Aktualisierung oder Betriebssystembereitstellung können Sie auf der Seite **Jobs and Logs Center** (Job- und Protokollcenter) einsehen. Weitere Informationen finden Sie unter [Viewing information in OMIMSSC](#) (Anzeigen von Informationen in OMIMSSC).

# Betriebssystembereitstellung mit der OMIMSSC-Konsolenerweiterung für SCVMM

## Info über diese Aufgabe

Gehen Sie wie folgt vor, um das Betriebssystem auf den ausgewählten Servern bereitzustellen:

### Schritte

- 1 Laden Sie das neueste Dell Deployment ToolKit (DTK) herunter und erstellen Sie ein Start-ISO-Image für die Windows Preinstallation Environment (WinPE). Weitere Informationen finden Sie unter [WinPE-Aktualisierung](#).
- 2 Erstellen Sie ein physisches Computerprofil in SCVMM. Weitere Information finden Sie in der SCVMM-Dokumentation.
- 3 Erstellen Sie eine Ziel-Host-Gruppe in SCVMM. Weitere Information finden Sie in der SCVMM-Dokumentation.
- 4 Erstellen Sie ein Hypervisor-Profil in der OMIMSSC-Konsolenerweiterung für SCVMM. Weitere Informationen finden Sie unter [Erstellen eines Hypervisor-Profiles](#).
- 5 Ermitteln Sie mithilfe der Seite **Discovery** (Ermittlung) einen Referenzserver. Weitere Informationen finden Sie unter [Ermitteln von Servern über manuelle Erkennung](#).
- 6 Erstellen Sie eine Betriebsvorlage. Weitere Informationen finden Sie unter [Erstellen einer Betriebsvorlage](#).
- 7 Weisen Sie eine Betriebsvorlage zu. Weitere Informationen finden Sie unter [Zuweisen einer Betriebsvorlage](#).
- 8 Stellen Sie eine Betriebsvorlage bereit. Weitere Informationen finden Sie unter [Bereitstellen einer Betriebsvorlage](#).

**Tabelle 3. Verschiedene Szenarien für die Hypervisor-Bereitstellung**

Wenn Sie die neuesten Treiber ab Werk und die bandexternen Treiber benötigen	Aktivieren Sie beim Erstellen eines Hypervisor-Profiles die LC-Treiberinitialisierung (Lifecycle Controller).
Wenn Sie die vorhandene Hardwarekonfiguration beibehalten möchten	Deaktivieren Sie bei der Erstellung der Betriebsvorlage das Kontrollkästchen für alle physischen Komponenten.

- 9 Den Jobstatus bei Firmware-Updates und OSD können Sie auf der Seite **Jobs and Logs Center** (Job- und Protokollcenter) anzeigen. Weitere Informationen finden Sie unter [Anzeigen von Informationen in OMIMSSC](#).

# Nicht-Windows-Betriebssystembereitstellungen mit OMIMSSC-Konsolenerweiterungen

## Info über diese Aufgabe

So stellen Sie Nicht-Windows-Betriebssysteme bereit:

### Schritte

- 1 Erstellen Sie eine Betriebsvorlage. Weitere Informationen finden Sie unter [Erstellen einer Betriebsvorlage](#).
- 2 Weisen Sie eine Betriebsvorlage zu. Weitere Informationen finden Sie unter [Zuweisen einer Betriebsvorlage](#).
- 3 Stellen Sie eine Betriebsvorlage bereit. Weitere Informationen finden Sie unter [Bereitstellen einer Betriebsvorlage](#).

### ANMERKUNG:

Falls die DHCP-Suche bei der Bereitstellung fehlschlägt, tritt auf dem Server eine Zeitüberschreitung auf und er wird nicht in die Sammlung **Managed Lifecycle Controller Lifecycle Controller (ESXi)** in SCCM verschoben.

# Anwenden von Aktualisierungen auf Server

## Info über diese Aufgabe

Sie können die ausgewählten Server oder Servergruppen unter Verwendung der folgenden Aktualisierungsquellen aktualisieren:

- Online FTP- und lokale FTP-Quelle
- Online HTTP und lokales HTTP
- Lokales Dell Repository Manager (DRM)-Repository

### Schritte

- 1 Im Vorfeld einer Aktualisierung sollten Sie sich zunächst alle Informationen zu den Aktualisierungsquellen und Aktualisierungsgruppen anschauen. Weitere Informationen zu Aktualisierungsquellen finden Sie im Kapitel zum Thema [Aktualisierungsquellen](#). Vergewissern Sie sich, dass eine Aktualisierungsquelle vorhanden ist. Weitere Informationen finden Sie unter [Creating an update source](#) (Erstellen einer Aktualisierungsquelle).
- 2 Führen Sie eine Serverermittlung durch oder synchronisieren Sie Ihre Server mit der registrierten MSSC-Umgebung. Weitere Informationen finden Sie im Kapitel zum Thema [Geräteermittlung und Synchronisierung](#). Vergewissern Sie sich, dass die Bestandsinformationen zu den Servern aktuell sind. Weitere Informationen finden Sie unter [Launching configuration and deployment](#) (Beginnen mit der Konfiguration und Bereitstellung).
- 3 Aktualisieren Sie die Server mithilfe einer der folgenden Optionen:
  - Wählen Sie die gewünschten Servergruppen aus, um die Aktualisierungen anzuwenden. Weitere Informationen finden Sie unter [Applying updates on servers](#) (Anwenden von Aktualisierungen auf Server).

**ANMERKUNG: Wählen Sie Zurückstufen zulassen aus, um die Firmware-Version der Komponenten zurückzustufen.**

- Verwenden Sie die Komponente Firmware-Aktualisierung unter Betriebsvorlage (Betriebsvorlage). Weitere Informationen finden Sie unter [Creating Betriebsvorlage](#) (Erstellen einer Betriebsvorlage).
- 4 Aktualisieren Sie die Aktualisierungsquelle per Abfrage und Benachrichtigung mit dem neuesten Katalog. Weitere Informationen finden Sie unter [Polling and notification](#) (Abfrage und Benachrichtigung).

## Konfigurieren von ersetzten Komponenten

Informationen zum Aktualisieren einer ersetzten Serverkomponente auf die erforderliche Firmware-Version und/oder zum Konfigurieren der alten Komponente finden Sie unter [Anwenden von Firmware- und Konfigurationseinstellungen](#).

## Exportieren und Importieren von Serverprofilen

So exportieren und importieren Sie ein Serverprofil:

- 1 Erstellen Sie einen Schutz-Vault. Weitere Informationen finden Sie unter [Erstellen eines Schutz-Vaults](#).
- 2 Exportieren Sie ein Serverprofil. Weitere Informationen finden Sie unter [Erstellen eines Export-Jobs](#).
- 3 Exportieren Sie ein Serverprofil einschließlich der RAID-Konfiguration und importieren Sie ein Serverprofil einschließlich der RAID-Konfiguration. Weitere Informationen finden Sie unter [Wiederherstellung](#).

# Profile

Mithilfe von Profilen können Sie Ihre Anmeldeinformationen verwalten und die zur Bereitstellung verwendeten WinPE-Abbilder anpassen. Unten sehen Sie eine Liste der in OMIMSSC unterstützten Profiltypen.

Themen:

- [Info zu Anmeldeprofilen](#)
- [Hypervisor-Profile](#)

## Info zu Anmeldeprofilen

Anmeldeprofile vereinfachen die Verwendung und Verwaltung von Benutzeranmeldeinformationen durch Authentifizieren der rollenbasierten Funktionen des Benutzers. Jedes Anmeldeprofil enthält einen Benutzernamen und ein Kennwort für ein einzelnes Benutzerkonto. Ein Anmeldeprofil authentifiziert die rollenbasierten Funktionen eines Benutzers. Das Gerät verwendet ein Anmeldeprofil zur Verbindung mit dem iDRAC der verwalteten Systeme.

Sie können Anmeldeprofile auch für den Zugriff auf die FTP-Site und die auf Windows-Freigaben verfügbaren Ressourcen und für die Verwendung unterschiedlicher Funktionen von iDRAC verwenden.

Sie können vier Typen von Anmeldeprofilen erstellen:

- Geräte-Anmeldeprofil – Dieses Profil wird für die Anmeldung am iDRAC oder am Chassis Management Controller (CMC) verwendet.

**ANMERKUNG:** Wird kein Standardprofil erstellt oder ausgewählt, wird die werksseitige iDRAC-Einstellung verwendet. Der Standardbenutzername lautet `root` und das Kennwort `calvin`.

Das Standard-iDRAC-Profil wird für den Zugriff auf den Server verwendet, wenn Sie einen Server ermitteln oder eine Synchronisierung durchführen.

**ANMERKUNG:** Im Standard-CMC-Profil lautet der Benutzername `root` und das Kennwort `calvin`. Damit wird zum Abrufen von Gehäuse-Informationen auf den modularen Server zugegriffen.

**ANMERKUNG:** Verwenden Sie das Geräte-Anmeldeprofil zum Ermitteln von Servern, Anmelden am CMC, Beheben von Synchronisierungsproblemen und zum Bereitstellen des Betriebssystems.

- Windows Credential Profile (Windows-Anmeldeprofil) – Dieses Profil wird bei der Erstellung einer DRM-Aktualisierungsquelle für den Zugriff auf Windows-Freigaben verwendet.
- FTP Credential Profile (FTP-Anmeldeprofil) – Dieses Profil wird für den Zugriff auf die FTP-Site verwendet.
- Proxy Server Credentials (Proxy-Server-Anmeldeinformationen) – Dieses Profil wird für die Bereitstellung von Proxy-Anmeldeinformationen für den Zugriff auf FTP-Sites für Aktualisierungen verwendet.

## Vordefinierte Anmeldeprofile

Das Konto **SYSTEM DEFAULT FTP** (SYSTEMSTANDARD-FTP) ist ein vordefiniertes Anmeldeprofil mit FTP-Anmeldeinformationen, für die als **Username** (Benutzername) und **Password** (Kennwort) der Wert **anonymous** (anonym) festgelegt ist. Dieses Profil kann nicht bearbeitet werden. Es wird für den Zugriff auf `ftp.dell.com` verwendet.

# Erstellen eines Anmeldeprofils

## Info über diese Aufgabe

Bei der Erstellung eines Anmeldeprofils sollten Sie Folgendes bedenken:

- Wenn ein Geräte-Anmeldeprofil erstellt wird, wird für die Serververwaltung ein zugehöriger **RunAsAccount** in **SCVMM** erstellt. Der Name dieses **RunAsAccount** lautet `Dell_CredentialProfileName`.
- Ist im iDRAC kein Anmeldeprofil hinterlegt, werden bei der automatischen Ermittlung die werkseitigen Standardeinstellungen des iDRAC verwendet. Der Standardbenutzername ist **root**, das zugehörige Kennwort **calvin**.

## Schritte

1 In OMIMSSC haben Sie zwei Möglichkeiten, ein Anmeldeprofil zu öffnen:

- Klicken Sie im OMIMSSC-Dashboard auf **Create Credential Profile** (Anmeldeprofil erstellen).
- Klicken Sie im Navigationsbereich auf **Profiles > Credential Profile** („Profile“ > „Anmeldeprofil“) und dann auf **Create** (Erstellen).

2 Wählen Sie auf der Seite **Credential Profile** (Anmeldeprofil) aus, welchen Typ von Anmeldeprofil Sie verwenden möchten.

OMIMSSC unterstützt vier Typen von Anmeldeprofilen. Ein Anmeldeprofil ist bereits vordefiniert. Sie können die folgenden vier Typen von Anmeldeprofilen erstellen:

- **Device Credential Profile** (Geräte-Anmeldeprofil): Dieses Profil dient zur Anmeldung beim iDRAC oder beim Chassis Management Controller (CMC).

**ANMERKUNG:** Wählen Sie bei der Erstellung eines Profils des Typs **Device Credential Profile** (Geräte-Anmeldeprofil) die Option **iDRAC** aus, um das Profil als Standardprofil für den iDRAC festzulegen. Wählen Sie **CMC** aus, um es als Standardprofil für den Chassis Management Controller (CMC) festzulegen. Wählen Sie **None** (Kein), wenn das Profil nicht als Standardprofil festgelegt werden soll.

- Wenn ein Geräte-Anmeldeprofil erstellt wird, wird für die Serververwaltung ein zugehöriger **RunAsAccount** in **SCVMM** erstellt. Sein Name lautet `Dell_CredentialProfileName`.
  - Wir empfehlen, den **RunAsAccount** weder zu bearbeiten noch zu löschen.
- Wenn Sie das Geräte-Anmeldeprofil löschen, wird auch der zugehörige **RunAsAccount** aus **SCVMM** gelöscht. Das entsprechende Anmeldeprofil wird dann in OMIMSSC nicht mehr angezeigt.
- **Windows Credential Profile** (Windows-Anmeldeprofil): Dieses Profil dient zum Zugriff auf freigegebene Ordner unter Windows.
- **FTP Credential Profile** (FTP-Anmeldeprofil): Dieses Profil dient zum Zugriff auf die FTP-Website.

**ANMERKUNG:** Das standardmäßig in der Appliance verfügbare FTP-Anmeldeprofil heißt **System Default FTP**.

- **SYSTEM DEFAULT FTP** (Standard-FTP-Profil für System): Dies ist ein vordefiniertes Anmeldeprofil mit FTP-Anmeldeinformationen. Das Passwortfeld ist bei diesem Typ kein Pflichtfeld.
- **Proxy-Server-Anmeldeinformationen:** Dieses Profil stellt Proxy-Anmeldeinformationen für FTP-Websites, die bei Firmware-Aktualisierungen verwendet werden.

3 Geben Sie unter **Domain** (Domäne) die Domänendetails für die Windows-Anmeldeinformationen an und unter **Proxy Server URL** (Proxy-Server-URL) die URL des Proxy-Servers im Format `http://hostname:port` oder `http://IPaddress:port`. Wählen Sie dann unter **Default Profile for** (Standardprofil für) aus, ob das Profil das Standardprofil für die Anmeldung beim iDRAC oder für die Anmeldung beim CMC sein soll. Wählen Sie **None** (Kein) aus, wenn Sie das Profil nicht als Standardprofil festlegen möchten.

**ANMERKUNG:** Die Option **Default Profile for** (Standardprofil für) ist nur für Geräte-Anmeldeprofile verfügbar.

4 Klicken Sie auf **Finish** (Fertigstellen), um das Profil zu erstellen.

# Ändern eines Anmeldeprofils

## Info über diese Aufgabe

Berücksichtigen Sie Folgendes, wenn Sie ein Anmeldeprofil ändern möchten:

- Nach dem Erstellen können Sie den Typ eines Anmeldeprofils nicht ändern. Sie können jedoch andere Felder ändern. Um die Änderungen anzuzeigen, aktualisieren Sie den Bildschirm.

- Sie können ein Anmeldeprofil eines Gerätetyps nicht ändern, wenn es gerade verwendet wird.
- Sie können ein Anmeldeprofil nicht ändern, wenn es verwendet wird.

### Schritte

- 1 Wählen Sie das Anmeldeprofil aus, das Sie ändern möchten, klicken Sie auf **Edit** (Bearbeiten) und aktualisieren Sie das Profil.
- 2 Um die Änderungen zu speichern, klicken Sie auf **Save** (Speichern).

## Löschen eines Anmeldeprofils

### Info über diese Aufgabe

Berücksichtigen Sie Folgendes, wenn Sie ein Anmeldeprofil löschen möchten:

- Wenn ein Geräte-Anmeldeprofil gelöscht wird, wird das zugehörige „**Ausführen als**“-Konto ebenfalls aus SCVMM gelöscht.
- Sobald der **RunAsAccount** aus SCVMM gelöscht wurde, ist das zugehörige Anmeldeprofil nicht mehr in der Appliance verfügbar.
- Wenn Sie ein Anmeldeprofil löschen möchten, das im Rahmen einer Serverermittlung verwendet wird, löschen Sie zuerst die ermittelten Serverinformationen und anschließend das Anmeldeprofil.
- Wenn Sie ein Geräte-Anmeldeprofil löschen möchten, das im Rahmen einer Bereitstellung verwendet wird, müssen Sie zunächst die in der SCVMM-Umgebung bereitgestellten Server löschen, bevor Sie das Anmeldeprofil löschen können.
- Sie können ein Anmeldeprofil, das in einer Aktualisierungsquelle verwendet wird, nicht löschen.

### Schritt

Wählen Sie das Anmeldeprofil aus, das Sie löschen möchten, und klicken Sie auf **Delete** (Löschen).

## Hypervisor-Profile

Ein Hypervisor-Profil enthält ein benutzerdefiniertes WinPE-ISO (das WinPE-ISO wird auch für die Hypervisor-Bereitstellung verwendet), eine Host-Gruppe und ein Host-Profil aus SCVMM sowie LC-Treiber für die Initialisierung.

**ANMERKUNG:** Hypervisor-Profile können nur für die OMIMSSC-Konsolenerweiterung für SCVMM angewendet werden.

## Erstellen eines Hypervisor-Profiles

Sie können ein Hypervisor-Profil erstellen und mithilfe dieses Profils das Betriebssystem auf Servern bereitstellen.

### Voraussetzungen

- Wenn Sie ein Hypervisor-Profil erstellen, wird gleichzeitig auch die erforderliche WinPE-ISO-Datei erstellt. Sie wird im freigegebenen Ordner von OMIMSSC IG abgelegt. Wie Sie das WinPE-Abbild aktualisieren können, erfahren Sie im Abschnitt zum Thema [WinPE-Aktualisierung](#).
- Erstellen Sie eine Hostgruppe, ein Hostprofil oder ein Profil für physische Computer in SCVMM.

### Schritte

- 1 Führen Sie eine der folgenden Aktionen in OMIMSSC durch:
  - Klicken Sie im Dashboard von OMIMSSC auf **Create Hypervisor Profiles** (Hypervisor-Profile erstellen).
  - Klicken Sie im linken Navigationsbereich auf **Profiles > Hypervisor Profiles > Create** („Profile“ > „Hypervisor-Profile“ > „Erstellen“).
- 2 Klicken Sie nun auf **Hypervisor Profile Wizard > Welcome > Next** („Assistent für Hypervisor-Profile“ > „Willkommen“ > „Weiter“).
- 3 Geben Sie unter **Hypervisor Profile** (Hypervisor-Profil) einen Namen für das Profil sowie eine Beschreibung ein und klicken Sie auf **Next** (Weiter).
- 4 Gehen Sie auf der Seite **SCVMM information** (SCVMM-Informationen) wie folgt vor:
  - a Wählen Sie unter **SCVMM Host Group Destination** (SCVMM-Hostgruppenziel) aus dem Drop-Down-Menü die SCVMM-Hostgruppe aus, der der Host hinzugefügt werden soll.

- b Wählen Sie unter **SCVMM Host Profile/Physical Computer Profile** (SCVMM-Hostprofil/SCVMM-Profil für physische Computer) das SCVMM-Hostprofil oder das SCVMM-Profil für physische Computer aus, das die auf die Server anzuwendenden Konfigurationsinformationen enthält.
- 5 Gehen Sie unter **WinPE Boot Image Source** (Quelle des WinPE-Startabbilds) wie folgt vor:
  - a Wählen Sie die gewünschte Methode für den Zugriff auf das Betriebssystem sowie die zugehörigen Einstellungen aus. Wechseln Sie anschließend in das Feld **Network WinPE ISO Name** (Name der WinPE-ISO-Datei auf der Netzwerkfreigabe).
  - b Wählen Sie die gewünschte Betriebssystem-ISO-Datei aus und klicken Sie auf **Next** (Weiter).
- 6 (Optional) Gehen Sie wie folgt vor, um die LC-Treiberinjektion zu aktivieren:
  - a Wählen Sie das Betriebssystem aus, das Sie bereitstellen möchten, damit die passenden Treiber geladen werden.
  - b Aktivieren Sie die Option **Enable LC Drivers Injection** (LC-Treiberinjektion aktivieren).
  - c Wählen Sie unter **Hypervisor Version** (Hypervisor-Version) die Hypervisor-Version aus.
- 7 Klicken Sie unter **Zusammenfassung** auf **Fertigstellen**.

## Ändern eines Hypervisor-Profiles

### Info über diese Aufgabe

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

- Sie können Hostprofile, Hostgruppen und Treiber vom Lifecycle Controller her ändern.
- Sie können den Namen des WinPE-ISO-Abbilds ändern. Das ISO-Abbild selbst lässt sich jedoch nicht ändern.

### Schritte

- 1 Wählen Sie das Profil aus, das Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.
- 2 Geben Sie die gewünschten Details ein und klicken Sie dann auf **Finish** (Fertigstellen).

## Löschen eines Hypervisor-Profiles

Wählen Sie das Profil aus, das Sie löschen möchten, und klicken Sie dann auf **Delete** (Löschen).

# Beginnen mit der Konfiguration und Bereitstellung

Auf der Seite **Configuration and Deployment** (Konfiguration und Bereitstellung) werden alle nicht zugewiesenen Server sowie alle Host-Server aufgeführt. Über den Host-Namen oder die IP-Adresse eines Servers können Sie die Details des jeweiligen Servers abrufen, zum Beispiel die iDRAC-IP-Adresse oder den Host-Namen, den Serverbezeichner, den Cluster-FQDN, die Service-Tag-Nummer des Gehäuses, das Servermodell, die Servergeneration, Angaben zu Prozessor und Speicher und den Konformitätsstatus. Wenn Sie den Mauszeiger auf der Spalte **Hardware Compatibility** (Hardwarekompatibilität) platzieren, wird jeweils die Version von BIOS, iDRAC, LC und den Treiberpaketen angezeigt.

## Info über diese Aufgabe

Bevor Sie die OMIMSSC-Konsolenerweiterungen starten, müssen Sie im iDRAC die Einstellung „System Lockdown Mode“ (Systemsperrmodus) überprüfen. Die Einstellung „System Lockdown Mode“ (Systemsperrmodus) ist im iDRAC für alle PowerEdge-Server ab Generation 14 verfügbar. Ist sie konfiguriert, ist die Systemkonfiguration gesperrt (inklusive der Firmware-Aktualisierungen). Sobald die Einstellung „System Lockdown Mode“ (Systemsperrmodus) aktiviert ist, können die Benutzer die Konfigurationseinstellungen nicht mehr ändern. Diese Einstellung soll unbeabsichtigte Änderungen am System verhindern. Der Status der Einstellung „System Lockdown Mode“ (Systemsperrmodus) auf einem Server wird durch ein Vorhängeschloss-Symbol vor seiner iDRAC-IP-Adresse angezeigt.

- Ist die Einstellung auf einem Server aktiviert, wird vor seiner iDRAC-IP-Adresse ein geschlossenes Vorhängeschloss angezeigt.
- Ist die Einstellung auf einem Server deaktiviert, wird vor seiner iDRAC-IP-Adresse ein offenes Vorhängeschloss angezeigt.

Weitere Informationen zum iDRAC-Systemsperrmodus finden Sie in der iDRAC-Dokumentation unter [dell.com/support](http://dell.com/support).

**ⓘ ANMERKUNG: Auf PowerEdge-Servern der 14. Generation müssen Sie die Einstellung „System Lockdown Mode“ (Systemsperrmodus) auf den verwalteten Hosts manuell über die iDRAC-Konsole deaktivieren.**

Auf der Seite **Configuration and Deployment** (Konfiguration und Bereitstellung) können Sie Folgendes tun:

- [Server ermitteln](#)
- [Seite aktualisieren, um die neuesten Informationen anzuzeigen](#)
- [Server aus OMIMSSC löschen](#)
- [Synchronisierungen mit registrierten MSSC-Umgebungen durchführen](#)
- [Synchronisierungsfehler beheben](#)
- [Betriebsvorlage zuweisen und die Konformität mit einer Betriebsvorlage prüfen](#)
- [Betriebsvorlage bereitstellen](#)
- [Host-Server der zugehörigen Clustergruppe und dem zugehörigen Chassis zuordnen](#)
- [iDRAC-Konsole starten](#)

**ⓘ ANMERKUNG: Wenn der Server zu keinem Gehäuse gehört, wird für Chassis Service Tag (Service-Tag-Nummer des Gehäuses) kein Wert angezeigt.**

**ⓘ ANMERKUNG: Ist der Host-Server Teil eines Clusters, können Sie anhand der Informationen in den Spalten Cluster FQDN (Cluster-FQDN) und Chassis Service Tag (Service-Tag-Nummer des Gehäuses) sehen, zu welcher Clustergruppe und welchem Gehäuse er gehört.**

**ⓘ ANMERKUNG: Für Server, die in früheren Versionen von OMIMSSC ermittelt wurden, müssen Sie zunächst erneut eine Ermittlung durchführen, damit Sie mit ihnen arbeiten können.**

**ⓘ ANMERKUNG: Wenn Sie sich als delegierter Administrator bei OMIMSSC anmelden, können Sie alle Host-Server und nicht zugewiesenen Server sehen, die nicht spezifisch zu dem betreffenden Benutzer gehören. Bevor Sie Aktionen auf diesen Servern durchführen, sollten Sie sich also vergewissern, dass Sie über die erforderlichen Berechtigungen verfügen.**

- ① **ANMERKUNG:** Ist der Server konform mit der ihm zugewiesenen Betriebsvorlage, wird neben der zugewiesenen Betriebsvorlage ein grünes Kästchen mit einem Häkchen angezeigt.
- ① **ANMERKUNG:** Ist der Server nicht mit der ihm zugewiesenen Betriebsvorlage konform, wird neben der zugewiesenen Betriebsvorlage eine rote Warnmeldung angezeigt.

So zeigen Sie Server an:

### Schritt

Klicken Sie in der OMIMSSC-Konsolenerweiterung auf **Configuration and Deployment** (Konfiguration und Bereitstellung).

- ① **ANMERKUNG:** Da diese OMIMSSC-Seite nicht benutzerspezifisch ist, werden auf ihr sämtliche Servergruppen aufgeführt, die in der registrierten MSSC-Umgebung vorhanden sind. Vergewissern Sie sich, dass Sie die nötigen Zugriffsrechte haben, um auf diesen Servern Aktionen durchzuführen.

Auf den Registerkarten **Unassigned Servers** (Nicht zugewiesene Server) und **Hosts** werden alle Server aufgeführt, die in der registrierten MSSC-Umgebung ermittelt oder aus ihr synchronisiert wurden.

# Ermitteln von Servern und Synchronisieren mit der MSSC-Konsole

Serverermittlung bedeutet, dass unterstützte PowerEdge-Bare-Metal-Server oder PowerEdge-Host-Server zu OMIMSSC hinzugefügt werden. Über eine Synchronisierung mit der MSSC-Konsole können Sie darüber hinaus Host-Server aus der SCCM-Konsole oder der SCVMM-Konsole zu OMIMSSC hinzufügen.

Themen:

- Referenzserverkonfigurationen
- Ermitteln von Servern in OMIMSSC
- Ermitteln von Servern in der OMIMSSC-Konsolenerweiterung für SCCM
- Ermitteln von Servern in der OMIMSSC-Konsolenerweiterung für SCVMM
- Systemanforderungen für verwaltete Systeme
- Ermitteln von Servern über die automatische Ermittlung
- Ermitteln von Servern über die manuelle Ermittlung
- Synchronisieren von OMIMSSC-Konsolenerweiterungen mit einer registrierten SCCM-Umgebung
- Synchronisieren der OMIMSSC-Konsolenerweiterung mit einer registrierten SCVMM-Umgebung
- Synchronisieren mit registriertem MSSC
- Beheben von Synchronisierungsfehlern
- Löschen von Servern aus OMIMSSC
- Starten der iDRAC-Konsole

## Referenzserverkonfigurationen

Eine Referenzserverkonfiguration ist eine Serverkonfiguration, in der die Startreihenfolge, das BIOS, die RAID-Einstellungen, die Hardwarekonfiguration, die Attribute für die Firmware-Aktualisierung und die Betriebssystemparameter optimal auf die Anforderungen der Organisation abgestimmt sind.

Die Ermittlung eines Referenzservers erfolgt über die Erfassung dieser Einstellungen in einer Betriebsvorlage. Diese Vorlage lässt sich anschließend auf alle Server mit derselben Hardwarekonfiguration replizieren.

## Ermitteln von Servern in OMIMSSC

OMIMSSC kann Hosts und nicht zugewiesene Server ermitteln. Die Informationen zu den ermittelten Servern werden in der OMIMSSC-Datenbank gespeichert.

Sobald ein Server ermittelt wurde, ist Folgendes zu beachten:

- Der ermittelte Server wird der Registerkarte **Hosts** oder der Registerkarte **Unassigned** (Nicht zugewiesen) auf der Seite **Configuration and Deployment** (Konfiguration und Bereitstellung) in OMIMSSC hinzugefügt.
- Der ermittelte Server wird als hardwarekompatibel gekennzeichnet, wenn die installierte Version der LC-Firmware, des iDRAC und des BIOS von OMIMSSC unterstützt werden. Weitere Informationen zu den unterstützten Versionen finden Sie in den *OpenManage Integration for Microsoft System Center Release Notes* (Versionshinweise für OpenManage Integration for Microsoft System Center).
- Der ermittelte Server belegt eine Lizenz.

Der Wert für **Licensed Nodes** (Lizenzierte Knoten) auf der Seite **License Center** (Lizenzcenter) wird um die Anzahl der ermittelten Server herabgesetzt.

- Wird ein PowerEdge-Server ermittelt, auf dem bereits ein Betriebssystem bereitgestellt ist und der bereits in der SCCM-Konsole oder der SCVMM-Konsole registriert ist, wird der Server als Host-Server auf der **Hosts**-Registerkarte der OMIMSSC-Konsolenerweiterung angezeigt, in der der Ermittlungsjob angestoßen wurde.
  - Wenn es sich bei dem Host um einen modularen Server handelt, wird auf der Seite **Configuration and Deployment** (Konfiguration und Bereitstellung) auch die Service-Tag-Nummer des Gehäuses angezeigt, in dem der Server installiert ist.
- Wird ein PowerEdge-Server ermittelt, der noch nicht in SCCM oder SCVMM aufgeführt ist, wird der Server in allen registrierten OMIMSSC-Konsolenerweiterungen auf der Registerkarte **Unassigned** als nicht zugewiesener Server aufgeführt.

Dell EMC Server können anhand ihrer iDRAC-IP-Adresse ermittelt werden. Hierzu stehen zwei Optionen zur Verfügung:

- [Auto-Ermittlung](#)
- [Manuelle Ermittlung](#)

## Ermitteln von Servern in der OMIMSSC-Konsolenerweiterung für SCCM

Nach der Ermittlung eines Servers wird der Server zu einer der folgenden vordefinierten SCCM-Gruppen oder -Sammlungen hinzugefügt – **All Lifecycle Controller Servers collection** (Sammlung aller Lifecycle Controller-Server) und **Import Dell Server collection** (Dell Server Sammlung importieren), die unter dem **Gerätesammlungen** erstellt werden.

Wenn der ermittelte Server nicht in SCCM vorhanden ist oder keine vordefinierten Gruppen oder Sammlungen in SCCM bestehen, werden die vordefinierten Sammlungen erstellt und die ermittelten Server werden der entsprechenden Gruppe hinzugefügt.

**ANMERKUNG:** Ein ermittelter Server wird als kompatibel mit der Hardware gekennzeichnet, wenn er unterstützte Versionen der LC-Firmware, von iDRAC oder dem BIOS enthält, die für die Interaktion mit OMIMSSC erforderlich sind. Weitere Informationen zu unterstützten Versionen finden Sie in den *Versionshinweisen zu OpenManage Integration for Microsoft System Center*.

## Ermitteln von Servern in der OMIMSSC-Konsolenerweiterung für SCVMM

Sie können Hyper-V-Hosts, modulare Hyper-V-Hosts und nicht zugewiesene Server in der OMIMSSC-Konsolenerweiterung für SCVMM ermitteln.

**ANMERKUNG:** Wenn der Host zu einem Cluster gehört, wird der vollständig qualifizierte Domänenname (FQDN) des Clusters angezeigt.

## Systemanforderungen für verwaltete Systeme

Verwaltete Systeme sind Systeme, die über OMIMSSC verwaltet werden. Für die Ermittlung von Servern mit der OMIMSSC-Konsolenerweiterung für SCCM oder der OMIMSSC-Konsolenerweiterung für SCVMM sind folgende Systemanforderungen erforderlich:

- Die OMIMSSC-Konsolenerweiterung für SCVMM unterstützt modulare und monolithische Servermodelle auf der 11. und späteren Generationen von PowerEdge-Servern.
- Die OMIMSSC-Konsolenerweiterung für SCCM unterstützt modulare, monolithische und Tower-Servermodelle auf der 11. und späteren Generationen von PowerEdge-Servern.
- Verwenden Sie für die Quell- und Zielkonfiguration denselben Festplattentyp: nur Solid-State (SSD), SAS oder nur Serial ATA (SATA).
- Für ein erfolgreiches Klonen 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 auf verwalteten Systemen „Collect System Inventory on Restart“ (CSIOR, Systembestandsaufnahme bei Neustart erfassen). Weitere Informationen finden Sie in der iDRAC-Dokumentation.

## Ermitteln von Servern über die automatische Ermittlung

Um die Server automatisch zu ermitteln, verbinden Sie den PowerEdge-Server mit dem Netzwerk und schalten Sie die Server für OMIMSSC ein. OMIMSSC ermittelt automatisch die nicht zugewiesenen Dell EMC-Server anhand der Remote-Aktivierungsfunktion von iDRAC. OMIMSSC arbeitet als Bereitstellungsserver und verwendet die iDRAC-Referenz für die automatische Ermittlung von Dell EMC-Servern.

- 1 Erstellen Sie in OMIMSSC ein Geräte-Anmeldeprofil für Dell EMC-Server (durch Angabe der iDRAC-Anmeldeinformationen und Festlegen dieses Profils als Standardprofil). Weitere Informationen finden Sie unter [Erstellen eines Anmeldeprofils](#).
- 2 Um Dell EMC-Server automatisch zu ermitteln, führen Sie die folgenden Aufgaben aus:
  - a Deaktivieren Sie in iDRAC das vorhandene Administratorkonto.

**ANMERKUNG:** Es wird empfohlen, ein Gastbenutzerkonto mit Operatorberechtigungen anzulegen, um sich bei iDRAC im Falle des Fehlschlagens der automatischen Ermittlung anzumelden.

- b Um die automatische Ermittlung auf dem Zielsystem zu aktivieren, aktivieren Sie in den **iDRAC Settings** (iDRAC-Einstellungen) unter **Remote Enablement** (Remote-Aktivierung) die Option **Enabled** (Aktiviert) für die Funktion **Enable Auto-Discovery** (Auto-Ermittlung aktivieren).
- c Geben Sie nach der Aktivierung der automatischen Ermittlung die IP-Adresse des Bereitstellungsservers an (IP-Adresse des Servers, auf dem OMIMSSC installiert ist) und starten Sie den Server neu.

## Ermitteln von Servern über die manuelle Ermittlung

Sie können für PowerEdge-Server eine manuelle Ermittlung auf Basis einer IP-Adresse oder eines IP-Bereichs durchführen. Zur Ermittlung eines Servers müssen Sie seine iDRAC-IP-Adresse und seine Geräteanmeldeinformationen angeben. Bei der Serverermittlung auf Basis eines IP-Bereichs müssen Sie einen IP-Bereich (IPv4) innerhalb eines Subnetzes in Form eines Startbereichs und eines Endbereichs angeben.

- 1 Führen Sie in der OMIMSSC-Konsole eine der folgenden Aktionen durch:
  - Klicken Sie im Dashboard auf **Nicht zugewiesene Server ermitteln**.
  - Klicken Sie im Navigationsbereich auf **Configuration and Deployment** (Konfiguration und Bereitstellung) und anschließend auf **Discover** (Ermitteln).
- 2 Wählen Sie auf der Seite **Discover** (Ermitteln) die gewünschte Option aus:
  - **Discover Using an IP Address** (Ermittlung auf Basis der IP-Adresse): Serverermittlung anhand einer IP-Adresse
  - **Discover Using an IP Range** (Ermittlung auf Basis eines IP-Bereichs): Ermittlung aller Server innerhalb eines bestimmten IP-Bereichs
- 3 Wählen Sie das gewünschte Geräte-Anmeldeprofil aus oder klicken Sie auf **Create New** (Neues erstellen), um ein Geräte-Anmeldeprofil zu erstellen.  
Das ausgewählte Profil wird auf alle Server angewandt.
- 4 Geben Sie unter **Dell iDRAC IP address** (Dell iDRAC-IP-Adresse) die IP-Adresse des Servers ein, der ermittelt werden soll.
- 5 Führen Sie unter **Über eine IP-Adresse oder einen IP-Adressbereich ermitteln** einen der folgenden Schritte aus:
  - Geben Sie unter **IP Address Start Range** (Ab IP-Adressbereich) und **IP Address End Range** (Bis IP-Adressbereich) die gewünschten IP-Adressbereiche ein. Diese Werte repräsentieren jeweils, ab welchem Bereich und bis zu welchem Bereich die Ermittlung durchgeführt werden soll.
  - Aktivieren Sie die Option **Enable Exclude Range** (Ausschlussbereich aktivieren), wenn Sie einen IP-Adressbereich ausschließen möchten. Geben Sie dann über **IP Address Start Range** (Ab IP-Adressbereich) und **IP Address End Range** (Bis IP-Adressbereich) den Bereich an, den Sie ausschließen möchten.
- 6 Geben Sie einen eindeutigen Jobnamen ein und klicken Sie auf **Finish** (Fertigstellen).
- 7 (Optional) Klicken Sie auf **Go to the Job List** (Zur Jobliste), um den Job zu verfolgen.  
Die Seite **Jobs and Logs Center** (Job- und Protokollcenter) wird angezeigt. Erweitern Sie auf der Registerkarte **Running** (Wird ausgeführt) den entsprechenden Job, um den Jobfortschritt zu sehen.

# Synchronisieren von OMIMSSC-Konsolenerweiterungen mit einer registrierten SCCM-Umgebung

Sie können alle in einer SCCM-Umgebung vorhandenen PowerEdge-Server mit OMIMSSC synchronisieren (sowohl Host-Server als auch nicht zugewiesene Server).

## Voraussetzungen

Vor einer Synchronisierung der PowerEdge-Server mit einer OMIMSSC-Konsolenerweiterung und der registrierten SCCM-Konsole oder SCVMM-Konsole müssen Sie Folgendes tun:

- Sie müssen sicherstellen, dass die Informationen aus dem standardmäßigen iDRAC-Anmeldeprofil der jeweiligen Server verfügbar sind.
- Sie müssen die Sammlung **Dell Default Collection** (Dell Standardsammlung) aktualisieren, bevor Sie OMIMSSC mit SCCM synchronisieren. Erkennt SCCM einen nicht zugewiesenen Server, wird dieser Server jedoch zur Sammlung **Import Dell server collection** (Sammlung zu importierender Dell Server) hinzugefügt. Damit er der Sammlung **Dell Default Collection** (Dell Standardsammlung) hinzugefügt wird, müssen Sie die iDRAC-IP-Adresse des Servers auf der OOB-Seite eintragen.

## Info über diese Aufgabe

Wird der Server nach der Synchronisierung vom OMIMSSC mit SCCM nicht in SCCM aufgeführt, werden die Sammlung **All Dell Lifecycle Controller Servers** (Alle Dell Lifecycle Controller-Server) und die Sammlung **Import Dell server** (Zu importierende Dell Server) unter **Device Collections** (Gerätesammlungen) erstellt und der Server wird der entsprechenden Gruppe hinzugefügt.

# Synchronisieren der OMIMSSC-Konsolenerweiterung mit einer registrierten SCVMM-Umgebung

Sie können alle in SCVMM-Konsolen verwalteten Hyper-V-Hosts, Hyper-V-Hostcluster, modularen Hyper-V-Hosts und nicht zugewiesenen Server von Dell EMC mit der OMIMSSC-Konsolenerweiterung für SCVMM synchronisieren. Nach der Synchronisierung erhalten Sie zudem die neuesten Bestandsinformationen zu der auf den Servern installierten Firmware.

Beachten Sie Folgendes, bevor Sie OMIMSSC mit SCVMM synchronisieren:

- Bei der Synchronisierung werden die Details des Standard-iDRAC-Anmeldeprofils der Server verwendet.
- Wenn die IP-Adresse des iDRAC nicht auf dem Baseboard Management Controller (BMC) des Host-Servers hinterlegt ist, können Sie den Host-Server nicht mit OMIMSSC synchronisieren. Konfigurieren Sie also zunächst den BMC in SCVMM (weitere Informationen siehe MSDN-Artikel unter [technet.microsoft.com](http://technet.microsoft.com)) und synchronisieren Sie erst dann OMIMSSC mit SCVMM.
- Da SCVMM R2 Unterstützung für eine große Anzahl von Hosts pro Umgebung bietet, ist die Synchronisierung ein zeitintensiver Vorgang. Die konkrete Synchronisierung läuft wie folgt ab:
  - Die in der SCVMM-Umgebung aufgeführten Hosts werden der Registerkarte **Hosts** in der OMIMSSC-Appliance hinzugefügt.
  - Wenn ein Server als nicht zugewiesener Server aufgeführt ist und SCVMM manuell hinzugefügt wird, wird er nach der Synchronisierung der Registerkarte **Hosts** in der OMIMSSC-Appliance hinzugefügt.
  - Wenn ein Host-Server zu einem Hyper-V-Cluster gehört, werden die Details des Clusters auf der Registerkarte **Hosts** aufgeführt. Der Host-Server wird der Cluster-Aktualisierungsgruppe hinzugefügt bzw. in diese Gruppe verschoben. Die entsprechenden Informationen sind auf der Seite **Maintenance Center** (Wartungcenter) einsehbar.
  - Wenn es sich bei dem Host um einen modularen Server handelt, wird der Registerkarte **Hosts** außerdem die Service-Tag-Nummer des Gehäuses hinzugefügt, in dem der Server installiert ist. Gehört der modulare Host-Server nicht zu einem Hyper-V-Cluster, wird er der Gehäuse-Aktualisierungsgruppe hinzugefügt bzw. in diese Gruppe verschoben. Die entsprechenden Informationen sind auf der Seite **Maintenance Center** (Wartungcenter) aufgeführt.
  - Alle Änderungen an den Host-Bestandsinformationen (Host-Name, iDRAC-IP-Adresse, Speicher, Cluster-Zugehörigkeit usw.) werden auf die Registerkarte **Hosts** übernommen.
  - Wurde eine Standardaktualisierungsquelle angegeben, werden die Firmware-Bestandsinformationen mit der Aktualisierungsquelle abgeglichen und die neuesten Informationen werden der Aktualisierungsgruppe hinzugefügt.

# Synchronisieren mit registriertem MSSC

Klicken Sie in OMIMSSC auf **Configuration and Deployment** (Konfiguration und Bereitstellung) und dann auf **Synchronize with OMIMSSC** (Mit OMIMSSC synchronisieren), um alle in der registrierten MSSC-Konsole aufgeführten Hosts mit der OMIMSSC-Appliance zu synchronisieren.

## Beheben von Synchronisierungsfehlern

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

### Info über diese Aufgabe

- ① **ANMERKUNG:** Beheben Sie für alle Server, die aufgrund von Problemen, wie ungültigen Anmeldeinformationen oder ungültiger iDRAC-IP-Adresse oder Konnektivität oder anderen Problemen, nicht synchronisiert sind, zuerst die Probleme und synchronisieren Sie sie erst danach.
- ① **ANMERKUNG:** Während der Neusynchronisierung werden Host-Server, die aus der registrierten MSSC-Umgebung gelöscht wurden, in die Registerkarte **Unassigned Servers** (Nicht zugewiesene Server) in die OMIMSSC-Konsolenerweiterungen verschoben. Wenn ein Server außer Betrieb genommen wurde, entfernen Sie diesen Server aus der Liste der nicht zugewiesenen Server.

So führen Sie eine Neusynchronisierung von Servern mit Problemen im Anmeldeprofil durch:

### Schritte

- 1 Klicken Sie in OMIMSSC auf **Configuration and Deployment** (Konfiguration und Bereitstellung) und dann auf **Resolve Sync Errors** (Synchronisierungsfehler beheben).
- 2 Wählen Sie die Server für die Neusynchronisierung und das Anmeldeprofil aus oder klicken Sie auf **Create New** (Neu erstellen), um ein Anmeldeprofil zu erstellen.
- 3 Geben Sie einen Job-Namen an und aktivieren Sie bei Bedarf die Option **Go to the Job List** (Zur Job-Liste wechseln), um den Job-Status automatisch anzuzeigen, sobald der Job gesendet wurde.
- 4 Klicken Sie auf **Finish** (Fertig stellen), um den Job zu senden.

## Löschen von Servern aus OMIMSSC

### Info über diese Aufgabe

Nach dem Löschen eines Servers wird die genutzte Lizenz freigegeben.

Sie können einen in OMIMSSC aufgelisteten Server basierend auf den folgenden Kriterien löschen:

- Ein nicht zugewiesener Server, der auf der Registerkarte **Unassigned servers** (Nicht zugewiesene Server) aufgeführt ist.
- Wenn Sie einen Host-Server löschen möchten, der in einer registrierten SCCM- oder SCVMM-Instanz bereitgestellt ist und auf der Registerkarte **Hosts** in OMIMSSC steht, müssen Sie den Server zuerst in SCCM oder SCVMM löschen und dann in OMIMSSC.

### Schritte

- 1 Klicken Sie in der OMIMSSC-Konsole auf **Configuration and deployment** (Konfiguration und Bereitstellung).
  - So löschen Sie nicht zugewiesene Server: Wählen Sie den Server auf der Registerkarte **Unassigned Servers** (Nicht zugewiesene Server) aus und klicken Sie auf **Delete** (Löschen).
  - So löschen Sie Host-Server: Wählen Sie auf der Registerkarte **Host Servers** (Host Server) den Server aus und klicken Sie auf **Delete** (Löschen).
- 2 Klicken Sie im Dialogfeld zur Bestätigung auf **Yes** (Ja).

# Starten der iDRAC-Konsole

Klicken Sie auf der Seite **Configuration and Deployment** (Konfiguration und Bereitstellung) auf der Registerkarte **Unassigned Servers** (Nicht zugewiesene Server) oder der Registerkarte **Hosts** unter **iDRAC IP** (iDRAC-IP) auf die iDRAC-IP-Adresse des Servers.

**ANMERKUNG:** Wenn Sie das Windows 2012 Betriebssystem und die iDRAC Firmware-Version ab 2.40.40.40 verwenden, aktivieren Sie die Unterstützung für TLS 1.1 oder höher je nach Web-Browser, um die iDRAC-Konsole zu starten.

# OMIMSSC-Lizenzierung

OMIMSSC verfügt über zwei Arten von Lizenzen:

- Testlizenz – Dies ist eine Testlizenz für fünf Server (Hosts oder nicht zugewiesen), die nach der Installation automatisch importiert wird. Diese Lizenz kann nur für die 11. und spätere Generationen der Dell EMC-Server verwendet werden.
- Produktionslizenz – Sie können eine Produktionslizenz von Dell EMC für eine beliebige Anzahl von mit OMIMSSC zu verwaltenden Servern erwerben. Diese Lizenz umfasst Produktsupport und OMIMSSC-Geräteaktualisierungen.

Wenn Sie eine Lizenz erwerben, steht die XML-Datei (Lizenzschlüssel) zum Herunterladen im Dell Digital Store bereit. Falls Sie Ihren Lizenzschlüssel nicht herunterladen können, suchen Sie im Dell Support unter [www.dell.com/support/softwarecontacts](http://www.dell.com/support/softwarecontacts) nach der lokalen Telefonnummer des Dell Supports für Ihr Produkt.

Sie können Server in OMIMSSC mit einer einzigen Lizenzdatei ermitteln. Wird ein Server in OMIMSSC ermittelt, wird eine Lizenz verwendet. Wird ein Server gelöscht, wird eine Lizenz freigegeben. In das Aktivitätsprotokoll von OMIMSSC wird für die folgenden Aktivitäten ein Eintrag aufgenommen:

- Lizenzdatei wurde importiert.
- Server wurde aus OMIMSSC gelöscht und die Lizenz freigegeben.
- Lizenz wird nach Ermittlung eines Servers verwendet.

Beim Upgrade einer Testlizenz auf eine Produktionslizenz wird die Testlizenz mit der Produktionslizenz überschrieben. Die Anzahl der **Lizenzierte Knoten** entspricht der Anzahl der erworbenen Produktionslizenzen.

Themen:

- [Optionen nach dem Hochladen von Lizenzen](#)
- [Erzwingung](#)
- [Importieren einer Lizenz in OMIMSSC](#)
- [Anzeigen von Lizenzdetails](#)

## Optionen nach dem Hochladen von Lizenzen

Nachfolgend sind die unterstützten Optionen für die Lizenzfunktion in OMIMSSC aufgeführt.

### Lizenzdatei für neue Einkäufe

Bei der Bestellung einer neuen Lizenz erhalten Sie eine E-Mail von Dell mit der Auftragsbestätigung und Sie können die neue Lizenzdatei aus dem Dell Digital Store herunterladen. Die Lizenz liegt im XML-Format vor. Falls die Lizenz in einer ZIP-Datei gepackt ist, entpacken Sie die XML-Lizenzdatei vor dem Hochladen aus der ZIP-Datei.

## Stacking-Lizenzen

Sie können mehrere Produktionslizenzen zur Erhöhung der Anzahl unterstützter Server bis zur Summe der Server in den hochgeladenen Lizenzen stapeln. Eine Testlizenz kann nicht gestapelt werden. Die Anzahl der unterstützten Server kann durch Stacking nicht erhöht werden und erfordert die Verwendung mehrerer Geräte.

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

## Ersatz von Lizenzen

Wenn ein Problem mit Ihrer Bestellung vorliegt oder wenn Sie versuchen, eine modifizierte oder beschädigte Datei hochzuladen, wird eine Fehlermeldung angezeigt. Sie können eine andere Lizenzdatei vom Dell Digital Store anfordern. Die erhaltene Ersatzlizenz enthält die gleiche Berechtigungs-ID wie die vorherige Lizenz. Beim Hochladen einer Ersatzlizenz wird die Lizenz ausgetauscht, falls bereits eine Lizenz mit der gleichen Berechtigungs-ID hochgeladen wurde.

## 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 mehrerer Lizenzdateien mit unterschiedlichen Berechtigungs-IDs zur Erhöhung der Anzahl der Server in OMIMSSC importieren.

## Erzwingung

## Aktualisieren von Lizenzen

Sie sind berechtigt, mit OMIMSSC mit der bestehenden Lizenzdatei für alle unterstützten Servergenerationen zu arbeiten. Falls die Lizenzdatei die neueste Servergeneration nicht unterstützt, müssen Sie neue Lizenzen erwerben.

## Testlizenz

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

## Lizenznutzung in OMIMSSC nach Serverermittlung

Wenn Sie versuchen, einen Host hinzuzufügen oder einen Bare-Metal-Server zu ermitteln, erhalten Sie eine Warnung bezüglich der Lizenznutzung und unter den folgenden Umständen wird empfohlen, neue Lizenzen zu erwerben:

- Wenn die Anzahl der lizenzierten Server die Anzahl der erworbenen Lizenzen überschreitet.
- Wenn die Anzahl der ermittelten 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 überschreiten.

① **ANMERKUNG:** Eine zeitweilig verlängerte Lizenz umfasst 20 Prozent der Gesamtzahl der erworbenen Lizenzen. Die Anzahl der tatsächlichen Lizenzen, die Sie in OMIMSSC verwenden können, ist also die Summe der erworbenen Lizenzen plus der zeitweilig verlängerten Lizenz.

## Importieren einer Lizenz in OMIMSSC

### Info über diese Aufgabe

Befolgen Sie die folgenden Schritte, um eine Lizenz nach dem Erwerb in OMIMSSC zu importieren:

### Schritte

- 1 Klicken Sie im Admin-Portal auf **License Center** (Lizenzcenter).
- 2 Klicken Sie auf **Import License** (Lizenz importieren) und wählen Sie die Lizenzdatei aus, die Sie aus dem Dell Digital Store heruntergeladen haben.

① **ANMERKUNG:** Sie können nur gültige Lizenzdateien importieren. Wenn die Datei beschädigt ist oder manipuliert wurde, wird eine entsprechende Fehlermeldung angezeigt. Laden Sie die Datei erneut aus dem Dell Digital Store herunter oder kontaktieren Sie einen Dell Mitarbeiter, um eine gültige Lizenzdatei zu erhalten.

## Anzeigen von Lizenzdetails

- 1 Öffnen Sie einen Browser und geben Sie die URL der OMIMSSC-Appliance ein.  
Die Anmeldeseite des Admin-Portals von OMIMSSC wird angezeigt.
- 2 Klicken Sie auf **License Center** (Lizenzcenter).  
Auf der nun geöffneten Seite werden folgende Informationen angezeigt:

**License Summary** (Lizenzübersicht): die Lizenzdetails für OMIMSSC

- **Licensed nodes** (Lizenzierte Knoten): Gesamtanzahl von erworbenen Lizenzen
- **Nodes in use** (Verwendete Knoten): Anzahl der ermittelten Server mit zugewiesener Lizenz
- **Nodes Available** (Verfügbare Knoten): verbleibende Anzahl von lizenzierten Knoten, die noch in OMIMSSC ermittelt werden dürfen

**Managing Licenses** (Lizenzen verwalten): Liste aller importierten Lizenzdateien inklusive Details zu den Dateien wie beispielsweise Berechtigungs-ID, Produktbeschreibung, Importdatum der Lizenzdatei, Startdatum der Lizenzlaufzeit und eine Liste der von der Lizenz unterstützten Servergenerationen

## Betriebsvorlage

Betriebsvorlage stellen Betriebssysteme bereit und aktualisieren Firmware-Versionen auf PowerEdge-Servern in der MSSC-Umgebung. Sie können die gesamte Serverkonfiguration eines Referenzservers erfassen und anschließend die Hardwarekonfigurationen konfigurieren, Firmware-Aktualisierungsattribute und Betriebssystemparameter in einer Betriebsvorlage festlegen und diese Vorlage auf verschiedenen Servern bereitstellen. Sie können auch den Compliance-Status eines Servers anhand einer zugewiesenen Betriebsvorlage überprüfen und die Unterschiede auf einer Zusammenfassungsseite anzeigen. Weitere Informationen zum Referenzserver finden Sie unter [Konfiguration von Referenzservern](#).

In der folgenden Tabelle sind alle Funktionen aufgeführt, die von Betriebsvorlagen unterstützt werden:

**Tabelle 4. Funktionalität von OMIMSSC**

Komponente	Konfiguration und Bereitstellung	Firmware-Aktualisierung	Anzeigen der Bestandsliste	Compliance-Status der Betriebsvorlage
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	<b>Ja</b>	–	Nein	–
RHEL	<b>Ja</b>	–	Nein	–
ESXI	<b>Ja</b>	–	Nein	–

Berücksichtigen Sie vor der Bereitstellung einer Betriebsvorlage die folgenden Punkte:

- Wenn Sie eine der Hardwarekomponenten für die Konfiguration (BIOS, RAID NIC/CNA, FC oder iDRAC) auswählen, müssen Sie Server des gleichen Modells auswählen.
- Wenn Sie eine Firmware-Komponente auswählen, können Sie die Firmware beliebiger Server aktualisieren.

Themen:

- [Vorbereitung auf die Bereitstellung](#)
- [Verwalten einer Betriebsvorlage](#)

## Vorbereitung auf die Bereitstellung

Erstellen Sie vor der Bereitstellung einer Betriebsvorlage ein WinPE-Image, eine Tasksequenz und eine Betriebsvorlage.

### Erstellen von WinPE-ISO-Images

Daraufhin wird den einzelnen Updates für die Windows Preinstallation Environment (WinPE) ein eindeutiger Job-Name zugewiesen. Für die Erstellung eines WinPE-ISO-Image ist ein PXE-Server (PreExecution Environment) erforderlich. Ein WinPE-ISO-Image wird aus dem

WinPE-Image und dem Dell OpenManage Deployment Toolkit (DTK) erstellt. Halten Sie den PXE-Server an, sobald ein WinPE-ISO-Image erstellt wurde. Stellen Sie sicher, dass entsprechende betriebssystembezogene Treiberpakete in Lifecycle Controller installiert sind. Verwenden Sie die neueste Version des DTK zur Erstellung eines WinPE-ISO-Image und die WinPE-Version der DTK-Dateien. Die DTK-Datei enthält die erforderlichen Firmware-Versionen für Server, auf denen Sie die Betriebssysteme bereitstellen.

#### Voraussetzung

**ANMERKUNG:** Verwenden Sie die neueste Version des DTK zur Erstellung eines WinPE-ISO-Image und die Dell OpenManage Deployment Toolkit for Windows-Datei. Die Dell OpenManage Deployment Toolkit for Windows-Datei enthält die erforderlichen Firmware-Versionen für Systeme, auf denen Sie die Betriebssysteme bereitstellen. Verwenden Sie die neueste Version der Datei und verwenden Sie nicht die Dell OpenManage Deployment Toolkit Windows Driver Cabinet-Datei für das WinPE-Update.

#### Schritte

- 1 Fügen Sie dem OMIMSSC-Gerät den PXE-Server hinzu.
- 2 Kopieren Sie nach dem Hinzufügen des PXE-Servers die **boot.wim**-Datei vom PXE-Server nach OMIMSSC IG für den SCVMM-WIM-Freigabeordner. Die Datei **boot.wim** befindet sich in folgendem Verzeichnis: C:\RemoteInstall\DCMgr\Boot\Windows\Images

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

## Extrahieren von DTK-Treibern

#### Info über diese Aufgabe

DTK ist eine selbstextrahierende ausführbare Datei.

So verwenden Sie DTK:

#### Schritte

- 1 Doppelklicken Sie auf die ausführbare DTK-Datei.
- 2 Um die DTK-Treiber zu extrahieren, wählen Sie den Ordner aus, z. B. C:\DTK501.
- 3 Kopieren Sie den extrahierten DTK-Ordner in den DTK-Freigabeordner von IG. Beispiel: \\OMIMSSC IG Share\DTK\DTK501.

**ANMERKUNG:** Wenn Sie ein Upgrade von SCVMM SP1 auf SCVMM R2 durchführen, führen Sie auch ein Upgrade auf Windows PowerShell 4.0 durch und erstellen Sie ein WinPE-ISO-Image.

## Aktualisieren des WinPE-Image

- 1 Wählen Sie in OMIMSSC unter **Image Source** (Image-Quelle) die Option **WinPE Update** (WinPE-Update) für den **Custom WinPE Image Path** (Benutzerdefinierter WinPE-Image-Pfad) aus und geben Sie den WinPE-Image-Pfad an.  
Beispiel: \\OMIMSSC IG Share\WIM\boot.wim.
- 2 Geben Sie unter **DTK-Pfad** für den **DTK-Treiberpfad** den Speicherort für die Dell Deployment Toolkit-Treiber an.  
Beispiel: \\OMIMSSC IG Share\DTK\DTK501.
- 3 Geben Sie eine der folgenden Dateien an:
  - WIM-Dateiname für SCCM
  - ISO-Dateiname für SCVMM
- 4 Um die Job-Liste anzuzeigen, wählen Sie **Zur Job-Liste wechseln** aus.  
Daraufhin wird den einzelnen Updates für die Windows Preinstallation Environment (WinPE) ein eindeutiger Job-Name zugewiesen.
- 5 Klicken Sie auf **Aktualisieren**.  
Das WinPE-ISO-Image mit dem in den vorhergehenden Schritten angegebenen Namen wird unter \\OMIMSSC IG Share\ISO erstellt.

## Tasksequenz

Die Tasksequenz wird verwendet, um das Betriebssystem-Image zu erfassen oder ein Betriebssystem auf der SCCM-Konsole bereitzustellen.

Vor der Erstellung einer Betriebsvorlage sollten die folgenden Vorbedingungen erfüllt sein.

- Stellen Sie in Configuration Manager sicher, dass das System ermittelt wurde und unter **Bestand und Kompatibilität > Gerätesammlungen > All Dell Lifecycle Controller Servers (Alle Dell Lifecycle Controller-Server)** vorhanden ist. Weitere Informationen finden Sie unter [Serverermittlung](#).
- Installieren Sie die neueste BIOS-Version auf dem System.
- Installieren Sie die neueste Version des Lifecycle Controllers auf dem System.
- Installieren Sie die neueste Version der iDRAC-Firmware auf dem System.

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

## Erstellen einer Tasksequenz

Eine Tasksequenz zum Konfigurieren von Servern kann auf zwei Arten erstellt werden:

- 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 Dell-spezifischen Tasksequenz

### Info über diese Aufgabe

So erstellen Sie eine Dell-spezifische Tasksequenz mit der Vorlage **OMIMSSC Server-Bereitstellungsvorlage**:

### Schritte

- 1 Starten Sie Configuration Manager.  
Es wird der Configuration Manager-Konsolenbildschirm 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 klicken Sie dann auf **OMIMSSC-Server-Bereitstellung > OMIMSSC-Server-Bereitstellungsvorlage erstellen**.

Der **OMIMSSC Serverbereitstellung-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 benutzerdefinierte 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 **<do not select now>** (<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 einer benutzerdefinierten Tasksequenz.

- 1 Starten Sie Configuration Manager.  
Die Configuration Manager-Konsole wird 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 benutzerdefinierte 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

### Info über diese Aufgabe

- ANMERKUNG:** Bei der Bearbeitung einer Tasksequenz in SCCM 2016 wird das Paket **Windows und ConfigMgr einrichten** nicht in der Meldung über fehlende Objektverweise aufgeführt. Fügen Sie das Paket hinzu, bevor Sie die Tasksequenz speichern.

### Schritte

- 1 Starten Sie Configuration Manager. Der Bildschirm „Configuration Manager“ wird angezeigt.
- 2 Wählen Sie im linken Fensterbereich **Software-Bibliothek > Betriebssysteme > Tasksequenz** aus.
- 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 benutzerdefinierte Aktion für die Dell-Serverbereitstellung wird geladen. Nun können Sie die Tasksequenz wie gewünscht anpassen.

- ANMERKUNG:** Wenn Sie eine Tasksequenz erstmals bearbeiten, wird die Fehlermeldung **Windows und Configuration Manager einrichten** angezeigt. Zur Behebung des Fehlers müssen Sie das Paket „**Configurations Manager Client Upgrade**“ (Client-Upgrade Configuration Manager) erstellen und auswählen. Weitere Informationen zur Erstellung von Paketen finden Sie in der Configuration Manager-Dokumentation auf [technet.microsoft.com](http://technet.microsoft.com).

## Erstellen eines Lifecycle Controller-Startdatenträgers

### Info über diese Aufgabe

Erstellen Sie mit dieser Funktion einen interaktionsfreien Startdatenträger für die Bereitstellung von Ihrem Tasksequenz-Datenträger.

- ANMERKUNG:** Diese Funktion kann nur für die **OMIMSSC-Konsolenerweiterung für SCCM** verwendet werden.

### Schritte

- 1 Starten Sie OMIMSSC und klicken Sie dann auf **Boot Media Creation** (Erstellung eines Startdatenträgers).
- 2 Geben Sie in **Image Source** (Image-Quelle) die ISO-Datei mit dem Betriebssystem-Image an. Weitere Informationen finden Sie unter [Tasksequenz-Datenträger erstellen \(Startfähiges ISO-Image\)](#).
- 3 Geben Sie in **Output File** (Ausgabedatei) den Namen der ISO-Datei an. Die ISO-Datei kann im Hintergrund (unbeaufsichtigt) ausgeführt werden.
- 4 (Optional) Um nach dem Starten des Jobs zur Seite **Jobs and logs** (Jobs und Protokolle) zu navigieren, aktivieren Sie das Kontrollkästchen **Go to the Job List** (Zur Job-Liste wechseln).
- 5 Klicken Sie auf **Update** (Aktualisieren), um die Ausgabedatei in der ISO-Freigabe zu speichern.

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

## Info über diese Aufgabe

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

## Schritte

- 1 Wählen Sie in Configuration Manager **Administration > Site-Konfiguration > Sites** aus.
- 2 Klicken Sie mit der rechten Maustaste auf **<Name des Standortservers>** und wählen Sie **Konfigurieren der Site-Komponenten** und dann **Bandexterne Verwaltungskomponenten** aus.  
Das Fenster **Bandexterne Verwaltungskomponenten – Eigenschaften** wird angezeigt.
- 3 Klicken Sie auf die Registerkarte **Lifecycle Controller**.
- 4 Klicken Sie unter **Standardfreigabeort für Startdatenträger des benutzerdefinierten Lifecycle Controllers** auf **Modifizieren**, um den Standardfreigabeort des benutzerdefinierten Lifecycle Controller-Startdatenträgers zu modifizieren.
- 5 Geben Sie im Fenster **Freigabeinformationen ändern** einen neuen Freigabennamen und Freigabepfad ein.
- 6 Klicken Sie auf **OK**.

# Tasksequenz-Datenträger erstellen (Startfähiges ISO-Image)

- 1 Klicken Sie in Configuration Manager unter **Software-Bibliothek** mit der rechten Maustaste auf **Tasksequenzen** und wählen Sie **Tasksequenz-Datenträger erstellen** aus.

## ANMERKUNG:

- Stellen Sie sicher, dass Sie das Boot Image über alle Verteilungspunkte hinweg verwalten und aktualisieren, bevor Sie diesen Assistenten starten.
- OMIMSSC: OMIMSSC bietet keine Unterstützung für das Standalone-Media-Verfahren zum Erstellen eines Tasksequenz-Datenträgers.

- 2 Wählen Sie im **Tasksequenz-Datenträgerassistenten Startfähigen Datenträger** aus 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 **Next** (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 das erstellte Boot Image nur mit DTK.

- 7 Wählen Sie aus dem Drop-Down-Menü den Verteilungspunkt aus und wählen Sie das Kontrollkästchen **Verteilungspunkte untergeordneter Sites anzeigen**.
- 8 Klicken Sie auf **Next** (Weiter).  
Der **Zusammenfassungsbildschirm** zeigt die Informationen zum Tasksequenz-Datenträger an.
- 9 Klicken Sie auf **Next** (Weiter).  
Der Fortschrittsbalken wird angezeigt.
- 10 Schließen Sie nach Abschluss des Vorgangs den Assistenten.

# Bereitstellen von nicht Windows-basierten Betriebssystemen

Beachten Sie die folgenden Punkte, wenn Sie nicht Windows-basierte Betriebssysteme auf den Zielsystemen bereitstellen möchten:

- Die nicht Windows-basierten ISO-Dateien sind entweder auf einer NFS (Network File System)- oder einer CIFS (Common Internet File System)-Freigabe mit Lese- und Schreibzugriff abgelegt.

- Bestätigen Sie, dass die virtuelle Festplatte auf dem Zielsystem verfügbar ist.
- Nach der Bereitstellung eines ESXi-Betriebssystems wird der Server in SCCM in die Sammlung **Managed Lifecycle Controller (ESXi)** (Verwaltet von Lifecycle Controller [ESXi]) verschoben.
- Nach der Bereitstellung eines nicht Windows-basierten Betriebssystems werden die Server in die Gruppe **Default Non-Windows Host Update Group** (Standardaktualisierungsgruppe für nicht Windows-basierte Hosts) verschoben.
- Es empfiehlt sich, den Netzwerkadapter mit der Netzwerkschnittstelle des Servers zu verbinden, auf dem das Betriebssystem bereitgestellt wird.

## Verwalten einer Betriebsvorlage

Sie können eine Betriebsvorlage in OMIMSSC erstellen, bearbeiten und löschen.

## Erstellen einer Betriebsvorlage

### Voraussetzungen

Bevor Sie eine Betriebsvorlage erstellen können, müssen Sie die folgenden Schritte durchführen:

- Ermitteln Sie über die Seite **Discovery** (Ermittlung) einen Referenzserver. Weitere Informationen finden Sie unter [Discovering servers using manual discovery](#) (Ermitteln von Servern über die manuelle Ermittlung).
- (Optional) Erstellen Sie eine Aktualisierungsquelle. Weitere Informationen finden Sie unter [Creating update source](#) (Erstellen einer Aktualisierungsquelle).
- (Optional) In OMIMSSC für SCCM:
  - Erstelle Sie eine Tasksequenz. Weitere Informationen finden Sie unter [Creating task sequence](#) (Erstellen einer Tasksequenz).
  - Zur Bereitstellung eines nicht Windows-basierten Betriebssystems: Erstellen Sie ein Geräte-Anmeldeprofil. Weitere Informationen finden Sie unter [Creating credential profile](#) (Erstellen eines Anmeldeprofils).
  - Erstellen Sie ein Startmedium für einen unbeaufsichtigten Start. Weitere Informationen finden Sie unter [Creating LC boot media](#) (Erstellen von LC-Startmedien).
- (Optional) In OMIMSSC für SCVMM:
  - Erstellen Sie ein Hypervisor-Profil. Weitere Informationen zur Erstellung von Hypervisor-Profilen finden Sie unter [Creating hypervisor profile](#) (Erstellen eines Hypervisor-Profiles).
  - Zur Bereitstellung eines Windows-Betriebssystems: Erstellen Sie ein Geräte-Anmeldeprofil. Weitere Informationen finden Sie unter [Creating credential profile](#) (Erstellen eines Anmeldeprofils).

### Info über diese Aufgabe

Zur Erstellung einer Betriebsvorlage können Sie die Konfiguration des Referenzservers erfassen. Sobald die Konfiguration erfasst wurde, können Sie die Vorlage direkt speichern oder die Attribute für Aktualisierungsquelle, Hardwarekonfiguration und Windows-Komponente nach Bedarf bearbeiten. Anschließend können Sie die Vorlage speichern und auf andere PowerEdge-Server des gleichen Typs anwenden.

### Schritte

- 1 Führen Sie in OMIMSSC einen der folgenden Schritte durch, um den Assistent für Betriebsvorlage zu öffnen:
  - Klicken Sie im Dashboard von OMIMSSC auf **Create Operational Template** (Betriebsvorlage erstellen).
  - Klicken Sie im Navigationsbereich auf **Profiles > Operational Template** („Profile“ > „Betriebsvorlage“) und anschließend auf **Create** (Erstellen).

Der Assistent **Operational Template** (Betriebsvorlage) wird angezeigt.

- 2 Geben Sie einen Namen für die Vorlage und eine Beschreibung ein. Außerdem müssen Sie die IP-Adresse des Referenzservers angeben. Klicken Sie dann auf **Next** (Weiter).

**① ANMERKUNG:** Die Konfiguration des Referenzservers kann mit dem iDRAC ab Version 2.0 erfasst werden.

- 3 Klicken Sie unter **Server Components** (Serverkomponenten) auf eine Komponente, um die verfügbaren Attribute und deren Werte aufzurufen.

Es gibt folgende Komponenten:

- Firmware-Aktualisierung
  - Hardwarekomponenten (RAID, NIC und BIOS)
  - Betriebssystem (Windows, ESXi oder RHEL)
- 4 (Optional) Bearbeiten Sie falls nötig die Werte der verfügbaren Attribute.
  - 5 Aktivieren Sie jeweils das Kontrollkästchen der verschiedenen Komponenten. Es wird ausschließlich die Komponentenkonfiguration der ausgewählten Komponenten angewendet, wenn die Betriebsvorlage auf erfasste Konfigurationen angewendet wird.  
Gehen Sie in der Komponente **Operating System** (Betriebssystem) je nach Bedarf nach einer der folgenden Anleitungen vor:
    - Zur Bereitstellung eines Windows-Betriebssystems mit SCCM: [Windows component for the OMIMSSC console extension for SCCM](#) (Windows-Komponente der OMIMSSC-Konsolenerweiterung für SCCM)
    - Zur Bereitstellung eines Windows-Betriebssystems mit SCVMM: [Windows component for the OMIMSSC console extension for SCVMM](#) (Windows-Komponente der OMIMSSC-Konsolenerweiterung für SCVMM)
    - OMIMSSC
    - Zur Bereitstellung eines nicht Windows-basierten Betriebssystems: [Non-Windows component for the OMIMSSC console extensions](#) (Für nicht Windows-basierte Betriebssysteme gedachte Komponente der OMIMSSC-Konsolenerweiterungen für SCVMM)
  - 6 Klicken Sie auf **Finish** (Fertigstellen), um das Profil zu speichern.

## Windows-Komponente der OMIMSSC-Konsolenerweiterung für SCCM

### Info über diese Aufgabe

Führen Sie während der Erstellung der Betriebsvorlage die folgenden Schritte für die Windows-Komponente durch:

#### Schritte

- 1 Wählen Sie eine Tasksequenz und eine Bereitstellungsmethode aus.

**ANMERKUNG:** Im Drop-Down-Menü werden nur die tatsächlich in Sammlungen bereitgestellten Tasksequenzen aufgeführt.

Weitere Informationen zu Tasksequenzen finden Sie unter [Task sequence](#) (Tasksequenz).

- 2 Wählen Sie unter **Deployment method** (Bereitstellungsmethode) eine der folgenden Optionen aus:
  - **Boot to network ISO** (Starten von einem Netzwerk-ISO-Abbild): Führt einen Neustart von dem angegebenen ISO-Abbild aus.
  - **Stage ISO to vFlash and Reboot** (ISO-Staging in vFlash mit Neustart): Lädt das ISO-Abbild in den vFlash-Speicher herunter und führt einen Neustart durch.
  - **Reboot to vFlash** (Neustart von vFlash): Führt einen Neustart vom vFlash-Speicher durch. Stellen Sie sicher, dass das ISO-Abbild im vFlash-Speicher abgelegt ist.

**ANMERKUNG:** Um die Option „Reboot to vFlash“ (Starten von vFlash) verwenden zu können, muss die im vFlash-Speicher erstellte Partition die Bezeichnung ISOIMG haben.

- 3 (Optional) Aktivieren Sie die Option **Use Network ISO as Fallback** (Netzwerk-ISO-Abbild als Fallback verwenden), wenn das Abbild auf der Netzwerkfreigabe verwendet werden soll, falls das Abbild im vFlash-Speicher beschädigt ist.
- 4 Geben Sie ein LC-Startmedium als Startabbild an. Optional: Aktivieren Sie die Option **Enable LC Drivers Injection** (LC-Treiberinjektion aktivieren). Weitere Informationen zur Erstellung von LC-Startmedien finden Sie unter [Create LC boot media](#) (Erstellen von LC-Startmedien).
- 5 Wählen Sie die erforderlichen Treiber für das Betriebssystem aus.

## Windows-Komponente für OMIMSSC-Konsolenerweiterungen für SCVMM

### Info über diese Aufgabe

Führen Sie bei der Erstellung der Betriebsvorlage für eine Windows-Komponente die folgenden Schritte durch:

#### Schritt

Wählen Sie Werte für **Hypervisor Profile** (Hypervisor-Profil), **Credential Profile** (Anmeldeprofil) und **Server IP from** (Server-IP von) aus.

**ANMERKUNG:** Die Werte für „Host Name“ (Host-Name) und „Server Management NIC“ (NIC für Serververwaltung) sind immer Poolwerte.

Wenn Sie für **Server IP from** (Server-IP von) die Option **Static** (Statisch) auswählen, müssen Sie das logische Netzwerk in SCVMM konfigurieren und für folgende Parameter Poolwerte angeben:

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

## Nicht Windows-basierte Komponente für OMIMSSC-Konsolenerweiterungen

### Info über diese Aufgabe

Führen Sie beim Erstellen der Betriebsvorlage die folgenden Schritte für nicht Windows-basierte Komponenten aus:

#### Schritt

Wählen Sie ein nicht Windows-basiertes Betriebssystem, die Betriebssystemversion, den Typ des freigegebenen Ordners, den Namen der ISO-Datei, den Speicherort der ISO-Datei und das Passwort für das Root-Konto des Betriebssystems aus.

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

Der Wert für **Host Name** (Host-Name) ist immer ein Poolwert. Wenn Sie DHCP deaktivieren, sind zudem die Werte für die folgenden Parameter immer Poolwerte:

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

**ANMERKUNG:** Bei der Bereitstellung nicht Windows-basierter Betriebssystem werden Freigaben des Typs NFS (Network File System) sowie Freigaben des Typs CIFS (Common Internet File System) unterstützt.

## Anzeigen von Betriebsvorlage

So zeigen Sie Betriebsvorlage-Vorlagen an:

Klicken Sie in der OMIMSSC-Konsole auf **Profiles and Templates** (Profile und Vorlagen) und anschließend auf **Operational Template** (Betriebsvorlage). Alle erstellten Betriebsvorlage-Vorlagen sind hier aufgeführt.

## Bearbeiten von Betriebsvorlage

### Info über diese Aufgabe

Sie können eine Betriebsvorlage zum Ändern der Aktualisierungsquelle, Hardwarekonfigurationen und Betriebssystemkomponenten des Referenzservers bearbeiten.

**ANMERKUNG:** Einige Attribute können von anderen Attributwerten abhängen. Wenn diese Attribute nicht aktualisiert werden, schlägt die Anwendung der Hardwarekonfiguration möglicherweise fehl. Es wird daher empfohlen, die Referenzkonfiguration nicht zu bearbeiten.

**ANMERKUNG:** Wenn Sie die Tasksequenz im SCCM 2016 bearbeiten, enthalten die Meldungen über fehlende Objektreferenzen das Paket Windows und ConfigMgr einrichten nicht. Fügen Sie das Paket hinzu und speichern Sie die Tasksequenz.

#### Schritte

1 Wählen Sie die Vorlage aus, die Sie bearbeiten möchten, und klicken Sie auf **Edit** (Bearbeiten).

Die Seite Betriebsvorlage (Betriebsvorlage) wird angezeigt.

- 2 Bearbeiten Sie den Namen und die Beschreibung der Vorlage (wenn erforderlich) und klicken Sie dann auf **Next** (Weiter).
- 3 Um die verfügbaren Attribute und deren Werte in **Server Components** (Serverkomponenten) anzuzeigen, klicken Sie auf eine Komponente.
- 4 Ändern Sie die Werte der verfügbaren Attribute, falls erforderlich.

**ANMERKUNG:** Aktivieren Sie das Kontrollkästchen neben jeder Komponente, da bei der Übernahme der Betriebsvorlage nur die ausgewählten Konfigurationen auf das Zielsystem angewendet werden.

**ANMERKUNG:** Unabhängig von der getroffenen Auswahl der Komponenten werden alle Konfigurationen in der Vorlage erfasst.

- 5 Führen Sie für die Betriebssystemkomponente abhängig von Ihren Anforderungen eine der folgenden Aufgaben durch:
  - Für Windows-Betriebssystembereitstellungen im SCCM siehe [Windows-Komponente für die OMIMSSC-Konsolenerweiterung für SCCM](#).
  - Für Windows-Betriebssystembereitstellungen im SCVMM siehe [Windows-Komponente für die OMIMSSC-Konsolenerweiterung für SCVMM](#).
  - Für Nicht-Windows-Betriebssystembereitstellungen siehe [Nicht-Windows-Komponente für die OMIMSSC-Konsolenerweiterungen](#).
- 6 Um das Profil zu speichern, klicken Sie auf **Fertig stellen**.

## Windows-Komponente der OMIMSSC-Konsolenerweiterung für SCCM

Befolgen Sie während der Bearbeitung der Betriebsvorlage die Anleitung unter [Windows OS component for OMIMSSC console extension for SCCM](#) (Windows-Komponente der OMIMSSC-Konsolenerweiterung für SCCM).

## Windows-Komponente der OMIMSSC-Konsolenerweiterung für SCVMM

Befolgen Sie während der Bearbeitung der Betriebsvorlage die Anleitung unter [Windows OS component for OMIMSSC console extension for SCVMM](#) (Windows-Komponente der OMIMSSC-Konsolenerweiterung für SCVMM).

## Nicht Windows-basierte Komponente für OMIMSSC-Konsolenerweiterungen

Führen Sie beim Bearbeiten der Betriebsvorlage die unter [Non-Windows OS component for OMIMSSC console extensions](#) (Nicht Windows-basierte Komponente für OMIMSSC-Konsolenerweiterungen) aufgeführten Schritte durch.

## Löschen einer Betriebsvorlage

Gehen Sie wie folgt vor, um eine Betriebsvorlage zu löschen:

### Info über diese Aufgabe

Stellen Sie vor dem Löschen einer Betriebsvorlage Folgendes sicher:

- Die ausgewählte Betriebsvorlage ist keinem Server zugeordnet. Wenn sie einem Server zugeordnet ist, heben Sie die Zuweisung auf und löschen Sie dann die Vorlage.
- Es werden keine mit der Betriebsvorlage verbundenen Jobs ausgeführt.

## Schritt

Wählen Sie die Vorlagen aus, die Sie löschen möchten, und klicken Sie dann auf **Delete** (Löschen). Klicken Sie zum Bestätigen auf **Yes** (Ja).

# Zuweisen einer Betriebsvorlage und Prüfen der Betriebsvorlage-Compliance

Weisen Sie einem Server eine Betriebsvorlage zu und prüfen Sie die Betriebsvorlage-Compliance. Nur nach dem Zuweisen einer Betriebsvorlage zu einem Server können Sie dessen Betriebsvorlage-Compliance-Status anzeigen. Sie können die Konfiguration eines Servers mit einer Betriebsvorlage vergleichen, indem Sie einem Server die Vorlage zuweisen. Nach dem Zuweisen einer Betriebsvorlage wird der Compliance-Job ausgeführt und bei Abschluss der Status der Betriebsvorlage angezeigt.

- 1 Klicken Sie in OMIMSSC auf **Configuration and Deployment** (Konfiguration und Bereitstellung). Wählen Sie die erforderlichen Server aus und klicken Sie auf **Assign Operational Template and Run Compliance** (Betriebsvorlage zuweisen und Compliance prüfen). Die Seite **Assign Betriebsvorlage and Run Compliance** (Betriebsvorlage zuweisen und Compliance prüfen) wird angezeigt.
- 2 Wählen Sie die Vorlage aus dem Drop-Down-Menü **Betriebsvorlage** (Betriebsvorlage) aus, geben Sie dem Job einen Namen und klicken Sie dann auf **Assign** (Zuweisen).  
Wenn der Server mit dem Vorlage kompatibel ist, wird ein **grünes** Häkchen angezeigt.

Nur wenn der Server nicht mit der Vorlage kompatibel ist, können Sie einen Zusammenfassungsbericht durch Klicken auf den Link mit dem Vorlagennamen anzeigen. Auf der Seite **Betriebsvorlage** (Betriebsvorlage) **Compliance-Summary Report** (Zusammenfassungsbericht) wird ein Zusammenfassungsbericht der Unterschiede zwischen der Vorlage und den Serverkonfigurationen angezeigt.

Um einen detaillierten Bericht anzuzeigen, führen Sie die folgenden Schritte aus:

- a Klicken Sie auf **View Detailed Compliance** (Detaillierte Compliance anzeigen). Hier werden die Komponenten, deren Attributwerte sich von der zugewiesenen Vorlage unterscheiden, angezeigt. Die Farben geben die verschiedenen Status der Betriebsvorlage-Compliance wieder.
  - Gelb – gibt an, dass die Konfiguration des Servers nicht mit den Vorlagenwerten übereinstimmt.
  - Rot – gibt an, dass die Komponente auf dem Server nicht vorhanden ist.

# Bereitstellen einer Betriebsvorlage

## Info über diese Aufgabe

Die Bereitstellung ist für Windows- und andere Betriebssysteme möglich, beispielsweise ESXi und RHEL.

- ① **ANMERKUNG:** Wenn nach der Bereitstellung des Windows 2016-Betriebssystems auf Dell PowerEdge-Servern der 12. Generation ein gelbes Warnsymbol unter Geräte-Manager erscheint, laden Sie die entsprechenden Treiber von [Dell.com/support](http://Dell.com/support) herunter und installieren Sie sie.

## Schritte

- 1 Klicken Sie in OMIMSSC auf **Configuration and Deployment** (Konfiguration und Bereitstellung). Wählen Sie die Server aus, auf denen Sie eine Vorlage bereitstellen möchten, und klicken Sie dann auf **Deploy Betriebsvorlage** (Betriebsvorlage bereitstellen). Daraufhin wird die Seite **Deploy Betriebsvorlage** (Betriebsvorlage bereitstellen) angezeigt.
- 2 (Optional) Klicken Sie auf **Export Pool Attributes** (Pool-Attribute exportieren), um alle in der ausgewählten Vorlage als Pool-Werte gekennzeichneten Attribute in eine CSV-Datei zu exportieren. Wenn Sie dies nicht tun möchten, fahren Sie mit Schritt 3 fort.

- ① **ANMERKUNG:** Fügen Sie vor dem Export der Pool-Werte die IP-Adresse des Servers, auf dem die OMIMSSC-Konsolenerweiterungen installiert sind, zur lokalen Intranet-Site hinzu. Weitere Informationen zum Hinzufügen der IP-Adresse im IE-Browser finden Sie unter [Browsereinstellungen](#).

- ① **ANMERKUNG:** Stellen Sie nach dem Export der Pool-Werte alle Werte für sämtliche als Pool-Werte markierten Attribute in der CSV-Datei bereit und speichern Sie die Datei. Wählen Sie unter Attribute Value Pool (Attributwerte-Pool) die Datei aus, um sie zu importieren.

① **ANMERKUNG:** Stellen Sie sicher, dass Sie eine CSV-Datei mit allen passenden Attributen auswählen und die iDRAC-IP oder iDRAC-Anmeldeinformationen sich wegen der Vorlage nicht ändern, da der Job nicht von OMIMSSC nachverfolgt wird, wenn die iDRAC-IP oder iDRAC-Anmeldeinformationen sich ändern, und als fehlgeschlagen gekennzeichnet wird, auch wenn der Job unter Umständen in iDRAC erfolgreich war.

① **ANMERKUNG:** Wenn nach der Bereitstellung des Windows 2016-Betriebssystems auf Dell PowerEdge-Servern der 12. Generation ein gelbes Warnsymbol unter Geräte-Manager erscheint, laden Sie die entsprechenden Treiber von [Dell.com/support](http://Dell.com/support) herunter und installieren Sie sie.

- 3 Geben Sie einen eindeutigen Jobnamen und eine Beschreibung für den Job an und klicken Sie dann auf **Deploy** (Bereitstellen). Klicken Sie auf **Go to the Job List** (Zur Job-Liste), um die Jobs anzuzeigen.

## Aufheben der Zuweisung einer Betriebsvorlage

- 1 Klicken Sie in OMIMSSC auf **Configuration and deployment** (Konfiguration und Bereitstellung).
- 2 Wählen Sie die Server aus, denen die Vorlage nicht mehr zugewiesen sein soll, und klicken Sie dann auf **Assign Betriebsvorlage and Run Compliance** (Betriebsvorlage zuweisen und Compliance prüfen).  
Die Seite **Assign Betriebsvorlage and Run Compliance** (Betriebsvorlage zuweisen und Compliance prüfen) wird angezeigt.
- 3 Wählen Sie die Option **Unassign** (Zuweisung aufheben) im Drop-down-Menü Betriebsvorlage (Betriebsvorlage) aus und klicken Sie auf **Assign** (Zuweisen).

# Integration mit Dell Repository Manager (DRM)

OMIMSSC ist mit DRM ab Version 2.2 integriert, sodass Serverbestandsinformationen bezüglich der bestehenden Server von der OMIMSSC-Appliance an DRM weitergegeben werden. Mithilfe der Bestandsdaten können Sie ein benutzerdefiniertes Repository in DRM erstellen und dieses als Aktualisierungsquelle in der OMIMSSC-Appliance festlegen, um Firmware-Aktualisierungen auf den Servern oder Servergruppen durchzuführen. Weitere Informationen über das Erstellen eines Repositorys in DRM finden Sie in den Dokumenten zu *Dell Repository Manager*.

## Info über diese Aufgabe

**ANMERKUNG:** Integrieren Sie nach dem Upgrade von OMIMSSC die OMIMSSC-Appliance erneut mit DRM, um die neusten Informationen über Server sehen zu können.

So erstellen Sie ein Repository für die OMIMSSC-Appliance mit DRM:

## Schritte

- 1 Öffnen Sie **Dell Repository Manager Data Center**.
- 2 Klicken Sie auf **Meine Repositories**, klicken Sie auf **Neue** und anschließend auf **Dell Konsolenintegration**.
- 3 Geben Sie die **URL (Rest-API)** in folgendem Format ein: `https:// IP address of appliance/genericconsolerepository/` . Klicken Sie anschließend auf **Next** (Weiter).
- 4 Geben Sie den **Benutzernamen** und das **Kennwort** an, die Sie in der OMIMSSC-Appliance verwendet haben, und klicken Sie auf **Ok** und erneut auf **Ok**.

# Maintenance

Auf der Seite **Maintenance Center** (Wartungcenter) können Sie Serverbestandsinformationen exportieren und festlegen, wann Jobs zur Serveraktualisierung ausgeführt werden sollen. Außerdem können Sie die bisherige Serverkonfiguration exportieren, um den Server später zurücksetzen zu können und die Konfiguration alter Komponenten auf Ersatzkomponenten anwenden zu können, und LC-Protokolle zur Fehlerbehebung exportieren.

Themen:

- [Allgemeines zu Firmware-Aktualisierungen](#)
- [Wiederherstellung](#)
- [Anwenden von Firmware- und Konfigurationseinstellungen](#)
- [Erfassen von LC-Protokollen](#)
- [Exportieren von Bestandsdaten](#)

## Allgemeines zu Firmware-Aktualisierungen

Wenn Sie sich an die Empfehlungen halten, können Sie dafür sorgen, dass die Firmware-Versionen von Dell EMC Serverkomponenten immer auf dem neuesten Stand sind. Sie können Aktualisierungsquellen und benutzerdefinierte Aktualisierungsgruppen erstellen oder die vordefinierten Aktualisierungsgruppen verwenden, um die Firmware-Aktualisierung durchzuführen. Zudem haben Sie die Möglichkeit zum Erstellen und Terminieren von Aufträgen für Firmware-Aktualisierungen sowie zum Konfigurieren von Benachrichtigungen, wenn neue Kataloge an der Aktualisierungsquelle verfügbar sind. Es wird ein Vergleichsbericht für die bestehende Firmware-Version und die Grundversion bereitgestellt. Basierend auf diesen Informationen können Sie eine Bestandsdatei erstellen. Außerdem können Sie die Informationen nach Art der Aktualisierung, Serverkomponente und Servermodell filtern. Sie können Aktualisierungen nur auf Servern mit kompatibler Hardware durchführen, da iDRAC-Aktualisierungen nur für die unterstützte Mindestversion und spätere Versionen verfügbar sind.

**ⓘ ANMERKUNG:** Wenn nach der Aktualisierung auf die neueste Version von OMIMSSC die Verbindung zu <ftp.dell.com> oder <downloads.dell.com> ausfällt, kann der standardmäßige Dell Online-FTP oder die Dell HTTP-Aktualisierungsquelle die Katalogdatei nicht herunterladen, weshalb der Vergleichsbericht nicht verfügbar ist. Um einen Vergleichsbericht anzuzeigen, bearbeiten Sie den standardmäßigen Dell Online-FTP oder die Dell HTTP-Aktualisierungsquelle, erstellen Sie Proxy-Anmeldeinformationen und wählen Sie dies dann im Drop-down-Menü **Select Update Source (Aktualisierungsquelle auswählen)** aus. Weitere Informationen zum Bearbeiten einer Aktualisierungsquelle finden Sie unter [Modifying update source \(Ändern einer Aktualisierungsquelle\)](#).

OMIMSSC bietet die folgenden Aktualisierungsaktionen auf der Seite **Maintenance Center** (Wartungcenter):

- Zurückstufen – Es ist eine frühere Version in der Aktualisierungsquelle verfügbar und Sie können die Firmware auf diese Version zurückstufen.
- Keine Maßnahme erforderlich – Die Firmware-Version entspricht der Ebene im Repository.
- Keine Aktualisierung verfügbar – Für die Komponente stehen keine Firmware-Aktualisierungen zur Verfügung.
- Aktualisieren (optional) – Die Aktualisierungen bestehen aus neuen Funktionen oder spezifischen, optionalen Konfigurationsaktualisierungen.
- Aktualisieren (dringend) – Es sind kritische Aktualisierungen verfügbar, die der Behebung von Sicherheits-, Leistungs- oder anderen Problemen in Komponenten, wie beispielsweise dem BIOS, dienen.
- Aktualisieren (empfohlen) – Es sind Aktualisierungen für Fehlerbehebungen oder Funktionsverbesserungen in OMIMSSC verfügbar. Außerdem sind Kompatibilitätskorrekturen für andere Firmwareaktualisierungen enthalten.

OMIMSSC bietet die folgenden Methoden für die Durchführung von Firmware-Aktualisierungen:

- **Aktualisieren unter Verwendung eines DRM Repositorys** – Exportieren Sie die Bestandsinformationen der ermittelten Server von der Appliance, um ein Repository in DRM anzulegen. Weitere Informationen über das Exportieren der Bestandsdaten finden Sie unter [Exporting inventory](#) (Exportieren von Bestandsdaten).
  - Nach dem Erstellen eines Repositorys in DRM, wählen Sie die relevanten Server aus und initiieren Sie eine Aktualisierung auf den Servern. Berücksichtigen Sie für die Vorbereitung der erforderlichen Aktualisierungen auch andere Faktoren wie das Testen in einer Testumgebung, Sicherheitsaktualisierungen, Anwendungsempfehlungen, Dell Ratschläge usw. Weitere Informationen über das Erstellen eines Repositorys finden Sie in den Dokumenten zu *Dell Repository Manager*, die unter **Dell.com/support/home** verfügbar sind.
- **Aktualisierung unter Verwendung von FTP oder HTTP** – Aktualisieren Sie Komponenten auf die neueste Version, die auf der FTP- oder HTTP-Site verfügbar ist. Dell IT legt vierteljährlich ein Repository an.
  - Integration in den Dell Online-Katalog – Stellen Sie im Falle einer FTP-Aktualisierungsquelle eine Verbindung zum Dell FTP her und laden Sie die Katalogdatei in das Cache-Verzeichnis herunter. Im Falle einer HTTP-Aktualisierungsquelle stellen Sie eine Verbindung zu `downloads.dell.com` her und legen Sie die Katalogdatei als Referenz-Bestandsaufnahme fest.
  - Zeigen Sie den Vergleichsreport mit der Aktualisierungsquelle an, wählen Sie die relevanten Server oder Serverkomponenten aus, und leiten Sie eine Aktualisierung auf den Servern ein.
- **Referenzierung des Firmware-Bestands und Vergleich** – Erstellen Sie eine Referenzbestandsdatei, die den Firmware-Bestand der ausgewählten Server der Servergruppen enthält. Später können Sie die Bestandsdaten von Servern, die auf der Appliance gespeichert sind, mit der abgelegten Referenzbestandsdatei vergleichen. Die Referenzdatei zum Serverbestand enthält Informationen zu einem einzelnen Server des gleichen Typs oder Modells oder zu mehreren Servern unterschiedlicher Typen oder Modelle.

## Anwenden von Aktualisierungen auf Server

### Voraussetzungen

Bevor Sie Aktualisierungen auf Server anwenden, müssen Sie Folgendes tun:

- Stellen Sie sicher, dass eine Aktualisierungsquelle verfügbar ist, entweder online unter der Dell FTP- oder HTTP-Adresse, unter der lokalen FTP- oder HTTP-Adresse oder in Dell Repository Manager (DRM). Nur dann können Aktualisierungen auf Server aufgespielt werden.
- Stellen Sie sicher, dass die iDRAC-Jobwarteschlange auf den zu aktualisierenden Servern leer ist, bevor Sie die Aktualisierungen anwenden.
- Stellen Sie sicher, dass der IG-Benutzer über lokale Administratorrechte auf allen Knoten im Cluster verfügt.
- Wenn Sie ein Firmware-Repository erstellen möchten: Stellen Sie sicher, dass der FTP-Server über den OMIMSSC-Host erreichbar ist und dass keine Netzwerkprobleme vorliegen. Stellen Sie außerdem sicher, dass die richtigen Anmeldeinformationen angegeben sind, wenn Sie einen Job zur Firmware-Aktualisierung erstellen.

### Info über diese Aufgabe

- ① **ANMERKUNG:** Sie können Firmware-Aktualisierungen auf eine einzelne Komponente eines Servers anwenden oder auf die gesamte Umgebung.
- ① **ANMERKUNG:** Wenn für einen Server oder eine Servergruppe keine anwendbaren Upgrades oder Downgrades verfügbar sind, hat eine Firmware-Aktualisierung keine Auswirkungen auf den oder die betreffenden Server.
- ① **ANMERKUNG:** Wenn Sie Informationen auf Komponentenebene aktualisieren möchten und die vorhandene Firmware-Version mit der in der Aktualisierungsquelle übereinstimmt, wird keine Maßnahme an der Komponente durchgeführt.
- ① **ANMERKUNG:** Sie können Aktualisierungen sofort auf Server oder eine Servergruppe anwenden oder einen Job zur Firmware-Aktualisierung erstellen, um sie zeitplanbasiert anzuwenden. Die zur Aktualisierung erstellten Jobs werden auf der Seite **Jobs and Logs Center** (Job- und Protokollcenter) aufgeführt.
- ① **ANMERKUNG:** Die CMC-Firmware lässt sich nicht direkt über die OMIMSSC-Appliance aktualisieren. Sie können jedoch die Firmware des im CMC registrierten modularen Servers aktualisieren. Informationen zur Aktualisierung der CMC-Firmware finden Sie im Abschnitt *Updating CMC firmware* (Aktualisieren der CMC-Firmware) im *Dell PowerEdge M1000e Chassis Management Controller Firmware User's Guide* (Benutzerhandbuch für die Firmware des Dell PowerEdge M1000e Chassis Management Controller). Informationen zur Aktualisierung der CMC-Firmware auf VRTX-Systemen finden Sie im Abschnitt *Updating firmware* (Aktualisieren der Firmware) im *Dell Chassis Management Controller for Dell PowerEdge VRTX User's Guide* (Benutzerhandbuch Dell Chassis Management Controller für Dell PowerEdge VRTX). Informationen zur Aktualisierung der CMC-Firmware auf FX2-Systemen finden Sie im Abschnitt *Updating firmware* (Aktualisieren der Firmware) im *Dell Chassis Management Controller for Dell PowerEdge FX2 User's Guide* (Benutzerhandbuch Dell Chassis Management Controller für Dell PowerEdge FX2).

**ANMERKUNG:** Wenn Sie die Option **Allow Downgrade (Downgrade zulassen)** auswählen, können Sie ein Downgrade der Firmware auf die jeweils vorgeschlagene Version durchführen. Wenn diese Option nicht ausgewählt ist, wird für Komponenten, für die ein Firmware-Downgrade erforderlich ist, keine Aktion durchgeführt.

### Schritte

- 1 Klicken Sie in OMIMSSC auf **Maintenance Center** (Wartungszentrum), wählen Sie den Server oder die Servergruppe sowie eine Aktualisierungsquelle aus und klicken Sie auf **Run Update** (Aktualisierung ausführen).
- 2 Geben Sie unter **Aktualisierungsdetails** den Job-Namen und die Beschreibung der Firmware-Aktualisierung an.
- 3 Wählen Sie unter **Aktualisierung planen** eine der folgenden Optionen aus:
  - **Run Now** (Jetzt ausführen): Die Aktualisierungen werden sofort angewendet.
  - Wählen Sie ein Datum und eine Uhrzeit für eine spätere Firmware-Aktualisierung aus.
- 4 Wählen Sie eine Aktualisierungsmethode aus. Zur Auswahl stehen **Agent-free Update** (Agentenlose Aktualisierung) und **Agent-free Staged Update** (Agentenlose Aktualisierung mit Staging). Klicken Sie dann auf **Finish** (Fertig stellen).
  - **Agentenlose Aktualisierungen mit Staging:** Alle direkt anwendbaren Firmware-Aktualisierungen, die keinen Neustart des Systems erfordern, werden direkt angewendet. Alle übrigen Aktualisierungen werden während des Systemneustarts angewendet. Die Aktualisierungen werden über den iDRAC durchgeführt. Die OMIMSSC-Appliance stuft die Aktualisierung als erfolgreich ein, wenn der iDRAC eine erfolgreiche Aktualisierung meldet. Die OMIMSSC-Appliance interagiert nicht mit dem Server, nachdem die Aktualisierungen angewendet wurden. Der gesamte Aktualisierungsjob schlägt fehl, sobald der Vorgang auf einem der zu aktualisierenden Server fehlschlägt.
  - **Agentenlose Aktualisierungen:** Die Firmware-Aktualisierung wird als Out-of-Band-Aktualisierung durchgeführt, falls erforderlich mit einem sofortigen Neustart.

**ANMERKUNG:** Cluster-Aktualisierungsgruppen werden über den Koordinator für Cluster-Aktualisierungen auf dem System abgewickelt, auf dem IG installiert ist. Der Aktualisierungsjob wird an die Microsoft-Funktion CAU (Cluster-Aware Update, clusterfähiges Aktualisieren) übergeben, unabhängig davon, welche Auswahl Sie im Drop-Down-Menü Update Methode (Aktualisierungsmethode) getroffen haben. Weitere Informationen finden Sie unter [Updates using CAU](#) (Durchführen von Aktualisierungen mit CAU).

**ANMERKUNG:** Sobald ein Job zur Firmware-Aktualisierung an den iDRAC übermittelt wurde, ruft die OMIMSSC-Appliance den Status des Jobs vom iDRAC ab und vermerkt Statusaktualisierungen auf der Seite **Jobs and Logs** (Jobs und Protokolle) im Admin-Portal. Gelegentlich sendet der iDRAC keine Statusaktualisierungen zu den von der OMIMSSC-Appliance verfolgten Jobs. Die OMIMSSC-Appliance wartet maximal sechs Stunden. Ist bis dahin keine Antwort des iDRAC eingegangen, wird der Job zur Firmware-Aktualisierung als fehlgeschlagen eingestuft.

## Aktualisierungen mit CAU

Aktualisierungen auf Servern erfolgen über den Cluster-Aktualisierungskoordinator, der sich auf dem gleichen System wie IG befindet, und nicht über iDRAC. Die Aktualisierungen erfolgen nicht stufenweise, sondern werden sofort angewendet. Mit CAU können Sie Unterbrechungen oder Serverausfallzeiten minimieren, wodurch eine kontinuierliche Verfügbarkeit der Arbeitslast ermöglicht wird. Daher gibt es keine Auswirkungen auf den von der Clustergruppe bereitgestellten Service. Weitere Informationen über CAU finden Sie im Abschnitt „Clusterfähiges Aktualisieren: Szenarioübersicht“ unter [technet.microsoft.com](http://technet.microsoft.com).

Überprüfen Sie vor dem Anwenden von Aktualisierungen auf eine Cluster-Aktualisierungsgruppe den Cluster-Verfügbarkeitsreport auf Folgendes:

- Es besteht Konnektivität zur Aktualisierungsquelle.
- Die Failover-Cluster sind verfügbar.
- Stellen Sie sicher, dass Windows Server 2012 oder Windows Server 2012 R2 oder Windows 2016 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.
- Es ist eine Firewall-Regel aktiviert, die das Remote-Herunterfahren jedes Knotens im Failover-Cluster erlaubt.
- Die Cluster-Gruppe sollte mindestens über zwei Knoten verfügen.
- Überprüfen Sie, ob der Cluster bereit für die Aktualisierung ist. Weitere Informationen zu CAU finden Sie im Abschnitt mit den Voraussetzungen und bewährten Verfahren für clusterfähiges Aktualisieren (CAU) unter [technet.microsoft.com](http://technet.microsoft.com).

- Erweitern Sie zur Durchführung einer Aktualisierung auf Komponentenebene die Servergruppen bis zur Komponentenebene, und klicken Sie auf **Aktualisierung ausführen**.
- Bei der Durchführung einer Firmware-Aktualisierung für PowerEdge-Server der 11. Generation kann die Firmware-Version der Netzteileneinheit nicht aktualisiert werden.

**ANMERKUNG:** Stellen Sie sicher, dass keine gravierenden Fehler und Warnungen im Bericht aufgeführt sind, die der Anwendung der CAU-Methode entgegenstehen.

Weitere Informationen zum Anwenden der Aktualisierungen finden Sie unter [Aktualisierung ausführen](#).

## Abfrage und Benachrichtigung

Sie können Abfragebenachrichtigungen konfigurieren, um Warnmeldungen zu erhalten, wenn neue Kataloge an der vordefinierten und benutzerseitig ausgewählten Standard-Aktualisierungsquelle verfügbar sind. Die Farbe der Benachrichtigungsglocke ändert sich in orange, wenn eine neue Katalogdatei an der Aktualisierungsquelle verfügbar ist. Klicken Sie auf das Glockensymbol, um den lokal zwischengespeicherten Katalog, der an der Aktualisierungsquelle verfügbar ist, zu ersetzen. Nachdem die alten Kataloge durch die neuesten Kataloge ersetzt wurden, wird die Glocke grün.

### Info über diese Aufgabe

So stellen Sie die Abfragehäufigkeit ein:

#### Schritte

- 1 Klicken Sie in OMIMSSC auf **Maintenance Center** (Wartungszentrum) und dann auf **Polling and Notification** (Abfrage und Benachrichtigung).
- 2 Wählen Sie aus, wie häufig die Abfrage stattfinden soll:
  - **Never** (Nie): Diese Option ist standardmäßig ausgewählt. Wählen Sie diese Option aus, um nur einmal in der geplanten Zeit Aktualisierungen für neue Kataloge, die an der Aktualisierungsquelle verfügbar sind, zu erhalten.
  - **Once a week** (Einmal pro Woche): Wählen Sie diese Option aus, um einmal pro Woche Aktualisierungen für neue Kataloge, die an der Aktualisierungsquelle verfügbar sind, zu erhalten.
  - **Once every 2 weeks** (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.
  - **Once a month** (Einmal pro Monat): Wählen Sie diese Option aus, um einmal pro Monat Aktualisierungen für neue Kataloge, die an der Aktualisierungsquelle verfügbar sind, zu erhalten.

## Aktualisierungsquellen – Übersicht

Aktualisierungsquellen ermöglichen Ihnen das Auswählen und Anwenden von Aktualisierungen von Dell Aktualisierungsquellen. Sie können Aktualisierungsquellen erstellen, anzeigen und verwalten. Folgende Typen für Aktualisierungsquellen werden unterstützt: DRM-Repository, FTP und HTTP. Sie können eine DRM-, HTTP- oder FTP-Aktualisierungsquelle erstellen und als Standardaktualisierungsquelle festlegen.

Aktualisierungsquellen enthalten die Katalogdateien mit den Dell Aktualisierungen (BIOS, Firmware, Anwendung, Treiber und Treiberpakete) und die eigenständige ausführbare Datei Dell Update Packages (DUPs).

Sie können die Bestandsaufnahmeinformationen der Aktualisierungsquelle mit den Bestandsaufnahmeinformationen eines ausgewählten Servers oder einer Servergruppe vergleichen und eine Grundlinienversion erstellen. Zudem können Sie die Aktualisierungsquelle ändern und die Bestandsaufnahmeinformationen des Servers oder einer Servergruppe mit den Versionsinformationen der ausgewählten Aktualisierungsquelle vergleichen.

Führen Sie ein Upgrade auf die neueste Firmware durch, um von verbesserter Sicherheit, Fehlerbehebungen und neuen Funktionen zu profitieren. Dell veröffentlicht die folgenden Aktualisierungen über PDK-Kataloge, die vierteljährlich per Dell FTP bekanntgegeben werden:

- Server-BIOS und Firmware
- Von Dell zertifizierte Betriebssystemtreiberpakete (für die Bereitstellung des Betriebssystems)

## Vordefinierte Aktualisierungsquellen und Standard-Aktualisierungsquellen

**DELL ONLINE CATALOG** (DELL ONLINE-KATALOG) ist eine vordefinierte FTP-Aktualisierungsquelle, die im OMIMSSC-Gerät nach einer Neuinstallation oder einem Upgrade verfügbar ist. Sie können den Namen einer vordefinierten Aktualisierungsquelle weder löschen noch ändern.

**DELL ONLINE HTTP CATALOG** (DELL ONLINE-HTTP-KATALOG) ist eine Standardaktualisierungsquelle, die im OMIMSSC-Gerät nach einer Neuinstallation oder einem Upgrade verfügbar ist. Sie können den Namen dieser Standardaktualisierungsquelle weder löschen noch ändern. Sie können jedoch eine andere Aktualisierungsquelle erstellen und sie als Standardaktualisierungsquelle kennzeichnen.

**ANMERKUNG:** Fügen Sie nach der Installation von OMIMSSC die Proxy-Details für die Aktualisierungsquellen **DELL ONLINE CATALOG (DELL ONLINE-KATALOG)** und **DELL ONLINE HTTP CATALOG (DELL ONLINE-HTTP-KATALOG)** hinzu, und speichern Sie sie.

## Verbindung testen

Verwenden Sie die Option **Verbindung testen**, um während der Erstellung der Aktualisierungsquelle zu überprüfen, ob der Speicherort der Aktualisierungsquelle unter Verwendung der genannten Anmeldeinformationen erreichbar ist.

Sie können die Aktualisierungsquelle erst erstellen, nachdem Sie bestätigt haben, dass der Speicherort des Katalogs über die bereitgestellten Anmeldeinformationen erreichbar ist.

## Einrichten von lokalem FTP

So richten Sie Ihre lokale FTP-Site ein:

- 1 Erstellen Sie eine Ordnerstruktur in Ihrem lokalen FTP, die ein exaktes Replikat der Online-FTP-Site **ftp.dell.com** darstellt.
- 2 Laden Sie das Paket **catalog.xml.gz** von der Online-FTP-Site herunter, und extrahieren Sie die enthaltenen Dateien.
- 3 Öffnen Sie die Datei **catalog.xml**, und ändern Sie den Eintrag **baseLocation** in Ihre lokale FTP-URL ab, und komprimieren Sie die Datei mit der Erweiterung **.gz**.  
Ändern Sie beispielsweise den Eintrag für **baseLocation** von `ftp.dell.com` in `ftp.yourdomain.com`.
- 4 Legen Sie die Katalogdatei und die DUP-Dateien in Ihren lokalen FTP-Ordner ab, dessen Struktur der von **ftp.dell.com** entspricht.

## Einrichten von lokalem HTTP

- 1 Erstellen Sie eine Ordnerstruktur in Ihrem lokalen HTTP, die ein exaktes Replikat von **downloads.dell.com** darstellt.
- 2 Laden Sie die Datei **catalog.xml.gz** aus der Online-HTTP-Quelle unter der Adresse `http://downloads.dell.com/catalog/catalog.xml.gz` herunter und extrahieren Sie die in ihr enthaltenen Dateien.
- 3 Extrahieren Sie die Datei **catalog.xml**, und ändern Sie den Eintrag **baseLocation** in Ihre lokale HTTP-URL ab, und komprimieren Sie die Datei mit der Erweiterung **.gz**.  
Tragen Sie beispielsweise für den Wert **baseLocation** statt **downloads.dell.com** einen Host-Namen oder eine IP-Adresse wie **hostname.com** ein.
- 4 Legen Sie die Katalogdatei mit der modifizierten Katalogdatei und den DUP-Dateien in Ihrem lokalen HTTP-Ordner ab, dessen Struktur der von **downloads.dell.com** entspricht.

## Anzeigen der Aktualisierungsquelle

- 1 Klicken Sie in **OMIMSSC** auf **Maintenance Center** (Wartungcenter).
- 2 Klicken Sie im **Wartungcenter** auf **Wartungseinstellungen** und dann auf **Aktualisierungsquelle**.  
Es werden alle erstellten Aktualisierungsquellen angezeigt, inklusive ihrer Beschreibung, ihres Quelltyps, ihres Speicherorts und des Namens des betreffenden Anmeldeprofils.

## Erstellen einer Aktualisierungsquelle

### Voraussetzungen

- Stellen Sie sicher, dass je nach Typ der Aktualisierungsquelle ein Windows- oder ein FTP-Anmeldeprofil verfügbar ist.
- Wenn Sie eine DRM-Aktualisierungsquelle erstellen, müssen DRM installiert und die Administratorrollen konfiguriert sein.

### Schritte

- 1 Klicken Sie in der OMIMSSC-Konsole auf **Maintenance Center** (Wartungcenter) und dann auf **Maintenance Settings** (Wartungseinstellungen).
- 2 Klicken Sie auf der Seite **Update Source** (Aktualisierungsquelle) auf **Create New** (Neu erstellen) und geben Sie den Namen und eine Beschreibung für die Aktualisierungsquelle an.
- 3 Wählen Sie einen der folgenden Typen für die Aktualisierungsquelle aus dem Drop-Down-Menü **Source Type** (Quellentyp) aus:
  - FTP Sources (FTP-Quellen) – Wählen Sie diese Option aus, um eine Online- oder lokale FTP-Aktualisierungsquelle zu erstellen.  
**ANMERKUNG:** Wenn Sie eine FTP-Quelle erstellen möchten, geben Sie Ihre FTP-Anmeldeinformationen zusammen mit Proxy-Anmeldeinformationen an, falls die FTP-Site über Proxy-Anmeldeinformationen erreichbar ist.
  - HTTP Sources (HTTP-Quellen) – Wählen Sie diese Option aus, um eine Online- oder lokale HTTP-Aktualisierungsquelle zu erstellen.  
**ANMERKUNG:** Wenn Sie eine Aktualisierungsquelle vom Typ HTTP erstellen möchten, geben Sie den vollständigen Pfad zum Katalog mit dem Namen des Katalogs sowie Ihre Proxy-Anmeldeinformationen für den Zugriff auf die Aktualisierungsquelle an.
  - DRM Repository (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-Anmeldeinformationen an und stellen Sie sicher, dass auf den freigegebenen Windows-Speicherort zugegriffen werden kann. Geben Sie in das Feld „Location“ (Speicherort) den vollständigen Pfad der Katalogdatei mit dem Dateinamen ein.
  - Inventory Output files (Bestandsaufnahme-Ausgabedateien) – Wählen Sie diese Option aus, um eine Gegenüberstellung der Firmware-Bestandsaufnahme und der Konfiguration des Referenzservers anzuzeigen.  
**ANMERKUNG:** Sie können nur einen Vergleichsreport anzeigen, wenn Sie „Inventory Output files“ (Bestandsaufnahme-Ausgabedateien) als Aktualisierungsquelle verwenden, die Bestandsaufnahmeinformationen eines Servers mit allen anderen Servern vergleicht.
- 4 Geben Sie in **Location** (Speicherort) die URL der Aktualisierungsquelle einer HTTP- oder FTP-Quelle an und den freigegebenen Windows-Speicherort für DRM.
  - ANMERKUNG:** Die lokale FTP-Site muss die Online-FTP-Site replizieren.
  - ANMERKUNG:** Die lokale HTTP-Site muss die Online-HTTP-Site replizieren.
  - ANMERKUNG:** Die Angabe von HTTP oder HTTPS in der URL für eine FTP-Quelle ist nicht erforderlich.
- 5 Um auf die Aktualisierungsquelle zuzugreifen, wählen Sie das erforderliche Profil für die Anmeldeinformationen in **Credentials** (Anmeldeinformationen) aus.
- 6 Wählen Sie in **Proxy Credentials** (Proxy-Anmeldeinformationen) die erforderlichen Proxy-Anmeldeinformationen aus, falls ein Proxy für den Zugriff auf die FTP- oder HTTP-Quelle benötigt wird.
- 7 (Optional) Um die Aktualisierungsquelle als Standardquelle zu verwenden, aktivieren Sie die Option **Make this as default source** (Als Standardquelle festlegen).
- 8 Um zu überprüfen, ob der Speicherort der Aktualisierungsquelle über diese Anmeldeinformationen erreichbar ist, klicken Sie auf **Test Connection** (Verbindung testen) und dann auf **Save** (Speichern).  
**ANMERKUNG:** Sie können die Aktualisierungsquelle erst nach dem erfolgreichen Testen der Verbindung erstellen.

## Ändern einer Aktualisierungsquelle

### Info über diese Aufgabe

Beachten Sie beim Ändern einer Aktualisierungsquelle die folgenden Punkte:

- Nach Erstellung einer Aktualisierungsquelle können Typ und Speicherort nicht mehr geändert werden.
- Sie können eine Aktualisierungsquelle sogar dann ändern, wenn die Aktualisierungsquelle durch einen laufenden oder geplanten Job verwendet wird oder wenn sie in einer Bereitstellungsvorlage verwendet wird. Beim Ändern einer verwendeten Aktualisierungsquelle wird eine Warnmeldung angezeigt. Klicken Sie auf **Confirm** (Bestätigen), um mit den Änderungen fortzufahren.
- Wird in der Aktualisierungsquelle eine Katalogdatei aktualisiert, wird die lokal zwischengespeicherte Katalogdatei nicht automatisch aktualisiert. Um die im Cache gespeicherte Katalogdatei zu aktualisieren, bearbeiten Sie die Aktualisierungsquelle oder löschen Sie sie und erstellen Sie sie neu.

### Schritt

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

## Löschen der Aktualisierungsquelle

### Info über diese Aufgabe

Sie können eine Aktualisierungsquelle löschen, wenn:

- Die Aktualisierungsquelle eine vordefinierte Aktualisierungsquelle (**Dell Online Catalog** (Dell Online-Katalog) und **DELL ONLINE HTTP CATALOG** (DELL ONLINE-HTTP-KATALOG) ist.
- Die Aktualisierungsquelle wird von einem laufenden Prozess oder einem geplanten Job verwendet.
- Die Aktualisierungsquelle ist eine Standard-Aktualisierungsquelle.

### Schritt

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

## Aktualisierungsgruppen

Aktualisierungsgruppen sind Gruppen von Servern, die die gleiche Aktualisierungsverwaltung erfordern. Es gibt zwei Arten von Aktualisierungsgruppen:

- Vordefinierte Aktualisierungsgruppen: Sie können nur die Server in der Gruppe sehen. Sie können die vordefinierten Aktualisierungsgruppen nicht manuell erstellen, ändern oder löschen.
- Benutzerdefinierte Aktualisierungsgruppen: Sie können Server in der Gruppe erstellen und warten.

**i ANMERKUNG: Alle Servergruppen, die in SCVMM vorhanden sind, sind in OMIMSSC aufgelistet, da OMIMSSC nicht benutzerspezifisch ist. Stellen Sie sicher, dass Sie Zugriff haben, um Vorgänge auf diesen Servern auszuführen.**

## Vordefinierte Aktualisierungsgruppen

Vordefinierte Aktualisierungsgruppen lassen sich wie folgt beschreiben und weisen das folgende Verhalten auf:

**Allgemeine Aktualisierungsgruppen:** Diese Gruppe besteht aus Hosts und nicht zugewiesenen Servern, die in einer einzelnen Sitzung aktualisiert werden.

**Alle Aktualisierungsgruppen:** Diese Gruppe besteht aus allen Servergruppen. Jede in OMIMSSC vorhandene Gruppe gehört zu allen Aktualisierungsgruppen. Diese Gruppe ist vom Typ „allgemeine Aktualisierungsgruppe“.

**Standard-Aktualisierungsgruppe für nicht zugewiesene Server:** Diese Gruppe besteht aus allen nicht zugewiesenen Servern, die keiner anderen Aktualisierungsgruppe angehören. Diese Gruppe ist vom Typ „allgemeine Aktualisierungsgruppe“. Die Server werden zur Standard-Aktualisierungsgruppe für nicht zugewiesene Server hinzugefügt, nachdem Folgendes erfolgt ist:

- Ermittlung oder erneute Ermittlung von Bare Metal-Servern
- Synchronisierung oder erneute Synchronisierung nach dem Löschen aus SCVMM (jedoch auf der OMIMSSC-Appliance vorhanden)

**Cluster-Aktualisierungsgruppe:** Diese Gruppe besteht aus den Windows-Server-Failover-Clustern. Wenn ein modularer Server einem Cluster angehört, wird er zur Cluster-Aktualisierungsgruppe hinzugefügt. Wenn ein modularer Dell PowerEdge-Server der 12. oder 13.

Generation zu einem Cluster gehört, werden die CMC-Informationen auch zu den Bestandsdaten auf der Seite **Maintenance Center** (Wartungszentrum) hinzugefügt.

Um herauszufinden, welcher Cluster-Aktualisierungsgruppe ein Server angehört, rufen Sie die Seite **Configuration and Deployment** (Konfiguration und Bereitstellung) auf. Dort werden der Hostname und der Cluster-FQDN aller in OMIMSSC aufgeführten Server angezeigt.

**Host-Aktualisierungsgruppe:** Diese Gruppe besteht aus Host-Servern. Aktualisierungen werden in einer einzigen Sitzung angewendet, was bedeutet, dass alle Server innerhalb der Gruppe zusammen aktualisiert werden.

**Standard-Host-Aktualisierungsgruppe:** Diese Gruppe besteht aus allen ermittelten Hosts, die keiner anderen Aktualisierungsgruppe angehören. Diese Gruppe ist vom Typ „Host-Aktualisierungsgruppe“.

**Gehäuse-Aktualisierungsgruppe:** Diese Gruppe besteht aus modularen Servern, die zu einem Gehäuse gehören und keiner Cluster-Gruppe angehören. PowerEdge-Server der 12. oder 13. Generation werden zusammen mit ihren CMC-Informationen erkannt. Standardmäßig wird eine Gruppe mit dem folgenden Benennungsformat erstellt: **Gehäuse-Service-Tag-Nummer-der-Gehäusegruppe**. Beispiel: `Chassis-GJDC4BS-Group`. Wenn ein modularer Server aus einer Cluster-Aktualisierungsgruppe gelöscht wird, wird der Server mitsamt CMC-Informationen zur Gehäuse-Aktualisierungsgruppe hinzugefügt. Auch wenn es keine modularen Server in der entsprechenden Gehäuse-Aktualisierungsgruppe gibt, weil alle modularen Server im Gehäuse einer Cluster-Aktualisierungsgruppe angehören, bleibt die Gehäuse-Aktualisierungsgruppe weiterhin bestehen, sie zeigt dann aber nur die CMC-Informationen.

**Standard-Aktualisierungsgruppe für nicht Windows-basierte Hosts:** Diese Gruppe besteht aus Servern mit einem anderen Betriebssystem als Windows.

## Benutzerdefinierte Aktualisierungsgruppen

Diese Gruppe ermöglicht es Ihnen, Aktualisierungsgruppen zu erstellen, zu ändern und zu löschen. Zu einer benutzerdefinierten Aktualisierungsgruppe können allerdings nur Server aus den **Standard-Aktualisierungsgruppen für nicht zugewiesene Server** und **Standard-Host-Aktualisierungsgruppen** hinzugefügt werden. Nach dem Hinzufügen eines Servers zu einer benutzerdefinierten Aktualisierungsgruppe wird der Server aus der vordefinierten Aktualisierungsgruppe entfernt und steht dann nur noch in der benutzerdefinierten Aktualisierungsgruppe zur Verfügung. Suchen Sie die erforderlichen Server mithilfe ihrer Service-Tag-Nummer, um sie zu einer benutzerdefinierten Aktualisierungsgruppe hinzuzufügen.

**ANMERKUNG:** Wenn ein Server aus MSSC gelöscht wird und Sie OMIMSSC mit einer registrierten MSSC-Instanz synchronisieren, wird der Server aus der benutzerdefinierten Aktualisierungsgruppe entfernt und in die entsprechende vordefinierte Gruppe verschoben.

## Aktualisierungsmethoden

Sie können Aktualisierungen auf ausgewählten Servergruppen anwenden, deren Hardware mit OMIMSSC kompatibel ist.

- Sie können die folgenden Aktualisierungen auf Servergruppen anwenden:
  - **Agentenlose stufenweise Aktualisierungen:** Es handelt sich um das Staging von Firmware-Aktualisierungen. Die Firmware-Aktualisierungen, die sofort anwendbar sind und keinen Neustart erfordern, werden sofort angewendet. Die übrigen Aktualisierungen, die einen Neustart des Systems erfordern, werden beim Neustart des Servers angewendet. Aktualisierungen werden mithilfe von iDRAC zum geplanten Zeitpunkt in Batches durchgeführt. Die Batch-Größe wird bei der Durchführung der Aktualisierung bestimmt. Aktualisieren Sie die Bestandsdaten, um zu überprüfen, ob alle Aktualisierungen angewendet wurden. Wenn der Vorgang auf nur einem Server fehlschlägt, schlägt der gesamte Job fehl.
  - **Agentenlose Aktualisierungen:** Es handelt sich um eine bandexterne Aktualisierung mit sofortigem Neustart des Servers.
  - **Clusterfähiges Aktualisieren (CAU):** Der Aktualisierungsvorgang wird durch Verwendung der Windows-CAU-Funktion auf Cluster-Aktualisierungsgruppen automatisiert, um die Verfügbarkeit des Servers zu gewährleisten. Weitere Informationen über CAU finden Sie unter [Aktualisierungen unter Verwendung von CAU](#).

## Anzeigen von Aktualisierungsgruppen

So zeigen Sie Aktualisierungsgruppen an:

- 1 Klicken Sie in **OMIMSSC** auf **Maintenance Center** (Wartungscenter) und dann auf **Maintenance Settings** (Wartungseinstellungen).
- 2 Klicken Sie bei den **Wartungseinstellungen** auf **Aktualisierungsgruppen**.  
Alle erstellten benutzerdefinierten Gruppen werden mit Namen, Gruppentyp und Anzahl von Servern in der Gruppe angezeigt.

## Erstellen von benutzerdefinierten Aktualisierungsgruppen

- 1 Klicken Sie in der OMIMSSC-Konsole auf **Maintenance Center** (Wartungscenter) und dann auf **Maintenance Settings** (Wartungseinstellungen).
- 2 Klicken Sie bei den **Wartungseinstellungen** auf **Aktualisierungsgruppen** und dann auf **Erstellen**.  
Die Seite **Firmware-Aktualisierungsgruppe** wird angezeigt.
- 3 Geben Sie einen Gruppennamen und eine Beschreibung ein. Und wählen Sie den Typ der zu erstellenden Aktualisierungsgruppe aus.  
In benutzerdefinierten Aktualisierungsgruppen können nur Server der folgenden Aktualisierungsgruppentypen enthalten sein:
  - Generic update group (Allgemeine Host-Aktualisierungsgruppe) – Diese Gruppe besteht aus Servern aus standardmäßigen, nicht zugewiesenen Aktualisierungsgruppen und Host-Aktualisierungsgruppen.
  - Host update group (Host-Aktualisierungsgruppe) – Diese Gruppe besteht aus Servern aus Standard-Host-Aktualisierungsgruppen.Es kann auch eine Kombination der Server aus den beiden Servergruppentypen verwendet werden.
- 4 Um der Aktualisierungsgruppe Server hinzuzufügen, suchen Sie nach den Servern anhand ihrer Service-Tag-Nummer. Um Server der Tabelle **Servers Included in the Update Group** (In der Aktualisierungsgruppe enthaltene Server) hinzuzufügen, klicken Sie auf den Pfeil nach rechts.
- 5 Um die benutzerdefinierte Aktualisierungsgruppe zu erstellen, klicken Sie auf **Save** (Speichern).

## Ändern von benutzerdefinierten Aktualisierungsgruppen

### Info über diese Aufgabe

Beachten Sie Folgendes, wenn Sie eine benutzerdefinierte Aktualisierungsgruppe ändern möchten:

- Der Typ einer Aktualisierungsgruppe kann nach der Erstellung nicht mehr geändert werden.
- Wenn Sie Server von einer benutzerdefinierten Aktualisierungsgruppe in eine andere verschieben möchten, haben Sie folgende Möglichkeiten:
  - a Sie können den Server aus der vorhandenen benutzerdefinierten Aktualisierungsgruppe entfernen. Er wird dann automatisch der vordefinierten Aktualisierungsgruppe hinzugefügt.
  - b Sie können die benutzerdefinierte Gruppe bearbeiten, der Sie den Server hinzufügen möchten, und den Server anhand seiner Service-Tag-Nummer suchen.

### Schritte

- 1 Klicken Sie in **OMIMSSC** auf **Maintenance Center** (Wartungscenter) und dann auf **Maintenance Settings** (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.

## Löschen von benutzerdefinierten Aktualisierungsgruppen

### Info über diese Aufgabe

Beachten Sie Folgendes, wenn Sie eine benutzerdefinierte 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.
- Sie können eine Aktualisierungsgruppe auch dann löschen, wenn Server in dieser Aktualisierungsgruppe vorhanden sind. Nach dem Löschen einer Aktualisierungsgruppe werden die Server jedoch zu ihren vordefinierten Aktualisierungsgruppen verschoben.

- Löschen Sie die geplanten Jobs, die mit einer benutzerdefinierten Aktualisierungsgruppe verbunden sind, bevor Sie die Servergruppe löschen.

### Schritte

- 1 Klicken Sie in OMIMSSC auf **Maintenance Center** (Wartungscenter) und dann auf **Maintenance Settings** (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.

## Anwenden von Filtern

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

### Info über diese Aufgabe

Die OMIMSSC-Appliance unterstützt drei Kategorien von Filtern:

- **Nature Of Update** (Art der Aktualisierung): Wählen Sie diesen Filter aus, wenn nur Serveraktualisierungen des ausgewählten Typs angezeigt werden sollen.
- **Component Type** (Komponententyp): Wählen Sie diesen Filter aus, wenn nur Serverkomponenten des ausgewählten Typs angezeigt werden sollen.
- **Server Model** (Servermodell): Wählen Sie diesen Filter aus, wenn nur Server des ausgewählten Modells angezeigt werden sollen.

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

### So wenden Sie Filter an:

#### Schritt

Klicken Sie in OMIMSSC auf **Maintenance Center** (Wartungscenter). Öffnen Sie dann das Drop-Down-Menü mit den Filtern und wählen Sie die gewünschten Filter aus.

#### Nächster Schritt

##### So entfernen Sie Filter:

Klicken Sie in OMIMSSC auf **Maintenance Center** (Wartungscenter). Klicken Sie dann auf **Clear Filters** (Filter löschen) oder deaktivieren Sie die ausgewählten Kontrollkästchen.

## Anzeigen und Aktualisieren der Firmware-Bestandsaufnahme

Sie können die Informationen zum Firmware-Bestand bestimmter Server oder Servergruppen anzeigen und aktualisieren.

Sie können die Bestandsinformationen zu einem Server oder einem Gehäuse mit einer ausgewählten Aktualisierungsquelle abgleichen und einen Vergleichsbericht erstellen. Sie können die Aktualisierungsquelle ändern, die Bestandsinformationen der ausgewählten Server, Servergruppen oder Gehäuse mit der neuen Aktualisierungsgruppe abgleichen und einen Vergleichsbericht erstellen.

Sie können die Firmware-Bestandsinformationen eines Servers, einer Servergruppe oder eines Gehäuses mit den neuesten Informationen aktualisieren. Wenn Sie die Komponenteninformationen eines Servers aktualisieren, werden die kompletten Bestandsinformationen des Servers aktualisiert.

**ANMERKUNG:** Wird eine Katalogdatei erstellt, wird eine lokale Kopie der Datei in OMIMSSC zwischengespeichert. Sie müssen also die Katalogdatei aktualisieren, um die neuesten Vergleichsbericht abrufen zu können. Zur Aktualisierung der Katalogdatei bearbeiten Sie die Aktualisierungsquelle und speichern sie. Alternativ können Sie die Aktualisierungsquelle löschen und neu erstellen.

**ANMERKUNG:** Bei einer Aktualisierung der Bestandsinformationen werden Serverinformationen wie „Driver Pack Version“ (Treiberpaket-Version) und „Drivers Available for OS“ (Verfügbare Treiber für das Betriebssystem) eines Servers in den Eigenschaften unter „Dell Out of Band Controllers (OOB)“ (Dell Out-of-Band-Controller [OOB]) in der SCCM-Konsole nicht aktualisiert. Zur Aktualisierung der Seite „OOB“ müssen Sie OMIMSSC mit SCCM synchronisieren.

**ANMERKUNG:** Wenn Sie ein Upgrade auf diese Version von OMIMSSC durchführen, werden für in früheren Versionen ermittelte Server nicht die neuesten Informationen angezeigt. Sie müssen erneut eine Ermittlung für die Server durchführen, um die neuesten Serverinformationen und einen korrekten Vergleichsbericht zu erhalten.

So können Sie die Firmware-Bestandsaufnahme für einen Server oder eine Servergruppe anzeigen oder aktualisieren:

- 1 Wählen Sie in **OMIMSSC** im **Maintenance Center** (Wartungszentrum) unter **Select Update Group** (Aktualisierungsgruppe auswählen) eine Aktualisierungsgruppe aus.
- 2 (Optional) Um die Aktualisierungsquelle zu ändern, wählen Sie eine andere Aktualisierungsquelle bei **Aktualisierungsquelle auswählen** aus.
- 3 Klappen Sie unter **Device Group/Servers** (Gerätegruppe/Server) in der Servergruppe die Serverebene und dann die Komponentenebene auf, um die aktuelle Version der Firmware, die Baseline-Version der Firmware und die von der OMIMSSC-Appliance vorgeschlagenen Aktualisierungsaktionen anzuzeigen.

**ANMERKUNG:**

In den Komponenteninformationen werden die NIC-bezogenen Informationen für PowerEdge-Server der 11. Generation wie folgt angezeigt:

- Wenn Sie für den Filter **Nature of Update** (Art der Aktualisierung) die Option **Urgent** (Dringend) auswählen, werden im Bericht ausschließlich die Komponenten angezeigt, für die dringende Aktualisierungen verfügbar sind. Beim Export dieses Berichts werden auch alle Komponenten mit Downgrade-Empfehlung exportiert, für die kritische Aktualisierungen verfügbar sind.
- Verfügt eine NIC über mehrere Netzwerkschnittstellen, wird in der Liste **Component Information** (Komponenteninformationen) nur ein einziger Eintrag für alle Schnittstellen angelegt. Nach der Firmware-Aktualisierung wird für alle NICs ein Upgrade durchgeführt.
- Wenn die bereits vorhandenen NICs um eine neue Karte ergänzt werden, wird die neue NIC in der Liste **Component Information** (Komponenteninformationen) als eine weitere Instanz aufgeführt. Nach der Firmware-Aktualisierung wird für alle NICs ein Upgrade durchgeführt.

- 4 Wählen Sie den Server oder die Gruppe von Servern aus, die Sie aktualisieren möchten, und klicken Sie dann auf **Bestandsaufnahme aktualisieren**.

## Wiederherstellung

Sie können das Serverprofil im Schutz-Vault speichern, indem Sie das Profil exportieren und das Profil auf demselben Server importieren, um einen früheren Zustand wiederherzustellen.

## Schutz-Vaults

Ein Schutz-Vault ist ein sicherer Speicherort, an dem Sie Serverprofile für einen Server oder eine Servergruppe exportieren und importieren können. Sie können dieses Serverprofil an einem freigegebenen Speicherort im Netzwerk speichern, indem Sie einen externen Vault erstellen, oder auf einer vFlash-SD-Karte, indem Sie einen internen Vault erstellen. Sie können gleichzeitig immer nur einen Server oder eine Servergruppe einem Schutz-Vault zuordnen. Allerdings können Sie einen Schutz-Vault mehreren Servern oder Servergruppen zuordnen.

## Erstellen eines Schutz-Vaults

### Voraussetzung

Stellen Sie sicher, dass auf den Schutz-Vault zugegriffen werden kann.

### Schritte

- 1 Klicken Sie in **OMIMSSC** auf **Maintenance Center** (Wartungszentrum) und dann auf **Maintenance Settings** (Wartungseinstellungen).
- 2 Klicken Sie im **Wartungszentrum** auf **Schutz-Vault** und dann auf **Erstellen**.
- 3 Wählen Sie den gewünschten Schutz-Vault-Typ aus und geben Sie die Details an.
  - Geben Sie beim Erstellen eines Schutz-Vaults vom Typ **Network Share** (Netzwerkfreigabe) einen Speicherort für die Profile, die Anmeldeinformationen für den Zugriff auf diesen Speicherort und eine Passphrase zur Sicherung des Profils an.

**ANMERKUNG:** Dieser Schutz Vault-Typ unterstützt 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.

## Modifizieren eines Schutz-Vaults

### Info über diese Aufgabe

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

### Schritte

- 1 Klicken Sie in **OMIMSSC** auf **Maintenance Center (Wartungcenter) > Maintenance Settings (Wartungseinstellungen) > Protection Vault (Schutz-Vault)**.
- 2 Wählen Sie zum Bearbeiten des Vaults den gewünschten Vault aus und klicken Sie auf **Edit** (Bearbeiten).

## Löschen eines Schutz-Vaults

### Info über diese Aufgabe

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 anschließend den Schutz-Vault.
- Mit dem Schutz-Vault ist ein geplanter Job verknüpft. Um einen solchen Schutz-Vault zu löschen, löschen Sie den geplanten Job und anschließend den Schutz-Vault.

### Schritte

- 1 Klicken Sie in **OMIMSSC** auf **Maintenance Center (Wartungcenter) > Maintenance Settings (Wartungseinstellungen) > Protection Vault (Schutz-Vault)**.
- 2 Wählen Sie den zu löschenden Vault aus und klicken Sie auf **Delete** (Löschen).

## Exportieren von Serverprofilen

Sie können Serverprofile exportieren, und zwar inklusive der auf den verschiedenen Komponenten installierten Firmware-Abbilder und der Konfiguration der verschiedenen Komponenten (BIOS, RAID, NIC, iDRAC, Lifecycle Controller). Die OMIMSSC-Appliance erstellt eine Datei mit allen Konfigurationen, die Sie auf einer vFlash-SD-Karte oder einer Netzwerkfreigabe speichern können. Sie können die Datei in einem Schutz-Vault Ihrer Wahl ablegen. Die Konfigurationsprofile von Servern oder Servergruppen können wahlweise sofort oder zeitplanbasiert an einem späteren Datum exportiert werden. Außerdem können Sie einen regelmäßigen Export festlegen, für den verschiedene Intervalle zur Auswahl stehen. Zu jedem beliebigen Zeitpunkt können Sie einen einzigen Job zum Konfigurationsexport für eine Servergruppe festlegen. Während des Exports von Konfigurationsprofilen können Sie auf dem betreffenden Server bzw. in der betreffenden Servergruppe keine weiteren Aktivitäten durchführen.

### Voraussetzung

Deaktivieren Sie die Option **F1/F2 Prompt on Error** (F1/F2-Aufforderung bei Fehler) unter **BIOS Settings** (BIOS-Einstellungen).

### Info über diese Aufgabe

- ANMERKUNG:** Stellen Sie sicher, dass der Job **Automatic Backup (Automatische Sicherung)** in iDRAC nicht für den gleichen Zeitpunkt geplant ist.
- ANMERKUNG:** Ein Export von Serverprofilen ist nicht möglich, wenn Sie Filter angewendet haben. Sie müssen alle angewendeten Filter löschen, bevor Sie Serverprofile exportieren können.
- ANMERKUNG:** Für den Export von Serverprofilen ist eine iDRAC Enterprise-Lizenz erforderlich.

**ANMERKUNG:** Vergewissern Sie sich vor dem Export eines Serverprofils, dass sich die IP-Adresse des Servers nicht geändert hat. Hat sich die Server-IP aufgrund eines anderen Vorgangs geändert, müssen Sie für den Server erneut eine Ermittlung in OMIMSSC durchführen, bevor Sie einen Zeitpunkt für die Ausführung des Jobs zum Exportieren des Serverprofils festlegen können.

### Schritte

- 1 Klicken Sie in OMIMSSC auf **Maintenance Center** (Wartungszentrum). Wählen Sie die Server aus, deren Profile Sie exportieren möchten, und klicken Sie auf **Export Server Profile** (Serverprofil exportieren).
- 2 Geben Sie im Fenster **Export Server Profile** (Serverprofil exportieren) die Details für den betreffenden Job ein und wählen Sie anschließend einen Schutz-Vault aus.

Weitere Informationen zu Schutz-Vaults finden Sie unter [Creation of protection vault](#) (Erstellen eines Schutz-Vaults).

Wählen Sie unter **Schedule Export Server Profile** (Zeitplan für den Export des Serverprofils festlegen) eine der folgenden Optionen aus:

- **Run Now** (Jetzt ausführen): Bei Auswahl dieser Option wird die Serverkonfiguration der ausgewählten Server oder Gruppe von Servern sofort exportiert.
- „Schedule“ (Zeitplan): Hier können Sie einen Zeitplan festlegen, gemäß dem die Serverkonfiguration der ausgewählten Gruppe von Servern exportiert werden soll.
  - **Never** (Nie): Wählen Sie diese Option aus, um das Serverprofil einmalig zur geplanten Zeit zu exportieren.
  - **Once a week** (Wöchentlich): Wählen Sie diese Option aus, um das Serverprofil wöchentlich zu exportieren.
  - **Once every 2 weeks** (Zweiwöchentlich): Wählen Sie diese Option aus, um das Serverprofil alle zwei Wochen zu exportieren.
  - **Once every 4 weeks** (Vierwöchentlich): Wählen Sie diese Option aus, um das Serverprofil alle vier Wochen zu exportieren.

## Importieren von Serverprofilen

Sie können ein Serverprofil importieren, das zuvor für den gleichen Server oder die gleiche Gruppe von Servern exportiert wurde. Durch Importieren eines Serverprofils kann die Konfiguration und die Firmware eines Servers in einem in diesem Profil gespeicherten Zustand wiederhergestellt werden. In solchen Fällen können Sie das Serverprofil auf diesem Server oder dieser Servergruppe ersetzen, indem Sie ein zuvor exportiertes Serverprofil dieses Servers oder dieser Servergruppe importieren.

### Info über diese Aufgabe

Es gibt zwei Möglichkeiten, Serverprofile zu importieren:

- Quick import server profile (Schnellimport des Serverprofils) – Mit dieser Funktion können Sie das zuletzt exportierte Serverprofil für diesen Server automatisch importieren. Für diesen Vorgang müssen Sie keine einzelnen Serverprofile für jeden Server auswählen.
- Custom import server profile (Benutzerdefinierter Import des Serverprofils) – Mit dieser Funktion können Sie Serverprofile für einzelne, ausgewählte 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 aus einer Liste der exportierten Serverprofile nur für diesen Server importieren. Sie können dieselben Serverprofile nicht für verschiedene Server oder Servergruppen importieren. Wenn Sie versuchen, ein Serverprofil eines anderen Servers oder einer anderen Servergruppe zu importieren, schlägt das Importieren des Serverprofils fehl.
- Falls für einen bestimmten Server oder eine Servergruppe kein Serverprofil-Image verfügbar ist und für diesen Server bzw. diese Servergruppe ein Job zum Importieren eines Serverprofils initiiert wird, schlägt dieser Job fehl. Den Aktivitätsprotokollen wird eine Protokollmeldung 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 Komponenteneinformationen wiederhergestellt mit Ausnahme der Informationen zu der fehlenden Komponente, die übersprungen wird. Diese Informationen sind nicht im Aktivitätsprotokoll von OMIMSSC verfügbar. Weitere Informationen über die fehlenden Komponenten finden Sie im **Lifecycle-Protokoll** von iDRAC.
- Sie können ein Serverprofil nicht nach Anwendung der Filter importieren. Um Serverprofile zu importieren, löschen Sie alle angewendeten Filter.

- Um Serverprofile zu importieren, müssen Sie über eine iDRAC Enterprise-Lizenz verfügen.

### Schritte

- 1 Wählen Sie in OMIMSSC unter **Maintenance Center** (Wartungszentrum) die Server aus, deren Profile Sie importieren möchten, und klicken Sie auf **Import Server Profile** (Serverprofil importieren).
- 2 Geben Sie die Details ein und wählen Sie den gewünschten **Import Server Profile Type** (Serverprofiltyp für den Import) aus.

① **ANMERKUNG: Preserve Data (Daten beibehalten) ist standardmäßig ausgewählt und behält die bestehende RAID-Konfiguration auf dem Server bei. Deaktivieren Sie das Kontrollkästchen, wenn Sie die in dem Serverprofil gespeicherten RAID-Einstellungen anwenden möchten.**

- 3 Um das Serverprofil zu importieren, klicken Sie auf **Finish** (Fertig stellen).

## Anwenden von Firmware- und Konfigurationseinstellungen

Die Teilersetzungsfunktion aktualisiert automatisch eine ersetzte Serverkomponente mit der erforderlichen Firmware-Version und/oder mit der Konfiguration der alten Komponente. Die Aktualisierung erfolgt automatisch, wenn Sie Ihr System nach dem Austausch der Komponente neu starten.

### Info über diese Aufgabe

So legen Sie die Parameter für die Teilersetzung fest:

### Schritte

- 1 Klicken Sie in OMIMSSC auf **Maintenance Center** (Wartungszentrum), wählen Sie die gewünschten Server oder die gewünschte Servergruppe aus und klicken Sie auf **Configure Part Replacement** (Teileaustausch konfigurieren).  
Das Fenster **Part Replacement Configuration** (Teileaustauschkonfiguration) wird angezeigt.
- 2 Sie können **CSIOR**, **Part Firmware Update** (Teile-Firmware-Aktualisierung) und **Part Configuration Update** (Teile-Konfigurationsaktualisierung) auf eine der folgenden Optionen festlegen und dann auf **Finish** (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.
  - Part firmware update (Teile-Firmware-Aktualisierung) – Je nach getroffener Auswahl wird die Firmware-Version der Komponente entweder wiederhergestellt, aktualisiert oder zurückgestuft.
    - **Disabled** (Deaktiviert) – Die Teile-Firmware-Aktualisierung ist deaktiviert und das Gleiche gilt für die ersetzte Komponente.
    - **Allow version upgrade only** (Nur Versionserweiterung zulassen) – Die erweiterte Firmware-Versionen werden auf die ersetzte Komponente angewendet, wenn die Firmware-Version der neuen Komponente älter als die vorhandene Version ist.
    - **Match firmware of replaced part** (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.
  - Part configuration update (Teile-Konfigurationsaktualisierung) – Je nach getroffener Auswahl wird die Firmware-Version der Komponente wiederhergestellt oder aktualisiert.
    - **Disabled** (Deaktiviert) – Die Teile-Konfigurationsaktualisierung ist deaktiviert und die gespeicherte Konfiguration der alten Komponente wird nicht auf die ersetzte Komponente angewendet.
    - **Apply always** (Immer anwenden) – Die Teile-Konfigurationsaktualisierung ist deaktiviert und die gespeicherte Konfiguration der alten Komponente wird auf die ersetzte Komponente angewendet.
    - **Apply only if firmware matches** (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

## Info über diese Aufgabe

In LC-Protokollen sind alle Aktivitäten vermerkt, die in der Vergangenheit auf einem verwalteten System ausgeführt wurden. Diese Protokolldateien sind für Serveradministratoren nützlich, da sie detaillierte Informationen zu empfohlenen Maßnahmen sowie andere technische Informationen enthalten, die bei der Fehlerbehebung hilfreich sind. Zu den in LC-Protokollen vermerkten Informationen gehören unter anderem Warnhinweise, Konfigurationsänderungen an den Hardwarekomponenten des Systems, Firmware-Änderungen aufgrund von Upgrades oder Downgrades, Informationen zu Teileaustauschen, Temperaturwarnungen, detaillierte Zeitstempel über den Beginn der Aktivität und der Schweregrad der Aktivität.

Es gibt zwei Möglichkeiten, LC-Protokolle zu erfassen:

- **Aktive LC-Protokolle:** Dies sind die neuesten LC-Protokolldateien. Sie können diese Protokolldateien einsehen, durchsuchen und in die Appliance exportieren. Sie können einen Job einrichten, um die LC-Protokolle zeitplanbasiert in der Appliance oder auf einer Netzwerkfreigabe zu erfassen. Zudem ist es möglich, eine Sicherungskopie der Protokolldatei auf der Netzwerkfreigabe zu speichern.
- **Vollständige LC-Protokolle:** Diese Protokolle enthalten aktive und archivierte LC-Protokolldateien. Da sie groß sind, werden sie ins Format `.gz` komprimiert und anschließend an den angegebenen Speicherort auf einer CIFS-Netzwerkfreigabe exportiert.

## Schritte

- 1 Klicken Sie in OMIMSSC auf **Maintenance Center** (Wartungszentrum). Wählen Sie einen Server oder eine Servergruppe aus und klicken Sie auf **Collect LC Logs** (LC-Protokolle erfassen).
- 2 Wählen Sie unter **LC Log Collection** (Erfassung von LC-Protokollen) eine der folgenden Optionen aus und klicken Sie auf **Finish** (Fertigstellen):
  - **Export Complete LC Logs (.gz)** (Vollständige LC-Protokolle exportieren [.gz]): Sowohl die aktiven als auch die archivierten LC-Protokolle werden auf eine CIFS-Netzwerkfreigabe exportiert. Dabei werden die Windows-Anmeldeinformationen angegeben. So ist beispielsweise `201607201030010597.xml.gz` der Name der LC-Datei, der das Datum und die Uhrzeit der Dateierstellung enthält.

**ANMERKUNG:** Die vollständigen LC-Protokolle sind große Dateien. Stellen Sie daher sicher, dass im freigegebenen Ordner genügend Speicherplatz frei ist.

**ANMERKUNG:** Das Exportieren vollständiger LC-Protokolle wird auf PowerEdge-Servern der 11. Generation nicht unterstützt.

**ANMERKUNG:** LC-Protokolle werden im folgenden Format `<YYYYMMDDHHMMSSSS>.<file format>` gespeichert.

- **Export Active Logs (Run now)** (Aktive Protokolle exportieren [Jetzt ausführen]): Diese Option exportiert alle aktiven Protokolle unverzüglich in die Appliance.
  - (Optional) Aktivieren Sie die Option **Back up LC logs on the network share** (LC-Protokolle auf die Netzwerkfreigabe sichern), um eine Sicherungskopie der LC-Protokolle auf der CIFS-Netzwerkfreigabe zu speichern. Dabei werden die Windows-Anmeldeinformationen angegeben.

**ANMERKUNG:** Stellen Sie auf PowerEdge-Servern der 11. Generation sicher, dass die neuesten Versionen von iDRAC und LC installiert sind, bevor Sie aktive Protokolle exportieren.

- **Schedule LC Log Collection** (Zeitplanbasierte Sammlung der LC-Protokolle): Hier können Sie festlegen an welchem Datum, zu welcher Uhrzeit und mit welcher Häufigkeit die aktiven LC-Protokolle exportiert werden sollen.
  - (Optional) Aktivieren Sie die Option **Back up LC logs on the network share** (LC-Protokolle auf die Netzwerkfreigabe sichern), um eine Sicherungskopie der LC-Protokolle auf der CIFS-Netzwerkfreigabe zu speichern. Dabei werden die Windows-Anmeldeinformationen angegeben.

Die verfügbaren Optionen für die Planung der Häufigkeit, um festzulegen, wie oft die LC-Protokolle erfasst werden sollen, sind:

- **Never** (Nie): Wählen Sie diese Option aus, um die LC-Protokolle einmalig zur geplanten Zeit zu exportieren.
- **Daily** (Täglich): Wählen Sie diese Option aus, um die LC-Protokolle täglich zur geplanten Zeit zu exportieren.
- **Once a week** (Wöchentlich): Wählen Sie diese Option aus, um die LC-Protokolle einmal pro Woche zur geplanten Zeit zu exportieren.

- **Once every 4 weeks** (Vierwöchentlich): Wählen Sie diese Option aus, um die LC-Protokolle alle vier Wochen zur geplanten Zeit zu exportieren.

**ANMERKUNG:** Die exportierte LC-Protokolldatei wird unter einem Ordnernamen der Service-Tag-Nummer des jeweiligen Servers gespeichert.

## Anzeigen von LC-Protokollen

Sie können alle aktiven LC-Protokolle anzeigen, nach ausführlicher Beschreibung suchen und die Protokolle im CSV-Format mit der Funktion „LC-Protokolle anzeigen“ herunterladen.

### Voraussetzung

Legen Sie die Browsereinstellungen wie unter [Browsereinstellungen](#) angegeben fest.

### Schritte

- 1 Klicken Sie in OMIMSSC auf **Maintenance Center** (Wartungszentrum). Wählen Sie einen Server oder eine Servergruppe aus und klicken Sie auf **View LC Logs** (LC-Protokolle anzeigen).
- 2 Alle Server in der ausgewählten Gruppe und die Server, für welche LC-Protokolle erfasst werden, werden mit ihren LC-Protokolldateien aufgelistet. Klicken Sie auf einen Dateinamen, um alle Protokolleinträge in der LC-Protokolldatei speziell für diesen Server anzuzeigen. Weitere Informationen finden Sie unter [Dateibeschreibung](#).
- 3 (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 einer LC-Datei gibt es zwei Möglichkeiten:

- Klicken Sie auf einen Dateinamen, um die LC-Protokolldatei zu öffnen, und suchen Sie im Suchfeld nach einer Beschreibung.
- Geben Sie eine Beschreibung in das Suchfeld ein und zeigen Sie dann alle LC-Dateien mit den Vorkommen dieses Texts an.

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

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

**ANMERKUNG:** Fügen Sie vor dem Herunterladen der LC-Protokolle das Gerät auf der lokalen Intranet-Site hinzu.

So fügen Sie der Site **Lokales Intranet** in **Internet Explorer** ein Gerät hinzu:

- a Öffnen Sie einen Browser, klicken Sie auf **Extras** und dann auf **Internetoptionen**.
- b Klicken Sie auf **Sicherheit > Lokales Intranet > Sites**.  
Die Seite **Lokales Intranet** wird angezeigt.
- c Klicken Sie auf **Erweitert**, geben Sie die Geräte-URL ein und klicken Sie auf **Hinzufügen**.

## Dateibeschreibung

Verwenden Sie dieses Fenster, um ausführliche Informationen zu empfohlenen Maßnahmen und andere technische Informationen zur Nachverfolgung oder zu Warnungen für einen bestimmten Server anzuzeigen.

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

- Sie können nach bestimmten Meldungsbeschreibungen suchen.
- Sie können die Protokolldateien entweder in dem Fenster anzeigen oder die Datei zum Anzeigen zusätzlicher Protokollmeldungen herunterladen.
- Sie können Kommentare eines Benutzers zu einer Aktivität anzeigen.

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

**ANMERKUNG:** Eine lange Meldung wird auf 80 Zeichen gekürzt.

**ANMERKUNG:** Klicken Sie auf Message ID (Meldungs-ID), um weitere Informationen zu der Meldung anzuzeigen.

# Exportieren von Bestandsdaten

Sie können in OMIMSSC die Bestandsdaten ausgewählter Server oder einer Gruppe von Servern in eine XML- oder CSV-Datei exportieren. Sie können diese Informationen in einem freigegebenen Windows-Verzeichnis oder auf einem Managementsystem speichern.

## Voraussetzung

**ANMERKUNG:** Sie können die XML-Datei in DRM importieren und ein Repository auf Basis der Bestandsdatei erstellen sowie eine Referenzkonfiguration.

Legen Sie die Browsereinstellungen wie unter [Browsereinstellungen](#) angegeben fest.

## Info über diese Aufgabe

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

## Schritte

- 1 Klicken Sie in **OMIMSSC** auf **Maintenance Center** (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 exportierte Datei umfasst Einzelheiten wie Servergruppen, die Service-Tag-Nummer des Servers, den Hostnamen oder die IP-Adresse, das Gerätemodell, den Komponentennamen, die aktuelle Firmware-Version auf dieser Komponente, die Firmware-Version der Aktualisierungsquelle und Aktualisierungsaktionen auf dieser Komponente.

## Nächste Schritte

Gehen Sie nach dem Exportieren der XML-Datei wie folgt vor, um ein Repository in DRM zu erstellen:

- 1 Klicken Sie auf **My Repositories (Meine Repositories) > New (Neu) > Dell Modular Chassis inventory (Bestand modulares Dell Gehäuse)**.
- 2 Geben Sie einen Namen und die Beschreibung im Abschnitt **Base Repository** (Basis-Repository) ein und klicken Sie auf **Next** (Weiter).
- 3 Klicken Sie zum Auswählen der von der Appliance exportierten Bestandsdatei im Abschnitt **Modular Chassis Inventory** (Bestand modulares Gehäuse) auf **Browse** (Durchsuchen) und dann auf **Next** (Weiter).  
Weitere Informationen über das Erstellen eines Repositoriums finden Sie in den Dokumenten zu *Dell Repository Manager*, die unter [Dell.com/support/home](http://Dell.com/support/home) verfügbar sind.

# Anzeigen von Informationen in OMIMSSC

Sie können alle Informationen über die Aktivitäten, die in OMIMSSC initiiert wurden, zusammen mit dem Status des Fortschritts eines Jobs und dessen Unteraufgabe über die Seite **Jobs and logs center** (Jobs und Protokollcenter) anzeigen. Jobs auch für eine bestimmte Kategorie gefiltert und angezeigt werden. Sie können die Jobs im OMIMSSC-Admin-Portal und in der OMIMSSC-Konsolenerweiterung anzeigen.

- Admin portal (Admin-Portal) – Zeigt alle von OMIMSSC-Benutzern initiierten Jobs an.
- OMIMSSC console (OMIMSSC-Konsole) – Zeigt die Jobs für einen bestimmten Benutzer und eine bestimmte Konsole an.

Job-Namen werden von Benutzern bereitgestellt oder vom System erzeugt und die Unteraufgaben werden entsprechend der IP-Adresse oder des Hostnamens des verwalteten Servers benannt. Erweitern Sie die Unteraufgabe, um die Aktivitätsprotokolle für diesen Job anzuzeigen. Es gibt vier Job-Kategorien:

- Running (Ausführen) – Zeigt alle Jobs an, die gerade ausgeführt werden (bzw. deren Fortschritt).
- Verlauf - Zeigt alle Jobs, die in der Vergangenheit ausgeführt wurden, mit deren Job-Status an.
- Scheduled (Geplante) – Zeigt alle für ein zukünftiges Datum und eine zukünftige Uhrzeit geplanten Jobs an. Sie können geplante Jobs auch abbrechen.
- Generic Logs (Allgemeine Protokolle) – Zeigt für das OMIMSSC-Gerät spezifische, allgemeine Protokollmeldungen, die nicht spezifisch für eine Unteraufgabe sind, und andere Aktivitäten für jeden Benutzer unter Angabe des Benutzernamens und des Konsole-FQDN an.
  - Appliance Log Messages (Geräteprotokollmeldungen) – Zeigt alle für das OMIMSSC-Gerät spezifischen Protokollmeldungen an, wie Neustarten des OMIMSSC-Geräts. Sie können diese Kategorie von Meldungen nur über das Admin-Portal anzeigen.
  - Allgemeine Protokollmeldungen - Zeigt alle Protokollmeldungen an, die den Jobs gemeinsam sind, die in den Registerkarten **Ausführen**, **Verlauf** und **Geplant** aufgeführt sind. Diese Protokolle beziehen sich auf eine bestimmte Konsole und einen bestimmten Benutzer.  
Wenn beispielsweise ein Firmware-Aktualisierungsjob für eine Servergruppe ausgeführt wird, werden auf der Registerkarte die Protokollmeldungen angezeigt, die das Erstellen des SUU-Repository (Server Update Utility) für diesen Job betreffen.

Die verschiedenen Zustände der im OMIMSSC-Gerät definierten Jobs sind:

- Canceled (Abgebrochen) – Der Job wurde manuell vom Benutzer oder beim Neustart des OMIMSSC-Geräts abgebrochen.
- Successful (Erfolgreich) – Der Job wurde erfolgreich abgeschlossen.
- Failed (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 zur gleichen Zeit an denselben Server gesendet werden, schlagen die Jobs fehl. Planen Sie daher die Jobs für unterschiedliche Zeitpunkte.

- Warten - Der Job befindet sich in einer Warteschlange, um ausgeführt zu werden.
- Wiederkehrender Zeitplan - Der Job wiederholt sich nach einem festgelegten Zeitintervall.

Themen:

- [Anzeigen von Jobs](#)
- [Verwalten von Jobs](#)

# Anzeigen von Jobs

## Info über diese Aufgabe

Sie können alle in OMIMSSC erstellten Jobs inklusive ihrer Statusinformationen anzeigen.

## Schritte

- 1 Klicken Sie in OMIMSSC auf **Jobs and Log Center** (Job- und Protokollcenter).
- 2 Klicken Sie auf eine der Registerkarten, um Jobs der betreffenden Kategorie anzuzeigen, z. B. **Scheduled** (Geplant), **History** (Verlauf) oder **Generic** (Allgemein).

Erweitern Sie einen Job, um alle in dem Job inbegriffenen Server zu sehen. Erweitern Sie nochmals, um die zu dem Job gehörenden Protokollnachrichten zu sehen.

**ANMERKUNG:** Alle jobbezogenen allgemeinen Protokollmeldungen sind unter der Registerkarte **Allgemeine** und nicht unter der Registerkarte **Ausführen** oder **Verlauf** aufgeführt.

- 3 (Optional) Filtern Sie nach den unterschiedlichen Jobkategorien. Den Status eines Jobs können Sie in der Spalte **Status** sehen.

# Verwalten von Jobs

## Voraussetzung

Vergewissern Sie sich, dass der Status des Jobs **Scheduled** (Geplant) lautet.

## Schritte

- 1 Führen Sie in OMIMSSC einen der folgenden Schritte durch:
  - Klicken Sie im Navigationsbereich auf **Wartungcenter** 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 **Cancel** (Abbrechen) und anschließend auf **Yes** (Ja).

# Fehlerbehebung

## Themen:

- Bereitstellungsoption wird in Tasksequenz nicht angezeigt
- VRTX-Gehäusegruppen werden doppelt erstellt
- Leere Cluster-Aktualisierungsgruppe wird bei automatischer Ermittlung oder Synchronisierung nicht gelöscht
- Aktualisierungsquelle kann nicht erstellt werden
- Fehler bei der Firmware-Aktualisierung wegen belegter Job-Warteschlange
- Firmware-Aktualisierung auf Cluster-Aktualisierungsgruppe schlägt fehl
- Fehler bei der Firmware-Aktualisierung auf Servern der 11. Generation
- Fehler bei der Firmware-Aktualisierung während der Verwendung der DRM-Aktualisierungsquelle
- Fehler bei einem geplanten Job für eine Aktualisierungsgruppe
- Fehler bei der Anwendung einer Betriebsvorlage
- Fehler beim Zugriff auf CIFS-Freigabe unter Verwendung des Hostnamens
- Fehler bei der FTP-Verbindung bei Verwendung der Standard-Aktualisierungsquelle des Systems
- Fehler beim Erstellen eines Repositorys während einer Firmware-Aktualisierung
- Benutzerdefinierte Aktualisierungsgruppe kann nicht gelöscht werden
- Fehler beim Anzeigen von Jobs und Protokollen
- Fehler beim Exportieren von LC-Protokollen im CSV-Format
- Serverprofile werden nicht exportiert
- Fehler beim Anzeigen des Dell EMC Logos im Admin-Portal von OMIMSSC
- Fehler beim Anzeigen von LC-Protokollen
- Firmware-Aktualisierung auf einigen Komponenten, unabhängig von der Auswahl
- Fehler bei der Hypervisor-Bereitstellung
- Hypervisor-Bereitstellungsfehler aufgrund von weiterhin vorhandenen Treiberdateien in der Bibliotheksfreigabe
- Fehler bei der Hypervisor-Bereitstellung mit Active Directory für die 11. Generation von PowerEdge-Blade-Servern
- Falsche Anmeldeinformationen während der Ermittlung
- IG-Installationsproblem während der Ausführung mehrerer Instanzen des Installationsprogramms auf dem gleichen Server
- Zeitüberschreitung beim Importieren des Serverprofils nach zwei Stunden
- Aktuelle Bestandsaufnahmeinformationen werden auch nach erfolgter Firmware-Aktualisierung nicht angezeigt
- SCVMM-Fehler 21119 beim Hinzufügen von Servern zu Active Directory

## Bereitstellungsoption wird in Tasksequenz nicht angezeigt

Nachdem die **OMIMSSC**-Konsolenerweiterung für SCCM deinstalliert und wieder neu installiert wurde, wird in den vorhandenen Tasksequenzen die Option OMIMSSC (Bereitstellen) nicht mehr angezeigt.

Öffnen Sie zur Umgehung dieses Problems eine Tasksequenz zur Bearbeitung, reaktivieren Sie die Option **Apply** (Anwenden) und klicken Sie dann auf **OK**. Die Option **Deploy** (Bereitstellen) wird nun wieder 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 die Option **Restart in Windows PE** (Neustart in Windows PE) aus. Geben Sie im Abschnitt **Description** (Beschreibung) ein beliebiges Zeichen ein und löschen Sie es wieder, ohne die Änderungen zu speichern.
- 3 Klicken Sie auf **OK**.  
Hierdurch wird die Option **Anwenden** erneut aktiviert.

## VRTX-Gehäusegruppen werden doppelt erstellt

Wenn modulare Server, die zuvor in einem anderen Gehäuse untergebracht waren, zu einem VRTX-Gehäuse hinzugefügt und ermittelt werden, tragen die modularen Server die Service-Tag-Informationen des vorherigen Gehäuses, sodass eine doppelte VRTX-Gehäusegruppe auf dem Gerät erstellt wird.

Um den Fehler zu beheben, führen Sie die folgenden Schritte aus:

- 1 Entfernen Sie einen modularer Server aus einem Gehäuse und fügen Sie ihn einem anderen Gehäuse hinzu. Weitere Informationen finden Sie im Abschnitt „Servermodule“ im *Dell PowerEdge VRTX Enclosure Owner's Manual* (Benutzerhandbuch zu Dell PowerEdge VRTX-Gehäusen).
- 2 Konfigurieren Sie CMC. Weitere Informationen finden Sie im Abschnitt zur Installation und Einrichtung von CMC *Chassis Management Controller Version 2.1 for Dell PowerEdge VRTX User's Guide* (Benutzerhandbuch für Chassis Management Controller Version 2.1 für Dell PowerEdge VRTX), das unter [dell.com/support/home](http://dell.com/support/home) verfügbar ist.

Falls nach der Durchführung der obigen Schritte weiterhin doppelte Einträge für Gehäusegruppen vorhanden sind, gehen Sie folgendermaßen vor, um das Problem zu umgehen:

- 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.

## Leere Cluster-Aktualisierungsgruppe wird bei automatischer Ermittlung oder Synchronisierung nicht gelöscht

Wird in der Appliance eine Clustergruppe erkannt, wird unter **Maintenance Center** (Wartungscenter) eine Cluster-Aktualisierungsgruppe mit allen in der Clustergruppe aufgeführten Servern erstellt. Falls über SCVMM alle Server aus diesem Cluster entfernt werden, wird bei einer nachfolgenden automatischen Ermittlung oder Synchronisierung mit SCVMM die leere Cluster-Aktualisierungsgruppe nicht aus dem **Wartungscenter** gelöscht.

Um dieses Problem zu umgehen, löschen Sie die leere Servergruppe, und ermitteln Sie die Server erneut.

## Aktualisierungsquelle kann nicht erstellt werden

Wenn die DNS (Domain Name System)-Netzwerkconfiguration der Appliance geändert wird, schlägt die Erstellung einer HTTP- oder FTP-Aktualisierungsquelle fehl.

Um dieses Problem zu umgehen, müssen Sie die Appliance zunächst neu starten und dann die HTTP- oder FTP-Aktualisierungsquelle erstellen.

## Fehler bei der Firmware-Aktualisierung wegen belegter Job-Warteschlange

Über die Appliance an den iDRAC gesendete Jobs zur Firmware-Aktualisierung schlagen fehl und im Hauptprotokoll der Appliance wird folgender Fehler erfasst: `JobQueue Exceeds the size limit. Delete unwanted JobID(s).`

Löschen Sie zur Umgehung dieses Problems alle abgeschlossenen Jobs aus dem iDRAC und versuchen Sie erneut, den Job zur Firmware-Aktualisierung durchzuführen. Wie Sie Jobs aus dem iDRAC löschen können, können Sie in der iDRAC-Dokumentation unter [dell.com/support/home](https://dell.com/support/home) nachlesen.

## Firmware-Aktualisierung auf Cluster-Aktualisierungsgruppe schlägt fehl

Wenn Sie einen Job zur Aktualisierung der Firmware in einer Cluster-Aktualisierungsgruppe geplant haben und dieser aus verschiedenen Gründen fehlschlägt, etwa, weil das IG nicht erreichbar ist, reagiert die Cluster-Gruppe nicht mehr. Es kann auch vorkommen, dass der Job in CAU aufgrund eines bereits laufenden Jobs abgebrochen wird, und die DUPs in die zur Cluster-Gruppe gehörenden Server-Cluster-Knoten heruntergeladen und dort abgelegt werden. Alle DUP-Dateien werden in einem Ordner mit der Bezeichnung „Dell Verbrauchsspeicher“ abgelegt.

Um dieses Problem zu umgehen, löschen Sie alle Dateien im Dell Ordner, und planen Sie anschließend einen Firmware-Aktualisierungs-Job.

## Fehler bei der Firmware-Aktualisierung auf Servern der 11. Generation

Ein Firmware-Aktualisierungs-Job, der auf PowerEdge-Servern der 11. Generation gestartet wurde, kann aufgrund von inkompatiblen Versionen von iDRAC und LC mit der folgenden Fehlermeldung fehlschlagen: `WSMan command failed to execute on server with iDRAC IP <IP address>`.

Um dieses Problem zu umgehen, aktualisieren Sie den iDRAC und LC auf die neuesten Versionen und starten Sie dann den Firmware-Aktualisierungsjob.

## Fehler bei der Firmware-Aktualisierung während der Verwendung der DRM-Aktualisierungsquelle

Der Firmware-Aktualisierungsjob kann fehlschlagen, wenn Sie die DRM-Aktualisierungsquelle mit unzureichendem Zugriff auf die freigegebenen Ordner verwenden. Falls das bereitgestellte Windows Anmeldeprofil während des Erstellens der DRM-Aktualisierungsquelle kein Teil der Administratorgruppe der Domäne 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 Objektberechtigungsbeiträge durch vererbte Berechtigungsbeiträge aus diesem Objekt ersetzen** und geben Sie dann den Ordner mit Lese- und Schreibzugriff für **Jeden** frei.

## Fehler bei einem geplanten Job für eine Aktualisierungsgruppe

Wenn Sie nach dem Planen eines Jobs auf einer Aktualisierungsgruppe alle Server aus der Aktualisierungsgruppe verschieben, sodass kein Server mehr in der Gruppe vorhanden ist, schlägt der geplante Job fehl.

Um das Problem zu umgehen, brechen Sie den geplanten Job ab, fügen Sie die Server einer anderen Aktualisierungsgruppe hinzu, und planen Sie anschließend einen Job für diese andere Aktualisierungsgruppe.

## Fehler bei der Anwendung einer Betriebsvorlage

Nach dem Senden des Betriebsvorlagen-Jobs über **Deploy** (Bereitstellen) an die ausgewählten Server sind die Attribute oder Attributwerte für die ausgewählte CSV-Datei nicht geeignet oder die iDRAC-IP oder iDRAC-Anmeldeinformationen wurden durch die Vorlage geändert, aber der Job in iDRAC ist erfolgreich. Der Status des Jobs wird jedoch in OMIMSSC aufgrund der ungültigen CSV-Datei als nicht erfolgreich/fehlgeschlagen dargestellt oder der Job kann wegen der iDRAC Änderungen auf dem Zielsystem nicht nachverfolgt werden.

Um dieses Problem zu umgehen, stellen Sie sicher, dass die ausgewählte CSV-Datei über die richtigen Attribute und Attributwerte verfügt und die iDRAC-IP oder die Anmeldeinformationen durch die Vorlage nicht geändert werden.

## Fehler beim Zugriff auf CIFS-Freigabe unter Verwendung des Hostnamens

Die modularen Server sind womöglich nicht in der Lage, mithilfe des Hostnamens auf die CIFS-Freigabe zuzugreifen, um Jobs in OMIMSSC auszuführen.

Geben Sie als Umgehungslösung die IP-Adresse des Servers an, auf dem sich die CIFS-Freigabe befindet.

## Fehler bei der FTP-Verbindung bei Verwendung der Standard-Aktualisierungsquelle des Systems

Nach der Einrichtung und Konfiguration oder Aktualisierung des Geräts kann der Zugriff auf die FTP-Site unter Verwendung der systemseitig erstellten Aktualisierungsquelle **Dell Online Catalog** (Dell Online-Katalog) fehlschlagen, wenn Proxy-Anmeldeinformationen erforderlich sind.

Für den Zugriff auf die FTP-Site unter Verwendung von **Dell Online-Katalog** als Aktualisierungsquelle, bearbeiten Sie die Proxy-Anmeldeinformationen, und fügen Sie sie hinzu.

## Fehler beim Erstellen eines Repositorys während einer Firmware-Aktualisierung

Die Erstellung eines Repositorys während einer Firmware-Aktualisierung kann unter anderem aufgrund von Netzwerkproblemen, falschen Anmeldeinformationen oder der Nichterreichbarkeit des Servers fehlschlagen.

Um dieses Problem zu umgehen, stellen Sie sicher, dass der FTP-Server für das System, auf dem die Appliance gehostet wird, erreichbar ist, dass keine Netzwerkprobleme vorliegen und dass die richtigen Anmeldeinformationen bei der Firmware-Aktualisierung eingegeben werden.

## Benutzerdefinierte Aktualisierungsgruppe kann nicht gelöscht werden

Wenn Sie einen Job auf einem Server geplant haben, der einer benutzerdefinierten Aktualisierungsgruppe angehört, diesen Server aus SCVMM löschen und eine Synchronisierung durchführen, wird der Server aus der benutzerdefinierten Aktualisierungsgruppe entfernt und in die entsprechende vordefinierte Gruppe verschoben. Sie können benutzerdefinierte Aktualisierungsgruppen nicht löschen, solange sie mit einem geplanten Job verknüpft sind.

Um dieses Problem zu umgehen, löschen Sie zuerst den geplanten Job auf der Jobseite und dann die benutzerdefinierte Aktualisierungsgruppe.

## Fehler beim Anzeigen von Jobs und Protokollen

Das **Jobs and Logs Center** (Jobs und Protokollcenter) wird in den OMIMSSC-Konsolenerweiterungen nicht angezeigt.

Um dieses Problem zu umgehen, registrieren Sie die Konsole erneut.

## Fehler beim Exportieren von LC-Protokollen im CSV-Format

Wenn Sie beim Anzeigen von LC-Protokollen versuchen, die Protokolldateien in das CSV-Format herunterzuladen, schlägt der Download-Vorgang fehl.

Um dieses Problem zu umgehen, fügen Sie den Geräte-FQDN im Browser der lokalen Intranet-Site hinzu. Weitere Informationen über das Hinzufügen des Geräts zum lokalen Intranet finden Sie unter [Anzeigen von LC-Protokollen](#).

## Serverprofile werden nicht exportiert

Nachdem Sie einen Job zum Exportieren eines Serverprofils geplant haben, wird das Serverprofil nicht exportiert und die Fehlermeldung „Die Selektoren für Ressource sind ungültig“ angezeigt.

Um dieses Problem zu umgehen, setzen Sie den iDRAC zurück, und planen Sie anschließend einen Job zum Exportieren eines Serverprofils. Weitere Informationen finden Sie in der iDRAC-Dokumentation unter [dell.com/support](http://dell.com/support).

## Fehler beim Anzeigen des Dell EMC Logos im Admin-Portal von OMIMSSC

Ist unter Windows 2016 Internet Explorer als Standardbrowser festgelegt, wird beim Start des Admin-Portals von OMIMSSC das Dell EMC Logo nicht angezeigt.

Um dieses Problem zu umgehen, gehen Sie wie folgt vor:

- Aktualisieren Sie Internet Explorer auf die neueste Version.
- Löschen Sie den Browserverlauf und fügen Sie dann die URL des Admin-Portals den Favoriten des Browsers hinzu.

## Fehler beim Anzeigen von LC-Protokollen

Wenn Sie nach dem Erfassen der LC-Protokolle die LC-Protokolldatei für einen Server anzeigen, wird die 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 und zeigen Sie anschließend die LC-Protokolle an. Weitere Informationen finden Sie in der iDRAC-Dokumentation unter [dell.com/support](http://dell.com/support).

## Firmware-Aktualisierung auf einigen Komponenten, unabhängig von der Auswahl

Gleiche Komponenten auf identischen Servern werden während einer Firmware-Aktualisierung unabhängig von der Auswahl der Komponenten auf einzelnen Servern aktualisiert. Dieses Verhalten tritt bei der 12. und 13. Generation der PowerEdge-Server mit einer Enterprise-Lizenz von iDRAC auf.

Um dieses Problem zu umgehen, gehen Sie wie folgt vor:

- Um nicht relevante Aktualisierungen auf identischen Servern zu vermeiden, wenden Sie zuerst die gemeinsamen Komponenten auf identischen Servern an und dann separat die spezifischen Komponenten für die einzelnen Server.
- Führen Sie stufenweise Aktualisierungen mit geplanten Ausfallzeiten durch, um die erforderliche Firmware-Aktualisierung umzusetzen.

## Fehler bei der Hypervisor-Bereitstellung

Die Hypervisor-Bereitstellung schlägt fehl, und das Aktivitätsprotokoll zeigt die folgende Fehlermeldung 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.

- Die Einstellungen für Virenschutz oder Firewall verhindern möglicherweise die erfolgreiche Ausführung des **WINRM**-Befehls.

Informationen zur Umgehung des Problems finden Sie im folgenden KB-Artikel: [support.microsoft.com/kb/961804](https://support.microsoft.com/kb/961804).

## Hypervisor-Bereitstellungsfehler aufgrund von weiterhin vorhandenen Treiberdateien in der Bibliotheks freigabe

Die Hypervisor-Bereitstellung schlägt fehl, und das Aktivitätsprotokoll zeigt den folgenden Fehler an:

### Info über diese Aufgabe

- **Error:** `Error while applying Hypervisor Profile to host <IP Address>. Failed with error : For input string: ""`
- **Information:** `Successfully deleted drivers from library share sttig.tejasqa.com for <server uuid>`
- **Error:** `Deleting staging share (drivers) for <server uuid> failed.`

Dieser Fehler kann aufgrund der vom VMM-Cmdlet `GET-SCJOB` status ausgegebenen Ausnahme auftreten und Treiberdateien bleiben in der Bibliotheks freigabe erhalten. Bevor Sie versuchen, den Vorgang zu wiederholen oder einen anderen Hypervisor bereitzustellen, müssen Sie diese Dateien aus der Bibliotheks freigabe entfernen.

So entfernen Sie Dateien aus der Bibliotheks freigabe:

### Schritte

- 1 Wählen Sie in der SCVMM-Konsole die Option **Bibliothek > Bibliotheksserver** und dann den IG-Server aus, der als Bibliotheksserver hinzugefügt wurde.
- 2 Wählen Sie im Bibliotheksserver die Bibliotheks freigabe aus, und löschen Sie sie.
- 3 Nachdem die Bibliotheks freigabe gelöscht wurde, verbinden Sie die IG-Freigabe über `\\<Integration Gateway server>\LCDriver\`.
- 4 Löschen Sie den Ordner mit den Treiberdateien.

Nun können Sie Betriebssysteme bereitstellen.

# Fehler bei der Hypervisor-Bereitstellung mit Active Directory für die 11. Generation von PowerEdge-Blade-Servern

Die Hypervisor-Bereitstellung schlägt bei Verwendung der Active Directory-Benutzeranmeldeinformationen auf der 11. Generation von PowerEdge-Blade-Servern fehl. Die 11. Generation von PowerEdge-Blade-Servern verwenden das IPMI-Protokoll (Intelligent Platform Management Interface) für die Kommunikation. Der IPMI-Standard wird jedoch nicht für die Verwendung von Anmeldeinformationen aus dem Active Directory-Setup unterstützt.

## Info über diese Aufgabe

Um dieses Problem zu umgehen und Betriebssysteme auf diesen Servern bereitzustellen, verwenden Sie unterstützte Anmeldeprofile.

## Schritt

# Falsche Anmeldeinformationen während der Ermittlung

- Falls während der Ermittlung falsche Anmeldeinformationen verwendet werden, stehen je nach iDRAC-Version unterschiedliche Lösungsoptionen zur Verfügung:
  - Wenn während der Ermittlung von PowerEdge-Servern der 12. Generation mit iDRAC ab Version 2.10.10.10 falsche Informationen im Anmeldeprofil hinterlegt sind, 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 Anmeldeprofildetails erneut versuchen, sobald die IP-Adresse entsperrt ist.
  - Wenn Sie PowerEdge-Server der 11. oder 12. Generation mit einer iDRAC-Version vor 2.10.10.10 ermitteln möchten und dies aufgrund der Eingabe falscher Anmeldeprofildetails fehlschlägt, wiederholen Sie die Serverermittlung mit den richtigen Anmeldeprofildetails.
  - In früheren iDRAC-Versionen als Version 2.10.10.10 können IP-Adressen blockiert werden. Weitere Informationen finden Sie in der iDRAC-Dokumentation unter **Dell.com/idracmanuals**. Je nach Bedarf können Sie die Blockierung von IP-Adressen auch deaktivieren. Außerdem können Sie überprüfen, ob die Funktion **iDRAC.IPBlocking.BlockEnable** in iDRAC aktiviert ist.
  - Wird das standardmäßige iDRAC-Anmeldeprofil geändert, nachdem ein Server ermittelt und der Appliance hinzugefügt wurde, lassen sich auf diesem Server keine Aktivitäten ausführen. Sie können erst mit dem Server arbeiten, nachdem Sie eine erneute Ermittlung mit dem neuen Anmeldeprofil durchgeführt haben.

# IG-Installationsproblem während der Ausführung mehrerer Instanzen des Installationsprogramms auf dem gleichen Server

Wenn Sie bereits mit der Installation des IG begonnen haben und versuchen, eine weitere Instanz des IG auszuführen, wird eine Fehlermeldung angezeigt. Nachdem Sie auf OK geklickt haben, werden Sie aufgefordert, eine weitere IG-MSI-Datei zu speichern.

Alternativ können Sie auch die Datei nicht speichern und mit der ersten Installation fortfahren.

# Zeitüberschreitung beim Importieren des Serverprofils nach zwei Stunden

Wenn Sie über die Appliance einen Job zum Import eines Serverprofils senden, wird nach zwei Stunden möglicherweise eine Zeitüberschreitung gemeldet.

Führen Sie die folgenden Schritte aus, um das Problem zu umgehen:

- 1 Drücken Sie F2, um die **BIOS-Einstellungen** aufzurufen.
- 2 Klicken Sie auf **System Setup** System-Setup, und wählen Sie **Miscellaneous Settings** (Verschiedene Einstellungen) aus.
- 3 Deaktivieren Sie **F1/F2 Prompt on Error** (Bei Fehler F1/F2-Eingabeaufforderung).

Nachdem Sie die folgenden Schritte ausgeführt haben, planen Sie den Job für das Importieren eines Serverprofils, und verwenden Sie ihn, um den Import erfolgreich durchzuführen.

## Aktuelle Bestandsaufnahmeinformationen werden auch nach erfolgter Firmware-Aktualisierung nicht angezeigt

Obwohl der Firmware-Aktualisierungs-Job auf einem PowerEdge-Server der 11. Generation abgeschlossen wurde, wird in der Bestandsaufnahme des Geräts nicht die neueste Firmware-Version angezeigt.

Auf dem Gerät ist das Aktualisieren der Bestandsaufnahme eine Aktivität, die sofort nach dem Abschluss eines Firmware-Aktualisierungs-Jobs ausgeführt wird. Die Firmware-Aktualisierung ist noch vor dem Abschluss der CSIOR-Aktivität des PowerEdge-Servers abgeschlossen, aufgrund dessen werden die älteren Firmware-Bestandsaufnahmeinformationen angezeigt.

Um dieses Problem zu umgehen, überprüfen Sie, ob die CSIOR-Aktivität auf dem PowerEdge Server abgeschlossen ist und aktualisieren Sie dann die Firmware-Bestandsaufnahme auf dem Gerät. Achten Sie außerdem darauf, den Server nach der Anwendung der agentenfreien stufenweisen Aktualisierung erneut zu starten. Weitere Informationen zum Aktualisieren der Bestandsaufnahme finden Sie unter [Anzeigen und Aktualisieren der Firmware-Bestandsaufnahme](#).

Weitere Informationen zu CSIOR finden Sie im Abschnitt „Fehlerbehebung“ in der aktuellen Version des *Dell Lifecycle Controller GUI User's Guide* (Benutzerhandbuch für die GUI von Dell Lifecycle Controller) unter [dell.com/support/home](http://dell.com/support/home).

## 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>.`

### Info über diese Aufgabe

Um dieses Problem zu umgehen, gehen Sie wie folgt vor:

#### Schritte

- 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 der OMIMSSC-Konsolenerweiterung für SCVMM durch.

Der Server wird auf der Registerkarte **Host** aufgelistet.

# Anhang

# Zugriff auf Dokumente von der Dell EMC Support-Website

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

- Für Dell EMC Enterprise System-Verwaltungsdokumente – [Dell.com/SoftwareSecurityManuals](https://www.dell.com/support/manuals)
- Für Dell EMC OpenManage-Dokumente – [Dell.com/OpenManageManuals](https://www.dell.com/support/manuals)
- Für Dell EMC Remote-Enterprise-System-Verwaltungsdokumente – [Dell.com/esmanuals](https://www.dell.com/support/manuals)
- Für Dokumente zu iDRAC und Dell EMC Lifecycle Controller – [Dell.com/idracmanuals](https://www.dell.com/support/manuals)
- Für Dell EMC OpenManage Connections Enterprise-System-Verwaltungsdokumente – [Dell.com/OMConnectionsEnterpriseSystemsManagement](https://www.dell.com/support/manuals)
- Für Dell EMC Betriebsfähigkeits-Tools-Dokumente – [Dell.com/ServiceabilityTools](https://www.dell.com/support/manuals)
- Für Client Command Suite-System-Verwaltungsdokumente – [Dell.com/DellClientCommandSuiteManuals](https://www.dell.com/support/manuals)
- a Rufen Sie die Website [Dell.com/Support/Home](https://www.dell.com/support/home) auf.
- b Klicken Sie auf **Wählen Sie aus allen Produkten**.
- c Klicken Sie im Abschnitt **Alle Produkte** auf **Software und Sicherheit**, und klicken Sie dann auf einen der folgenden Links:
  - **Verwaltung von Systemen der Enterprise-Klasse**
  - **Remote-Verwaltung von Systemen der Enterprise-Klasse**
  - **Wartungstools**
  - **Dell Client Command Suite**
  - **Connections Client-Systemverwaltung**
- d Um ein Dokument anzuzeigen, klicken Sie auf die jeweilige Produktversion.
- Verwendung von Suchmaschinen:
  - Geben Sie den Namen und die Version des Dokuments in das Kästchen „Suchen“ ein.

## Kontaktaufnahme mit Dell

### Voraussetzung

- ANMERKUNG:** Wenn Sie nicht über eine aktive Internetverbindung verfügen, können Sie Kontaktinformationen auch auf Ihrer Auftragsbestätigung, dem Lieferschein, der Rechnung oder im Dell-Produktkatalog finden.

### Info über diese Aufgabe

Dell stellt verschiedene onlinebasierte und telefonische Support- und Serviceoptionen bereit. Da die Verfügbarkeit dieser Optionen je nach Land und Produkt variiert, stehen einige Services in Ihrer Region möglicherweise nicht zur Verfügung. So erreichen Sie den Vertrieb, den Technischen Support und den Kundendienst von Dell:

### Schritte

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