




Dell Lifecycle Controller Integration Version 1.3 for Microsoft System Center Virtual Machine Manager 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.

© 2014 - 2016 Dell Inc. Alle Rechte vorbehalten. Dieses Produkt ist durch US-amerikanische und internationale Urheberrechtsgesetze und nach sonstigen Rechten an geistigem Eigentum geschützt. Dell und das Dell Logo sind Marken von Dell Inc. in den Vereinigten Staaten und/oder anderen Geltungsbereichen. Alle anderen in diesem Dokument genannten Marken und Handelsbezeichnungen sind möglicherweise Marken der entsprechenden Unternehmen.

2016 - 10

Rev. A00

Inhaltsverzeichnis

1 Info zu Dell Lifecycle Controller Integration for Microsoft System Center Virtual Machine Manager.....	7
Was ist neu in dieser Version?.....	7
Vorhandene Funktionen.....	7
2 Installieren und Einrichten des DLCI-Konsolen-Add-In	10
Installieren des DLCI-Konsolen-Add-In.....	10
Entfernen oder Reparieren des DLCI-Konsolen-Add-In.....	10
Importieren des DLCI-Konsolen-Add-In in VMM.....	11
Anzeigen des DLCI-Konsolen-Add-In.....	11
3 Erste Schritte.....	12
Anmelden am DLCI-Verwaltungsportal für SCVMM	12
DLCI-Verwaltungsportal für SCVMM.....	12
Anmelden am DLCI-Konsolen-Add-In für SCVMM.....	13
DLCI-Konsolen-Add-In für SCVMM	13
4 Arbeitsabläufe.....	15
Info über Gold-Konfigurationen.....	15
Erstellen von Gold-Konfigurationen.....	15
Erstellen, Verwalten und Löschen von Anmeldeprofilen.....	15
Erstellen, Verwalten und Löschen von Aktualisierungsquellen.....	16
Erstellen, Verwalten und Löschen von benutzerdefinierten Aktualisierungsgruppen.....	16
Anwenden von Aktualisierungen auf Server.....	16
Erstellen, Verwalten und Löschen von Schutz-Vaults.....	16
Exportieren von Serverprofilen.....	17
Importieren von Serverprofilen.....	17
Hypervisor-Bereitstellung.....	17
Löschen von Servern.....	17
Konfigurieren von ersetzten Komponenten.....	17
Erfassen und Anzeigen von LC-Protokollen.....	18
5 Einrichten der Umgebung für die Hypervisor-Bereitstellung.....	19
6 Serverermittlung.....	20
Systemanforderungen für verwaltete Systeme	21
Aktivieren von CSIOR auf verwalteten Systemen.....	21
Ermitteln von Servern über die automatische Ermittlung.....	21
Ermitteln von Servern über die manuelle Ermittlung.....	22
Löschen von Servern aus der DLCI-Konsole.....	22
Anzeigen der Gerätebestandsaufnahme.....	22
Synchronisierung mit SCVMM.....	23



Synchronisieren des Geräts mit SCVMM.....	24
Beheben von Synchronisierungsfehlern.....	24
Starten der iDRAC-Konsole.....	24

7 Lizenz für das Gerät 25

8 Server-Verwaltung..... 26

Integration in DRM.....	27
Filter.....	27
Aktualisierungsquellen – Übersicht.....	27
Vordefinierte Aktualisierungsquellen und Standard-Aktualisierungsquellen.....	28
Verbindung testen.....	28
Einrichten von lokalem FTP.....	28
Einrichten von lokalem HTTP.....	29
Anzeigen der Aktualisierungsquelle.....	29
Erstellen einer Aktualisierungsquelle.....	29
Ändern einer Aktualisierungsquelle.....	29
Löschen der Aktualisierungsquelle.....	30
Aktualisierungsgruppen.....	30
Vordefinierte Aktualisierungsgruppen.....	30
Benutzerdefinierte Aktualisierungsgruppen.....	31
Aktualisierungsmethoden.....	31
Anmerkungen zu Aktualisierungsgruppen.....	31
Anzeigen von Aktualisierungsgruppen.....	32
Erstellen von benutzerdefinierten Aktualisierungsgruppen.....	32
Ändern von benutzerdefinierten Aktualisierungsgruppen.....	32
Löschen von benutzerdefinierten Aktualisierungsgruppen.....	32
Anwenden von Aktualisierungen auf Server.....	33
Abfrage und Benachrichtigung.....	34
Einstellen von Benachrichtigungen.....	34
Schutz-Vaults.....	34
Erstellen eines Schutz-Vaults.....	34
Modifizieren eines Schutz-Vaults.....	35
Löschen eines Schutz-Vaults.....	35
Teilersetzung.....	35
Anwenden von Firmware- und Konfigurationseinstellungen.....	36
Erfassung von Lifecycle Controller-Protokollen.....	36
Erfassen von LC-Protokollen.....	36
Anzeigen von LC-Protokollen.....	37
Exportieren der Bestandsaufnahme.....	37
Anzeigen und Aktualisieren der Firmware-Bestandsaufnahme.....	38
Exportieren von Serverprofilen.....	39
Erstellen eines Export-Jobs.....	39
Abbrechen eines Jobs für den Export der Serverkonfiguration.....	40
Importieren von Serverprofilen.....	40
Importieren von Serverprofilen.....	40



Verwalten von Jobs.....	41
Abbrechen eines Jobs für die Firmware-Aktualisierung.....	41
9 Profile und Vorlagen.....	42
Info zu Anmeldeprofilen.....	42
Vordefinierte Anmeldeprofile.....	42
Erstellen eines Anmeldeprofils.....	42
Ändern eines Anmeldeprofils.....	43
Löschen eines Anmeldeprofils.....	43
Erstellen eines Hardwareprofils.....	43
Ändern eines Hardwarekonfigurationsprofils.....	44
Löschen eines Hardwareprofils.....	44
Erstellen eines Hypervisor-Profiles.....	45
Ändern eines Hypervisor-Profiles.....	45
Löschen eines Hypervisor-Profiles.....	45
Ergänzende Informationen zu WinPE.....	46
Info zur Hypervisor-Bereitstellung.....	46
Erstellen von Bereitstellungsvorlagen.....	47
Ändern einer Bereitstellungsvorlage.....	47
Löschen einer Bereitstellungsvorlage.....	47
10 Bereitstellen von Hypervisoren.....	48
11 Anzeigen von Informationen auf dem Gerät.....	49
Jobs und Protokollcenter.....	49
Anzeigen verwalteter Jobs.....	50
Abbrechen geplanter Jobs.....	50
12 Fehlerbehebung.....	51
Leere Cluster-Aktualisierungsgruppe wird bei automatischer Ermittlung oder Synchronisierung nicht gelöscht.....	51
Ermittlungs-Jobs werden nicht gesendet	51
VRTX-Gehäusegruppen werden doppelt erstellt	51
Exportieren des Konfigurationsprofils eines anderen Servers nach Änderung der IP-Adresse.....	51
Fehler beim Anwenden der RAID-Konfiguration.....	52
Aktualisierungsquelle kann nicht erstellt werden.....	52
Fehler bei der Firmware-Aktualisierung wegen belegter Job-Warteschlange.....	52
Fehler bei der Firmware-Aktualisierung während der Verwendung der DRM-Aktualisierungsquelle	52
Geplanter Job auf einer Aktualisierungsgruppe schlägt fehl.....	52
Firmware-Aktualisierung auf Cluster-Aktualisierungsgruppe schlägt fehl.....	53
Fehler bei der Firmware-Aktualisierung auf Servern der 11. Generation.....	53
Fehler bei der FTP-Verbindung bei Verwendung der Standard-Aktualisierungsquelle des Systems.....	53
Fehler beim Erstellen eines Repositories während einer Firmware-Aktualisierung.....	53
Benutzerdefinierte Aktualisierungsgruppe kann nicht gelöscht werden.....	53
Fehler beim Exportieren von LC-Protokollen im CSV-Format.....	54
Fehler beim Anzeigen von LC-Protokollen	54
Serverprofile werden nicht exportiert	54



Firmware-Aktualisierung auf einigen Komponenten, unabhängig von der Auswahl.....	54
IG-Installationsproblem während der Ausführung mehrerer Instanzen des Installationsprogramms auf dem gleichen Server	54
Zeitüberschreitung beim Importieren des Serverprofils nach zwei Stunden.....	54
Fehler bei der Hypervisor-Bereitstellung.....	55
Hypervisor-Bereitstellungsfehler aufgrund von weiterhin vorhandenen Treiberdateien in der Bibliotheks freigabe.....	55
Aktuelle Bestandsaufnahmeinformationen werden auch nach erfolgter Firmware-Aktualisierung nicht angezeigt.....	56
SCVMM-Fehler 21119 beim Hinzufügen von Servern zu Active Directory.....	56
Hypervisor-Bereitstellung schlägt bei Verwendung von Active Directory für die 11. Generation von PowerEdge-Blade-Servern fehl.....	56
RAID-Konfigurationsfehler für virtuelle Festplatten mit RAID 10.....	56
Fehler bei der Konfiguration von RAID aufgrund der Konfiguration von Hotspares auf Software-RAID S130.....	57

13 Zugriff auf Dokumente der Dell Support-Website..... 58



Info zu Dell Lifecycle Controller Integration for Microsoft System Center Virtual Machine Manager

Dell Lifecycle Controller Integration (DLCI) for Microsoft System Center Virtual Machine Manager (SCVMM) ermöglicht die Hardwarekonfiguration und vereinfacht und verbessert Firmware-Aktualisierungen und Hypervisor-Bereitstellungen auf Dell Servern. Dieses Plugin verwendet die Remote-Bereitstellungsfunktion des Integrierter Dell Remote Access Controller (iDRAC), wobei Lifecycle Controller eine nahtlose Benutzererfahrung bietet. Sie können Dell Wertergänzungen über Microsoft System Center-Konsolen zum Verwalten virtualisierter Umgebungen verwenden.

Informationen zu Microsoft System Center Virtual Machine Manager finden Sie in der Microsoft-Dokumentation.

Was ist neu in dieser Version?

Folgende Funktionen sind für diese Version verfügbar:

- Bestandsaufnahme-Export im CSV-Format - Nach dem Vergleich der Server-Bestandsaufnahmen mit der Aktualisierungsquelle können Sie den Vergleichsreport in die **CSV**-Datei exportieren.
- Teilersetzung - Wiederherstellung der Firmware-Version oder Konfiguration oder beides auf der neuen Serverkomponente.
- Erfassen und Anzeigen von LC-Protokollmeldungen - Exportieren, Anzeigen, Herunterladen in CSV und Suchen der LC-Protokollmeldungen.
- Jobs und Aktivitätsprotokolle - Verbesserte Darstellung von Jobs und Aktivitätsprotokollen für eine bessere Benutzererfahrung.
- Bereitstellen von Windows Server 2016 - Unterstützung für die Bereitstellung von Windows Server 2016.
- 64-Bit Dell Update Packages (DUPs) - Unterstützung für die Aktualisierung der Firmware-Version mit 64-Bit-DUPs.
- Unterstützung für System Center 2016 Virtual Machine Manager (SC2016 VMM) - Sie können DLCI for SCVMM auf SC2016 VMM installieren.

Vorhandene Funktionen

Mit DLCI for SCVMM können Sie weiterhin Folgendes ausführen:

- Aktualisierungsquellen – Erstellen Sie ein Repository unter Verwendung von DRM oder durch Verbindung mit einer FTP-Site.
 - Integration in DRM – Exportieren Sie die Bestandsaufnahmedaten des Systems von DLCI for SCVMM nach DRM, und verwenden Sie DRM zur Vorbereitung eines Repositories.
 - FTP – Stellen Sie eine Verbindung zu Dell FTP her (lokal oder online), und rufen Sie die neuesten Dell Online-Kataloge ab.
 - HTTP – Unterstützung für Aktualisierungsquellen vom Typ HTTP (Hypertext Transfer Protocol).
- Verbindung testen – Ermöglicht das Validieren des Speicherorts der Aktualisierungsquelle und der Anmeldeinformationen, bevor die Aktualisierungsquelle erstellt wird.
- Aktualisierungsgruppen – Ermöglicht das Zusammenfassen von Servern zum Erstellen, Verwalten und Durchführen von Firmware-Aktualisierungen auf benutzerdefinierten Aktualisierungsgruppen.
- Abfrage und Benachrichtigungen – Ermöglicht das Konfigurieren von Benachrichtigungen, wenn neue Kataloge an der Aktualisierungsquelle verfügbar sind.
- Schutz-Vaults – Speicherorte zum Ablegen der Systemkonfigurationsprofile.
- Serverprofile exportieren – Ermöglicht den Export von Serverprofilen an einen internen oder externen Speicherort, einschließlich der Firmware-Images auf Komponenten, wie z. B. Basic Input Output System (BIOS), Redundant Array of Independent Disks (RAID), Netzwerkschnittstellen-Controller (NIC), integrated Dell Remote Access Controller (iDRAC), LC usw.
- Serverprofile importieren – Ermöglicht den Import von Serverprofilen, wenn das vorhandene Serverprofil beschädigt ist, wahlweise mit oder ohne die derzeitigen RAID-Einstellungen für den Server oder die Servergruppen.



- Filter – Filter dienen der Anzeige bestimmter Informationen basierend auf den im **Wartungscenter** ausgewählten Kriterien.
- Zurückstufen zulassen – Wenn diese Option aktiviert ist, können Sie die Firmware auf eine frühere Version zurückstufen.
- Clusterfähiges Aktualisieren (CAU) – Automatisiert den Software-Aktualisierungsvorgang durch Verwendung der Microsoft-Funktionen auf Cluster-Aktualisierungsgruppen unter Aufrechterhaltung der Serververfügbarkeit.
- Integration in Dell Repository Manager (DRM) – Bereitstellung der Bestandsaufnahmeinformationen vorhandener Server vom Gerät an den DRM.
- Automatische Ermittlung nicht zugewiesener Dell Server – Verbinden Sie die werksseitig von Dell bereitgestellten Server mit dem Netzwerk, schalten Sie die Server ein, und geben Sie die Details zum bereitstellenden Server für das DLCI-Gerät ein, um die Server automatisch zu ermitteln.

Durch die Appliance ermittelte Server werden als nicht zugewiesene Server bezeichnet, und diese Server stehen für die Bereitstellung des Hypervisor zur Verfügung.

- Manuelle Erkennung nicht zugewiesener Dell-Server – Erkennen der 11., 12. und 13. Generation von PowerEdge-Servern und die Bereitstellung der Server in einer virtuellen Umgebung.
- Anzeigen der Bestandsliste der ermittelten Server – es werden zentrale Inventardetails zu den Dell Servern bereitgestellt.
- Serverübereinstimmung überprüfen – Zur Verwendung der auf dem Gerät verfügbaren Funktionen müssen Dell Server über die erforderlichen Firmware-Versionen von iDRAC, LC und BIOS (Grundlegendes Eingabe-/Ausgabesystem) verfügen. Informationen zu den Versionsnummern finden Sie in den *Versionshinweisen zu DLCI for SCVMM*.
- Vorbereitung einer optimalen Serverkonfiguration (Gold-Konfiguration) – Replizieren Sie diese Konfiguration auf den Servern, die in der virtuellen Umgebung bereitgestellt werden. Sie haben zudem folgende Möglichkeiten:
 - Bearbeiten und Ändern der goldenen Konfiguration der Startreihenfolge und des BIOS
 - Anpassen einer dedizierten Hot Spare (DHS) -Strategie für RAID
- Erstellen und Verwalten von Vorlagen und Profilen
- Anpassen der Microsoft Windows Preinstallation Environment (WinPE) – Vorbereitung benutzerdefinierter WinPE-Images mit aktuellen Dell OpenManage Deployment Toolkit (DTK) -Treibern
- Nutzen der LC-Driver Injection-Funktion für die neuesten, werksseitig bereitgestellten Server, in deren Lieferumfang die neuesten Treiberpakete enthalten sind

Bereitstellen von Hypervisors mit oder ohne Lifecycle Controller (LC) Driver Injection – Führen Sie auf dem Gerät die Hypervisor-Bereitstellung auf der Grundlage der Gold-Konfiguration aus.

- Starten der iDRAC-Konsole von der DLCI-Konsole aus, um Inventarinformationen anzuzeigen und Fehlerbehebungen durchzuführen.
- Vereinfachte Lizenzierung – Zur Verwaltung Ihrer Lizenzen ist Dell Connections License Manager (DCLM) nicht mehr erforderlich. Weitere Informationen zur Lizenzierung finden Sie im **Lizenzcenter** im Verwaltungsportal.
- Neue Profiltypen für Anmeldeinformationen:
 - Geräte-Anmeldeprofil – Dieses Profil wird für die Anmeldung am iDRAC oder am Chassis Management Controller (CMC) verwendet.
 - Windows-Anmeldeprofil – Verwenden Sie dieses Profil für den Zugriff auf Windows-Freigaben.
 - FTP-Anmeldeprofil – Verwenden Sie dieses Profil für den Zugriff auf die FTP-Site.
 - Proxy-Server-Anmeldeinformationen – Verwenden Sie diese Option zur Angabe der Proxy-Anmeldeinformationen.
- Ermittlung – Ermitteln Sie Server mit Cluster-Details, falls der Host Teil eines Clusters ist, bzw. mit Gehäusedetails, falls es sich um einen modularen Server handelt.
- Synchronisierung mit SCVMM – Synchronisieren Sie alle Dell Host-Systeme, die in der SCVMM-Umgebung aufgeführt sind, mit DLCI für SCVMM, wobei es sich bei den Hosts um von SCVMM verwalteten Hyper-V-Hosts handelt.
 - Synchronisierungsfehler beheben – Führen Sie eine erneute Synchronisierung der Host-Server durch, die bei einem früheren Versuch nicht synchronisiert wurden.
- Serververwaltung – Verwaltung von Dell Servern in der SCVMM-Umgebung und Aufrechterhaltung der Server auf dem neuesten Stand gemäß Dell Empfehlungen, basierend auf der aktuellen Firmware und anderen Aktualisierungen. Die Serververwaltung wird für Dell PowerEdge-Server der 11. bis 13. Generation unterstützt.

- Wesentliche Funktionen der Serververwaltung:
 - * Anzeigen eines Vergleichsreports – Anzeigen von Vergleichsreports mit Kritizität von einer Aktualisierungsquelle und anschließendes Erstellen einer Grundlinienversion. Die Kritizität entspricht der Wichtigkeit einer Aktualisierung.
 - * Aktualisieren und Exportieren der Firmware-Bestandsaufnahme – Sie können die Firmware-Bestandsaufnahme aktualisieren und die Details in das xml-Format exportieren.
 - * Anwenden von Aktualisierungen – Wenden Sie Firmware-Aktualisierungen an, oder planen Sie Aktualisierungen.
 - * Anwenden spezifischer Aktualisierungen – Wenden Sie lediglich bestimmte Komponentenaktualisierungen an oder die neueste auf Dell FTP verfügbare Aktualisierung.
 - * Anwenden von Aktualisierungen vor der Betriebssystembereitstellung – Unter Verwendung einer geeigneten Aktualisierungsquelle können Sie vor einer Betriebssystembereitstellung Firmware-Aktualisierungen anwenden.
- Remote-Aktualisierung von Servern (1:1 oder 1:n) für die neuesten Firmware-Versionen von:
 - * BIOS
 - * NIC oder LAN auf der Hauptplatine (LOM)
 - * Netzteileneinheiten (PSUs) ab der 12. Generation von PowerEdge-Servern
 - * PowerEdge RAID Controller (PERC) oder Serial Attached SCSI (SAS)
 - * Rückwandplatine
 - * iDRAC (modular und monolithisch) mit LC



ANMERKUNG: Die verfügbaren Komponenten sind unter „Dell Server“ aufgeführt.

Installieren und Einrichten des DLCI-Konsolen-Add-In

Das Installieren und Einrichten des DLCI-Konsolen-Add-In für SCVMM umfasst Folgendes:

- Überprüfen und vervollständigen Sie ggf. die Systemanforderungen, und installieren Sie anschließend das **DLCI-Konsolen-Add-In für SCVMM**. Weitere Informationen finden Sie unter [Installieren des DLCI-Konsolen-Add-Ins](#).
- Importieren Sie die DLCI-Konsole in die VMM-Konsole. Weitere Informationen finden Sie unter [Importieren der DLCI-Konsole in die VMM-Konsole](#).
- Zeigen Sie die DLCI-Konsole in der VMM-Konsole an. Weitere Informationen finden Sie unter [Anzeigen der DLCI-Konsole](#).

Installieren des DLCI-Konsolen-Add-In

Bevor Sie mit dem Gerät arbeiten, müssen Sie die DLCI-Konsole auf dem System installieren, auf dem die SCVMM-Konsole installiert ist. Nach der Installation der DLCI-Konsole können Sie diese in die SCVMM-Konsole importieren.

Voraussetzungen: Die SC2012 VMM R2-, SC2012 VMM SP1- oder SC2016 VMM-Konsole ist installiert.

Wenn Sie die DLCI-Konsole zum ersten Mal über **Setup und Konfiguration** installieren, starten Sie mit Schritt 3, andernfalls starten Sie mit Schritt 1.

Um die DLCI-Konsole zu installieren, führen Sie folgende Schritte durch:

1. Klicken Sie im **DLCI-Verwaltungsportal für SCVMM** auf **Downloads**.
2. Klicken Sie im **Installationsprogramm für das DLCI-Konsolen-Add-In für SCVMM** auf **Installationsprogramm herunterladen**, und speichern Sie die Datei an einem geeigneten Speicherort.
3. Führen Sie das Installationsprogramm aus.
4. Klicken Sie auf der Begrüßungsseite des **DLCI-Konsolen-Add-Ins für SCVMM** auf **Weiter**.
5. Wählen Sie im Bildschirm **Lizenzvereinbarung** die Option **Ich stimme den Bedingungen der Lizenzvereinbarung zu** aus, und klicken Sie dann auf **Weiter**.
6. Im Fenster **Zielordner** ist standardmäßig ein Installationsordner ausgewählt. Um den Speicherort zu ändern, klicken Sie auf **Ändern**, führen Sie die gewünschten Änderungen durch, und klicken Sie dann auf **Weiter**.
7. Klicken Sie auf der Seite **Zur Installation des Programms bereit** auf **Installieren**.
8. Klicken Sie auf der Seite **InstallShield-Assistent abgeschlossen** auf **Fertigstellen**.

Entfernen oder Reparieren des DLCI-Konsolen-Add-In

Führen Sie zum Entfernen oder Reparieren des DLCI-Konsolen-Add-In folgende Schritte durch:

1. Führen Sie das Installationsprogramm für das **DLCI-Konsolen-Add-In für SCVMM** aus.
2. Wählen Sie unter **Programmwartung** die Option **Entfernen** oder **Reparieren** aus, und klicken Sie dann auf **Weiter**.
3. Klicken Sie unter **Bereit zum Reparieren oder Entfernen des Programms** auf **Installieren**.
4. Wenn der Task zum Entfernen oder Reparieren abgeschlossen ist, klicken Sie auf **Fertigstellen**.

Importieren des DLCI-Konsolen-Add-In in VMM

Um das DLCI-Gerät verwenden zu können, importieren Sie die DLCI-Konsole in die VMM-Konsole.

Voraussetzungen: Damit die Verbindung mit dem Gerät funktioniert, löschen Sie im Web-Browser die Proxy-Einstellungen. Wenn die Web-Browser-Proxy-Einstellungen jedoch konfiguriert sind, nehmen Sie den vollständig qualifizierten Domännennamen (Fully Qualified Domain Name, FQDN) des Geräts in die Proxy-Ausnahmeliste auf.

So importieren Sie die DLCI-Konsole in die VMM-Konsole:

1. Klicken Sie in SCVMM auf **Einstellungen**.
2. Klicken Sie in der Multifunktionsleiste **Startseite** auf **Add-In-Konsole importieren**.
3. Klicken Sie auf **Assistent „Konsolen-Add-In importieren“** → **Zu importierendes Add-In auswählen**, durchsuchen Sie das DLCI-Konsolen-Add-In für SCVMM (**DLCI_VMM_Console_Addin.zip**) und wählen Sie es aus; klicken Sie anschließend auf **Weiter**.
4. Bestätigen Sie unter **Einstellungen bestätigen**, dass die Einstellungen gemäß Anforderungen festgelegt wurden, und klicken Sie dann auf **Fertigstellen**.
Die DLCI-Konsole wird in die VMM-Konsole importiert und ist unter **VMs und Dienste** → **Alle Hosts** verfügbar.

Anzeigen des DLCI-Konsolen-Add-In

So zeigen Sie das DLCI-Konsolen-Add-In in SCVMM an:

1. Wählen Sie in der SCVMM-Konsole **Struktur** und dann **Alle Host-Gruppen** aus.
 **ANMERKUNG: Um die DLCI-Konsole zu starten, können Sie eine beliebige Host-Gruppe auswählen, auf die Sie Zugriff haben.**
2. Wählen Sie in der Multifunktionsleiste **Startseite DLCI-Konsole** aus.

Erste Schritte

Verwaltungssysteme sind die Systeme, auf denen DLCI for SCVMM (auch bekannt als Gerät und Gerätekomponenten) installiert sind. Das Gerät besteht aus folgenden Komponenten:

- Dell Lifecycle Controller Integration (DLCI) Integration Gateway for Microsoft System Center Virtual Machine Manager (SCVMM), auch bekannt als DLCI Integration Gateway for SCVMM.
- Dell Lifecycle Controller Integration (DLCI)-Konsolen-Add-In für Microsoft System Center Virtual Machine Manager (SCVMM), auch bekannt als DLCI-Konsolen-Add-In für SCVMM.

Anmelden am DLCI-Verwaltungsportal für SCVMM

Führen Sie zur Anmeldung am DLCI-Verwaltungsportal für SCVMM folgende Schritte durch:

1. Notieren Sie in der Appliance die URL des DLCI-Verwaltungsportals für SCVMM.
2. Rufen Sie in einem Web-Browser die URL **https://<IP Address>** oder den **<FQDN>** auf.
Beispiel: **192.168.20.30** oder **DLCIforSCVMM.myorgdomain.com**.
3. Melden Sie sich am DLCI-Verwaltungsportal für SCVMM mit den Benutzer-Anmeldeinformationen an, die bei der Konfiguration der Appliance bereitgestellt werden.

DLCI-Verwaltungsportal für SCVMM

Die Benutzeroberfläche des DLCI-Verwaltungsportals für SCVMM enthält die folgenden Optionen:

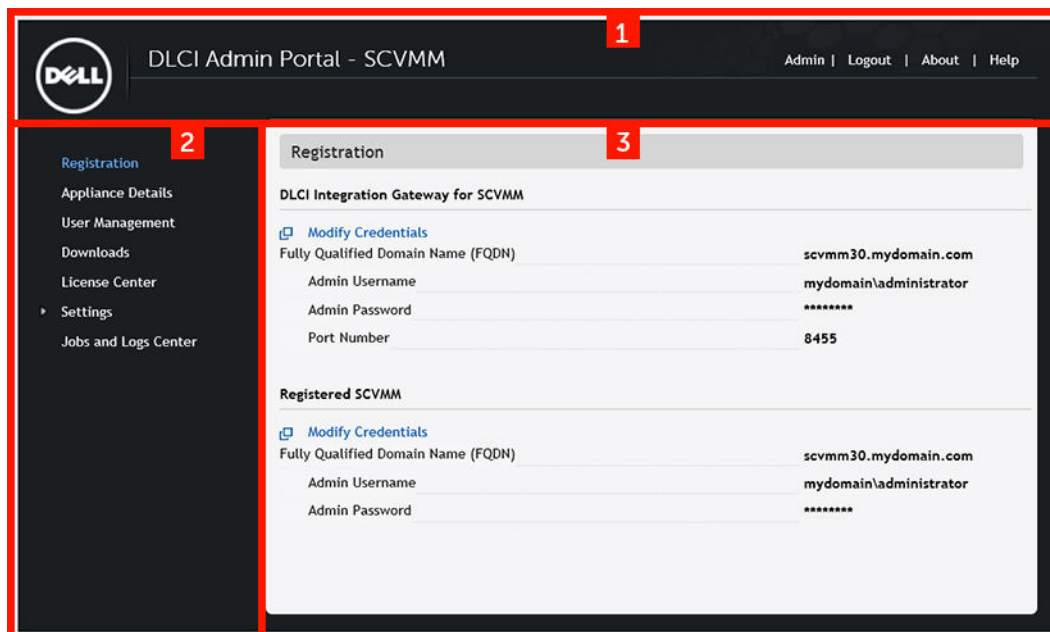


Abbildung 1. DLCI-Verwaltungsportal für SCVMM

1. Der Kopfteilbanner enthält den Namen des Produkts und die folgenden Optionen:

- **Admin.** – Zeigt die Informationen des Benutzers an, der am DLCI-Verwaltungsportal für SCVMM angemeldet ist.
 - **Abmeldung** – Ermöglicht es Ihnen, sich vom DLCI-Verwaltungsportal für SCVMM abzumelden.
 - **Info** – Bietet Informationen zur jeweiligen Version von DLCI for SCVMM.
 - **Hilfe** – Startet die kontextabhängige Online-Hilfe.
2. Der Navigationsbereich enthält die folgenden Optionen (weitere Informationen zu den einzelnen Optionen finden Sie in der Online-Hilfe):
- **Registrierung**
 - **Appliance-Details**
 - **Benutzerverwaltung**
 - **Downloads**
 - **Lizenzcenter**
 - **Settings (Einstellungen)**
 - **Service Pack-Aktualisierungen**
 - **Protokolle**
 - **Jobs und Protokollcenter**
3. Der Konsolenbereich zeigt Informationen zur Option an, die Sie im Navigationsbereich ausgewählt haben.

Anmelden am DLCI-Konsolen-Add-In für SCVMM

So melden Sie sich am DLCI-Konsolen-Add-In für SCVMM an:

1. Wählen Sie in SCVMM **Struktur** und dann **Alle Hosts** aus.
2. Wählen Sie in der Multifunktionsleiste **Startseite DLCI-Konsole** aus.

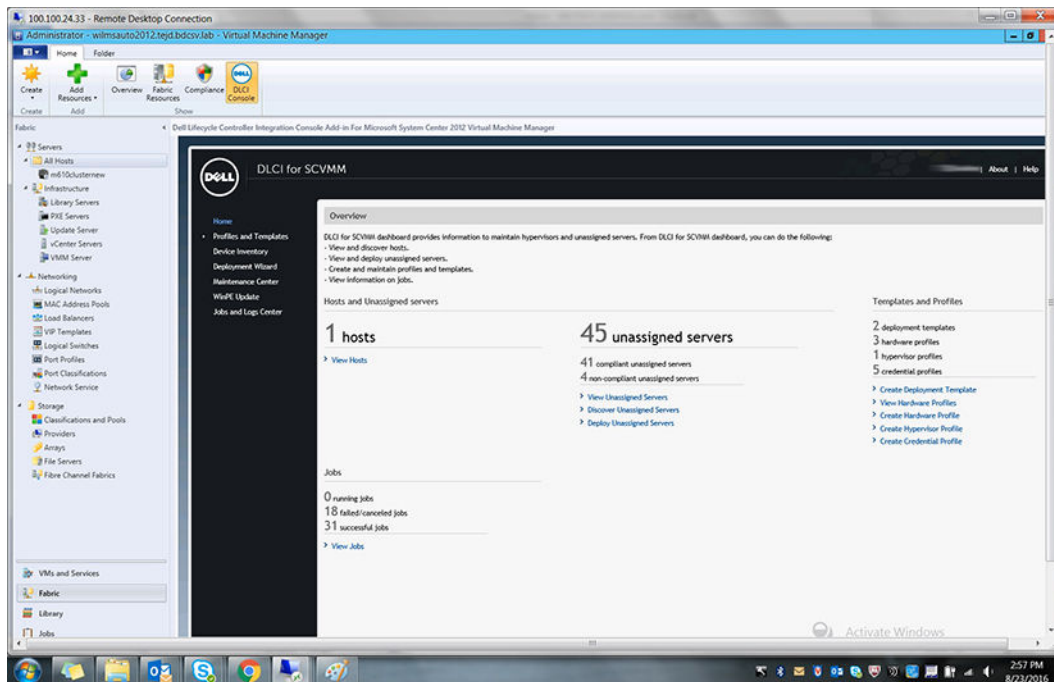


Abbildung 2. —DLCI-Konsolen-Add-In für SCVMM

DLCI-Konsolen-Add-In für SCVMM

Die DLCI-Konsolen-Add-In-Benutzeroberfläche enthält die folgenden Optionen:



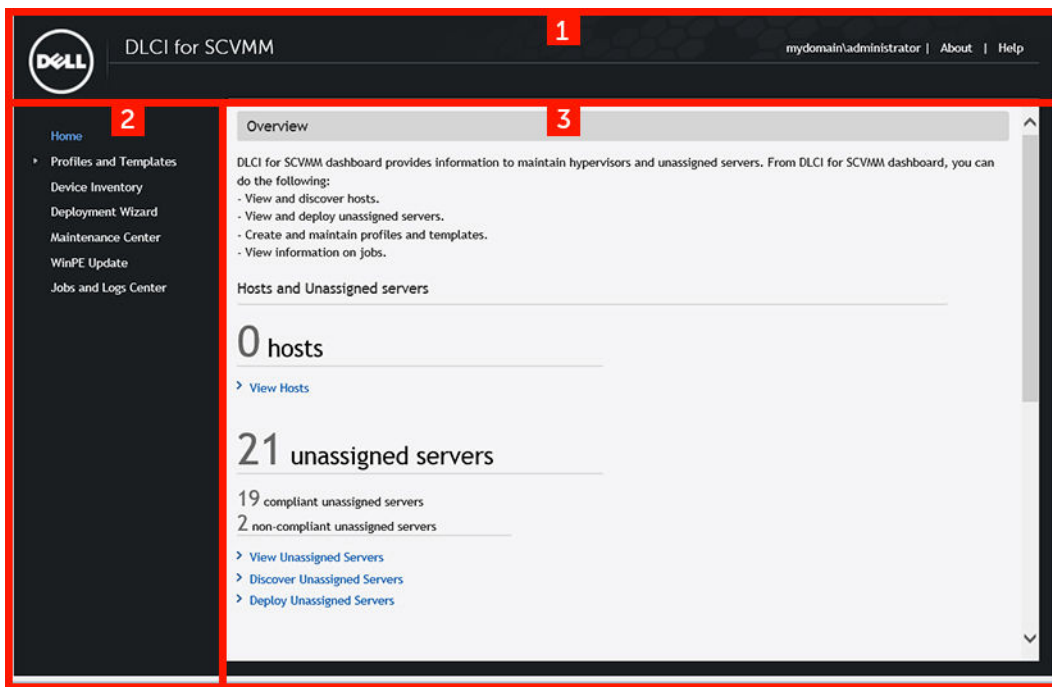


Abbildung 3. DLCI-Konsolen-Add-In für SCVMM

1. Der Kopfzeilenbereich enthält den Namen des Produkts und die folgenden Optionen:
 - **<Domäne>\Administrator** – Zeigt Informationen zum Benutzer an, der bei DLCI for SCVMM angemeldet ist.
 - **Info** – Bietet Informationen zur jeweiligen Version von DLCI for SCVMM.
 - **Hilfe** – Startet die kontextabhängige Online-Hilfe.
2. Der Navigationsbereich umfasst die folgenden Optionen:
 - **Startseite** – Zeigt das DLCI for SCVMM-Dashboard an.
 - **Profile und Vorlagen**
 - **Bereitstellungsvorlage**
 - **Hardwareprofil**
 - **Hypervisor-Profil**
 - **Anmeldeprofil**
 - **Gerätebestandsaufnahme**
 - **Bereitstellungsassistent**
 - **Wartungszentrum**
 - **Ergänzende Informationen zu WinPE**
 - **Jobs und Protokollzentrum**
3. Der Konsolenbereich zeigt Informationen zur Option an, die Sie im Navigationsbereich ausgewählt haben.

 **ANMERKUNG:** Wenn Sie sich innerhalb der DLCI-Konsole für SCVMM in einem Assistenten befinden (z. B. für das Hardwareprofil) und Sie zu einer anderen Registerkarte oder einem anderem Link in der SCVMM-Konsole navigieren und dann das DLCI-Konsolen-Add-In für SCVMM erneut anzeigen, werden die von Ihnen angegebenen Informationen nicht gespeichert, und die DLCI-Konsole zeigt die Startseite an.

Arbeitsabläufe

Dieser Abschnitt enthält die folgenden Arbeitsabläufe:

- [Erstellen von Gold-Konfigurationen](#)
- [Erstellen und Verwalten von Anmeldeprofilen](#)
- [Erstellen und Verwalten von Aktualisierungsquellen](#)
- [Erstellen und Verwalten von benutzerdefinierten Aktualisierungsgruppen](#)
- [Anwenden von Aktualisierungen auf Server](#)
- [Bereitstellen von Hypervisors](#)
- [Erstellen, Verwalten und Löschen von Schutz-Vaults](#)
- [Exportieren von Serverprofilen](#)
- [Importieren von Serverprofilen](#)
- [Löschen von Servern](#)
- [Konfigurieren von ersetzten Komponenten](#)
- [Erfassen und Anzeigen von LC-Protokollen](#)

Info über Gold-Konfigurationen

Eine Serverkonfiguration mit der bevorzugten Startsequenz und den für die Organisation idealen BIOS- und RAID-Einstellungen wird als Gold-Konfiguration bezeichnet. Diese Einstellungen werden in einem Hardwareprofil erfasst und während der Hypervisor-Bereitstellung auf identischen Servern bereitgestellt.

Erstellen von Gold-Konfigurationen

So erstellen und verwenden Sie eine goldene Konfiguration:

1. Stellen Sie sicher, dass der Server mit der idealen Konfiguration ermittelt wurde und verfügbar ist. Weitere Informationen über die Serverermittlung finden Sie je nach Anforderung unter [Ermitteln von Servern über die automatische Ermittlung](#) oder [Ermitteln von Servern über die manuelle Ermittlung](#).
2. Stellen Sie sicher, dass die Serverbestandsaufnahme auf dem neuesten Stand ist. Weitere Informationen finden Sie unter [Anzeigen und Aktualisieren der Firmware-Bestandsaufnahme](#).
3. Um die ideale Konfiguration aufzuzeichnen, erstellen Sie ein Hardwareprofil. Informationen zum Erstellen eines Hardwareprofils finden Sie unter [Erstellen eines Hardwareprofils](#).
4. Informationen zum Ändern von Konfigurationen finden Sie unter [Ändern eines Hardwarekonfigurationsprofils](#).

Erstellen, Verwalten und Löschen von Anmeldeprofilen

Informationen zum Erstellen eines Anmeldeprofils finden Sie unter [Erstellen eines Anmeldeprofils](#).

Informationen zum Verwalten eines Anmeldeprofils finden Sie unter [Ändern eines Anmeldeprofils](#).



Informationen zum Löschen eines Anmeldeprofils finden Sie unter [Löschen eines Anmeldeprofils](#).

Erstellen, Verwalten und Löschen von Aktualisierungsquellen

Informationen zum Erstellen einer Aktualisierungsquelle finden Sie unter [Erstellen einer Aktualisierungsquelle](#).

Informationen zum Verwalten einer Aktualisierungsquelle finden Sie unter [Ändern einer Aktualisierungsquelle](#).

Informationen zum Löschen einer Aktualisierungsquelle finden Sie unter [Löschen einer Aktualisierungsquelle](#).

Erstellen, Verwalten und Löschen von benutzerdefinierten Aktualisierungsgruppen

Informationen zum Erstellen einer benutzerdefinierten Aktualisierungsgruppe finden Sie unter [Erstellen von benutzerdefinierten Aktualisierungsgruppen](#).

Informationen zum Verwalten einer benutzerdefinierten Aktualisierungsgruppe finden Sie unter [Modifizieren von benutzerdefinierten Aktualisierungsgruppen](#).

Informationen zum Löschen einer benutzerdefinierten Aktualisierungsgruppe finden Sie unter [Löschen von benutzerdefinierten Aktualisierungsgruppen](#).


Anwenden von Aktualisierungen auf Server

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

- Online FTP- und lokale FTP-Quelle
- Online HTTP und lokales HTTP
- Lokales DRM Repository

So wenden Sie Aktualisierungen auf ausgewählte Server oder Servergruppen an:

1. Bevor Sie mit dem Aktualisieren beginnen, lesen Sie die Informationen zu Aktualisierungsquellen und Aktualisierungsgruppen. Weitere Informationen finden Sie unter [Serververwaltung](#).
2. Ermitteln Sie die Server. Weitere Informationen hierzu finden Sie unter [Ermitteln von Servern über die automatische Ermittlung](#) und [Ermitteln von Servern über die manuelle Ermittlung](#).
3. Synchronisieren Sie die in der SCVMM-Umgebung vorhandenen Server mit DLCI for SCVMM. Weitere Informationen zur Synchronisierung finden Sie unter [Synchronisierung mit SCVMM](#).
4. Stellen Sie sicher, dass die Serverbestandsaufnahme auf dem neuesten Stand ist. Weitere Informationen finden Sie unter [Anzeigen der Gerätebestandsaufnahme](#).
5. Stellen Sie sicher, dass eine Aktualisierungsquelle erstellt wurde. Weitere Informationen finden Sie unter [Erstellen einer Aktualisierungsquelle](#).
6. Stellen Sie sicher, dass die Aktualisierungsquelle regelmäßig mit dem neuesten Katalog aktualisiert wird, indem Sie die Funktion „Abfrage und Benachrichtigung“ verwenden. Weitere Informationen finden Sie unter [Abfrage und Benachrichtigung](#).
7. Stellen Sie sicher, dass die erforderlichen Servergruppen für die Anwendung der Aktualisierungen ausgewählt sind. Weitere Informationen finden Sie unter [Anwenden von Aktualisierungen auf Server](#).

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

Erstellen, Verwalten und Löschen von Schutz-Vaults

1. Informationen zum Erstellen eines Schutz-Vaults finden Sie unter [Erstellen eines Schutz Vault](#).
2. Informationen zum Verwalten eines Schutz-Vaults finden Sie unter [Modifizieren eines Schutz Vault](#).
3. Informationen zum Löschen eines Schutz-Vaults finden Sie unter [Löschen eines Schutz Vault](#).

Exportieren von Serverprofilen

So exportieren Sie eine Serverkonfiguration:

1. Erstellen Sie einen Schutz-Vault. Weitere Informationen finden Sie unter [Erstellen eines Schutz-Vaults](#).
2. Sie können ein Serverprofil sofort exportieren, oder den Export für einen späteren Zeitpunkt planen. Weitere Informationen finden Sie unter [Erstellen eines Export-Jobs](#).

Importieren von Serverprofilen

So 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. Importieren Sie ein exportiertes Serverprofil mit oder ohne die RAID-Konfiguration. Weitere Informationen finden Sie unter [Importieren von Serverprofilen](#).

Hypervisor-Bereitstellung

Sie können unter Verwendung des Geräts die Firmware-Aktualisierung und die Hypervisor-Bereitstellung basierend auf der Gold-Konfiguration durchführen. Nutzen Sie die LC-Driver Injection-Funktion für die neuesten, werksseitig bereitgestellten Server, in deren Lieferumfang die neuesten Treiberpakete enthalten sind. Sie können die Treiberpakete auch bei der Hypervisor-Bereitstellung oder Firmware-Aktualisierung aktualisieren und auf diese Weise die gleichen Vorteile einer Installation aktueller Treiber nutzen.

Tabelle 1. 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	Wählen Sie beim Erstellen einer Bereitstellungsvorlage nur das Hypervisor-Profil aus.

Wenn Sie die Hypervisor-Bereitstellung verwenden möchten, finden Sie weitere Informationen unter den folgenden Themen:

1. [Info zu Bereitstellungen](#)
2. [Erstellen von Anmeldeprofilen](#)
3. [Erstellen von Aktualisierungsquellen](#)
4. [Erstellen von Hardwareprofilen](#)
5. [Erstellen von Hypervisor-Profilen](#)
6. [Erstellen von Bereitstellungsvorlagen](#)
7. (Optional) [Erstellen von benutzerdefinierten Aktualisierungsgruppen](#)
8. (Optional) [Anwenden von Aktualisierungen auf Servern](#)
9. [Bereitstellen von Hypervisoren](#)

Löschen von Servern

Weitere Informationen zum Löschen von Servern auf dem Gerät finden Sie unter [Löschen von Servern aus der DLCI-Konsole](#).

Konfigurieren von ersetzten Komponenten

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



Erfassen und Anzeigen von LC-Protokollen

Informationen zum Exportieren und Anzeigen der LC-Protokolldateien finden Sie unter [LC-Protokollerfassung](#).

Einrichten der Umgebung für die Hypervisor-Bereitstellung

So richten Sie eine Umgebung für die Bereitstellung des Hypervisors ein:

1. Bereiten Sie [Gold-Konfigurationen](#) vor.
2. Erstellen Sie ein physisches Computerprofil in SCVMM. Weitere Informationen finden Sie in der SCVMM-Dokumentation.
3. Erstellen Sie eine Ziel-Host-Gruppe in SCVMM. Weitere Informationen finden Sie in der SCVMM-Dokumentation.
4. Laden Sie das neueste Dell Deployment ToolKit (DTK) herunter, und erstellen Sie ein Start-ISO-Image für die Windows Preinstallation Environment (WinPE). Weitere Informationen hierzu finden Sie unter [WinPE-Aktualisierung](#).
5. Richten Sie die Systeme für die automatische Ermittlung ein. Weitere Informationen finden Sie unter [Ermitteln von Servern über die automatische Ermittlung](#).
6. (Optional) Erstellen Sie eine Aktualisierungsquelle. Weitere Informationen finden Sie unter [Erstellen einer Aktualisierungsquelle](#).
7. (Optional) Erstellen Sie eine benutzerdefinierte Aktualisierungsgruppe. Weitere Informationen finden Sie unter [Erstellen von benutzerdefinierten Aktualisierungsgruppen](#).
8. (Optional) Erstellen Sie ein Hardwareprofil. Weitere Informationen finden Sie unter [Erstellen eines Hardwareprofils](#).
9. Erstellen Sie ein Hypervisor-Profil. Weitere Informationen finden Sie unter [Erstellen eines Hypervisor-Profiles](#).
10. Erstellen Sie eine Bereitstellungsvorlage. Weitere Informationen finden Sie unter [Erstellen einer Bereitstellungsvorlage](#).
11. Nachdem die Systeme ermittelt wurden und auf dem Gerät verfügbar sind, führen Sie optional eine Firmware-Aktualisierung und dann die Hypervisor-Bereitstellung durch. Weitere Informationen zur Anwendung von Aktualisierungen finden Sie unter [Anwenden von Aktualisierungen auf Servern](#). Weitere Informationen zur Bereitstellung des Hypervisors finden Sie unter [Bereitstellen von Hypervisors](#).
12. Zeigen Sie den Job-Status zur Firmware-Aktualisierung und zur Bereitstellung an. Weitere Informationen finden Sie unter [Jobs und Protokollcenter](#).

Serverermittlung

Sie können eine bandexterne Ermittlung nicht zugewiesener Dell Server durchführen und alle Informationen zu den Dell Servern in das Gerät importieren.

Sie können Hyper-V-Hosts und modulare Hyper-V-Hosts zusammen mit nicht zugewiesenen Servern ermitteln. Nach der Ermittlung werden die Server der entsprechenden vordefinierten Aktualisierungsgruppe hinzugefügt. Weitere Informationen zur Klassifizierung von Gruppen finden Sie unter [Aktualisierungsverwaltung](#).

Anmerkungen zur Ermittlung von Servern:

- Wenn Sie einen Dell PowerEdge-Server mit einem Betriebssystem ermitteln, der in SCCM oder SCVMM vorhanden ist, wird dieser Server als Host-Server aufgeführt und als kompatibel oder nicht kompatibel gekennzeichnet.
 - Ein Host-Server ist kompatibel, wenn er bestimmte Mindestversionen von LC-Firmware, BIOS und iDRAC enthält, die für die Interaktion mit dem Gerät erforderlich sind.
 - Wenn es sich bei dem Host um einen modularen Server handelt, wird auch die Service-Tag-Nummer des Gehäuses angezeigt, das den Server enthält.
 - Wenn der Host zu einem Cluster gehört, wird der vollständig qualifizierte Domänenname (FQDN) des Clusters angezeigt.
- Wenn Sie einen Dell PowerEdge-Server ermitteln, der nicht in SCCM oder SCVMM aufgeführt ist, wird dieser Server als nicht zugewiesener Server aufgeführt und basierend auf dessen Versionen von LC-Firmware, iDRAC und BIOS als kompatibel oder nicht kompatibel gekennzeichnet.
- Wenn Sie falsche Anmeldeinformationen angeben, stehen je nach iDRAC-Version folgende Lösungen zur Verfügung:
 - Wenn Sie bei der Ermittlung von Dell PowerEdge-Servern der 12. Generation mit einer iDRAC-Version ab 2.10.10.10 falsche Details im Anmeldeprofil angeben, schlägt die Serverermittlung mit dem folgenden Verhalten fehl:
 - * Beim ersten Fehlversuch wird die Server-IP-Adresse nicht blockiert.
 - * Beim zweiten Fehlversuch wird die Server-IP-Adresse 30 Sekunden lang blockiert.
 - * Ab dem dritten Fehlversuch wird die Server-IP-Adresse 60 Sekunden lang blockiert.

Sie können die Serverermittlung mit den richtigen 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.
- Bei iDRAC-Versionen vor 2.10.10.10 ist die Blockierung der IP-Adressen konfigurierbar. Weitere Informationen finden Sie in der iDRAC-Dokumentation unter dell.com/support/home. Je nach Anforderung können Sie die Blockierung der IP-Adressen auch deaktivieren. Sie können außerdem überprüfen, ob die Funktion **iDRAC.IPBlocking.BlockEnable** in iDRAC aktiviert ist.
- Wenn das Standard-iDRAC-Anmeldeprofil geändert wird, nachdem ein Server ermittelt und dem Gerät hinzugefügt wurde, können Sie keine Aktivitäten mehr auf dem Server ausführen. Damit Sie den Server wieder verwenden können, führen Sie eine Neuermittlung des Servers mit dem neuen Anmeldeprofil aus.

Sie können Dell Server auch mithilfe der folgenden Optionen ermitteln:

- [Automatische Ermittlung](#) von Servern.
- [Manuelle Ermittlung](#) anhand der IP-Adressen.

Systemanforderungen für verwaltete Systeme

Verwaltete Systeme sind die Systeme, die unter Verwendung des Geräts verwaltet werden. Beachten Sie die folgenden Systemanforderungen, wenn Sie mit dem Gerät verwaltete Systeme ermitteln möchten:

- Bei Dell PowerEdge-Servern der 11., 12. und 13. Generation unterstützt das Gerät modulare und monolithische Servermodelle.
- 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.
- Der Startmodus „Unified Extensible Firmware Interface“ (UEFI) wird nicht unterstützt.
- Die RAID-Konfiguration auf externen Controllern wird nicht unterstützt.
- Aktivieren Sie die CSIOR-Funktion (Systembestandsaufnahme bei Neustart durchführen) auf verwalteten Systemen. Weitere Informationen finden Sie unter [Aktivieren von CSIOR auf verwalteten Systemen](#).

Aktivieren von CSIOR auf verwalteten Systemen

So aktivieren Sie CSIOR für Dell PowerEdge-Server der 12. und 13. Generation:

1. Drücken Sie während des POST-Vorgangs die Taste **F2**, um das **System-Setup** aufzurufen.
2. Wählen Sie **iDRAC-Einstellungen** aus, und klicken Sie auf **Lifecycle Controller**.
3. Setzen Sie unter **Bei Neustart Systeminformationen sammeln (CSIOR)** den Wert auf **Aktiviert**.

So aktivieren Sie CSIOR für die 11. Generation der PowerEdge-Server:

1. Starten Sie das System neu.
2. Wenn Sie während des POST-Vorgangs (Power On Self Test, Einschaltselbsttest) vom System aufgefordert werden, das iDRAC-Dienstprogramm einzugeben, drücken Sie **STRG + E**.
3. Wählen Sie aus den verfügbaren Optionen **Systemdienste** aus, und drücken Sie auf **Eingabe**.
4. Wählen Sie **Systembestandsaufnahme bei Neustart sammeln** aus und drücken Sie auf die Nach-rechts- oder Nach-unten-Taste und ändern Sie die Einstellung auf **Aktiviert**.

Ermitteln von Servern über die automatische Ermittlung

Schließen Sie die Dell-Server an das Netzwerk an, und schalten Sie die Server ein, damit die DLCI-Appliance die Server automatisch erkennen kann. Die Appliance erkennt nicht zugeordnete Dell-Server automatisch unter Verwendung der Remote-Aktivierungsfunktion des iDRAC. Die Appliance funktioniert wie die Provisioning-Server und verwendet die iDRAC-Referenz zur automatischen Ermittlung von Dell Servern.

So führen Sie die automatische Erkennung auf Dell-Servern durch:

1. Erstellen Sie auf dem Gerät ein Geräte-Anmeldeprofil für Dell Server (indem Sie die iDRAC-Anmeldeinformationen angeben und sie als Standardeinstellung kennzeichnen). Weitere Informationen finden Sie unter [Erstellen eines Anmeldeprofils](#).
2. In Dell-Servern, die Sie automatisch erkennen möchten, führen Sie die folgenden Schritte aus:
 - a. Deaktivieren Sie die vorhandenen Admin-Konten in iDRAC.
 - b. Aktivieren Sie bei den iDRAC-Einstellungen, in der Remote-Aktivierung, die automatische Ermittlung.
 - c. Geben Sie nach der Aktivierung der automatischen Ermittlung die IP-Adresse des Bereitstellungsservers (d. h. der DLCI-Appliance) ein, und starten Sie den Server neu.



Ermitteln von Servern über die manuelle Ermittlung

Sie können Server manuell über eine IP-Adresse oder einen IP-Adressbereich ermitteln. Geben Sie zur Ermittlung von Servern die iDRAC-IP-Adresse und die Geräte-Anmeldeinformationen der Server an. Wenn Sie Server über einen IP-Adressbereich ermitteln, geben Sie einen IP-Bereich (IPv4) (in einem Subnetz) an.

So führen Sie eine automatische Ermittlung von Dell-Servern durch:

1. Führen Sie im DLCI-Konsolen-Add-In für SCVMM einen der folgenden Schritte aus:
 - Klicken Sie im Dashboard auf **Nicht zugewiesene Server ermitteln**.
 - Klicken Sie im Navigationsbereich auf **Gerätebestandsaufnahme**, und klicken Sie unter **Bestandsaufnahme** auf **Ermitteln**.
2. Wählen Sie in **Ermitteln** die erforderliche Option aus:
 - **Über eine IP-Adresse ermitteln**
 - **Über einen IP-Adressbereich ermitteln**
3. Wählen Sie das gewünschte Geräte-Anmeldeprofil aus, oder klicken Sie auf **Neu erstellen**, um ein Anmeldeprofil zu erstellen.
4. Führen Sie unter **Über eine IP-Adresse oder einen IP-Adressbereich ermitteln** einen der folgenden Schritte aus:
 - Wenn Sie die Option **Über eine IP-Adresse ermitteln** ausgewählt haben, geben Sie die IP-Adresse des Servers an, den Sie ermitteln möchten.
 - Wenn Sie die Option **Über einen IP-Adressbereich ermitteln** ausgewählt haben, geben Sie den IP-Adressbereich an, den Sie einschließen möchten, und wenn Sie einen IP-Adressbereich ausschließen müssen, wählen Sie **Ausschlussbereich aktivieren** aus, und geben Sie den Bereich an, den Sie ausschließen möchten.
5. Geben Sie einen eindeutigen Job-Namen an und klicken Sie auf **Fertigstellen**.
6. (Optional) Wählen Sie die Option **Zur Job-Liste wechseln** aus, um diesen Job zu verfolgen.
Die Seite **Jobs und Protokollcenter** wird angezeigt. Erweitern Sie in der Registerkarte **Ausführen** den Ermittlungsjob, um den Fortschritt dieses Jobs anzuzeigen.

Löschen von Servern aus der DLCI-Konsole

Sie können die nicht zugewiesenen Server und Host-Server basierend auf den folgenden Kriterien löschen:

- Sie können einen nicht zugewiesenen Server löschen, der auf dem Gerät aufgeführt wird.
- Wenn ein Host-Server in SCVMM bereitgestellt wurde und auf dem Gerät vorhanden ist, löschen Sie zuerst den Server in SC2012 VMM und dann den Server aus dem Gerät.

In der DLCI-Konsole:

- So löschen Sie nicht zugewiesene Server: Wählen Sie in **Nicht zugewiesene Server** den Server aus, und klicken Sie auf **Löschen**. Klicken Sie dann in der Bestätigungsmeldung auf **Ja**.
- So löschen Sie Host-Server: Wählen Sie in **Host-Server** den Server aus, und klicken Sie auf **Löschen**. Klicken Sie dann in der Bestätigungsmeldung auf **Ja**.

Anzeigen der Gerätebestandsaufnahme

Auf der Seite **Gerätebestandsaufnahme** werden nicht zugewiesene Server und Host-Server aufgeführt. Unter Verwendung des Host-Namens oder der IP-Adresse des Servers können Sie Details zum Server anzeigen, z. B. den Übereinstimmungsstatus, Firmware-Versionen und so weiter.

Auf der Seite „Gerätebestandsaufnahme“ können Sie folgende Aktionen ausführen:

- [Server ermitteln](#)
- Server-Informationen aktualisieren
- [Löschen von Servern aus der DLCI-Konsole](#)
- [Synchronisierung mit SCVMM](#)

- [Beheben von Synchronisierungsfehlern](#)
- Host-Server mit Cluster-Gruppe korrelieren und dem Gehäuse, dem der Server angehört
- [Starten der iDRAC-Konsole](#)

Wenn der nicht zugewiesene Server ein modularer Server ist, wird die Gehäuse-Service-Tag-Nummer den Bestandsaufnahmedetails des Gehäuses hinzugefügt, in dem der modulare Server enthalten ist.

Wenn der Host-Server Teil eines Clusters ist, können Sie zum Korrelieren eines Servers zu seiner Cluster-Gruppe und zum Abrufen der Gehäuseinformationen den Cluster-FQDN sowie die Gehäuse-Service-Tag-Nummer heranziehen.

Um die Server verwenden zu können, die mit einer früheren Version des Geräts ermittelt wurden, ermitteln Sie die Server erneut.

So zeigen Sie Server an:

Klicken Sie in der DLCI-Konsole auf **Gerätebestandsaufnahme**.

Synchronisierung mit SCVMM

Sie können alle Dell Hyper-V-Hosts, Hyper-V-Host-Cluster und modularen Hyper-V-Hosts in der SCVMM-Umgebung mit dem Gerät synchronisieren. Nach der Synchronisierung können Sie die neueste Firmware-Bestandsaufnahme der Server abrufen.

Anmerkungen zur Synchronisierung:

- Bei der Synchronisierung werden die Details des Standard-iDRAC-Anmeldeprofils der Server verwendet.
- Wenn der Baseboard Management Controller (BMC) des Servers in SCVMM nicht mit der iDRAC-IP-Adresse konfiguriert ist, können Sie den Host-Server nicht mit dem Gerät synchronisieren. Konfigurieren Sie daher zuerst BMC in SCVMM (weitere Informationen finden Sie im MSDN-Artikel unter `technet.microsoft.com`) und synchronisieren Sie anschließend das Gerät mit SCVMM.
- Da SCVMM R2 sehr viele Hosts in der Umgebung unterstützt, ist die Synchronisierung ein relativ zeitintensiver Vorgang. Die Synchronisierung erfolgt folgendermaßen:
 - a. Die in der SCVMM-Umgebung aufgeführten Hosts werden der Registerkarte **Hosts** des Geräts hinzugefügt.
 - b. Während der Neusynchronisierung werden Host-Server, die aus der SCVMM-Umgebung gelöscht werden, auf die Registerkarte **Nicht zugewiesen** im Gerät verschoben. Wenn ein Server stillgelegt ist, entfernen Sie diesen Server aus der Liste der nicht zugewiesenen Server.
 - c. Wird ein Server als nicht zugewiesener Server aufgeführt und SCVMM manuell hinzugefügt, wird der Server nach der Synchronisierung der Registerkarte **Hosts** des Geräts hinzugefügt.
 - d. Gehört ein Host-Server einem Hyper-V-Cluster an, sind die Details zum Cluster in der Gerätebestandsaufnahme verfügbar. Der Host-Server wird der Cluster-Aktualisierungsgruppe hinzugefügt, bzw. in diese verschoben.
 - e. Wenn es sich bei dem Host um einen modularen Server handelt, wird die Service-Tag-Nummer des Gehäuses, das den modularen Server enthält, auf der Seite „Gerätebestandsaufnahme“ hinzugefügt. Ist der modulare Server kein Bestandteil eines Hyper-V-Clusters, wird der Host-Server der Gehäuse-Aktualisierungsgruppe hinzugefügt, bzw. in diese verschoben.
 - f. Alle Änderungen, die an den Details der Host-Bestandsaufnahme vorgenommen werden, z. B. Host-Name, iDRAC-IP-Adresse, Speicher, Cluster-Zugehörigkeit usw., werden in der Gerätebestandsaufnahme aktualisiert.
 - g. DLCI for SCVMM kann die neuesten Informationen der Firmware-Bestandsaufnahme bereitstellen. Wurde eine Standard-Aktualisierungsquelle angegeben, wird die Firmware-Bestandsaufnahme mit der Aktualisierungsquelle verglichen, und die neuesten Informationen werden der Aktualisierungsgruppe hinzugefügt.

Synchronisieren des Geräts mit SCVMM

So führen Sie eine Synchronisierung durch:

Klicken Sie in **DLCI for SCVMM** auf **Gerätebestandsaufnahme** und dann auf **Synchronisierung mit SCVMM**.

Beheben von Synchronisierungsfehlern

Die Server, die nicht mit dem Gerät synchronisiert sind, werden mit ihrer iDRAC-IP-Adresse und ihrem Host-Namen aufgeführt. Berücksichtigen Sie Folgendes, wenn Sie Synchronisierungsfehler beheben:

- Wenn Server aufgrund von Problemen mit Anmeldeinformationen, iDRAC, Konnektivität oder sonstigen Problemen nicht synchronisiert wurden, beheben Sie zuerst diese Probleme, und versuchen Sie die Synchronisierung anschließend erneut.


So führen Sie eine Neusynchronisierung der Server durch:

1. Klicken Sie im DLCI-Konsolen-Add-In für SCVMM auf **Gerätebestandsaufnahme** und dann auf **Synchronisierungsfehler beheben**.
2. Wählen Sie die Server aus, die Sie synchronisieren möchten, und wählen Sie das gewünschte Anmeldeprofil aus bzw. erstellen Sie ein neues.
3. Geben Sie einen Job-Namen an und klicken Sie auf **Fertigstellen**.
4. (Optional) Wählen Sie die Option **Zur Job-Liste wechseln** aus, um den Job-Status automatisch anzuzeigen, sobald der Auftrag gesendet wurde.

Starten der iDRAC-Konsole

So starten Sie die iDRAC-Konsole:

Klicken Sie in der **Gerätebestandsaufnahme** unter **Nicht zugewiesene Server** oder unter **Hosts** auf die **iDRAC-IP-Adresse**.

 **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.

Lizenz für das Gerät

Die Funktionen für die agentenlose Konfiguration, Betriebssystembereitstellung, Firmware-Aktualisierung, Teilersetzung, Export und Import von Serverprofilen in DLCI for SCVMM unterliegen einer Lizenz. Es stehen fünf Lizenzen zu Testzwecken ohne zusätzliche Kosten zur Verfügung. Zum Herunterladen dieser fünf Lizenzen wechseln Sie zu marketing.dell.com/software-download-DLCISCVMM. Weitere Informationen zur Lizenzierung finden Sie auf der Dell TechCenter-Website auf der Wiki-Seite zu OpenManage Integration Suite for Microsoft System Center.


Zum Anzeigen der Lizenzdetails über das **DLCI-Verwaltungsportal für SCVMM** starten Sie das **Lizenzcenter**.

Server-Verwaltung

Über das **Wartungcenter** können Sie alle Aufgaben durchführen, die mit der Verwaltung von Dell Aktualisierungen in der SCVMM-Umgebung einhergehen. So können Sie beispielsweise, den Dell Empfehlungen entsprechend, stets aktuelle Firmware-Versionen der Dell Serverkomponenten vorhalten.

Sie können Schutz-Vaults, Aktualisierungsquellen und benutzerdefinierte Gruppen anzeigen, erstellen und verwalten und vordefinierte Aktualisierungsgruppen anzeigen. Sie können Jobs für Firmware-Aktualisierungen erstellen und planen sowie Benachrichtigungen einrichten, um benachrichtigt zu werden, sobald neue Kataloge an der Aktualisierungsquelle verfügbar sind. Für die vorhandene Firmware-Version und Basislinienversion wird ein Vergleichsreport bereitgestellt. Auf der Grundlage dieser Informationen können Sie eine Bestandsdatei anlegen und Serverprofile importieren und exportieren. Sie haben außerdem die Möglichkeit, die Informationen nach Aktualisierungstyp, Serverkomponente und Servermodell zu filtern.

Sie können Aktualisierungen nur auf kompatiblen Servern durchführen, da iDRAC-Aktualisierungen nur für die minimale kompatible Version und spätere Versionen verfügbar sind.

 **ANMERKUNG: Wenn nach der Aktualisierung auf die neueste Version von DLCI for SCVMM die Verbindung zu ftp.dell.com oder downloads.dell.com fehlschlägt, kann die Katalogdatei nicht über die standardmäßige Dell Online FTP-Site oder die Dell HTTP-Aktualisierungsquelle heruntergeladen werden, und es ist folglich kein Vergleichsreport verfügbar. Um einen Vergleichsreport zu erhalten, bearbeiten Sie die standardmäßige Dell Online-FTP-Site oder die Dell HTTP-Aktualisierungsquelle, erstellen Sie Proxy-Anmeldeinformationen, und wählen Sie diese über das Drop-Down-Menü Aktualisierungsquelle auswählen aus. Weitere Informationen zum Bearbeiten einer Aktualisierungsquelle finden Sie unter [Modifizieren einer Aktualisierungsquelle](#).**

DLCI for SCVMM bietet die folgenden Aktualisierungsmaßnahmen:

- 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 anderer Probleme in Komponenten, wie beispielsweise dem BIOS, dienen.
- Aktualisierung (empfohlen) – Die Aktualisierungen enthalten Fehlerbehebungen oder Funktionserweiterungen für das Produkt. Außerdem sind Fixes für die Kompatibilität mit anderen Firmware-Aktualisierungen enthalten.

DLCI for SCVMM bietet die folgenden Methoden für die Durchführung von Firmware-Aktualisierungen:

- **Aktualisierung unter Verwendung des DRM-Repositorys** – Exportieren Sie die Bestandsaufnahme-Dateien der ermittelten Server auf dem Gerät, um ein Repository in DRM vorzubereiten. Weitere Informationen zum Exportieren der Bestandsaufnahme-Dateien finden Sie unter [Exportieren der Bestandsaufnahme](#).
 - Nach der Erstellung des Repositorys in DRM wählen Sie die relevanten Server aus und initiieren Sie eine Aktualisierung auf den Servern. Berücksichtigen Sie weitere Faktoren, wie z. B. Testen auf der Testumgebung, Sicherheitsaktualisierungen, Anwendungsempfehlungen, Dell Empfehlungen usw.), und bereiten Sie die erforderlichen Aktualisierungen vor. Weitere Informationen zum Erstellen eines Repositorys finden Sie in den Dokumenten zu *Dell Repository Manager* unter dell.com/support/home.
- **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 entsprechendes Repository an.

- Integration in den Dell Online-Katalog – Stellen Sie im Falle einer FTP-Aktualisierungsquelle eine Verbindung zu 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 von Firmware-Bestandsaufnahme und Vergleich** – Erstellen Sie eine Referenz-Bestandsaufnahme, in der die Firmware-Bestandsaufnahme der ausgewählten Server oder Gruppen von Servern enthalten ist. Später können Sie die Bestandsaufnahmeinformationen der auf dem Gerät vorhandenen Server mit der gespeicherten Referenz-Bestandsaufnahme abgleichen. Die Referenz-Bestandsaufnahme für Server kann Bestandsaufnahmeinformationen eines einzelnen Servers eines bestimmten Typs oder Modells enthalten oder aber mehrere Server unterschiedlichen Typs oder Modells.

Integration in DRM

DLCI for SCVMM ist in DRM ab Version 2.2 integriert und ermöglicht die Bereitstellung von Bestandsaufnahmeinformationen vorhandener Server vom Gerät an den DRM. Mithilfe dieser Bestandsaufnahmeinformationen können Sie ein benutzerdefiniertes Repository in DRM erstellen und dieses im Gerät als Aktualisierungsquelle festlegen, um Firmware-Aktualisierungsjobs auf Servern oder auf einer Gruppe von Servern durchzuführen. Weitere Informationen zum Erstellen eines Repositories in DRM finden Sie in der Dokumentation zu *Dell Repository Manager*.

 **ANMERKUNG: Führen Sie nach der Aktualisierung auf DLCI for SCVMM Version 1.2 eine Neuermittlung der Server durch, um die Bestandsaufnahmeinformationen zu aktualisieren, die von DRM genutzt werden.**

So erstellen Sie ein Repository für das Gerät unter Verwendung von DRM:

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/`, und klicken Sie anschließend auf **Weiter**.
4. Geben Sie den **Benutzernamen** und das **Kennwort** ein, das auf dem Gerät verwendet wurde, klicken Sie auf **OK** und anschließend erneut auf **OK**.

Filter

Sie können Filter anwenden, um nur bestimmte Informationen im Vergleichsreport anzuzeigen. Das Gerät unterstützt drei Kategorien von Filtern:

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

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

So wenden Sie Filter an:

Klicken Sie im DLCI-Konsolen-Add-In auf **Wartungszentrum**, klicken Sie auf das Drop-down-Menü für Filter, und wählen Sie anschließend die Filter aus.

So entfernen Sie Filter:

Klicken Sie im DLCI-Konsolen-Add-In auf **Wartungszentrum**, und klicken Sie anschließend auf **Filter löschen**, oder deaktivieren Sie die betreffenden Kontrollkästchen.

Aktualisierungsquellen – Übersicht

Aktualisierungsquellen ermöglichen Ihnen das Auswählen und Anwenden von Aktualisierungen aus Dell Aktualisierungsquellen. Sie können die Aktualisierungsquellen erstellen, anzeigen und verwalten. Die unterstützten Typen von Aktualisierungsquellen lauten



DRM Repository, FTP und HTTP. Sie können eine DRM-, HTTP- oder FTP-Aktualisierungsquelle erstellen und diese als Standardquelle festlegen.

Aktualisierungsquellen verfügen über Katalogdateien, die Dell Aktualisierungen (BIOS, Firmware, Anwendung, Treiber und Treiberpakete) und die eigenständige ausführbare Datei mit der Bezeichnung Dell Update Packages (DUPs) enthalten. Eine lokale Kopie der Katalogdatei wird zum Zeitpunkt der Erstellung in den Cache des Geräts eingelesen. Wird eine Katalogdatei an der Aktualisierungsquelle aktualisiert, wird die lokal in den Cache eingelesene Katalogdatei nicht automatisch aktualisiert. Zum Aktualisieren der in den Cache eingelesenen Katalogdatei müssen Sie die Aktualisierungsquelle entweder bearbeiten oder löschen und neu erstellen.

Sie können die an der Aktualisierungsquelle verfügbaren Bestandsaufnahmeinformationen mit denen eines ausgewählten Servers oder einer ausgewählten Servergruppe vergleichen und eine Grundlinienversion erstellen. Sie können die Aktualisierungsquelle auch ändern und die Bestandsaufnahmeinformationen der Server oder Servergruppen mit den Versionsinformationen an der ausgewählten Aktualisierungsquelle vergleichen.

Dell empfiehlt, eine Aktualisierung auf die neueste Firmware durchzuführen, damit Sie von Sicherheitslösungen, Bugfixes und neuen Funktionen profitieren können. Dell veröffentlicht monatlich die folgenden Aktualisierungen über PDK-Kataloge auf Dell FTP:

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

Vordefinierte Aktualisierungsquellen und Standard-Aktualisierungsquellen

Der **DELL ONLINE-KATALOG** ist eine vordefinierte Aktualisierungsquelle vom Typ FTP, die nach einer Neuinstallation oder Aktualisierung im Gerät verfügbar ist. Der Name einer vordefinierten Aktualisierungsquelle kann nicht gelöscht oder geändert werden.

Der **DELL ONLINE-HTTP-KATALOG** ist eine Standard-Aktualisierungsquelle, die nach einer Neuinstallation oder Aktualisierung im Gerät verfügbar ist. Der Name dieser Standard-Aktualisierungsquelle kann nicht gelöscht oder geändert werden. Sie können jedoch eine andere Aktualisierungsquelle erstellen und diese als Standard-Aktualisierungsquelle festlegen.

ANMERKUNG:

- Fügen Sie nach der Installation von DLCI for SCVMM die Proxy-Details für die Aktualisierungsquellen **DELL ONLINE-KATALOG** und **DELL ONLINE-HTTP-KATALOG** hinzu, und speichern Sie sie.
- Legen Sie nach der Aktualisierung auf DLCI for SCVMM Version 1.2 den **DELL ONLINE-HTTP-KATALOG** als Standard-Aktualisierungsquelle fest.

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

So richten Sie einen HTTP-Server auf einem lokalen System ein:

1. Erstellen Sie eine Ordnerstruktur in Ihrem lokalen HTTP, die ein exaktes Replikat von **downloads.dell.com** darstellt.
2. Laden Sie das Paket **catalog.xml.gz** der Online-HTTP-Site vom Speicherort **http://downloads.dell.com/catalog/catalog.xml.gz** herunter, und extrahieren Sie die darin 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**.
Ändern Sie beispielsweise den Eintrag für **baseLocation** von **downloads.dell.com** in **hostname.com**.
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

So zeigen Sie die Aktualisierungsquelle an:

1. Klicken Sie in **DLCI for SCVMM** auf **Wartungcenter**.
2. Klicken Sie im **Wartungcenter** auf **Wartungseinstellungen** und dann auf **Aktualisierungsquelle**.

Erstellen einer Aktualisierungsquelle

Voraussetzungen:

- Je nach Typ der Aktualisierungsquelle ist ein Windows- oder ein FTP-Anmeldeprofil erforderlich.
- Wenn Sie eine DRM-Aktualisierungsquelle erstellen möchten, stellen Sie sicher, dass DRM installiert ist und die Administratorrollen konfiguriert sind.

So erstellen Sie eine Aktualisierungsquelle:

1. Klicken Sie im **DLCI-Konsolen-Add-In für SCVMM** auf **Wartungcenter** und dann auf **Wartungseinstellungen**.
2. Klicken Sie bei **Aktualisierungsquelle** auf **Neu erstellen**, und machen Sie die erforderlichen Angaben.
 - 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.
 - Wenn Sie eine DRM-Quelle erstellen möchten, geben Sie Ihre Windows-Anmeldeinformationen an, und stellen Sie sicher, dass der freigegebene Windows-Speicherort zugreifbar ist. Geben Sie in das Feld für den Speicherort den vollständigen Pfad zur Katalogdatei mit dem Dateinamen ein.
3. (Optional) Um die Aktualisierungsquelle als Standardquelle zu verwenden, wählen Sie die Option **Als Standardquelle festlegen** aus.
4. Klicken Sie auf **Verbindung testen**, um den Speicherort der Aktualisierungsquelle zu verifizieren, und klicken Sie dann auf **Speichern**.

 **ANMERKUNG: Verwenden Sie nur 32-Bit-DUPs zur Erstellung der Aktualisierungsquelle in DRM.**

- 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.

 **ANMERKUNG: Nachdem der Speicherort verifiziert wurde, können Sie die Aktualisierungsquelle erstellen.**

Ändern einer Aktualisierungsquelle

Berücksichtigen Sie Folgendes, wenn Sie eine Aktualisierungsquelle ändern möchten:

- Nach Erstellung einer Aktualisierungsquelle können Typ und Speicherort nicht mehr geändert werden.
- Sie können eine Aktualisierungsquelle selbst dann ändern, wenn sie gerade von einem anderen Prozess, von einem geplanten Job oder in einer Bereitstellungsvorlage verwendet wird. Beim Ändern einer derzeit in Verwendung befindlichen Aktualisierungsquelle wird eine Warnmeldung angezeigt. Klicken Sie auf **Bestätigen**, um mit den Änderungen fortzufahren.



So ändern Sie eine Aktualisierungsquelle:

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

Löschen der Aktualisierungsquelle

In den folgenden Fällen kann die Aktualisierungsquelle nicht gelöscht werden:

- Der Aktualisierungsquelle ist eine vordefinierte Aktualisierungsquelle – **Dell Online-Katalog** und **DELL ONLINE-HTTP-KATALOG**.
- Die Aktualisierungsquelle wird in einer Bereitstellungsvorlage verwendet.
- Die Aktualisierungsquelle wird von einem derzeit laufenden Job oder einem geplanten Job verwendet.
- Die Aktualisierungsquelle ist eine Standard-Aktualisierungsquelle.

So löschen Sie eine Aktualisierungsquelle:

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

Aktualisierungsgruppen

Aktualisierungsgruppen sind eine Zusammenfassung von Servern, die eine identische Aktualisierungsverwaltung erfordern. Es gibt zwei Typen von Aktualisierungsgruppen: vordefinierte und benutzerdefinierte Aktualisierungsgruppen. Sie können die vordefinierten Gruppen anzeigen, jedoch nur benutzerdefinierte Aktualisierungsgruppen erstellen und verwalten.

 **ANMERKUNG: Nach der Aktualisierung von DLCI for SCVMM Version 1.1 auf Version 1.2 werden alle zuvor ermittelten Server den Allgemeinen Aktualisierungsgruppen oder den Host-Aktualisierungsgruppen hinzugefügt. Um die Server der jeweiligen vordefinierten Aktualisierungsgruppe hinzuzufügen, ermitteln Sie die Server erneut.**

Vordefinierte Aktualisierungsgruppen

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

- **Allgemeine Aktualisierungsgruppen**
 - **Alle Aktualisierungsgruppen**
 - **Standardmäßige, nicht zugewiesene Server-Aktualisierungsgruppen**
- **Cluster-Aktualisierungsgruppen**
- **Host-Aktualisierungsgruppen**
 - **Standard-Host-Aktualisierungsgruppen**
- **Gehäuse-Aktualisierungsgruppen**

Allgemeine Aktualisierungsgruppen – Diese Gruppe besteht aus Hosts und nicht zugewiesenen Servern, die in einer einzigen Sitzung aktualisiert werden.

Alle Aktualisierungsgruppen – Diese Gruppe besteht aus allen Servergruppen. Jede auf dem Gerät vorhandene Gruppe gehört dieser Gruppe an. Diese Gruppe ist vom Typ „Allgemeine Aktualisierungsgruppe“.

Standardmäßige, nicht zugewiesene Server-Aktualisierungsgruppe – Diese Gruppe besteht aus allen nicht zugewiesenen Servern, die keiner anderen Gruppe angehören. Diese Gruppe ist vom Typ „Allgemeine Aktualisierungsgruppe“. Die Server werden nach folgenden Ereignissen der standardmäßigen, nicht zugewiesenen Server-Aktualisierungsgruppe hinzugefügt:

- Ermittlung oder erneute Ermittlung von Bare Metal-Servern
- Synchronisierung oder erneute Synchronisierung, nach dem Löschen aus SCVMM (jedoch auf dem Gerät vorhanden)

Cluster-Aktualisierungsgruppe – Diese Gruppe besteht aus Windows Server Failover-Clustern. Gehört ein modularer Server einem Cluster an, wird er der Cluster-Aktualisierungsgruppe hinzugefügt. Gehört ein modularer Dell PowerEdge-Server der 12. oder 13.

Generation einem Cluster an, werden außerdem die CMC-Informationen zur Bestandsaufnahme auf der Seite **Wartungcenter** hinzugefügt.

Um herauszufinden, welcher Cluster-Aktualisierungsgruppe ein Server angehört, rufen Sie die Seite „Gerätebestandsaufnahme“ auf. Dort werden der Host-Name und der Cluster-FQDN aller auf dem Gerät aufgeführten Server angezeigt.

Host-Aktualisierungsgruppe – Diese Gruppe besteht aus Host-Servern. Aktualisierungen werden in einer einzigen Sitzung angewendet, d. h. alle Server innerhalb der Gruppe werden zusammen aktualisiert.

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 einem Gehäuse und keiner Cluster-Gruppe angehören. Dell PowerEdge-Server der 12. oder 13. Generation werden zusammen mit ihren CMC-Informationen ermittelt. Standardmäßig wird die Gruppe im Namensformat **Chassis-Service-tag-of-Chassis-Group** erstellt, z. B. `Chassis-GJDC4BS-Group`. Wird ein modularer Server aus einer Cluster-Aktualisierungsgruppe gelöscht, wird der Server zusammen mit den CMC-Informationen der Gehäuse-Aktualisierungsgruppe hinzugefügt. Auch wenn keine modularen Server in der entsprechenden Gehäuse-Aktualisierungsgruppe vorhanden sind, existiert diese weiterhin, da alle modularen Server des Gehäuses einer Cluster-Aktualisierungsgruppe angehören. Es werden jedoch lediglich die CMC-Informationen angezeigt.

Benutzerdefinierte Aktualisierungsgruppen

Sie können benutzerdefinierte Aktualisierungsgruppen erstellen, ändern und löschen. Sie können ihnen jedoch nur Server hinzufügen, die aus den **Standardmäßigen, nicht zugewiesenen Aktualisierungsgruppen** und den **Standard-Host-Aktualisierungsgruppen** stammen. Nachdem Sie einen Server zu einer benutzerdefinierten Aktualisierungsgruppe hinzugefügt haben, ist dieser nicht mehr in der vordefinierten Aktualisierungsgruppe enthalten und nur noch in der benutzerdefinierten Aktualisierungsgruppe verfügbar. Wenn Sie Server zu einer benutzerdefinierten Aktualisierungsgruppe hinzuzufügen möchten, machen Sie sie anhand ihrer Service-Tag-Nummer ausfindig.

Aktualisierungsmethoden

Sie können ausgewählte Aktualisierungen auf ausgewählte kompatible Servergruppen anwenden.

- Sie können die folgenden Aktualisierungen auf Servergruppen anwenden:
 - **Agentenlose, stufenweise Aktualisierung** – Die Firmware-Aktualisierung erfolgt stufenweise. 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 nächsten Neustart des Servers angewendet. Die Aktualisierungen werden unter Verwendung von iDRAC zur jeweils geplanten Uhrzeit stapelweise durchgeführt. Die Stapelgröße wird bei der Durchführung der Aktualisierung festgelegt. Aktualisieren Sie die Bestandsaufnahme, um zu überprüfen, ob alle Aktualisierungen angewendet wurden. Der gesamte Aktualisierungsjob schlägt fehl, sobald der Vorgang auf einem einzigen Server misslingt.
 - **Agentenlose Aktualisierung** – Eine bandexterne Aktualisierung mit sofortigem Neustart des Servers.
 - **Clusterfähiges Aktualisieren (CAU)** – Automatisierung des Aktualisierungsvorgangs unter Verwendung der Windows-CAU-Funktion auf Cluster-Aktualisierungsgruppen zur Aufrechterhaltung der Serververfügbarkeit. Aktualisierungen auf den Servern erfolgen über einen Cluster-Aktualisierungskoordinator, der auf demselben System vorhanden ist, auf dem auch Integration Gateway (IG) installiert ist, und nicht über iDRAC. Die Aktualisierungen werden nicht stufenweise sondern sofort angewendet. Mit CAU können Sie Unterbrechungen oder Serverausfallzeiten minimieren und eine kontinuierliche Verfügbarkeit der Arbeitslast sicherstellen. Der von der Cluster-Gruppe bereitgestellte Dienst wird daher nicht beeinträchtigt. Weitere Informationen zu CAU finden Sie im Abschnitt über clusterfähiges Aktualisieren unter technet.microsoft.com.

Anmerkungen zu Aktualisierungsgruppen

- Sie können vordefinierte Aktualisierungsgruppen nicht manuell erstellen, ändern oder löschen.
- Sie können die CMC-Firmware nicht direkt über das Gerät aktualisieren. Sie können jedoch die Firmware des im CMC vorhandenen modularen Servers aktualisieren. Informationen zum Aktualisieren des CMC finden Sie unter „Aktualisieren der CMC-Firmware“ im CMC-Benutzerhandbuch *Dell PowerEdge M1000e Chassis Management Controller Firmware User's Guide*.



Informationen zum Aktualisieren des CMC in VRTX finden Sie unter „Aktualisieren der Firmware“ im CMC-VRTX-Benutzerhandbuch *Dell Chassis Management Controller for Dell PowerEdge VRTX User's Guide*. Informationen zum Aktualisieren des CMC in FX2 finden Sie unter „Aktualisieren der Firmware“ im CMC-FX2-Benutzerhandbuch *Dell Chassis Management Controller for Dell PowerEdge FX2 User's Guide*.

Anzeigen von Aktualisierungsgruppen

So zeigen Sie Aktualisierungsgruppen an:

1. Klicken Sie in **DLCI for SCVMM** auf **Wartungcenter** und dann auf **Wartungseinstellungen**.
2. Klicken Sie bei den **Wartungseinstellungen** auf **Aktualisierungsgruppen**.

Erstellen von benutzerdefinierten Aktualisierungsgruppen

So erstellen Sie eine benutzerdefinierte Aktualisierungsgruppe:

1. Klicken Sie in **DLCI for SCVMM** auf **Wartungcenter** und dann auf **Wartungseinstellungen**.
2. Klicken Sie bei den **Wartungseinstellungen** auf **Aktualisierungsgruppen** und dann auf **Erstellen**. Die Seite **Firmware-Aktualisierungsgruppe** wird angezeigt.
3. Geben Sie die Details an, und wählen Sie den Typ der zu erstellenden Aktualisierungsgruppe aus. In benutzerdefinierten Aktualisierungsgruppen können nur Server der folgenden Aktualisierungsgruppentypen enthalten sein:
 - Allgemeine Host-Aktualisierungsgruppe – Diese Gruppe besteht aus Servern aus standardmäßigen, nicht zugewiesenen Aktualisierungsgruppen und Host-Aktualisierungsgruppen.
 - Host-Aktualisierungsgruppe – Diese Gruppe besteht aus Servern aus Standard-Host-Aktualisierungsgruppen.
4. Wenn Sie Server zu einer Aktualisierungsgruppe hinzuzufügen möchten, machen Sie sie anhand ihrer Service-Tag-Nummer auffindig, und klicken Sie auf **Speichern**.

Ändern von benutzerdefinierten Aktualisierungsgruppen

Berücksichtigen Sie Folgendes, wenn Sie eine benutzerdefinierte Aktualisierungsquelle modifizieren möchten:

- Der Typ einer Aktualisierungsgruppe kann nach der Erstellung nicht mehr geändert werden.
- So verschieben Sie Server zwischen zwei benutzerdefinierten Aktualisierungsgruppen:
 - Entfernen Sie den Server aus der vorhandenen benutzerdefinierten Aktualisierungsgruppe. Er wird automatisch der vordefinierten Aktualisierungsgruppe hinzugefügt.
 - Bearbeiten Sie jetzt die benutzerdefinierte Gruppe, zu der der Server hinzugefügt wird, und suchen Sie anschließend anhand der Service-Tag-Nummer nach dem Server.

So ändern Sie eine benutzerdefinierte Aktualisierungsgruppe:

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

Löschen von benutzerdefinierten Aktualisierungsgruppen

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 löschen, auch wenn Server darin vorhanden sind. Nach dem Löschen der Aktualisierungsgruppe werden die Server allerdings in ihre jeweilige vordefinierte Aktualisierungsgruppe verschoben.

So löschen Sie eine benutzerdefinierte Aktualisierungsgruppe:

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

Anwenden von Aktualisierungen auf Server

Sie können Aktualisierungen entweder sofort anwenden oder die Aktualisierungen auf Server oder Servergruppen durch Erstellen eines Firmware-Aktualisierungsjobs planen. Die für Aktualisierungen erstellten Jobs sind auf der Seite **Jobs und Protokollcenter** aufgeführt. Sie können außerdem die Firmware-Version auf die vorgeschlagene Version zurückstufen, indem Sie **Zurückstufen zulassen** auswählen. Ist diese Option nicht markiert, wird für Komponenten, die eine Zurückstufung erfordern, keine Maßnahme durchgeführt.

ANMERKUNG:

- Sie können Firmware-Aktualisierungen auf eine einzelne Komponente eines Servers anwenden oder auf die gesamte Umgebung.
- Wenn für einen Server oder eine Servergruppe keine anwendbaren Upgrades oder Downgrades verfügbar sind, hat die Durchführung einer Firmware-Aktualisierung keine Auswirkung auf den Server bzw. die Servergruppe.
- 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.

Voraussetzungen:

- Um Aktualisierungen auf Servern durchzuführen, benötigen Sie verfügbare Aktualisierungsquellen auf einer Dell Online-FTP-Site, einer lokalen FTP-Site, einer HTTP-Site oder Dell Repository Manager (DRM).
- Löschen Sie vor dem Anwenden der Aktualisierungen die iDRAC Job-Warteschlange auf den Servern, auf denen die Aktualisierungen angewendet werden.
- Stellen Sie sicher, dass der IG-Benutzer über lokale Administratorrechte auf allen Cluster-Knoten verfügt.
- 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.
 - Validieren Sie die konfigurierten Optionen für das Ausführen von Aktualisierungen. Weitere Informationen finden Sie im Abschnitt mit den Voraussetzungen und bewährten Verfahren für clusterfähiges Aktualisieren (CAU) unter technet.microsoft.com.
 - 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.

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

So wenden Sie Aktualisierungen auf Servern an:


1. Klicken Sie im DLCI-Konsolen-Add-In für SCVMM auf **Wartungcenter**, wählen Sie den Server oder die Servergruppe sowie eine Aktualisierungsquelle aus, und klicken Sie anschließend auf **Aktualisierung ausführen**.

ANMERKUNG:

- 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 Dell PowerEdge-Server der 11. Generation kann die Firmware-Version der Netzteileneinheit nicht aktualisiert werden.
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:



- **Jetzt ausführen** – Die Aktualisierungen werden sofort angewendet.
 - Wählen Sie das Datum und die Uhrzeit für die Planung einer künftigen Firmware-Aktualisierung aus.
4. Wählen Sie die Aktualisierungsmethode **Agentenfreie Aktualisierung** oder **Agentenfreie, stufenweise Aktualisierung** aus, und klicken Sie anschließend auf **Fertigstellen**.

 **ANMERKUNG:** Nach dem Senden eines Firmware-Aktualisierungsjobs an den iDRAC interagiert das Gerät mit dem iDRAC, um den Status des Jobs zu ermitteln, und zeigt Statusaktualisierungen auf der Seite Jobs und Protokolle in der Verwaltungskonsole an. In manchen Fällen macht iDRAC keine Angaben zu Statusaktualisierungen für die vom Gerät verfolgten Jobs. Das Gerät wartet maximal 6 Stunden auf eine Antwort des iDRAC. Bleibt diese aus, wird der Job-Status der Firmware-Aktualisierung als fehlgeschlagen betrachtet.

Abfrage und Benachrichtigung

Sie können das System so konfigurieren, dass Sie benachrichtigt werden, wenn neue Kataloge für vom System generierte und für Standard-Aktualisierungsquellen verfügbar sind.

Die Farbe der Benachrichtigungsglocke wechselt auf orange, wenn eine neue Katalogdatei an der Aktualisierungsquelle verfügbar ist. Klicken Sie auf das Glockensymbol, um den im lokalen Cache enthaltenen Katalog durch den an der Aktualisierungsquelle verfügbaren Katalog zu ersetzen. Nachdem die alten Kataloge durch die neuesten ersetzt wurden, wechselt die Farbe der Glocke auf grün.

Einstellen von Benachrichtigungen

So stellen Sie die Abfragehäufigkeit ein:

1. Klicken Sie in **DLCI for SCVMM** auf **Wartungszentrum**, dann auf **Wartungseinstellungen** und schließlich auf **Abfrage und Benachrichtigung**.
2. Wählen Sie aus, wie häufig die Abfrage stattfinden soll:
 - **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.
 - **Einmal pro Woche** – Wählen Sie diese Option aus, um einmal pro Woche Aktualisierungen für neue Kataloge, die an der Aktualisierungsquelle verfügbar sind, zu erhalten.
 - **Einmal alle 2 Wochen** – Wählen Sie diese Option aus, um alle zwei Wochen Aktualisierungen für neue Kataloge, die an der Aktualisierungsquelle verfügbar sind, zu erhalten.
 - **Einmal pro Monat** – Wählen Sie diese Option aus, um einmal pro Monat Aktualisierungen für neue Kataloge, die an der Aktualisierungsquelle verfügbar sind, zu erhalten.

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 der Schutz-Vault zugreifbar ist.

So erstellen Sie einen Schutz-Vault:

1. Klicken Sie in **DLCI for SCVMM** auf **Wartungszentrum** und dann auf **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 erforderlichen Details an.
 - Wenn Sie einen Schutz-Vault vom Typ **Netzwerkfreigabe** erstellen möchten, geben Sie den Speicherort zum Speichern der Profile, Anmeldeinformationen für den Zugriff auf diesen Speicherort und eine Passphrase für die Sicherheit der Profile an. Dieser Schutz-Vault-Typ unterstützt die CIFS-Dateifreigabe (Common Internet File System).

- 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

Berücksichtigen Sie Folgendes, wenn Sie einen Schutz-Vault ändern möchten:

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

So ändern Sie einen Schutz Vault:

1. Klicken Sie in **DLCI for SCVMM** auf **Wartungszentrum** und dann auf **Wartungseinstellungen**.
2. Klicken Sie im **Wartungszentrum** auf **Schutz-Vault** und anschließend auf **Bearbeiten**, um den Vault zu modifizieren.

Löschen eines Schutz-Vaults

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

- Der Schutz-Vault ist einem Server oder einer Gruppe von Servern zugeordnet.
- Es ist ein geplanter Job mit dem Schutz-Vault verbunden. In dem Fall können Sie jedoch den geplanten Job löschen und danach den Schutz-Vault.

1. Klicken Sie in **DLCI for SCVMM** auf **Wartungszentrum** und dann auf **Wartungseinstellungen**.
2. Klicken Sie im **Wartungszentrum** auf **Schutz-Vault** und anschließend auf **Löschen**, um den Vault zu löschen.

Teilersetzung

Die Teilersetzungsfunktion aktualisiert automatisch eine ersetzte Serverkomponente auf die erforderliche Firmware-Version oder die Konfiguration der alten Komponente oder beides. Die Aktualisierung wird automatisch ausgeführt, wenn Sie Ihr System nach dem Ersetzen der Komponente neu starten.

Die folgenden Optionen werden unterstützt:

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



- **Ändern Sie nicht den Wert auf dem Server** - Die vorhandene Konfiguration wird beibehalten.

Anwenden von Firmware- und Konfigurationseinstellungen

So legen Sie die Parameter für die Teilersetzung fest:

1. Wählen Sie im **DLCI-Konsolen-Add-In für SCVMM** unter **Wartungszentrum** die Server oder Servergruppe aus, und klicken Sie dann auf **Teilersetzung konfigurieren**.
Das Fenster **Teilersetzung konfigurieren** wird angezeigt.
2. Legen Sie die Werte für **CSIOR**, **Teile-Firmware-Aktualisierung** und **Teile-Konfigurationsaktualisierung** fest, und klicken Sie dann auf **Fertigstellen**.

Erfassung von Lifecycle Controller-Protokollen

LC-Protokolle liefern Aufzeichnungen über vergangene Aktivitäten auf einem verwalteten System. Diese Protokolldateien sind für die Serveradministratoren nützlich, da sie detaillierte Informationen zu empfohlenen Maßnahmen und andere technische Informationen enthalten, die für die Fehlerbehebung nützlich sind.

Die verschiedenen Arten von Informationen in LC-Protokollen sind Warnhinweise, Konfigurationsänderungen an den System-Hardwarekomponenten, Firmware-Änderungen aufgrund eines Upgrades oder Downgrades, Ersatzteile, Temperaturwarnungen, detaillierte Zeitstempel über den Beginn der Aktivität, Schweregrad der Aktivität und so weiter.

Es gibt zwei Möglichkeiten, LC-Protokolle zu erfassen:

- **Aktive LC-Protokolle** - Das sind die letzten LC-Protokolldateien. Sie können diese Protokolldateien anzeigen, durchsuchen und in die Appliance exportieren. Sie können einen Auftrag planen, um die LC-Protokolle auf der Appliance oder einer Netzwerkfreigabe zu erfassen. Außerdem können Sie eine Sicherung der Protokolldatei in der Netzwerkfreigabe speichern.
- **Vollständige LC-Protokolle** - Diese Protokolle enthalten aktive und archivierte LC-Protokolldateien. Sie sind groß und werden daher im `.gz`-Format komprimiert und an den angegebenen Speicherort auf CIFS-Netzwerkfreigabe exportiert.

Erfassen von LC-Protokollen

1. Wählen Sie im **DLCI-Konsolen-Add-In für SCVMM** unter **Wartungszentrum** einen Server oder eine Servergruppe aus, und klicken Sie dann auf **LC-Protokolle erfassen**.
2. Wählen Sie in **LC-Protokollerfassung** eine der folgenden Optionen aus und klicken Sie auf **Fertigstellen**.
 - **Vollständige LC-Protokolle (.gz) exportieren** - Die aktiven und archivierten LC-Protokolle werden nach Angabe der Windows-Anmeldeinformationen in eine CIFS-Netzwerkfreigabe exportiert.

ANMERKUNG:

- Stellen Sie sicher, dass der freigegebene Ordner über ausreichend Speicherplatz zum Speichern der vollständigen LC-Protokolle verfügt, da es sich um große Dateien handelt.
- Das Exportieren vollständiger LC-Protokolle wird für Dell PowerEdge-Servern der 11. Generation nicht unterstützt.
- LC-Protokolle werden im folgenden Format gespeichert: `<YYYYMMDDHHMMSSSS>.<file format>`.
So ist beispielsweise `201607201030010597.xml.gz` der Name der LC-Datei, der das Datum und die Uhrzeit der Dateierstellung enthält.
- **Aktive Protokolle exportieren (Jetzt ausführen)** - Wählen Sie diese Option aus, um die aktiven Protokolle sofort in die Appliance zu exportieren.
 - (Optional) Aktivieren Sie die Option **LC-Protokolle auf der Netzwerkfreigabe sichern**, um eine Sicherungskopie der LC-Protokolle nach Angabe der Windows-Anmeldeinformationen auf der CIFS-Netzwerkfreigabe zu speichern.
- **ANMERKUNG: Stellen Sie sicher, dass Sie die neuesten Versionen von iDRAC und LC aktualisieren, bevor Sie die aktiven LC-Protokolle für Dell PowerEdge-Server der 11. Generation exportieren.**
- **LC-Protokollerfassung planen** - Wählen Sie ein Datum, eine Uhrzeit und eine Häufigkeit für den Export der aktiven LC-Protokolle aus.
 - (Optional) Aktivieren Sie die Option **LC-Protokolle auf der Netzwerkfreigabe sichern**, um eine Sicherungskopie der LC-Protokolle nach Angabe der Windows-Anmeldeinformationen auf der CIFS-Netzwerkfreigabe zu speichern.

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

- **Nie** – Wählen Sie diese Option aus, um die LC-Protokolle nur einmal zur geplanten Zeit zu exportieren.
- **Täglich** – Wählen Sie diese Option aus, um die LC-Protokolle täglich zur geplanten Zeit zu exportieren.
- **Einmal pro Woche** – Wählen Sie diese Option aus, um die LC-Protokolle einmal pro Woche zur geplanten Zeit zu exportieren.
- **Einmal alle 4 Wochen** – Wählen Sie diese Option aus, um die LC-Protokolle alle vier Wochen zur geplanten Zeit zu exportieren.

 **ANMERKUNG: Die exportierte LC-Protokolldatei wird unter einem Ordernamen 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.

1. Wählen Sie im **DLCI-Konsolen-Add-In für SCVMM** unter **Wartungszentrum** einen Server oder eine Servergruppe aus, und klicken Sie dann auf **LC-Protokolle anzeigen**.
Alle Server in der ausgewählten Gruppe und die Server, für welche LC-Protokolle erfasst werden, werden mit ihren LC-Protokolldateien aufgelistet.
2. Klicken Sie auf den Dateinamen, um alle Protokolleinträge in der LC-Protokolldatei speziell für diesen Server anzuzeigen.
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 der LC-Datei gibt es zwei Möglichkeiten:

- Klicken Sie auf den Dateinamen, öffnen Sie die LC-Protokolldatei und suchen Sie eine Beschreibung im Suchfeld.
- Geben Sie eine Beschreibung in das Suchfeld ein, und zeigen Sie dann alle LC-Dateien mit den Instanzen der folgenden Beschreibung an.

 **ANMERKUNG:**

- Wenn die Beschreibung der LC-Protokollmeldung lang ist, wird die Meldung auf 80 Zeichen gekürzt.
- Die neben der LC-Protokollmeldung angezeigte Zeit folgt der iDRAC-Zeitzone.
- Fügen Sie vor dem Herunterladen der LC-Protokolle das Gerät auf der Site **Lokales Intranet** hinzu.

So fügen Sie das Gerät auf der Site **Lokales Intranet** hinzu:

- a. Öffnen Sie **Internet Explorer**, klicken Sie auf **Extras** und dann auf **Internetoptionen**.
- b. Klicken Sie auf **Sicherheit**, wählen Sie **Lokales Intranet** aus, und klicken Sie dann auf **Sites**. Die Seite **Lokales Intranet** wird angezeigt.
- c. Klicken Sie auf **Erweitert**, geben Sie die Appliance-URL ein, und klicken Sie auf **Hinzufügen**.

Exportieren der Bestandsaufnahme

In DLCI for SCVMM können Sie die Bestandsaufnahme ausgewählter Server und Servergruppen in eine Datei im XML- oder CSV-Format exportieren. Sie können diese Informationen in einem freigegebenen Windows-Verzeichnis oder auf einem Verwaltungssystem speichern. Sie haben außerdem die Möglichkeit, die XML-Datei in DRM zu importieren, um auf der Grundlage der Bestandsaufnahme eine Repository und eine Referenzkonfiguration zu erstellen.

Wenn Sie Internet Explorer Version 10 und höher verwenden und die Firmware-Bestandsaufnahme der Server oder Servergruppen exportieren möchten, fügen Sie die IP-Adresse des Konsolen-Add-Ins zur Site **Lokales Intranet** hinzu. Vor dem Exportieren der Bestandsaufnahme führen Sie folgende Schritte durch:


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**.



Wenn Sie nur die Komponenteninformationen eines Servers auswählen und exportieren, werden die vollständigen Bestandsaufnahme-Informationen des Servers exportiert.

So exportieren Sie die Bestandsaufnahme der ermittelten Server:

1. Klicken Sie im **DLCI-Konsolen-Add-In für SCVMM** auf **Wartungszentrum**.
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.

 **ANMERKUNG:** Um ein Repository in DRM zu erstellen, führen Sie nach dem Exportieren der XML-Datei Folgendes durch:

1. Klicken Sie auf **Meine Repositories, Neu** und dann auf **Dell Modulargehäuse - Bestandsaufnahme**.
2. Geben Sie einen Namen und die Beschreibung im Abschnitt **Basisrepository** ein und klicken Sie auf **Weiter**.
3. Klicken Sie auf **Durchsuchen**, wählen Sie die exportierte Bestandsaufnahme-Datei aus der Appliance im Abschnitt **Modulargehäuse - Bestandsaufnahme** aus, und klicken Sie dann auf **Weiter**. Weitere Informationen zum Erstellen eines Repositories finden Sie in den Dokumenten zu *Dell Repository Manager* unter dell.com/support/home.

Anzeigen und Aktualisieren der Firmware-Bestandsaufnahme

Sie können die Firmware-Bestandsaufnahme kompatibler Dell Server anzeigen und aktualisieren, nachdem Sie einen Server oder eine bestimmte Gruppe von Servern ausgewählt haben.

Sie können einen Vergleichsreport der Server- oder Gehäusebestandsaufnahme mit einer ausgewählten Aktualisierungsquelle anzeigen. Sie können die Aktualisierungsquelle ändern und einen Vergleichsreport der Bestandsaufnahme-Informationen der ausgewählten Server, Servergruppen oder Gehäuse mit der geänderten Aktualisierungsquelle anzeigen.

Sie können die Firmware-Bestandsaufnahme für einen Server, eine Servergruppe oder ein Gehäuse aktualisieren, um die neuesten Informationen anzuzeigen. Wenn Sie die Komponenteninformationen eines Servers aktualisieren, werden die kompletten Bestandsaufnahme-Informationen des Servers aktualisiert.

 **ANMERKUNG:**

- DLCI for SCVMM Version 1.2 wird mit einem Katalog geliefert, der eine frühere Version des Vergleichsreports für die vordefinierte FTP- und HTTP-Aktualisierungsquelle anzeigt. Laden Sie daher den neuesten Katalog herunter, um den neuesten Vergleichsreport anzuzeigen.
- Wenn Sie eine Aktualisierung auf diese Version von DLCI for SCVMM durchführen, werden die neuesten Informationen zu den Servern, die in früheren Versionen ermittelt wurden, nicht angezeigt. Um die neuesten Server-Informationen und einen korrekten Vergleichsreport zu erhalten, ermitteln Sie die Server erneut.

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

1. Wählen Sie im **DLCI-Konsolen-Add-In für SCVMM** unter **Wartungszentrum** eine Aktualisierungsgruppe bei **Aktualisierungsgruppe auswählen** aus.
2. (Optional) Um die Aktualisierungsquelle zu ändern, wählen Sie eine andere Aktualisierungsquelle bei **Aktualisierungsquelle auswählen** aus.
3. Um die Firmware-Informationen der aktuellen Version, die Grundlinienversion und die vom Gerät empfohlene Aktualisierungsmaßnahme anzuzeigen, erweitern Sie die Servergruppe bei **Gerätegruppe/Server** zunächst bis zur Serverebene und dann bis zur Komponentenebene.



ANMERKUNG:

Beim Anzeigen der Informationen auf Komponentenebene werden die NIC-bezogenen Informationen für PowerEdge-Server der 11. Generation wie folgt angezeigt:

- Nach dem Filtern nach **Aktualisierungsart** und Festlegen des Kriteriums **Dringend** wird ein Report angezeigt, der nur die Komponenten mit dringenden Aktualisierungen enthält. Wird dieser Report exportiert, werden auch Komponenten mit Zurückstufungsmaßnahmen, die wiederum kritische Aktualisierungen enthalten, exportiert.
- Wenn mehrere Netzwerkschnittstellen in einer einzigen NIC-Karte vorhanden sind, gibt es in der Liste der **Komponenteninformationen** nur einen Eintrag für alle Schnittstellen. Nachdem die Firmware-Aktualisierung angewendet wurde, werden alle NIC-Karten aktualisiert.
- Wird eine NIC-Karte zusammen mit den vorhandenen Karten hinzugefügt, wird die neu hinzugefügte NIC-Karte als weitere Instanz in der Liste der **Komponenteninformationen** aufgeführt. Nachdem die Firmware-Aktualisierung angewendet wurde, werden alle NIC-Karten aktualisiert.

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

Exportieren von Serverprofilen

Sie können ein Serverprofil exportieren, einschließlich der installierten Firmware-Images auf den verschiedenen Komponenten (wie BIOS, RAID, NIC, iDRAC, Lifecycle Controller) und einschließlich der Konfiguration dieser Komponenten. Das Gerät erstellt eine Datei, in der alle Konfigurationen enthalten sind, und die Sie dann auf einer vFlash SD-Karte oder einer Netzwerkfreigabe speichern können. Wählen Sie einen beliebigen Schutz-Vault aus, um diese Datei dort abzulegen. Sie können die Konfigurationsprofile für einen Server oder eine Servergruppe sofort exportieren, oder den Export für einen späteren Zeitpunkt planen. Außerdem besteht die Möglichkeit, eine Wiederholungsoption auszuwählen, um festzulegen, wie oft die Serverprofile exportiert werden sollen. Sie können gleichzeitig immer nur einen Job für den Export der Konfiguration einer Servergruppe planen. Während die Konfigurationsprofile eines Servers oder einer Servergruppe exportiert werden, können Sie keine andere Maßnahme an dem Server oder der Servergruppe durchführen.



ANMERKUNG:

- Stellen Sie sicher, dass der Job **Automatisches Backup** in iDRAC nicht zur gleichen Zeit geplant ist.
- Nach dem Anwenden von Filtern können keine Serverprofile exportiert werden. Löschen Sie alle aktivierten Filter, um die Serverprofile zu exportieren.

Erstellen eines Export-Jobs

So exportieren Sie die Serverkonfigurationen:

Voraussetzungen: Deaktivieren Sie die Option **F1/F2 Prompt on Error** (Bei Fehler F1/F2-Eingabeaufforderung) in den **BIOS-Einstellungen**.

1. Klicken Sie im **DLCI-Konsolen-Add-In für SCVMM** auf **Wartungszentrum** und dann auf **Serverprofil exportieren**.
2. Geben Sie bei **Profil exportieren** die Job-Details an, und wählen Sie einen Schutz-Vault aus.

Wählen Sie bei **Serverprofil exportieren** Folgendes aus:

- **Jetzt ausführen** – Bei Auswahl dieser Option wird die Serverkonfiguration der ausgewählten Server oder Gruppe von Servern sofort exportiert.
- **Zeitplan** – Legen Sie einen Zeitplan für das Exportieren der Serverkonfiguration der ausgewählten Gruppe von Servern fest.
 - **Nie** – Wählen Sie diese Option aus, um das Serverprofil nur einmal während der geplanten Zeit zu exportieren.
 - **Einmal pro Woche** – Wählen Sie diese Option aus, um das Serverprofil einmal pro Woche zu exportieren.
 - **Einmal alle 2 Wochen** – Wählen Sie diese Option aus, um das Serverprofil alle zwei Wochen zu exportieren.
 - **Einmal alle 4 Wochen** – Wählen Sie diese Option aus, um das Serverprofil alle vier Wochen zu exportieren.



Abbrechen eines Jobs für den Export der Serverkonfiguration

So brechen Sie einen Export-Job ab:

1. Klicken Sie im **DLCI-Konsolen-Add-In für SCVMM** auf **Wartungszentrum** und dann auf **Jobs verwalten**.
2. Wählen Sie im Filter **Export- und Import-Jobs** aus, wählen Sie die zu löschenden Jobs aus, und stellen Sie sicher, dass sich diese im Zustand **Geplant** befinden.
3. Klicken Sie auf **Abbrechen** und anschließend auf **Ja**.

Importieren von Serverprofilen

Sie können ein Serverprofil importieren, das zuvor für den gleichen Server oder die gleiche Gruppe von Servern exportiert wurde. Das Importieren eines Serverprofils bietet sich an, wenn Konfiguration und Firmware des Servers entsprechend dem im Profil gespeicherten Zustand wiederhergestellt werden sollen. In einem solchen Fall können Sie das Serverprofil auf dem Server oder auf der Gruppe von Servern ersetzen, indem Sie das zuvor exportierte Profil wieder importieren.

Es gibt zwei Möglichkeiten, Serverprofile zu importieren:

- Schnellimport des Serverprofils – Diese Option ermöglicht Ihnen den automatischen Import des zuletzt für diesen Server exportierten Serverprofils. Sie müssen für diesen Vorgang keine bestimmten Serverprofile für den Server auswählen.
- Benutzerdefinierter Import des Serverprofils – Mit dieser Option 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 nur für diesen Server ein Serverprofil aus der Liste der exportierten Serverprofile auswählen. Ein und dasselbe Serverprofil kann nicht für unterschiedliche Server oder Servergruppen importiert werden. Wenn Sie versuchen, das Serverprofil eines anderen Servers oder einer anderen Servergruppe zu importieren, schlägt der Import-Job fehl.
- Falls für einen bestimmten Server oder eine Gruppe von Servern kein Serverprofil-Image verfügbar ist und für diesen Server bzw. diese Servergruppe ein Job zum Importieren eines Serverprofils initiiert wird, schlägt dieser Job fehl. Im Aktivitätsprotokoll wird eine Protokollmeldung mit Einzelheiten zu dem Fehler hinzugefügt.
- Wenn nach dem Exportieren eines Serverprofils Komponenten aus dem Server entfernt und anschließend ein Job zum Importieren des Profils gestartet wird, werden alle Komponenteninformationen wiederhergestellt, mit Ausnahme der Informationen zu den fehlenden Komponenten (diese werden übersprungen). Diese Informationen sind nicht im Aktivitätsprotokoll des DLCI for SCVMM verfügbar. Weitere Angaben zu den fehlenden Komponenten finden Sie im iDRAC **LifeCycle-Protokoll**.
- Nach dem Anwenden von Filtern können keine Serverprofile importiert werden. Löschen Sie alle aktivierten Filter, um die Serverprofile zu importieren.

Importieren von Serverprofilen

So importieren Sie die Bestandsaufnahme von ermittelten Servern:

1. Wählen Sie in **DLCI for SCVMM** unter **Wartungszentrum** die Server aus, deren Profile Sie importieren möchten, und klicken Sie auf **Serverprofil importieren**.
2. Geben Sie die erforderlichen Details ein, wählen Sie den **Typ des Serverprofilimports** aus, und klicken Sie anschließend auf **Fertigstellen**.



ANMERKUNG: Deaktivieren Sie die Option Daten beibehalten, wenn Sie die derzeitigen RAID-Konfigurationen des Servers nicht beibehalten möchten.

Verwalten von Jobs

Sämtliche Jobs für die Firmware-Aktualisierung und den Export und Import von Serverkonfigurationen werden mit ihren jeweiligen Statusinformationen aufgeführt. Sie können nur die geplanten Jobs abbrechen.

Abbrechen eines Jobs für die Firmware-Aktualisierung

Voraussetzungen: Stellen Sie sicher, dass sich der Job im Zustand **Geplant** befindet.

So brechen Sie einen geplanten Firmware-Aktualisierungs-Job ab:

1. Klicken Sie in **DLCI for SCVMM** auf **Wartungszentrum** und dann auf **Jobs verwalten**.
2. Wählen Sie die Jobs aus, die Sie abbrechen möchten, klicken Sie auf **Abbrechen** und anschließend auf **Ja**.



Profile und Vorlagen

Info zu Anmeldeprofilen

Anmeldeprofile vereinfachen die Verwendung und Verwaltung von Benutzer-Anmeldeinformationen durch Authentifizierung der rollenbasierten Fähigkeiten des Benutzers. Jedes Anmeldeprofil enthält einen Benutzernamen und ein Kennwort für einen einzelnen Benutzer. Durch das Anmeldeprofil werden die rollenbasierten Fähigkeiten des Benutzers authentifiziert. Das Gerät verwendet Anmeldeprofile, um die Verbindung zum iDRAC der verwalteten Systeme herzustellen.

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:

- Wenn kein Standardprofil erstellt oder ausgewählt wurde, wird die werksseitige iDRAC-StandardEinstellung verwendet. Der Standardbenutzername ist `root` und das Kennwort lautet `calvin`.
 - * Das Standard-iDRAC-Profil wird für den Zugriff auf den Server verwendet, wenn Sie einen Server ermitteln oder eine Synchronisierung durchführen.
- Das Standard-CMC-Profil verwendet den Benutzernamen `root` und das Kennwort `calvin`. Es wird verwendet, um Zugriff auf den modularen Server zu erhalten, um Informationen über das Gehäuse abzurufen.
- Verwenden Sie das Geräte-Anmeldeprofil zum Ermitteln von Servern, Anmelden am CMC, Beheben von Synchronisierungsproblemen und zum Bereitstellen des Betriebssystems.
- Windows-Anmeldeprofil – Dieses Profil wird für den Zugriff auf Windows-Freigaben während der Erstellung einer DRM-Aktualisierungsquelle verwendet.
- FTP-Anmeldeprofil – Dieses Profil wird für den Zugriff auf die FTP-Site verwendet.
- 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** ist ein vordefiniertes Anmeldeprofil vom Typ FTP-Anmeldeinformationen, dessen **Benutzername** und **Kennwort** `anonym` sind. Es ist nicht editierbar. Das Profil wird für den Zugriff auf `ftp.dell.com` verwendet.

Erstellen eines Anmeldeprofils

Berücksichtigen Sie Folgendes, wenn Sie ein Anmeldeprofil erstellen möchten:

- Wenn ein Geräte-Anmeldeprofil erstellt wird, wird ein zugehöriges **„Ausführen als“-Konto** in **SCVMM** zur Verwaltung des Servers angelegt. Der Name dieses Kontos ist `Dell_CredentialProfileName`.
 - (Empfohlen) Bearbeiten oder löschen Sie das **„Ausführen als“-Konto** nicht.
- Wenn keine Anmeldeprofile erstellt wurden und kein Standard-Anmeldeprofil für iDRAC verfügbar ist, wird während der automatischen Ermittlung das werksseitig eingestellte iDRAC-Standard-Anmeldeprofil verwendet. Der Standard-Benutzername lautet **root** und das Kennwort **calvin**.

So erstellen Sie ein Anmeldeprofil:

1. Führen Sie im DLCI-Konsolen-Add-In für SCVMM einen der folgenden Schritte aus:
 - Klicken Sie im Dashboard auf **Anmeldeprofil erstellen**.
 - Klicken Sie im Navigationsbereich auf **Profile und Vorlagen** → **Anmeldeprofil**, und klicken Sie dann auf **Erstellen**.
2. Wählen Sie unter **Anmeldeprofil** den gewünschten Anmeldeprofiltyp aus, geben Sie die Benutzer-Anmeldeinformationen ein, und klicken Sie anschließend auf **Fertigstellen**.

 **ANMERKUNG: Wählen Sie bei der Erstellung des Geräte-Anmeldeprofils die Option iDRAC aus, um es als Standardprofil für iDRAC festzulegen, oder wählen Sie CMC aus, um es als Standardeinstellung für den Chassis Management Controller (CMC) festzulegen. Wählen Sie Keines aus, wenn das Profil nicht als Standardprofil verwendet werden soll.**

Ändern eines Anmeldeprofils

Berücksichtigen Sie Folgendes, wenn Sie ein Anmeldeprofil ändern möchten:

- Nach der Erstellung können Sie den Typ eines Anmeldeprofils nicht mehr ändern. Sie können jedoch Änderungen an anderen Feldern vornehmen. Aktualisieren Sie den Bildschirm, um die Änderungen anzuzeigen.
- Sie können ein Geräte-Anmeldeprofil, das für die Hypervisor-Bereitstellung verwendet wird, nicht ändern.

So ändern Sie ein Profil mit Anmeldeinformationen:

Wählen Sie das Profil mit Anmeldeinformationen aus, das Sie ändern möchten, klicken Sie auf **Bearbeiten**, und aktualisieren Sie das Profil nach Bedarf.

Löschen eines Anmeldeprofils

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.
- Nachdem das **„Ausführen als“-Konto** aus SCVMM gelöscht wurde, ist das entsprechende Anmeldeprofil nicht mehr auf dem Gerät 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, löschen Sie zuerst die in der SCVMM-Umgebung bereitgestellten Server und anschließend das Anmeldeprofil.
- Sie können ein Anmeldeprofil, das in einer Aktualisierungsquelle verwendet wird, nicht löschen.

So löschen Sie ein Profil mit Anmeldeinformationen:

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

Erstellen eines Hardwareprofils

Sie können ein Hardwareprofil mithilfe eines Servers mit Gold-Konfiguration erstellen und dann dieses Profil zur Durchführung von Hardwarekonfigurationen auf verwalteten Systemen verwenden.

Bevor Sie Hardwarekonfigurationen auf verwaltete Systeme anwenden, stellen Sie sicher, dass die verwalteten Systeme bezüglich der folgenden Kriterien dem Server mit der goldenen Konfiguration entsprechen:

- Verfügbare Komponenten
- Servermodell
- RAID-Controller
- Festplatten:
 - Anzahl der Festplatten



- Größe der Festplatten
- Festplattentyp

 **ANMERKUNG:** Nachdem Sie eine Aktualisierung von DLCI for SCVMM Version 1.0.1 auf Version 1.2 durchgeführt haben, bearbeiten und speichern Sie die in DLCI for SCVMM Version 1.2 erstellten Hardwareprofile, bevor Sie sie auf Server anwenden.

So erstellen Sie ein Hardwareprofil:

1. Führen Sie auf der Seite für das DLCI-Konsolen-Add-In für SCVMM die folgenden Schritte aus:
 - Klicken Sie im Dashboard auf **Hardwareprofil erstellen**.
 - Klicken Sie im Navigationsfenster auf **Profile und Vorlagen** → **Hardwareprofil**, und klicken Sie anschließend auf **Erstellen**.
2. Klicken Sie auf dem Willkommensbildschirm für das **Hardwareprofil** auf **Weiter**.
3. Geben Sie unter **Profil** den Profilnamen und eine Beschreibung sowie die iDRAC-IP-Adresse des Referenzservers ein, und klicken Sie dann auf **Weiter**.
Die Hardware-Informationen des Referenzservers werden erfasst und als erforderliches Profil gespeichert. Während der Bereitstellung wird dieses Profil auf die Server angewendet.
4. Wählen Sie in **Profildetails** die BIOS-, Start- und RAID-Einstellungen aus, passen Sie DHS je nach Anforderung an, und klicken Sie anschließend auf **Weiter**.

 **ANMERKUNG:**

Unabhängig von Ihren Auswahl-Voreinstellungen werden alle Informationen während der Hardwareprofilerstellung gesammelt; während der Bereitstellung werden jedoch nur Ihre Voreinstellungen angewendet.

Beispiel: Wenn Sie eine RAID-Einstellung ausgewählt haben, werden alle Informationen über BIOS-, Start- und RAID-Einstellungen erfasst; während der Bereitstellung werden jedoch nur die RAID-Einstellungen angewendet.

Die in der **RAID-Konfiguration** aufgeführte Chipsatz-SATA-Controller-Konfiguration wird nicht unterstützt.

5. Klicken Sie unter **Zusammenfassung** auf **Fertigstellen**.
Sie können dieses Hardwareprofil verwenden und es auf die erforderlichen verwalteten Systeme anwenden.

Ändern eines Hardwarekonfigurationsprofils

Berücksichtigen Sie Folgendes, wenn Sie ein Hardwarekonfigurationsprofil ändern möchten:

- Sie können die BIOS-Einstellungen und die Startreihenfolge ändern.
- Bei PowerEdge-Servern der 11. und 12. Generation können Sie DHS für RAID in **Eines** oder **Keines** ändern. Bei PowerEdge-Servern der 13. Generation können Sie lediglich die vorhandenen RAID-Einstellungen des Servers beibehalten.

So bearbeiten Sie ein Hardwarekonfigurationsprofil:

1. Klicken Sie im DLCI-Konsolen-Add-In für SCVMM auf **Hardwareprofil**.
2. Wählen Sie das Profil aus, das Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.

 **ANMERKUNG:** Die in der RAID-Konfiguration aufgeführte Chipsatz-SATA-Controller-Konfiguration wird nicht unterstützt.

3. Nehmen Sie die erforderlichen Änderungen vor, und klicken Sie auf **Fertigstellen**.

Löschen eines Hardwareprofils

Berücksichtigen Sie Folgendes, wenn Sie ein Hardwareprofil löschen möchten:

- Wenn Sie ein Hardwareprofil löschen, wird die zu diesem Hardwareprofil gehörende Deployment-Vorlage aktualisiert.

So löschen Sie ein Hardwarekonfigurationsprofil:

1. Klicken Sie im DLCI-Konsolen-Add-In für SCVMM auf **Hardwareprofil**.

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

Erstellen eines Hypervisor-Profiles

Sie können ein Hypervisor-Profil erstellen und es verwenden, um das Betriebssystem auf den Servern bereitzustellen. Ein Hypervisor-Profil enthält ein benutzerdefiniertes WinPE-ISO-Image (das WinPE-ISO-Image wird auch für die Bereitstellung des Hypervisor verwendet), eine Host-Gruppe und ein Host-Profil, das von SCVMM übernommen wurde, sowie LC-Treiber für die Injection-Funktion.

Voraussetzungen:

- Das erforderliche WinPE-ISO-Image wurde erstellt, und die ISO-Datei ist im freigegebenen Ordner des DLCI Integration Gateway for SCVMM verfügbar. Informationen zum Aktualisieren des WinPE-Images finden Sie unter [WinPE-Image-Aktualisierung](#).
- In SCVMM werden eine Host-Gruppe, ein Host-Profil oder ein physisches Computerprofil erstellt.

So erstellen Sie ein Hypervisor-Profil:

- Führen Sie im DLCI-Konsolen-Add-In für SCVMM einen der folgenden Schritte aus:
 - Klicken Sie im Dashboard auf **Hypervisor-Profil erstellen**.
 - Klicken Sie im linken Navigationsbereich auf **Profile und Vorlagen**, dann auf **Hypervisor-Profil** und schließlich auf **Erstellen**.
- Klicken Sie im **Hypervisor-Profil-Assistenten** auf der Seite **Willkommen** auf **Weiter**.
- Geben Sie unter **Hypervisor-Profil** einen Namen und eine Beschreibung für das Profil ein, und klicken Sie dann auf **Weiter**.
- Geben Sie auf der Informationsseite für **SCVMM** die Informationen zum **Ziel der SCVMM-Host-Gruppe** und zum **SCVMM-Host-Profil/Physikalischen Computerprofil** ein.
- Geben Sie unter **Quelle für das WinPE-Start-Image** den Namen für die **<Network WinPE ISO file name>.iso** ein, und klicken Sie dann auf **Weiter**.
- (Optional) Um die Injection-Funktion von LC-Treibern zu aktivieren, wählen Sie, wenn diese Option aktiviert ist, das Betriebssystem aus, das Sie bereitstellen möchten, so dass die passenden Treiber ausgewählt werden können. Wählen Sie **Injection-Funktion für LC-Treiber aktivieren** und in **Hypervisor-Version** die erforderliche Hypervisor-Version aus.
- Klicken Sie unter **Zusammenfassung** auf **Fertigstellen**.

Ändern eines Hypervisor-Profiles

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

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

So bearbeiten Sie ein Hypervisor-Profil:

- Wählen Sie im DLCI-Konsolen-Add-In für SCVMM unter **Hypervisor-Profil** das Profil aus, das Sie ändern möchten, und klicken Sie dann auf **Bearbeiten**.
- Geben Sie die gewünschten Details ein, und klicken Sie dann auf **Fertigstellen**.

Löschen eines Hypervisor-Profiles

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

- Wenn ein Hypervisor-Profil gelöscht wird, dann wird auch die zum Hypervisor-Profil gehörende Bereitstellungsvorlage gelöscht.




So löschen Sie ein Hypervisor-Profil:

Wählen Sie im DLCI-Konsolen-Add-In für SCVMM unter **Hypervisor-Profil** das Profil aus, das Sie löschen möchten, und klicken Sie dann auf **Löschen**.

Ergänzende Informationen zu WinPE

Für die Erstellung eines WinPE-Image ist ein SCVMM-PreExecution Environment-Server (PXE) erforderlich. Es wird ein WinPE-ISO aus dem WinPE-Image und dem Dell OpenManage Deployment Toolkit (DTK) erstellt.

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

So erstellen Sie ein WinPE-ISO-Image:

1. Fügen Sie der Appliance den PXE-Server hinzu.
2. Kopieren Sie nach dem Hinzufügen des PXE-Servers die Datei **boot.wim** vom PXE-Server in den freigegebenen WIM-Ordner des DLCI Integration Gateway for SCVMM. Die Datei **boot.wim** befindet sich im folgenden Pfad: **C:\RemoteInstall\DCMgr\Boot\Windows\Images**.

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

DTK ist eine selbstextrahierende ausführbare Datei.

So verwenden Sie DTK:

1. Doppelklicken Sie auf die ausführbare DTK-Datei.
2. Wählen Sie den Ordner aus, in den die DTK-Treiber extrahiert werden sollen, z. B. **C:\DTK501**.
3. Kopieren Sie den extrahierten DTK-Ordner in den DTK-Freigabeordner für das Integration Gateway. Beispiel: **\\DLCI IG Share\DTK\DTK501**.

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

So aktualisieren Sie ein WinPE-Image:

1. Wählen Sie in der DLCI-Konsole die Option **WinPE-Update** unter **Image-Quelle** für den **benutzerdefinierten WinPE-Image-Pfad** aus, und geben Sie den WinPE-Image-Pfad an.
Beispiel: **\\DLCI 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: **\\DLCI IG Share\DTK\DTK501**.
3. Geben Sie einen ISO-Namen an.
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 erstellten Namen wird unter **\\DLCI IG Share\ISO** erstellt.

Info zur Hypervisor-Bereitstellung


Die Hypervisor-Bereitstellung ist ein profilbasierter Arbeitsablauf. Dieser Arbeitsablauf ermöglicht Ihnen die Angabe von Hardwarekonfigurationen, Hypervisor-Konfigurationen, SCVMM-Konfigurationen und von Aktualisierungsquellen für Firmware-Aktualisierungen. Selbst wenn eine Firmware-Aktualisierung fehlschlägt, können Sie mit der Hypervisor-Bereitstellung fortfahren. Allerdings werden alle Komponenten der ausgewählten Server oder Servergruppen während der Hypervisor-Bereitstellung

aktualisiert. Der Arbeitsablauf verwendet ein logisches Netzwerk und ein Host-Profil, das in SCVMM verfügbar ist und zum Zeitpunkt der Erstellung des Hypervisor-Profiles zusammen mit der Hardwarekonfiguration benötigt wird, um den Hypervisor auf dem Gerät bereitzustellen. Die Hypervisor-Bereitstellung unterstützt die 1:1- und die 1:n-Bereitstellung.

Erstellen von Bereitstellungsvorlagen

Sie können Bereitstellungsvorlagen mit dem erforderlichen Hardware- und Hypervisor-Profil und einer Aktualisierungsquelle erstellen, und die Bereitstellungsvorlage auf nicht zugewiesene Server anwenden. Sie müssen die Vorlage somit nur einmal erstellen, und können sie mehrfach verwenden.

So erstellen Sie eine Bereitstellungsvorlage:

1. Führen Sie in der Appliance einen der folgenden Schritte aus:
 - Klicken Sie auf dem Appliance-Dashboard auf **Deployment-Vorlage erstellen**.
 - Klicken Sie im Navigationsbereich der Appliance auf **Profile und Vorlagen**, und klicken Sie dann auf **Deployment-Vorlage**.
2. Geben Sie unter **Bereitstellungsvorlage** den Namen und eine Beschreibung der Vorlage ein, und wählen Sie anschließend ein Hypervisor-Profil, ein Hardwareprofil und eine Aktualisierungsquelle aus.
3. (Optional) Wählen Sie eine Aktualisierungsquelle und ein Hardwareprofil aus. Um mit der Bereitstellung fortzufahren, selbst wenn die Firmware-Aktualisierung fehlschlägt, wählen Sie die Option **OSD auch bei Fehlschlägen der Firmware-Aktualisierung fortsetzen** aus.
 **ANMERKUNG: Standardmäßig wird das Zurückstufen nicht unterstützt.**
4. (Optional) Wenn Sie das Hardware- oder Hypervisor-Profil noch nicht erstellt haben, können Sie die Profile erstellen, indem Sie auf **Neu erstellen** klicken.

Ändern einer Bereitstellungsvorlage

 **ANMERKUNG: Sie können Name, Beschreibung und Auswahl des Hypervisor-Profiles, des Hardwareprofils und der Aktualisierungsquelle ändern.**

So bearbeiten Sie eine Bereitstellungsvorlage:

1. Klicken Sie im DLCI-Konsolen-Add-In für SCVMM auf **Bereitstellungsvorlagen**.
2. Wählen Sie die Bereitstellungsvorlage aus, die Sie ändern möchten, und klicken Sie auf **Bearbeiten**.
3. Nehmen Sie die erforderlichen Änderungen vor, und klicken Sie auf **Fertigstellen**.

Löschen einer Bereitstellungsvorlage

 **ANMERKUNG: Durch das Löschen einer Bereitstellungsvorlage werden die zugehörigen Hardware- und Hypervisor-Profile und die Aktualisierungsquelle nicht beeinträchtigt.**

So löschen Sie eine Bereitstellungsvorlage:

1. Klicken Sie im DLCI-Konsolen-Add-In für SCVMM auf **Bereitstellungsvorlagen**.
2. Wählen Sie die Bereitstellungsvorlage aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.

Bereitstellen von Hypervisors

Betriebssysteme werden nur auf kompatiblen Servern bereitgestellt.

Aktualisieren Sie vor der Hypervisor-Bereitstellung die Firmware-Versionen auf die jeweils neueste Version, die unter ftp.dell.com oder downloads.dell.com verfügbar ist, und fahren Sie anschließend mit der Hypervisor-Bereitstellung fort.

So führen Sie eine Bereitstellung auf Servern aus:

1. Führen Sie auf dem Gerät die folgenden Schritte aus:
 - Klicken Sie im Dashboard auf **Nicht zugewiesene Server bereitstellen**.
 - Klicken Sie im Navigationsbereich auf **Bereitstellungsassistent**.
2. Klicken Sie unter **Willkommen** auf **Weiter**.
3. Wählen Sie in **Server auswählen** die Server aus, auf die Sie bereitstellen möchten, und überprüfen Sie sie auf verfügbare Lizenzen und klicken Sie dann auf **Weiter**.
4. Wählen Sie unter **Vorlagen und Profile** die entsprechende Bereitstellungsvorlage und das zugehörige Geräte-Anmeldeprofil aus.

 **ANMERKUNG:**

- Stellen Sie sicher, dass Sie das Hypervisor-Profil auswählen, das von Ihnen für OSD und Firmware-Aktualisierungsjobs erstellt wurde.
- Sie können mehrere Anmeldeinformationsprofile mehreren Servern zuweisen.

Sie können auch eine Bereitstellungsvorlage und ein Profil mit Anmeldeinformationen erstellen.

5. Wählen Sie unter **Server-Identifikation** Server aus, und geben Sie den Hostnamen, die MAC-Adresse und die Netzwerkinformationen an, die Sie auf die Server anwenden möchten, entweder statisch oder DHCP, und klicken Sie dann auf **Weiter**.
6. Geben Sie unter **Job-Details** einen Job-Namen an, um den Job und den Bereitstellungsstatus zu verfolgen, und klicken Sie auf **Weiter**.
7. Überprüfen Sie in der **Zusammenfassung** die Bereitstellungsoptionen, die Sie angegeben haben, und klicken Sie auf **Fertigstellen**.
8. Klicken Sie im Feld **Bestätigung** auf **Ja**.

 **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 herunter und installieren Sie sie.**

Anzeigen von Informationen auf dem Gerät

Jobs und Protokollcenter

Die Seite **Jobs und Protokollcenter** enthält Informationen über alle Aktivitäten, die in DLCI for SCVMM initiiert werden. Sie können den Fortschrittstatus eines Jobs und seine Teilaufgaben anzeigen. Sie können Jobs auch für eine bestimmte Kategorie filtern und anzeigen. Sie können die Jobs im DLCI-Verwaltungsportal für SCVMM und im DLCI-Konsolen-Add-In für SCVMM anzeigen. Job-Namen werden durch Benutzer bereitgestellt oder vom System generiert, und die Teilaufgaben werden nach der IP-Adresse oder dem Host-Namen des verwalteten Servers bezeichnet. Erweitern Sie die Teilaufgabe zum Anzeigen der Aktivitätsprotokolle für diesen Job. Es gibt vier Arten von Jobs:

- Ausführen - Zeigt alle Jobs an, die gerade ausgeführt werden (bzw. deren Fortschrittstatus).
- Verlauf - Zeigt alle Jobs, die in der Vergangenheit ausgeführt wurden, mit deren Job-Status an.
- Geplant - Zeigt alle für ein zukünftiges Datum und eine zukünftige Uhrzeit geplanten Jobs an. Sie können die geplanten Jobs auch abbrechen.
- Allgemeine Protokolle - Zeigt die gerätespezifischen, gemeinsamen Protokollmeldungen an, die nicht spezifisch für eine Teilaufgabe und andere Aktivitäten sind.
 - Geräte-Protokollmeldungen - Zeigt alle gerätespezifischen Protokollmeldungen, wie z. B. das Neustarten des Geräts. Sie können diese Kategorie von Meldungen nur über das Verwaltungsportal anzeigen.
 - Allgemeine Protokollmeldungen - Zeigt alle Protokollmeldungen an, die den Jobs gemeinsam sind, die in den Registerkarten **Ausführen**, **Verlauf** und **Geplant** aufgeführt sind.
Wenn beispielsweise ein Firmware-Aktualisierungsjob für eine Gruppe von Servern ausgeführt wird, werden auf der Registerkarte die Protokollmeldungen angezeigt, die das Erstellen des SUU-Repositorys für diesen Job betreffen.

Die verschiedenen Zustände der im Gerät definierten Jobs sind:

- Abgebrochen - Der Job wurde manuell vom Benutzer abgebrochen, oder als das Gerät neu gestartet wurde.
- Erfolgreich - Der Job wurde erfolgreich abgeschlossen.
- Fehlgeschlagen - Der Job war nicht erfolgreich.
- In Bearbeitung - Der Job wird gerade ausgeführt.
- Geplant - Der Job wurde für einen späteren Zeitpunkt geplant.
- Warten - Der Job befindet sich in einer Warteschlange, um ausgeführt zu werden.
- Wiederkehrender Zeitplan - Der Job wiederholt sich nach einem festgelegten Zeitintervall.

 **ANMERKUNG: Wenn gleiche Jobs zur gleichen Zeit von verschiedenen oder gleichen Benutzern geplant werden, kann der Job fehlschlagen. Stellen Sie daher sicher, dass gleiche Jobs nicht zur gleichen Zeit geplant werden.**

So zeigen Sie die Jobs und das Protokollcenter an:

1. Klicken Sie in **DLCI for SCVMM** auf **Jobs und Protokollcenter**.
Standardmäßig wird die Registerkarte **Ausführen** angezeigt.
2. Um eine bestimmte Kategorie von Jobs anzuzeigen, klicken Sie auf die gewünschte Registerkarte.
Erweitern Sie die Jobkategorie, um alle im Job enthaltenen Server anzuzeigen. Erweitern Sie weiter, um die Protokollmeldungen für diesen Job anzuzeigen.

**ANMERKUNG:**

- Alle jobbezogenen allgemeinen Protokollmeldungen sind unter der Registerkarte **Allgemeine** und nicht unter der Registerkarte **Ausführen** oder **Verlauf** aufgeführt.
- Nach der Aktualisierung auf DLCI for SCVMM Version 1.3 werden in der Registerkarte **Verlauf** keine Teilaufgaben-Informationen mehr für Jobs angezeigt, die mit früheren Versionen von DLCI for SCVMM ausgeführt werden.

3. (Optional) Filtern Sie die Jobs anhand des Jobtyps.

Anzeigen verwalteter Jobs

So zeigen Sie die verwalteten Jobs an:

Führen Sie im DLCI-Konsolen-Add-In für SCVMM einen der folgenden Schritte aus:

- 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**.

Abbrechen geplanter Jobs

1. Führen Sie im DLCI-Konsolen-Add-In für SCVMM einen der folgenden Schritte aus:

- Klicken Sie im Navigationsbereich auf **Wartungcenter** und dann auf **Jobs verwalten**.
- Klicken Sie im Navigationsbereich auf **Jobs und Protokollcenter** und wählen Sie dann die Registerkarte **Geplant** aus.

2. Wählen Sie die Jobs aus, die Sie abbrechen möchten, und klicken Sie dann auf **Abbrechen**.

Fehlerbehebung

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

Wenn eine Cluster-Gruppe auf dem Gerät ermittelt wird, wird im **Wartungszentrum** eine Cluster-Aktualisierungsgruppe angelegt, in der alle Server aufgeführt sind. Werden später alle Server aus diesem Cluster über SCVMM entfernt und eine automatische Ermittlung oder Synchronisierung mit dem SCVMM-Vorgang durchgeführt, wird die leere Cluster-Aktualisierungsgruppe nicht aus dem **Wartungszentrum** gelöscht.

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

Ermittlungs-Jobs werden nicht gesendet

Wenn Sie die Rücktaste drücken, um eine Fehlermeldung auf dem Ermittlungsbildschirm zu beenden, werden die nachfolgenden Ermittlungs-Jobs nicht für die Back-End-Verarbeitung gesendet.

Um dieses Problem zu umgehen, schließen Sie den aktuellen Ermittlungsbildschirm, und starten Sie den Bildschirm neu über die Seite **Bestandsaufnahme**. Senden Sie den neuen Ermittlungs-Job, nachdem Sie die erforderlichen Eingaben vorgenommen haben.

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 modularen Server aus einem Gehäuse, und fügen Sie ihn einem anderen Gehäuse hinzu. Weitere Informationen finden Sie im Abschnitt über Servermodule im Benutzerhandbuch für Dell PowerEdge VRTX-Gehäuse mit dem Titel *Dell PowerEdge VRTX Enclosure Owner's Manual*.
2. Konfigurieren Sie CMC. Weitere Informationen finden Sie im Abschnitt zur Installation und Einrichtung von CMC im Benutzerhandbuch für Chassis Management Controller Version 2.1 für Dell PowerEdge VRTX mit dem Titel *Chassis Management Controller Version 2.1 for Dell PowerEdge VRTX User's Guide*, das unter 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.

Exportieren des Konfigurationsprofils eines anderen Servers nach Änderung der IP-Adresse

Wenn ein Job vom Typ **Serverprofil exportieren** auf einem Server geplant ist und die IP-Adresse des Servers einem anderen Server zugewiesen wird, exportiert das Gerät das Serverprofil dieses neuen Servers.



Um das Problem zu umgehen, stornieren Sie den Job **Serverprofil exportieren**, ermitteln Sie den Server neu, dessen IP-Adresse sich geändert hat, und planen Sie anschließend den Job **Serverprofil exportieren** auf diesem Server.

Fehler beim Anwenden der RAID-Konfiguration

Das Anwenden eines Hardwareprofils mit der RAID-Konfiguration kann mit folgenden Fehlermeldungen fehlschlagen: `Error An unknown exception has occurred and has been logged in the extended logs .`

`Error RAID configuration failed with error: An unknown exception has occurred and has been logged in the extended logs. <iDRAC IP address>`

`Error 0_EX_MSG`

Um dieses Problem zu umgehen, schalten Sie für den Server das **System aus und ein** und wenden Sie die Hardwarekonfiguration erneut an.

Aktualisierungsquelle kann nicht erstellt werden

Wenn die DNS-Netzwerkkonfiguration (Domain Name System) des Geräts geändert wird, können keine Aktualisierungsquellen vom Typ HTTP oder FTP erstellt werden.

Um dieses Problem zu umgehen, führen Sie einen Neustart des Geräts aus, und erstellen Sie anschließend die Aktualisierungsquelle vom Typ HTTP oder FTP.

Fehler bei der Firmware-Aktualisierung wegen belegter Job-Warteschlange

Firmware-Aktualisierungs-Jobs, die vom Gerät an iDRAC gesendet werden, schlagen fehl, und im Hauptprotokoll des Geräts wird folgender Fehler angezeigt: `JobQueue Exceeds the size limit. Delete unwanted JobID(s).`

Um dieses Problem zu umgehen, löschen Sie manuell die abgeschlossenen Jobs in iDRAC, und wiederholen Sie den Firmware-Aktualisierungs-Job. Weitere Informationen zum Löschen von Jobs in iDRAC finden Sie in der iDRAC-Dokumentation unter dell.com/support/home.

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 Repositories 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.

Geplanter Job auf einer Aktualisierungsgruppe schlägt fehl

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.

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-Aktualisierungsjob, der auf Dell 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 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-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 das Gerät 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 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 Appliance-FQDN im Browser unter der lokalen Intranetsite hinzu. Weitere Informationen über das Hinzufügen der Appliance im lokalen Intranet finden Sie im Abschnitt [Anzeigen von LC-Protokollen](#).

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](#).

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](#).

Firmware-Aktualisierung auf einigen Komponenten, unabhängig von der Auswahl

Gleiche Komponenten auf identischen Servern werden unabhängig von der auf den einzelnen Servern vorgenommenen Komponentenauswahl bei der Firmware-Aktualisierung aktualisiert. Dieses Verhalten wurde bei Dell PowerEdge-Servern der 12. und 13. Generation mit einer Enterprise-Lizenz für iDRAC festgestellt.

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.

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

Nach dem Senden eines Jobs zum Importieren eines Serverprofils im Gerät kann es sein, dass nach Ablauf von zwei Stunden eine Zeitüberschreitung eintritt.

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.

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.

Hypervisor-Bereitstellungsfehler aufgrund von weiterhin vorhandenen Treiberdateien in der Bibliotheksfreigabe

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

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

Diese Fehler können aufgrund einer Ausnahmeausgabe durch den VMM-Befehls-Let `GET-SCJOB status` auftreten, und die Treiberdateien bleiben in der Bibliothek erhalten. Bevor Sie versuchen, den Vorgang zu wiederholen oder einen anderen Hypervisor bereitzustellen, müssen Sie diese Dateien aus der Bibliotheksfreigabe entfernen.

So entfernen Sie Dateien aus der Bibliotheksfreigabe:

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

Nun können Sie Betriebssysteme bereitstellen.



Aktuelle Bestandsaufnahmeinformationen werden auch nach erfolgter Firmware-Aktualisierung nicht angezeigt

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

Die Aktualisierung der Bestandsaufnahme auf einem Gerät wird unmittelbar nach Abschluss eines Firmware-Aktualisierungs-Jobs durchgeführt. Die Firmware-Aktualisierung wird noch vor der CSIOR-Aktivität des PowerEdge-Servers durchgeführt, weshalb noch die früheren Firmware-Bestandsaufnahmeinformationen angezeigt werden.

Um dieses Problem zu umgehen, überprüfen Sie, ob der CSIOR-Vorgang auf dem PowerEdge-Server abgeschlossen wurde, und aktualisieren Sie anschließend auf dem Gerät die Firmware-Bestandsaufnahme. Stellen Sie außerdem sicher, dass Sie den Server nach der Anwendung einer agentenfreien, stufenweisen Aktualisierung neu 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.

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 computer was expected to join Active Directory using the computer name <host.domain>.`

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

1. Warten Sie einige Zeit, um zu sehen, ob der Server zu Active Directory hinzugefügt wird.
2. Wenn der Server nicht zu Active Directory hinzugefügt wird, fügen Sie den Server manuell zu Active Directory hinzu.
3. Fügen Sie den Server zu SCVMM hinzu.
4. Nachdem der Server zu SCVMM hinzugefügt wurde, führen Sie eine Neuermittlung des Servers in der DLCI-Konsole durch. Der Server wird auf der Registerkarte **Host** aufgelistet.

Hypervisor-Bereitstellung schlägt bei Verwendung von Active Directory für die 11. Generation von PowerEdge-Blade-Servern fehl

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

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

RAID-Konfigurationsfehler für virtuelle Festplatten mit RAID 10

Die RAID-Konfiguration schlägt fehl, wenn virtuelle Datenträger mit RAID-Level 10 für Controller H200 erstellt werden und mehr als vier physische Laufwerke verwenden.

RAID 10 mit mehr als vier physischen Festplatten schlägt fehl

Verwenden Sie zur Umgehung dieses Problems die minimale Anzahl der für diese RAID-Stufe erforderlichen physischen Festplatten.

Fehler bei der Konfiguration von RAID aufgrund der Konfiguration von Hotspares auf Software-RAID S130

Die RAID-Konfiguration auf Software-RAID-Controller S130 schlägt fehl, wenn versucht wird, die RAID-Konfiguration mit mehr als drei Hot-Spares, einschließlich globales Hot-Spare GHS und DHS, auszuführen.
So umgehen Sie dieses Problem:

- Verwenden Sie nur drei Hot-Spares (GHS und DHS) zur Anwendung auf einem Profil.
- Verwenden Sie die PowerEdge RAID-Controller-Karte (PERC).



Zugriff auf Dokumente der Dell Support-Website

Sie können auf eine der folgenden Arten auf die folgenden Dokumente zugreifen:

- Verwendung der folgenden Links:
 - Für alle Enterprise-System-Verwaltungsdokumente – [Dell.com/SoftwareSecurityManuals](https://www.dell.com/support/manuals)
 - Für OpenManage-Dokumente – [Dell.com/OpenManageManuals](https://www.dell.com/support/manuals)
 - Für Remote-Enterprise-System-Verwaltungsdokumente – [Dell.com/esmanuals](https://www.dell.com/support/manuals)
 - Für Dokumente zu iDRAC und Lifecycle Controller – [Dell.com/idracmanuals](https://www.dell.com/support/manuals)
 - Für OpenManage Connections Enterprise-System-Verwaltungsdokumente – [Dell.com/OMConnectionsEnterpriseSystemsManagement](https://www.dell.com/support/manuals)
 - Für 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)
- Gehen Sie auf der Dell Support-Website folgendermaßen vor:
 - a. Rufen Sie die Website [Dell.com/Support/Home](https://www.dell.com/support/home) auf.
 - b. Klicken Sie unter **Wählen Sie ein Produkt** auf **Software und Sicherheit**.
 - c. Klicken Sie im Gruppenfeld **Software & Sicherheit** auf einen der folgenden Links:
 - **Enterprise-Systemverwaltung**
 - **Remote Enterprise-Systemverwaltung**
 - **Tools für die Betriebsfähigkeit**
 - **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.