




Dell Lifecycle Controller 2 Remote Services
Version 1.00.00 Benutzerhandbuch



Anmerkungen, Vorsichtshinweise und Warnungen

-  **ANMERKUNG:** Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie den Computer besser einsetzen können.
-  **VORSICHT:** Ein VORSICHTSHINWEIS macht aufmerksam auf mögliche Beschädigung der Hardware oder Verlust von Daten bei Nichtbefolgung von Anweisungen.
-  **WARNUNG:** Durch eine WARNUNG werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

Irrtümer und technische Änderungen vorbehalten.

© 2012 Dell Inc. Alle Rechte vorbehalten.

Die Vervielfältigung oder Wiedergabe dieser Unterlagen in jeglicher Weise ohne vorherige schriftliche Genehmigung von Dell Inc. ist strengstens untersagt.

In diesem Text verwendete Marken: Dell™, das Dell Logo, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ und Vostro™ sind Marken von Dell Inc. Intel®, Pentium®, Xeon®, Core® und Celeron® sind eingetragene Marken der Intel Corporation in den USA und anderen Ländern. AMD® ist eine eingetragene Marke und AMD Opteron™, AMD Phenom™ und AMD Sempron™ sind Marken von Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS® und Windows Vista® und Active Directory® sind Marken oder eingetragene Marken der Microsoft Corporation in den USA und/oder anderen Ländern. Red Hat® und Red Hat® Enterprise Linux® sind eingetragene Marken von Red Hat, Inc. in den USA und/oder anderen Ländern. Novell® ist eine eingetragene Marke und SUSE® ist eine Marke von Novell Inc. in den USA und anderen Ländern. Oracle ist eine eingetragene Marke von Oracle® Corporation und/oder ihren Tochterunternehmen. Citrix®, Xen®, XenServer® und XenMotion® sind eingetragene Marken oder Marken von Citrix Systems, Inc. in den USA und/oder anderen Ländern. VMware®, Virtual SMP®, vMotion®, vCenter® und vSphere® sind eingetragene Marken oder Marken von VMware, Inc. in den USA oder anderen Ländern. IBM® ist eine eingetragene Marke von International Business Machines Corporation.

Andere in diesem Dokument möglicherweise verwendete Marken und Handelsnamen beziehen sich auf die entsprechenden Eigentümer oder deren Produkte. Dell Inc. erhebt keinen Anspruch auf Marken und Handelsbezeichnungen mit Ausnahme der eigenen.

2012 - 03

Rev. A00

Inhaltsverzeichnis

Anmerkungen, Vorsichtshinweise und Warnungen.....	2
Kapitel 1: Einführung.....	9
Vorteile der Verwendung von iDRAC7 mit Lifecycle-Controller.....	9
Wichtige Funktionen.....	9
Warum sollte ich die Remote Services verwenden?.....	10
Lizenzierbare Funktionen in Lifecycle-Controller.....	10
Webdienste für Verwaltung.....	11
Standard-DMTF.....	11
Dell-Erweiterungen.....	11
Weitere nützliche Dokumente.....	13
Kontaktaufnahme mit Dell.....	14
Kapitel 2: Verwenden von Remote-Services.....	15
Allgemeine Voraussetzungen vor der Verwendung der Remote-Services.....	15
Web Services-Setup.....	15
WinRM-Client.....	15
OpenWSMan-Client.....	16
Verwenden von Anwendungen.....	16
Anwendungsstruktur.....	16
Anleitung zum Lesen von Anwendungen.....	16
Anwendungsszenarien.....	16
Kapitel 3: Auto-Ermittlung und Handshake.....	19
iDRAC für Auto-Ermittlung konfigurieren.....	19
Zeichenkettenformat Bereitstellungsserver.....	20
Einstellen der Bereitstellung auf dem gewünschten Speicherort.....	20
Auto-Ermittlung des verwalteten Systems.....	21
Konfiguration von DHCP oder DNS.....	21
Anzeigen des Ermittlungsstatus auf der Frontblendenanzeige.....	21
Die Auto-Ermittlung in neuen Umgebungen neu einleiten.....	22
Kapitel 4: Lizenzenverwaltung.....	23
Anzeigen der installierten Lizenzen.....	23
Anzeigen von lizenzierbaren Geräten.....	23
Installieren einer Lizenz.....	23
Referenzen für das Installieren einer Lizenz.....	24

Ersetzen einer Lizenz.....	24
Löschen einer Lizenz.....	24
Exportieren einer Lizenz.....	25
Kapitel 5: Verwaltung von Zertifikaten.....	27
Erstellen von benutzerdefinierten Root-Client-Zertifikaten für den Bereitstellungsserver.....	27
Benutzerdefinierte Serverzertifikate bereitstellen.....	27
Benutzerdefinierte Zertifikate löschen.....	27
Benutzerdefiniertes Löschen des öffentlichen Schlüssels.....	28
Benutzerdefiniertes Löschen des Client-Zertifikates.....	28
Ändern des Web Server oder WS-MAN-Verschlüsselungszertifikates und des privaten Schlüssels von PKCS #12.....	28
Verwaltung von Server-Zertifikaten.....	28
Referenzen für die Verwaltung von Serverzertifikaten.....	29
Directory CA-Zertifikatverwaltung.....	29
Referenzen für die Verwaltung von Directory CA-Zertifikaten.....	29
Kapitel 6: Bereitstellen des Betriebssystems.....	31
Bereitstellen des Betriebssystems.....	31
Referenzen für die Betriebssystembereitstellung.....	32
Remote-Dateifreigabe verwenden.....	33
Start auf ISO während der Serverwartung.....	34
Referenzen für das Starten auf ISO während der Server-Wartung.....	35
Auf ISO starten - Methodenvergleich.....	36
Einmalige Startsequenz.....	37
Info - Aufgabenkennungen.....	38
Kapitel 7: Verwalten von Aufgaben.....	41
Aufgabentypen.....	41
Benutzererstellte Aufgaben.....	42
Aufgaben-Zeitplan.....	42
Löschen einer Aufgabe.....	42
Zeitliche Planung separater Aufgaben für mehrere Aktionen.....	42
Mehrere Zielaufgaben durchführen.....	43
Spezifizieren der Startzeit und Endzeit.....	43
Automatisches Löschen von Aufgaben.....	43
Alle Aufgaben löschen.....	44
Kapitel 8: Verwalten der RAID-Konfiguration.....	45
RAID-Controller anzeigen.....	45
Erstellen aufgeteilter (sliced) virtueller Laufwerke.....	45
RAID-Konfiguration.....	45

Szenario nach der Konfiguration des RAID-Setups.....	48
Referenzen zur Konfiguration von RAID.....	48
Konvertieren eines SATA-Laufwerks vom RAID-Modus in einen Nicht-RAID-Zustand.....	49
Referenzen für das Konvertieren eines SATA-Laufwerks.....	49
Kapitel 9: Verwalten von Netzwerkgeräten.....	51
Anzeigen der Netzwerkgerät-Bestandsliste.....	51
Anzeigen der Netzwerkgerät-Attribute.....	51
Festlegen der Netzwerkgerät-Attribute.....	51
Löschen der ausstehenden Werte.....	52
Aktivieren oder Deaktivieren der Partition auf der CNA.....	52
Ändern der Merkmale und der Bandbreite einer Partition für einen CNA.....	53
Referenzen zum Ändern der Merkmale.....	54
Einrichten der virtuellen Adressattribute.....	55
Referenzen zu virtuellen Adressattributen.....	55
Einrichten der Attribute „Boot Target-SCSI“ und „FCoE“.....	55
Kapitel 10: Bestandsliste und Protokolle.....	57
Abruf des Hardwarebestandes.....	57
Exportieren der aktuellen Hardware-Bestandsliste.....	57
Lifecycle-Protokoll.....	57
Exportieren des Lifecycle-Protokolls.....	58
Löschen der Konfiguration und Zurücksetzen auf die Standardeinstellungen.....	58
Kapitel 11: Remote-Aktualisierungen.....	59
Verwendung von Remote-Aktualisierung.....	59
Unterstützte Geräte.....	59
Remote-Aktualisierung über den URI.....	60
Remote-Aktualisierung planen.....	60
Zurücksetzen auf vorhergehende Versionen.....	61
Verwenden der Remote-Firmware-Bestandsaufnahme.....	61
Unterstützte Geräte.....	61
Abruf des Firmwarebestandes.....	62
Typen der Remote-Planung.....	62
Sofortige Aktualisierung.....	62
Geplante Aktualisierung.....	63
Zeitplanungs-Neustartverhalten einrichten.....	63
Verwaltung der Teilersetzung.....	63
Bezug/Einstellung von Teile-Firmware- und Konfigurationsaktualisierungsattributen.....	64
Kapitel 12: Sichern und Wiederherstellen.....	65
Exportieren von Serverprofilen auf die iDRAC vFlash-Karte oder die Netzwerkfreigabe.....	65

Funktion oder Systemverhalten zum Exportieren des Server-Profiles.....	66
Referenzen zum Exportieren des Serverprofils.....	67
Importieren des Serverprofils von einer iDRAC vFlash-Karte oder einer Netzwerkfreigabe.....	67
Szenario nach der Wiederherstellung.....	69
System- bzw. Funktionsverhalten für Szenario nach der Wiederherstellung.....	69
Referenzen zum Importieren des Server-Profiles.....	70
Kapitel 13: Verwalten der vFlash SD-Karte.....	71
Anzeige der Bestandsliste der vFlash SD-Karte.....	71
Anzeige der Partitionen auf der vFlash SD-Karte.....	71
Erstellen und Modifizieren einer Partition auf einer vFlash SD Card.....	71
Kapitel 14: iDRAC-Konfigurationen.....	73
Abrufen und Festlegen der iDRAC-Attribute.....	73
Referenzen zum Abrufen und Festlegen der iDRAC-Attribute.....	73
iDRAC-Attribute ().....	74
Abrufen und Festlegen von iDRAC-Benutzern und -Rollen.....	76
Referenzen zum Abrufen und Festlegen von iDRAC-Benutzern und -Rollen.....	77
Weiterleiten von Änderungen an der iDRAC-IP-Adresse.....	78
Funktion oder Systemverhalten zum Weiterleiten von Änderungen an der iDRAC-IP-Adresse.....	78
Referenzen zum Weiterleiten von Änderungen an der iDRAC-IP-Adresse.....	78
Kapitel 15: Verwaltung der BIOS- und Startkonfiguration.....	81
Anzeigen der Bestandsliste der BIOS-Attribute.....	81
Einstellen der BIOS-Attribute.....	81
Einmalige Startsequenz.....	81
Festlegen, Ändern und Löschen des BIOS-Kennworts.....	82
Referenzen zum Festlegen, Ändern und Löschen des BIOS-Kennworts.....	83
Kapitel 16: Andere Anwendungsfall-Szenarios.....	85
Abrufen des Remotedienststatus.....	85
Referenzen zum Abrufen des Remotedienststatus.....	85
Kapitel 17: Remote Services-Profile.....	87
Profil „Betriebssystembereitstellung“.....	87
Betriebssystembereitstellung - Methoden.....	87
Profil „Lifecycle-Controller-Management“.....	88
LC Service-Methoden.....	88
Methoden zur automatischen Erkennung.....	88
Export- und Importmethoden.....	89
Lifecycle Protokollierungsmethoden.....	89
Methode für die Hardware-Bestandsliste.....	89

Profil „Einfaches NIC“	89
„Einfaches NIC“ - Methoden.....	90
Profil „BIOS- und Startverwaltung“	90
BIOS- und Startverwaltung - Methoden.....	91
Profil „Persistenter Speicher“	92
vFlash SD Card Methods.....	92
Profil „RAID“	93
RAID-Methoden.....	94
Profile „Hardware-Bestandslisten“	95
Profil „Aufgabensteuerung“	96
„Aufgabensteuerung“ - Methoden.....	97
Profil „Netzteil“	97
Profil zur Stromzustandsverwaltung.....	97
Profil zur Stromzustandsverwaltung – Methoden.....	97
Profil zum Datensatzprotokoll.....	98
Profil zum Datensatzprotokoll-Methoden.....	98
Profil zur rollenbasierten Autorisierung.....	98
Profil zur rollenbasierten Autorisierung – Methoden.....	99
Profil zu Sensoren.....	99
Profil zum Serviceprozessor.....	99
Dienstprozessorprofil - Methoden.....	99
Ereignisfilterprofil.....	100
Ereignisfilterprofil - Methoden.....	100
Lizenz-Verwaltungsprofil.....	100
Lizenzverwaltungsprofil - Methoden.....	100
Profil der iDRAC-Karte.....	101
Profil der iDRAC-Karte – Methoden.....	101
Basisserver und Profil zum physischen Bestand.....	101
Profil für Basis-Server und physische Anlagen - Methoden.....	102
Systeminfoprofil.....	102
Systeminfo-Methoden.....	102
Profil zur einfachen Identitätsverwaltung.....	102
Einfache Identität - Methoden.....	103
Kapitel 18: Fehlerbehebung und häufig gestellte Fragen.....	105
Fehlermeldungen.....	105
Automatische Ermittlung - LCD Meldungen.....	105
Häufig gestellte Fragen (FAQs).....	106
Kapitel 19: Schema.....	109
Lifecycle Protokoll-Schema.....	109

Kapitel 20: Leicht zu verwendende Systemkomponentenbezeichnungen.....111

Einführung

Der Dell Lifecycle-Controller bietet eine erweiterte integrierte Systemverwaltung. Er enthält 1GB verwalteten und persistenten Speicher, der zusätzlich zu den iDRAC-Funktionen Systemverwaltungsfunktionen einbettet.

Die Dell Lifecycle-Controller Remote Services ermöglichen darüberhinaus die Systemverwaltung mit einer One-to-Many Methode. Remote Services steht unter Verwendung der auf dem Web Service for Management (WS-MAN)-Protokoll basierenden Webdienst-Schnittstelle für die Bereitstellung und Verwaltung durch den iDRAC zur Verfügung. Die Schnittstelle zielt darauf ab, viele Aufgaben zu vereinfachen, wozu u. A. die Remote-Bereitstellung von Betriebssystemen (OS), die Remote-Aktualisierung und -Bestandsaufnahme und die Remote-Einrichtung und -Konfiguration von bereits bereitgestellten und neuen Dell-Systemen gehören.

Remotedienste sind mittels der sicheren Webdienst-Schnittstelle über das Netzwerk zugänglich und können durch Anwendungen und Skripte programmgesteuert genutzt werden. Die Remote-Dienste ermöglichen Verwaltungskonsolen die Durchführung der One-To-Many-Bare-Metal-Server-Bereitstellung. Die Kombination einer neuen Auto-Ermittlungsfunktion zur Identifizierung und Authentifizierung des angeschlossenen Dell-Systems im Netzwerk und Integration mit den One-To-Many-Verwaltungskonsolen reduziert die manuellen Schritte, die für die Serverbereitstellung erforderlich sind.

Vorteile der Verwendung von iDRAC7 mit Lifecycle-Controller

Zu den Vorteilen gehört:

- Erhöhte Verfügbarkeit — Frühe Benachrichtigungen bei möglichen oder tatsächlichen Fehlern, die dabei helfen, einen Serverausfall zu verhindern, bzw. die Wiederherstellungszeit nach einem Ausfall zu verkürzen.
- Verbesserte Produktivität und niedrigere Betriebskosten — Das Erweitern der Reichweite von Administratoren auf eine größere Anzahl von weit entfernten Servern kann IT-Personal produktiver machen, während Betriebskosten für z.B. Reisen gesenkt werden.
- Sichere Umgebung — Durch Bereitstellung des sicheren Zugriffs auf entfernte Server können Administratoren bei gleichzeitiger Aufrechterhaltung der Server- und Netzwerksicherheit wichtige Verwaltungsfunktionen durchführen.
- Erweiterte integrierte Verwaltung durch Lifecycle-Controller – Lifecycle-Controller bietet durch die Lifecycle-Controller-GUI Remote Services (WS-Management-)-Schnittstellen für eine in Dell OpenManage Essentials und Partnerkonsolen integrierte Remote-Bereitstellung die Bereitstellung und eine vereinfachte Wartbarkeit.

Lesen Sie für weitere Informationen zu iDRAC7 das *Benutzerhandbuch für den integrierten Dell Remote Access Controller* auf support.dell.com/manuals.

Wichtige Funktionen

Remote Services ermöglicht es der Dell Verwaltungskonsole, dem Dell Modular Chassis Management Controller, Partnerkonsolen, durch Kunden erstellten Konsolen und Skripts, Systemverwaltungsaufgaben aus der Ferne durchzuführen, wie z.B:

- Betriebssystem- und Treiberinstallation
- Lizenzverwaltung
- Durchführen von Aktualisierungen der BIOS-Firmware

- Teilersatzverwaltung
- Durchführen von Aktualisierungen der Firmware von Komponenten
- Einholung von Informationen der Hardware-Bestandsaufnahme
- Abrufen und Einrichten der NIC-/CNA- und RAID-Konfiguration
- Abrufen und Einrichten der BIOS-Konfiguration und der BIOS-Kennwörter
- Das Lebensdauerprotokoll exportieren.
- Exportieren des aktuellen und werkseitigen Hardware-Bestandprotokolls
- Verwaltung, Anbindung und Starten von vFlash SD-Kartenpartitionen
- Aktivierung der Verschlüsselung auf dem Controller unter Verwendung eines lokalen Schlüssels und Sperren der virtuellen Laufwerke.
- Exportieren und Importieren des Serverprofils
- Zeitplan und Nachverfolgung des Status von Aktualisierungs- und Konfigurationsaufgaben

Warum sollte ich die Remote Services verwenden?

Remote Services bietet die folgenden Vorteile und Funktionen:

- Nutzt Ihre vorhandene Konsole für die One-to-Many-Serverbereitstellung.
- Nutzt auf dem verwalteten System keine Systemressourcen des Betriebssystems.
- Stellt einen sicheren Kommunikationspfad für die Verwaltung zur Verfügung.
- Reduziert manuelle Eingriffe und erhöht die Effizienz während der Bereitstellung von Servern.
- Ermöglicht die zeitliche Planung von Konfigurationsänderungen und -aktualisierungen, wodurch Ausfallzeiten aufgrund von Wartungen reduziert werden.
- Ermöglicht das Skripting der Windows- und Linux-Befehlszeilenschnittstelle (CLI).
- Ermöglicht die Integration mit Konsolen durch WS-MAN-Schnittstellen.
- Unterstützt die betriebssystemagnostische Software-Aktualisierung.

Lizenzierbare Funktionen in Lifecycle-Controller

Lifecycle-Controllerfunktionen sind je nach Typ der von Ihnen gekauften Lizenz verfügbar (Basic Management, iDRAC7 Express, iDRAC7 Express for Blades, oder iDRAC7 Enterprise). In der Webschnittstelle des Lifecycle-Controllers stehen nur lizenzierte Funktionen zur Verfügung. Lesen Sie für weitere Informationen über die Lizenzverwaltung den *iDRAC7 User's Guide*. Die folgende Tabelle enthält die auf Basis der gekauften Lizenz verfügbaren Lifecycle-Controllerfunktionen.

Tabelle 1. Lizenzierbare Funktionen

Funktion	Basisverwaltung mit IPMI	iDRAC7 Express	iDRAC7 Express für Blades	iDRAC7 Enterprise
Firmware-Aktualisierung	Ja	Ja	Ja	Ja
Betriebssystembereitstellung	Ja	Ja	Ja	Ja
Gerätekonfiguration	Ja	Ja	Ja	Ja
Diagnose	Ja	Ja	Ja	Ja
Server-Profil Export und Import	-	-	-	Ja
Teilersetzung	-	-	-	Ja

Funktion	Basisverwaltung mit IPMI	iDRAC7 Express	iDRAC7 Express für Blades	iDRAC7 Enterprise
Lokale Aktualisierungen	Ja	Ja	Ja	Ja
Treiberpakete	Ja	Ja	Ja	Ja
Remote-Services (über WSMAN)		Ja	Ja	Ja

Webdienste für Verwaltung

WS-MAN ist ein Simple Object Access Protocol (SOAP)-basiertes Protokoll, das für die Systemverwaltung entworfen wurde. Es wird von der Distributed Management Task Force (DMTF) veröffentlicht und bietet ein interoperables Protokoll, mit dem Geräte Daten über Netzwerke freigeben und austauschen können. Die Implementierung von „Lifecycle-Controller-Remotedienste - WS-Verwaltung“ erfüllt die DMTF-WS-MAN-Spezifikation der Version 1.0.0.

Dell Lifecycle-Controller - Remotedienste nutzen WS-MAN zur Übertragung von DMTF Common Information Model (CIM)-basierten Verwaltungsinformationen. Die CIM-Informationen definieren die Semantik und Typen der Informationen, die in einem verwalteten System verändert werden können. Dell nutzt die WS-MAN-Schnittstelle, um den Remote-Zugriff auf die Lifecycle- Vorgänge der Hardware zu ermöglichen.

Die Dell-embedded Schnittstellen zur Verwaltung der Serverplattform sind in Profile gegliedert, wobei jedes Profil die spezifischen Schnittstellen für eine bestimmte Management-Domäne oder einen Funktionsbereich definiert. Darüber hinaus hat Dell eine Reihe von Modell- und Profilerweiterungen definiert, die Schnittstellen für weitere Funktionen bieten. Die durch WS-MAN verfügbaren Daten und Verfahren werden von der Instrumentationsschnittstelle der Lifecycle-Controller - Remotedienste bereitgestellt und sind den folgenden DMTF-Profilen und Dell-Erweiterungsprofilen zugewiesen:

Standard-DMTF

- **Basisserver** – definiert CIM-Klassen für die Darstellung des Host-Servers.
- **Basismetrik** – definiert die CIM-Klassen für die Funktionalität zur Modellierung und Kontrolle von Metriken, die für die verwalteten Elemente erfasst werden.
- **Dienstprozessor** – definiert CIM-Klassen für die Modellierung von Dienstprozessoren.
- **Physische Anlage** – definiert CIM-Klassen für die Darstellung der physischen Aspekte der verwalteten Elemente.
- **SM CLP Admin Domain (SM-CLP-Administrator-Domäne)** – Definiert CIM-Klassen für die Darstellung der CLP-Konfiguration.
- **Stromzustandsverwaltung** – definiert CIM-Klassen für Stromsteuerungsvorgänge.
- **Befehlszeilenprotokolldienst** – definiert CIM-Klassen für die Darstellung der CLP-Konfiguration.
- **Datensatzprotokoll** – definiert CIM-Klassen für die Darstellung verschiedener Arten von Protokollen.
- **Rollenbasierte Autorisierung** – definiert CIM-Klassen für die Darstellung von Rollen.
- **SMASH-Erfassung** – definiert CIM-Klassen für die Darstellung der CLP-Konfiguration.
- **Profilregistrierung** – definiert CIM-Klassen für die Anzeige der Profilimplementierungen.
- **Einfache Identitätsverwaltung** – definiert CIM-Klassen für die Darstellung von Identitäten.

Dell-Erweiterungen

- **Dell BS-Bereitstellung** – definiert CIM- und Dell-Erweiterungsklassen für die Darstellung der Konfiguration von Betriebssystembereitstellungsfunktionen.

- **Dell-Softwareaktualisierungsprofil** – definiert CIM- und Dell-Erweiterungen zum Darstellen der Dienstklasse und Methoden zum Aktualisieren von BIOS, Komponenten-Firmware, Lifecycle-Controller-Firmware, Diagnose und Treiberpaket.
- **Dell-Softwarebestandsaufnahmeprofil** – definiert CIM- und Dell-Erweiterungen zum Darstellen der derzeit installierten Versionen von BIOS, Komponenten-Firmware, Diagnose, Lifecycle-Controller und Treiberpaket. Außerdem werden die im Lifecycle-Controller verfügbaren Versionen von BIOS- und Firmware-Aktualisierungsabbilder für ein Rollback und eine Neuinstallation dargestellt.
- **Dell Auftragssteuerungsprofil** – Definiert CIM- und Dell-Erweiterungen zum Verwalten von Aufträgen, die durch Aktualisierungsaufforderungen erstellt werden. Aufträge können erstellt, gelöscht, modifiziert und in Auftragswarteschlangen zusammengesetzt werden, um während eines einzelnen Neustarts mehrere Aktualisierungen zu sequenzieren und auszuführen.
- **Dell Lifecycle-Controller-Verwaltungsprofil** — Definiert CIM- und Dell-Erweiterungen für die Einholung und Einstellung von Attributen zur Verwaltung der automatischen Ermittlung, die Teilersetzung, die Lifecycle-Protokolls und den Export von Hardware-Bestandsaufnahmen.
- **Stromversorgungsprofil** — Beschreibt die Eigenschaften und Methoden in Bezug auf die Verwaltung der Stromversorgungen eines Systems.
- **SMASH-Bestandsprofil** — Definiert die Bestände, die die Systems Management - Command Line Protocol (SM-CLP) Zieladressierung unterstützen.
- **Dell RAID-Profil** — Beschreibt die Klassen, Eigenschaften und Methoden für die Repräsentation und Konfiguration von RAID-Speicher.
- **„Dell Simple NIC“-Profil** – Beschreibt die Klassen, Eigenschaften und Methoden für die Repräsentation und Konfiguration der NIC- und CNA-Netzwerk-Controller.
- **„Dell Persistent Storage“-Profil** — Beschreibt die Klassen, Eigenschaften und Methoden zur Repräsentation und Verwaltung der Partitionen von vFlash SD-Karten auf Plattformen von Dell.
- **Dell BIOS und Startverwaltungsprofil** — Beschreibt die Klassen, Eigenschaften und Methoden zur Repräsentation der Konfiguration des System-BIOS Setups und zur Verwaltung der Startreihenfolge des Systems.
- **Dell CPU-Profil** — Beschreibt die Eigenschaften und Schnittstellen zur Ausführung von Systemverwaltungsaufgaben in Bezug auf die Verwaltung von Prozessoren.
- **Dell Lüfterprofil** — Beschreibt die Eigenschaften und Schnittstellen zur Ausführung von Systemverwaltungsaufgaben in Bezug auf die Verwaltung von Lüftern.
- **Dell iDRAC-Karte-Profil** — Beschreibt die Eigenschaften und Schnittstellen zur Ausführung von Systemverwaltungsaufgaben in Bezug auf die Verwaltung von Basiseigenschaften der iDRAC-Karte.
- **Dell Speicherinformationsprofil**— Beschreibt die Eigenschaften und Schnittstellen zur Ausführung von Systemverwaltungsaufgaben in Bezug auf die Verwaltung der Speicherkarten (DIMMs).
- **Dell PCI-Geräteprofil** — Beschreibt die Eigenschaften und Schnittstellen zur Ausführung von Systemverwaltungsaufgaben in Bezug auf die Verwaltung der PCI-Geräte eines Systems.
- **Dell Systeminformationsprofil**— Beschreibt die Eigenschaften und Schnittstellen zur Ausführung von Systemverwaltungsaufgaben in Bezug auf die Verwaltung des Host-Systems.
- **Dell Videoprofil**— Beschreibt die Eigenschaften und Schnittstellen zur Ausführung von Systemverwaltungsaufgaben in Bezug auf die Verwaltung der Videocontroller eines Systems.
- **Dell Lizenzverwaltungsprofil** — Beschreibt die Klassen, Eigenschaften und Methoden für die Verwaltung der Lizenzen-Funktion auf den verwalteten Systemen.
- **Dell Ereignisfilterprofil** — Beschreibt die Klassen, Eigenschaften und Methoden zur Anzeige der Ereignisfilter und zum Festlegen von Aktionen und Benachrichtigungen für die Ereignisse.
- **Dell Sensorenprofil** — Beschreibt die Klassen, Eigenschaften und Methoden zur Verwaltung der Sensoren im verwalteten System.
- **Dell Energiezustandsverwaltungsprofil** — Beschreibt die Klassen, Eigenschaften und Methoden zur Verwaltung der Energie eines Systems.
- **Datensatzprotokoll** – definiert CIM-Klassen für die Darstellung verschiedener Arten von Protokollen.

Die Lifecycle-Controller - Remotedienste WS-MAN-Implementierung verwendet SSL an Port 443 für Transportsicherheit und unterstützt Basic-Authentifizierung. Webdiensteschnittstellen können durch wirksame Nutzung von Client-

Infrastruktur, z. B. Windows WinRM und Powershell CLI sowie Open Source-Dienstprogramme wie WSMANCLI und Anwendungsprogrammierungsumgebungen wie Microsoft .NET, eingesetzt werden.

Weitere nützliche Dokumente

Zusätzlich zu dieser Anleitung können Sie auf die folgenden Anleitungen zugreifen, die unter support.dell.com/manuals zur Verfügung stehen. Klicken Sie auf der Seite **Manuals** (Handbücher) auf **Software** → **Systems Management** (Systemverwaltung). Klicken Sie auf den entsprechenden Produktlink auf der rechten Seite, um auf die Dokumente zuzugreifen.

- *iDRAC7 Version 1.00.00 Infodatei* enthält Informationen über Einschränkungen, bekannte Probleme und Lösungen usw. zu den Lifecycle-Controller-Remote-Services.
- *Lifecycle-Controller-Webdienste Schnittstellenanleitung (Windows und Linux)* enthält Beispiele zur Verwendung der verschiedenen Methoden.
- *Dell Lifecycle-Controller Benutzernanleitung* enthält Informationen über die Verwendung der GUI-basierten Systemkonsole vor Laden des Betriebssystems.
- *Handbuch für die Systemverwaltungsübersicht* enthält Kurzinformationen über unterschiedliche, zum Durchführen von Systemverwaltungsaufgaben verfügbare Software.
- *Integrierter Dell Remote-Zugriff-Controller 7 (iDRAC7) Benutzerhandbuch* enthält Informationen über Konfiguration und Verwendung eines iDRAC7 für Rack, Tower- und Blade-Server, um per Remote-Zugriff Ihr System und dessen freigegebene Ressourcen über ein Netzwerk zu verwalten und zu überwachen.
- *Dell Repository Manager Benutzerhandbuch* stellt Informationen über das Erstellen aus Dell Update Packages (DUPs) bestehenden benutzerangepassten Paketen und Repositories für Systeme bereit, auf denen Microsoft Windows-Betriebssysteme ausgeführt werden.
- Im Abschnitt *Von Lifecycle-Controller unterstützte Dell-Systeme und Betriebssysteme* der Dell Systems Software Support Matrix wird eine Liste der Dell-Systeme und Betriebssysteme, die auf den Zielsystemen bereitgestellt werden können, zur Verfügung gestellt.
- *Technisches Handbuch für PERC H710, H710P und H810* enthält Spezifikationen und konfigurationsbezogene Informationen über die PERC H710-, H710P- und H810-Controller.
- *Dell Systems Build and Update Utility (SBUU) Benutzeranleitung* enthält Informationen über Bereitstellung und Aktualisierung von Dell-Systemen.
- Das *Glossar* enthält Informationen zu den in diesem Dokument verwendeten Begriffen.

Die folgenden Systemdokumente sind erhältlich, um weitere Informationen zur Verfügung zu stellen:


- *iDRAC7 Übersichts- und Funktionshandbuch* enthält Informationen über iDRAC7, seine lizenzierbaren Funktionen und Lizenzupgradeoptionen.
- In den mit dem System gelieferten Sicherheitshinweisen finden Sie wichtige Informationen zur Sicherheit und zu den Betriebsbestimmungen. Weitere Betriebsbestimmungen finden Sie auf der Website zur Einhaltung gesetzlicher Vorschriften unter www.dell.com/regulatory_compliance. Garantieinformationen können möglicherweise als separates Dokument beigelegt sein.
- In den zusammen mit der Rack-Lösung gelieferten *Anleitung für die Rack-Installation* wird beschrieben, wie das System in einem Rack installiert wird.
- Das *Handbuch zum Einstieg* enthält eine Übersicht über die Systemfunktionen, die Einrichtung des Systems und technische Daten.
- Im *Benutzerhandbuch* erhalten Sie Informationen über Systemfunktionen, zur Fehlerbehebung am System und zum Installieren oder Austauschen von Systemkomponenten.

Es stehen zusätzliche Implementierungsanleitungen, Informationsberichte, Profilspezifikationen, Dateien mit Klassendefinitionen (**.mof**) und Code-Beispiele zur Verfügung, auf die Sie über die folgenden Speicherorte zugreifen können:

- Lifecycle-Controller-Seite auf Dell TechCenter — delltechcenter.com/page/Lifecycle+Controller

- Lifecycle-Controller WS-Management Script Center — delltechcenter.com/page/Scripting+the+Dell+Lifecycle+Controller
- MOFs und Profile — delltechcenter.com/page/DCIM.Library
- DTMF-Website- www.dmtf.org/standards/profiles/
- *Lifecycle-Controller Web Services-Schnittstellenrichtlinie – Windows und Linux*

Kontaktaufnahme mit Dell

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

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

1. Besuchen Sie support.dell.com.
2. Wählen Sie Ihre Supportkategorie.
3. Wenn Sie kein US-Kunde sind, wählen Sie unten auf support.dell.com ihren Ländercode aus oder wählen Sie **All** (Alle), um weitere Auswahlmöglichkeiten anzuzeigen.
4. Klicken Sie je nach Bedarf auf den entsprechenden Service- oder Support-Link.

Verwenden von Remote-Services

Dieser Abschnitt beschreibt einige der Voraussetzungen die Ihnen bei den ersten Schritten mit der Remote-Services-Funktionalität und der effektiven Verwendung der neuen Funktionen helfen, um bessere Ergebnisse zu erzielen.

Allgemeine Voraussetzungen vor der Verwendung der Remote-Services

Für eine erfolgreiche Ausführung von Remoteaufgaben auf dem Server müssen Sie sicherstellen, dass die folgenden Vorbedingungen erfüllt sind:

- Lifecycle-Controller 2 Version 1.00.00 wurde installiert.
- iDRAC7-Firmware Version 1.00.00
- Die aktuelle BIOS-Version ist installiert. Weitere Informationen zu den mit Dell-Systemen verknüpften BIOS-Versionen finden Sie unter *iDRAC7-Version 1.00.00 Infodatei*.
- Für die Ausführung der Aufgaben steht ein für die WS-Verwaltung aktiviertes Dienstprogramm bereit.
- Laden Sie das aktuelle Handbuch *Lifecycle-Controller Web Services - Schnittstellenrichtlinie für Windows and Linux* herunter. Weitere Informationen finden Sie unter delltechcenter.com/page/Lifecycle+Controller.
- Collect System Inventory on Restart (CSIOR - Bei Neustart Systeminformationen sammeln) ist aktiviert.

Web Services-Setup

Stellen Sie beim Einstellen des Systems sicher, dass die folgenden Bedingungen zutreffen:

- Verwenden Sie für den Zugriff auf Remote-Services die folgenden Tools:
 - Auf Windows basierter WinRM-Client, welcher bereits auf dem Betriebssystem installiert ist, anderenfalls können Sie ihn unter support.microsoft.com/kb/968930 herunterladen.
 - Linux-basierte Clients, wie z.B. das auf OpenWSMan (Open-Source) basierte CLI. Weitere Informationen finden Sie unter openwsman.org.
 - Java-basierter Client, wie z.B. das Open-Source Projekt **Wiseman**. Weitere Informationen finden Sie unter wiseman.dev.java.net.
- Stellen Sie sicher, dass Sie die IP-Adresse der Systeme in Ihrem Netzwerk kennen. Sie müssen auch in der Lage sein, sich mit iDRAC zu verbinden. Lesen Sie für weitere Informationen unter support.dell.com/manuals nach.
- Stellen Sie die ordnungsgemäße Netzwerkkonfiguration des Clients und verwalteten Servers sicher. Überprüfen Sie die Konnektivität mittels des Ping-Dienstprogramms. Stellen Sie anschließend sicher, dass der Client und das Netzwerk die HTTP- und SSL-Protokolle zulassen.


WinRM-Client

Installieren Sie für die Verwendung der Remote-Services-Funktionen den WinRM-Client auf der Konsole. Microsoft Windows 7, Microsoft Windows Vista und Microsoft Windows Server 2008 enthalten eine Standardkomponente, die WS-MAN genannt wird. Diese Komponente enthält den WinRM-Client. Für Microsoft Windows XP und Microsoft Server 2003 können Sie diese Komponente unter support.microsoft.com/kb/968929 herunterladen und installieren. Sie müssen über lokale Administratorrechte für Installation verfügen.

Sie müssen den Client für die Verbindung konfigurieren. Weitere Informationen finden Sie unter *Lifecycle-Controller-Webdienste – Schnittstellenrichtlinie - Windows Version*.

OpenWSMan-Client

Der OpenWSMan-Client ist die WS-Verwaltungs-CLI, die Teil des Open-Source Projekts Openwsman ist. Gehen Sie zum Herunterladen, Erstellen, Installieren und Verwenden der WS-Management CLI und OpenWSMan-Pakete von sourceforge.net auf openwsman.org, um Download-Links zu erhalten.

 **ANMERKUNG:** Sie müssen den Client für die Verbindung konfigurieren. Weitere Informationen zur Konfiguration finden Sie unter *Lifecycle-Controller Web Services – Schnittstellenrichtlinie – Linux Version*.

Verwenden von Anwendungen

Anwendungsstruktur

Die folgenden Anwendungen sind als Referenz verfügbar:

- **Vorbedingungen** – Listet die Vorbedingungen vor der Ausführung des Szenarios auf.
- **Funktionsbeschreibung** – Beschreibt das Szenario und bietet eine Kurzbeschreibung zu den Funktionen.
- **Wichtig** – Listet sämtliche Sonderbedingungen auf, die während der Ausführung des Szenarios auftreten.
- **Funktion oder Systemverhalten** – Listet die Funktionsweise der Funktions- und Systemantworten auf.
- **Nachträgliche Bedingungen** – Listet die Aufgaben mit nachträglichen Bedingungen auf, die durch den Anwender bzw. durch das System aufgeführt werden müssen.
- **Referenzen** – Nennt den Speicherort des Handbuchs Lifecycle Controller Web Services – Schnittstellenrichtlinie – Windows und Linux, in dem Sie detailliertere Informationen zur Ausführung der Schritte finden.

Anleitung zum Lesen von Anwendungen

- Lesen und vollziehen Sie das Szenario nach.
- Richten Sie die erforderliche Infrastruktur ein, und führen Sie alle Vorbedingungsaufgaben ab.
- Halten Sie sämtliche Sonderbedingungen ein.
- Vollziehen Sie nach, wie die Funktion funktioniert und wie das System reagiert.
- Führen Sie diese Schritte aus, und orientieren Sie sich dabei an der Referenztafel, aus der Sie die entsprechenden Aufgabendetails in *Lifecycle-Controller Web Services – Schnittstellenrichtlinie – Windows und Linux* und Zusatzinformationen wie z. B. Methoden, Klassen, Ein- und Ausgabeparameter entnehmen können, die im Profildokument und der MOF-Datei enthalten sind.

Anwendungsszenarien

- [Exportieren von Serverprofilen auf die iDRAC vFlash-Karte oder die Netzwerkfreigabe](#)
- [Importieren des Serverprofils von einer iDRAC vFlash-Karte oder einer Netzwerkfreigabe](#)
- [RAID-Konfiguration](#)
- [Ändern der Merkmale und der Bandbreite einer Partition für einen CNA](#)
- [Einrichten der virtuellen Adressattribute](#)
- [Einrichten der Attribute „Boot Target–iSCSI“ und „FCoE“](#)
- [Abrufen und Festlegen der iDRAC-Attribute](#)
- [Abrufen und Festlegen von iDRAC-Benutzern und -Rollen](#)

- [Weiterleiten von Änderungen an der iDRAC-IP-Adresse](#)
- [Festlegen, Ändern und Löschen des BIOS-Kennworts](#)
- [Abrufen des Remotedienststatus](#)

Auto-Ermittlung und Handshake

Die Funktion der Auto-Ermittlung im iDRAC erlaubt neu installierten Servern, automatisch die Remote-Verwaltungskonsole zu ermitteln, die den Bereitstellungsserver hostet. Der Bereitstellungsserver stellt dem iDRAC benutzerdefinierte Administrator-Anmeldeinformationen zur Verfügung, damit die Verwaltungskonsole das neu installierte verwaltete System ermitteln und verwalten kann.

Falls Sie ausdrücklich ein Dell-System bestellt haben, bei dem die Auto-Ermittlungsfunktion **Aktiviert** ist (die Werkseinstellung ist **Deaktiviert**), wird der iDRAC mit aktiviertem DHCP und deaktivierten Benutzerkonten geliefert. Wenn die Funktion der Auto-Ermittlung auf **Deaktiviert** gesetzt ist, können Sie diese Funktion manuell aktivieren und das Standard-Administratorkonto über die *iDRAC7 Settings Utility* (iDRAC6-Einstellungen-Dienstsprogramm) deaktivieren. Weitere Informationen zur Auto-Ermittlung finden Sie unter [Lifecycle-Controller-Verwaltungsprofil](#).

Sie können zum Einstellen der IP-Adresseneigenschaft des Bereitstellungsservers unter Verwendung von WS-Management die Methode **SetAttribute()** der Klasse `DCIM_LCService` aufrufen. Beziehen Sie sich weitere Informationen über die Verwendung der **SetAttribute()** Aufrufe auf das `DCIM_LCManagement`-Profil oder den *Lifecycle-Controller Interface Guide (Windows and Linux)*, der auf delltechcenter.com/page/Lifecycle+Controller zur Verfügung steht.


Für eine erfolgreiche Ausführung von Remoteaufgaben auf dem Server müssen Sie sicherstellen, dass die folgenden Vorbedingungen erfüllt sind:

- [Allgemeine Voraussetzungen vor der Verwendung der Remote-Services](#)
- Dell Deployment Pack wird auf dem Bereitstellungsserver installiert.
- Collect System Inventory on Restart (CSIOR) ist aktiviert.

iDRAC für Auto-Ermittlung konfigurieren

So aktivieren Sie die Auto-Ermittlungs-Funktion manuell:

1. Installieren Sie das System am gewünschten Speicherort.
2. Schalten Sie das verwaltete System ein.
3. Drücken Sie während des Systemstarts **<F2>**.
Die Seite **System-Setup-Hauptmenü** wird angezeigt.
4. Klicken Sie auf **iDRAC-Einstellungen**.
Die Seite **iDRAC-Einstellungen** wird angezeigt.
5. Legen Sie die folgenden Einstellungen fest:
 - Netzwerkeinstellungen— Stellen Sie **NIC aktivieren auf Aktiviert** ein (nur für Bladeserver).
 - Allgemeine Einstellungen— Stellen Sie **Auto-Konfiguration Domänenname auf aktiviert** ein.
 - IPv4-Einstellungen — Stellen Sie **IPv4 aktivieren auf Aktiviert** ein.

 **ANMERKUNG:** Obwohl die Infrastruktur IPv6 unterstützt, ist dieses während der automatischen Ermittlung deaktiviert. Es kann nach Bereitstellen des Servers aktiviert werden.

- DHCP — Stellen Sie **DHCP aktivieren auf Aktiviert** ein und stellen Sie **DHCP zum Bezug von DNS-Server-Adressen verwenden auf Aktiviert** ein.
6. Klicken Sie auf **Zurück** und klicken Sie auf **Benutzerkonfiguration**.

Die Seite **Benutzerkonfiguration** wird angezeigt.

7. Wählen Sie unter **Benutzer aktivieren Deaktiviert** aus.

Hierdurch wird das standardmäßige Administratorkonto deaktiviert.

8. Klicken Sie auf **Zurück** und klicken Sie auf **Remote-Aktivierung**.

Die Seite **Remote-Aktivierung** wird angezeigt.

9. Wählen Sie unter **Automatische Ermittlung aktivieren Automatische Ermittlung** aus.



ANMERKUNG: Sie müssen zum Aktivieren der Funktion zur automatischen Ermittlung das Administratorkonto deaktivieren.

10. Geben Sie im Kästchen **Bereitstellungsserver** die IP-Adresse des Bereitstellungsservers oder eine Hostnamen-Zeichenkette ein. Die folgenden Bedingungen gelten für das Verwenden eines Befehls zum Einrichten der Bereitstellungsserver-IP-Adresse oder des Host-Namens:

- Stellen Sie beim Ausstellen von `racadm racresetcfg` oder dem Aktualisieren des iDRAC7 sicher, dass Sie während des Zurücksetzens des iDRAC7 auf die Standardeinstellungen die Option **Konfiguration beibehalten** aktivieren. Wenn diese option deaktiviert wird, wird die IP bzw. der Hostname des Servers gelöscht.
- Die Auto-Ermittlungsfunktion verwendet die/den neu eingestellte(n) IP-Adresse oder Hostnamen nicht für etwaige laufende Handshakes, sondern verwendet dies nur während des nächsten Handshake-Vorgangs.

11. Klicken Sie auf **Zurück** und dann auf **Fertig stellen**.

12. Klicken Sie auf **Ja**, um die Änderungen zu speichern. Drücken Sie <Esc>, um das **System-Setup** zu beenden.

Zeichenkettenformat Bereitstellungsserver

Die Funktion „Auto-Ermittlung“ unterstützt die Einstellung mehrerer IP-Adressen und/oder Hostnamen unter Verwendung des folgenden Formats:

- Die Zeichenkette ist eine Liste mit IP-Adressen und/oder Hostnamen und Schnittstellen, deren Einträge durch Kommas getrennt sind.
- Host-Name ist gültig.
- IPv4-Adresse – beginnt mit ‘(‘ und endet mit ‘)’, wenn gleichzeitig mit einem Host-Namen angegeben.
- Auf jede IP-Adresse bzw. auf jeden Host-Namen kann optional ein ‘:’ und eine Schnittstellenummer folgen.
- Beispiele gültiger Zeichenketten sind – hostname, hostname.domain.com

Einstellen der Bereitstellung auf dem gewünschten Speicherort

So stellen Sie die Bereitstellung auf dem gewünschten Speicherort ein:

1. Schalten Sie das verwaltete System ein.
2. Drücken Sie während des Systemstarts <F10> **Lifecycle Controller**.
Die Seite **Lifecycle Controller** wird angezeigt.
3. Navigieren Sie zu **System-Setup** → **Erweiterte Konfiguration** → **iDRAC-Einstellungen** .
4. Klicken Sie auf **Weiter**, um auf die folgenden Seiten zu navigieren und verschiedene Einstellungen anzugeben:
 - Netzwerkeinstellungen— Stellen Sie **NIC aktivieren** auf **Aktiviert** ein (nur für Bladeserver).
 - Allgemeine Einstellungen— Stellen Sie **Auto-Konfiguration Domänenname** auf **aktiviert** ein.
 - IPv4-Einstellungen — Stellen Sie **IPv4 aktivieren** auf **Aktiviert** ein.



ANMERKUNG: Obwohl die Infrastruktur IPv6 unterstützt, ist dieses während der automatischen Ermittlung deaktiviert und kann nach Bereitstellen des Servers aktiviert werden.

- DHCP — Stellen Sie **DHCP aktivieren** auf **Aktiviert** ein und stellen Sie **DHCP zum Bezug von DNS-Server-Adressen verwenden** auf **Aktiviert** ein.
5. Klicken Sie auf der letzten Seite auf **Übernehmen**.
 6. Klicken Sie auf **Fertig stellen**.
 7. Klicken Sie auf **Beenden und Neustarten**.

Auto-Ermittlung des verwalteten Systems

So ermitteln Sie das verwaltete System automatisch:

1. Schließen Sie das System ans Netzwerk an.
2. Schalten Sie das verwaltete System ein.

Das System führt die folgenden Vorgänge durch:

- iDRAC startet, ruft die Bereitstellungsserver-IP-Adressen oder -Host-Namen von DHCP/DNS ab und gibt sich als Bereitstellungsserver zu erkennen.
- Der Bereitstellungsserver überprüft und akzeptiert die sichere Handshake-Sitzung vom iDRAC.
- Der Bereitstellungsserver bietet benutzerdefinierte Benutzeranmeldeinformationen mit Administratorrechten zu iDRAC.
- iDRAC empfängt und vervollständigt das sichere Handshake.

Nachdem das verwaltete System ermittelt wurde, kann iDRAC über die neu erhaltenen Anmeldeinformationen verwaltet werden und Aufgaben wie die Remote-Betriebssystembereitstellung und Systemverwaltungs-Tasks durchführen.

Konfiguration von DHCP oder DNS

Bevor Sie das System in das Netzwerk einbinden und die Auto-Ermittlungsfunktion aktivieren, ist sicherzustellen, dass der DHCP-Server (Dynamic Host Configuration Protocol)/das Domain Name System (DNS) konfiguriert ist. Wenn die Bereitstellungsserver-IP-Adresse oder der Hostname durch einen WS-Management-Befehl, oder durch die Verwendung von F2- oder F10-basierten Bereitstellungsservereingaben nicht bereitgestellt wird, dann verwenden Sie eine der folgenden DHCP- oder DNS-basierten Methoden zur Konfiguration von DHCP oder DNS, sodass iDRAC den Domännennamen oder die Adresse des Bereitstellungsservers ermitteln kann:

- Der DHCP-Server bietet eine Liste mit Bereitstellungsserver-Standorten, deren Einträge durch Kommas getrennt sind. Es wird hierfür eine Vendor-Scope-Option 43 der Klasse, LifecycleController, Option 1 verwendet. Diese Standorte können ein Host-Name oder eine IP-Adresse sein und optional eine Schnittstelle enthalten. Der iDRAC löst den Host-Namen der Verwaltungskonsole über ein DNS-Lookup in eine IP-Adresse auf.
- Der DNS-Server spezifiziert die Dienstopcion `_dcimprovsrv._tcp`, die in eine IP-Adresse aufgelöst wird.
- Der DNS-Server spezifiziert den standardmäßigen „Host A“-Datensatz der automatischen Ermittlung namens `DCIMCredentialServer`, wodurch in die IP-Adresse des Bereitstellungsservers aufgelöst wird.

Weitere Informationen zur Konfiguration von DHCP und DNS finden Sie unter *Netzwerk-Setup-Spezifikation für die Lifecycle-Controller-Auto-Ermittlung* im Dell Enterprise Technology Center unter www.delltechcenter.com/page/Lifecycle+Controller.

Anzeigen des Ermittlungsstatus auf der Frontblendenanzeige

Sie können den Status der Ermittlung und den Handshake-Fortschritt auf der Anzeige der Frontblende anzeigen lassen:

-  **ANMERKUNG:** Die Frontblendenanzeige ist nur auf Rack- und Towerservern verfügbar. Bei Bladeservern müssen Sie die Frontblendenanzeige auf dem CMC anzeigen lassen.

- In Betrieb
- Gestoppt
- Unterbrochen
- Abgeschlossen


Wenn der Auto-Ermittlungsvorgang läuft, können Sie seinen Fortschrittscode anzeigen lassen, der entsprechend Auskunft darüber gibt, wie weit der letzte Versuch gekommen ist (d.h. ob Ermittlung und Handshake blockiert werden, weil die NIC deaktiviert ist, oder ein Administratorkonto aktiviert ist, usw.). Sie können auch die verbleibende Zeit vor einer Zeitüberschreitung anzeigen lassen.

Die Auto-Ermittlung in neuen Umgebungen neu einleiten

Sie können die Auto-Ermittlung auch dann unter Verwendung der Remote-Services neu einleiten, wenn das System zuvor die Auto-Ermittlung abgeschlossen hat. Verwenden Sie zur erneuten Einleitung die folgenden Optionen:

- Ob die Auto-Ermittlung sofort ausgeführt wird oder beim nächsten Aus- und Einschaltvorgang. Diese Eingabe ist obligatorisch.
- Bereitstellungsserver-IP-Adresse oder Host-Name. Dies ist optional.

Sie müssen z.B. die Auto-Ermittlung neu einleiten, um das verwaltete System von einem Datacenter in ein anderes zu verschieben. Die Auto-Ermittlungseinstellungen bleiben gemeinsam mit den für die Ermittlung verwendeten Anmeldeinformationen erhalten. Wenn das System im neuen Datacenter eingeschaltet wird, wird die Auto-Ermittlung gemäß den werkseitigen Standardeinstellungen ausgeführt und erstellt für das neue Datacenter die neuen iDRAC-Benutzeranmeldeinformationen.

 **ANMERKUNG:** iDRAC-Administrator oder ein iDRAC-Benutzer mit Rechten zum Ausführen von Serverbefehlen (Execute Server Command) wird benötigt, um WS-Management-Befehle auszuführen.

Die folgenden Vorgänge werden während der Neueinleitung der Auto-Ermittlung standardmäßig durchgeführt:

- NIC aktivieren (Blade-Server)
- IPv4 aktivieren
- DHCP aktivieren
- Löscht alle Administratorkonten mit Ausnahme von Benutzer-ID 2, die das standardmäßige „root“-Administratorkonto ist.
- Active Directory deaktivieren
- DNS-Serveradresse vom DHCP abrufen
- DNS-Domänenname vom DHCP abrufen

Lizenzenverwaltung

Sie können die Lizenzen zum Aktivieren oder Deaktivieren der verschiedenen Systemverwaltungsfunktionen verwalten. Unter Verwendung der Remote-Dienste können Sie folgendes tun:

- Bezug einer Liste mit installierten Lizenzen
- Bezug einer Liste mit lizenzierbaren Geräten
- Installieren oder Löschen einer Lizenz
- Exportieren der Lizenz

Anzeigen der installierten Lizenzen

- Führen Sie den Auflistungsvorgang in der Klasse `DCIM_License` durch, um die Instanzeigenschaften aller auf dem System installierten Lizenzen anzuzeigen.
- Führen Sie den „Get“ (Einholen)- Vorgang in der Klasse `DCIM_License` unter Verwendung der richtigen Instanzkennungen der benötigten Lizenz durch, um die zugehörigen Eigenschaften anzuzeigen.

Anzeigen von lizenzierbaren Geräten

- Führen Sie den Auflistungsvorgang in der Klasse `DCIM_LicensableDevice` durch, um die Instanzeigenschaften aller auf dem System installierten lizenzierbaren Geräten anzuzeigen.
- Führen Sie den „Get“ (Einholen)-Vorgang in der Klasse `DCIM_LicensableDevice` unter Verwendung der richtigen Instanzkennungen des benötigten lizenzierbaren Geräts durch, um die zugehörigen Eigenschaften anzuzeigen.

Installieren einer Lizenz

Für eine erfolgreiche Ausführung von Remoteaufgaben auf dem Server müssen Sie sicherstellen, dass die folgenden Vorbedingungen erfüllt sind:

- [Allgemeine Vorbedingungen vor Verwendung der Remote-Services](#)
- Wenn Sie eine Netzwerkfreigabe verwenden, dann richten Sie eine CIFS- oder NFS-Freigabe ein und kopieren Sie die Lizenz auf die Netzwerkfreigabe.

So installieren Sie eine Lizenz:

1. Listen Sie die Klasse `DCIM_LicensableDevice` auf, um die verfügbaren lizenzierbaren Geräte anzuzeigen. Notieren Sie sich die FQDD des lizenzierbaren Geräts, auf dem die Lizenz installiert wird.
2. Beziehen Sie sich auf die Eigenschaft `LicenseList`, um zu überprüfen, dass die Lizenzen derzeit nicht auf dem lizenzierbaren Gerät installiert sind. Die Eigenschaft `LicenseList` zeigt die Liste der Entitlements-IDs (Berechtigungskennungen) an, die derzeit auf dem Gerät installiert sind. Wenn Lizenzen installiert sind, dann löschen Sie die Lizenzen unter Verwendung der Methode `DeleteLicense()`, indem Sie die Entitlement-ID der Lizenz als Eingabeparameter verwenden. Verwenden Sie alternativ dazu die FQDD des lizenzierbaren Geräts als Eingabeparameter, um alle auf diesem Gerät installierten Lizenzen zu löschen.
3. Sie können entweder die Methode `ImportLicense()` oder die Methode `ImportLicenseFromNetworkShare()` verwenden.

4. Installation unter Verwendung der Methode **ImportLicense()**:
 - Codieren Sie die Lizenzdatei mit Base64.
 - Verwenden Sie die codierte Lizenzdatei und die FQDD des lizenzierten Geräts zur Vorbereitung der Eingabeparameter.
 - Rufen Sie die Methode **ImportLicense()** auf.
5. Installation unter Verwendung der Methode **ImportLicenseFromNetworkShare()**:
 - Verwenden Sie die Netzwerkfreigabeparameter und die FQDD des lizenzierten Geräts zur Vorbereitung der Eingabeparameter.
 - Rufen Sie die Methode **ImportLicenseFromNetworkShare()** auf.
 - Führen Sie den Get-Vorgang auf die Klasse `DCIM_LifecycleJob` aus, indem Sie die zurückgegebene Aufgabenkennung (Job-ID) als Instanzkennung (Instanz-ID) zur Anzeige des Status der Lizenzimportierungsaufgabe (`import license`) verwenden.

Referenzen für das Installieren einer Lizenz

Lesen Sie die folgenden Dokumente, um weitere Informationen zu erhalten:

- **Profil** — Dell_LicenseManagement-Profil
- **MOFs**
 - `DCIM_LicensableDevice.mof`
 - `DCIM_License.mof`
 - `DCIM_LicenseManagementService.mof`
 - `DCIM_LCElementConformsToProfile.mof`
 - `DCIM_LCRegisteredProfile.mof`

Für weitere Informationen, siehe:

- [Allgemeine Vorbedingungen vor Verwendung der Remote-Services](#)
- [In Lifecycle-Controller lizenzierte Funktionen](#)

Ersetzen einer Lizenz

So ersetzen Sie eine Lizenz:

1. Zählen Sie die Klasse `DCIM_LicensableDevice` auf, um die FQDD des lizenzierten Geräts zu erhalten.
2. Zeigen Sie die Eigenschaft `LicenseList` an und notieren Sie sich die Berechtigungs-ID der zu ersetzenden Lizenz.
3. Codieren Sie die neue Lizenzdatei mit Base64.
4. Unter Verwendung der verschlüsselten Lizenzdatei wird die FQDD des lizenzierten Geräts und die Berechtigungs-ID der alten Lizenz zur Vorbereitung der Eingabeparameter verwendet.
5. Rufen Sie zum Ersetzen einer Lizenz die Methode **ReplaceLicense()** auf.

Löschen einer Lizenz

Eine einzelne Lizenz kann unter Verwendung der Berechtigungs-ID der Lizenz und Aufrufen der Methode **DeleteLicense()** gelöscht werden. Alternativ dazu können alle Lizenzen von einem lizenzierten Gerät gelöscht werden, indem die FQDD des lizenzierten Geräts verwendet, und die Methode **DeleteLicense()** aufgerufen wird.

Exportieren einer Lizenz

Sie können die Lizenzen exportieren, indem Sie eine der vier Exportmethoden verwenden:

- **ExportLicense()** — Diese Methode exportiert eine durch die Berechtigungs-ID spezifizierte Einzellizenz. Die Lizenz ist ein Ausgabeparameter der Methode und base64-codiert.
- **ExportLicenseToNetworkShare()** — Diese Methode exportiert eine durch die Berechtigungs-ID spezifizierte Einzellizenz auf eine NFS- oder CIFS-Netzwerkfreigabe.
- **ExportLicenseByDevice()** — Diese Methode exportiert alle Lizenzen, die auf einem lizenzierbaren Gerät installiert sind. Die Lizenzen sind ein Ausgabeparameter der Methode und base64-codiert.
- **ExportLicenseByDeviceToNetworkShare()** — Diese Methode exportiert alle Lizenzen, die auf einem lizenzierbaren Gerät installiert sind auf eine NFS- oder CIFS-Netzwerkfreigabe.



ANMERKUNG: Wenn von einem lizenzierbaren Einzelgerät mehrere Lizenzen exportiert werden, werden an die Dateinamen die Suffixe **_0.xml**, **_1.xml**, **_2.xml**, und so weiter angehängt.

Verwaltung von Zertifikaten

Verwenden Sie die Zertifikatverwaltungsfunktion, um die benutzerdefinierten Zertifikate auf iDRAC7 zu übertragen und zur Verbesserung der Sicherheit ein eindeutiges Zertifikat auf Basis der Service-Tag-Nummer eines Systems zu erstellen. Während Sie den Auftrag in Arbeit geben, können Sie Dell zur Rücksetzung des Systems auf die Werkseinstellungen mit dem Zertifikat Ihrer Wahl auffordern, indem Sie den bei Dell erhältlichen Vorgang Custom Factory Install (CFI) verwenden.

Erstellen von benutzerdefinierten Root-Client-Zertifikaten für den Bereitstellungsserver

Die Methode **DownloadClientCerts()** in der Klasse `DCIM_LCService` kann aufgerufen werden, um ein benutzerdefiniert signiertes Client-Zertifikat für die Auto-Ermittlung zu erzeugen. Für diese Methode wird ein von einer Zertifizierungsstelle erstelltes Schlüsselzertifikat sowie in Beziehung stehende Hash- und Kennwortparameter als Eingabe verwendet. Das bereitgestellte Schlüsselzertifikat wird zum Signieren eines Zertifikats verwendet, das die Service-Tag-Nummer des Systems als allgemeiner Name (CN, Common Name) enthält. Durch diese Methode wird eine Auftrags-ID ausgegeben, die zum Überprüfen des Erfolgs des Herunterladevorgangs, der Erstellung und der Installation des privaten Auto-Ermittlungs-Client-Zertifikats verwendet werden kann. Beispiele für Aufrufe von Befehlszeilen unter Verwendung von WinRM und WSMANCLI finden Sie unter *Lifecycle-Controller Web Services – Schnittstellenrichtlinie – Windows und Linux*.

Benutzerdefinierte Serverzertifikate bereitstellen

Die Methode **DownloadServerPublicKey()** der Klasse `DCIM_LCService` kann zum Übertragen des CA-Zertifikats aufgerufen werden, das für die Signierung aller Bereitstellungsserver im Bereitstellungsnetzwerk verwendet wird.


 **ANMERKUNG:** Das vertrauenswürdige CA-Zertifikat wird zum Authentifizieren aller Bereitstellungsserver verwendet.

Stellen Sie sicher, dass das Bereitstellungsserverzertifikat selbst-signiert ist, bevor Sie es auf dem iDRAC verwenden.

Für diese Methode wird ein von einer Zertifizierungsstelle erstelltes Schlüsselzertifikat sowie in Beziehung stehende Hash- und Hashtypparameter als Eingabe verwendet. Durch Anwendung dieser Methode wird eine Auftrags-ID ausgegeben, die zum Überprüfen des Erfolgs der Verarbeitung und Installation des öffentlichen Schlüssels des Bereitstellungsservers verwendet werden kann. Beispiele für Aufrufe von Befehlszeilen unter Verwendung der WS-Verwaltungsdienstprogramme finden Sie unter *Lifecycle Controller Web Services – Schnittstellenrichtlinie – Windows und Linux Version*. CIM-Profilspezifizierung und zugehörige MOF-Dateien stehen unter delltechcenter.com/page/DCIM.Library zur Verfügung

Benutzerdefinierte Zertifikate löschen

Sie können alle benutzerdefinierten Zertifikate löschen, die auf dem verwalteten System hochgeladen oder erstellt werden. Unter Verwendung dieser Funktion können Sie alle benutzerdefiniert signierten Zertifikate vom Server löschen, wann immer dies notwendig ist.

 **ANMERKUNG:** Diese Funktion löscht nicht die Werkzertifikate.

Benutzerdefiniertes Löschen des öffentlichen Schlüssels

Verwenden Sie die Methode **DeleteAutoDiscoveryServerPublicKey()** in der Klasse `DCIM_LCService` zum Löschen des CA-Zertifikates, das zum Validieren oder Authentifizieren von Server-Zertifikaten verwendet wird.

Benutzerdefiniertes Löschen des Client-Zertifikates

Verwenden Sie die Methode **DeleteAutoDiscoveryClientCerts()** in der Klasse `DCIM_LCService` zum Löschen eines Client-Zertifikates und privaten Schlüssels.

Ändern des Web Server oder WS-MAN-Verschlüsselungszertifikates und des privaten Schlüssels von PKCS #12

Um das Zertifikat und Schlüssel zu ändern:

1. Generieren Sie eine CSR und einen privaten Schlüssel. Die CSR muss durch eine ZS signiert werden.
2. Kombinieren Sie das Zertifikat mit dem privaten Schlüssel und verschlüsseln Sie es anschließend als PKCS#12-Datei.
3. BASE64-kodieren Sie die PKCS#12-Datei, um sie von binär auf Text zu konvertieren, sodass Sie diese als WS-MAN Parameter weitergeben können.
4. Kopieren Sie den Inhalt des aktiven Zertifikates in eine XML-Datei.

Verwaltung von Server-Zertifikaten


Für eine erfolgreiche Ausführung von Remoteaufgaben auf dem Server müssen Sie sicherstellen, dass die folgenden Vorbedingungen erfüllt sind:

- [Allgemeine Voraussetzungen vor der Verwendung der Remote-Services](#)
- Uhrzeit wurde korrekt auf iDRAC eingestellt.

Das Zertifikat ist auf einigen Systemen abgelaufen und muss erneut hochgeladen werden. Das Zertifikat authentifiziert Web-GUI, WS-Management, RACADM, Active Directory und LDAP-Sitzungen.

So verwalten Sie Server-Zertifikate:

 **ANMERKUNG:** Die Methode startet alle Webdienste neu und schließt alle aktiven Sitzungen.

 **ANMERKUNG:** Die CA, die das neue Serverzertifikat signiert hat, muss auf allen Clients zur vertrauenswürdigen Root-CA-Liste hinzugefügt werden.

1. Erstellen Sie eine CSR und einen privaten Schlüssel (ohne Kennwortschutz) — `openssl req -new -nodes`.
2. Signieren Sie die CSR entweder unter Verwendung von „`openssl ca`“, oder laden Sie sie auf einen signierenden Webserver hoch.
3. Kopieren Sie das Zertifikat und den privaten Schlüssel in eine Datei (PEM-Datei) — `cat cert.pem key.txt > cert_key.pem`.
4. Konvertieren Sie `cert_key.pem` nach pkcs12 — `openssl pkcs12 -export -in cert_key.pem -passin file:password.txt -out new.pfx`
5. Codieren Sie die pkcs12 base64-Datei — `openssl base64 -export -in new.pfx -out new_pfx.txt`.

6. Verwenden Sie den Inhalt von **new_pfx.txt** als einen Parameter für den WS-Management-Befehl.
7. Rufen Sie die Methode **SetCertificateAndPrivateKey()** mit den erforderlichen Parametern auf.
Nach Festlegen des Serverzertifikats starten die Webdienste neu. Alle Sitzungen werden beendet und neue WS-Management-Befehle müssen das neue Serverzertifikat akzeptieren.

Referenzen für die Verwaltung von Serverzertifikaten


 **ANMERKUNG:** Die in dieser Tabelle referenzierten Abschnitte enthalten ausschließlich allgemeine Beispiele.

Tabelle 2. Schrittnummer und Speicherort

Schrittnummer	Speicherort der Speicherrichtlinie für Lifecycle-Controller-Webdienste (Windows oder Linux)
-	12.10 — iDRAC-Zertifikat und privaten Schlüssel festlegen
Profile	
DCIM_LCManagement Profile	
MOFs	
DCIM_LCService.mof	

Directory CA-Zertifikatverwaltung

Zum Authentifizieren von Active Directory- oder LDAP-Sitzungen muss das vertrauenswürdige Stamm-CA-Zertifikat hochgeladen werden.

Für eine erfolgreiche Ausführung von Remoteaufgaben auf dem Server müssen Sie sicherstellen, dass die folgenden Vorbedingungen erfüllt sind:

- [Allgemeine Vorbedingungen vor der Verwendung der Remotedienste](#)
- Uhrzeit auf iDRAC wurde korrekt eingestellt.

So verwalten Sie Directory-CA-Zertifikate:

 **ANMERKUNG:** Die Methode startet alle Webdienste neu und schließt alle aktiven Sitzungen.

1. Laden Sie das CA-Zertifikat vom LDAP- oder AD-Server herunter.
2. Verwenden Sie openssl oder ein anderes Tool, um es im base64-Format zu codieren.
3. Rufen Sie die Methode **SetPublicCertificate()** mit den erforderlichen Parametern auf.
Nach Einstellen des Serverzertifikates werden die Webdienste neu gestartet. WS-Management-Befehle müssen das neue Serverzertifikat akzeptieren.

Referenzen für die Verwaltung von Directory CA-Zertifikaten

 **ANMERKUNG:** Die in dieser Tabelle referenzierten Abschnitte enthalten ausschließlich allgemeine Beispiele.

Tabelle 3. Schrittnummer und Speicherort

Schrittnummer	Speicherort der Speicherrichtlinie für Lifecycle Controller-Webdienste (Windows oder Linux)
-	12.9 — Öffentliche Zertifikate festlegen
Profile	

Schrittnummer	Speicherort der Speicherrichtlinie für Lifecycle Controller-Webdienste (Windows oder Linux)
DCIM_LCService	
MOFs	
DCIM_LCService.mof	

Bereitstellen des Betriebssystems

Die Funktionen der Betriebssystembereitstellung im Remote-Zugriff ermöglichen die Bereitstellung eines Betriebssystems im Remote-Zugriff unter Verwendung von WS-MAN-Webdienstprotokollen und CIFS- und NFS-Netzwerk-Dateifreigabe-Protokollen. Detaillierte Angaben zu den Schnittstellenspezifikationen und den Dateien zur Klassendefinition (.mof) finden Sie im Lifecycle-Controller-Bereich im Dell Enterprise Technology Center unter **delltechcenter.com**. Die folgenden Funktionen stehen in Form extrinsischer Methoden zur Verfügung, die je nach Anwendungsfall in verschiedenen Kombinationen verwendet werden können, um eine End-to-End OS-Bereitstellung auf dem Server durchzuführen:

- Aktivieren Sie per Remote-Verbindung die lokale Anzeige der integrierten Treiber für das ausgewählte Betriebssystem als ein emuliertes USB-Gerät für den Server, das automatisch während der Installation installiert wird.
- Laden Sie per Remote-Verbindung integrierte Treiber für ein gewähltes Betriebssystem auf einer CIFS- oder NFS-Netzwerkfreigabe, die später für die Betriebssystembereitstellung genutzt werden kann.
- Starten Sie auf ein ISO-Abbild, das auf einer Netzwerkfreigabe liegt, um eine Installation des Betriebssystems zu initiieren.
- Laden Sie das ISO auf eine vFlash SD-Karte herunter und starten Sie von der Karte, um eine Installation des Betriebssystems zu initiieren.
- Verbinden Sie ein ISO über das Netzwerk, binden Sie es als virtuelles USB CD-ROM-Gerät in den Server ein und starten Sie den Server bei jedem Neustart des Servers von dem ISO aus.
- Einmalige Startsequenz in das PXE.
- Einmalige Startsequenz auf die Festplatte.

Lesen Sie für weitere Informationen [Betriebssystembereitstellungsprofil](#)

Bereitstellen des Betriebssystems

Für eine erfolgreiche Ausführung von Remoteaufgaben auf dem Server müssen Sie sicherstellen, dass die folgenden Vorbedingungen erfüllt sind:



- [Allgemeine Voraussetzungen vor der Verwendung der Remote-Services](#)
- Startlaufwerk ist für die Installation des Betriebssystems auf dem Server vorhanden.
- Es wird empfohlen, dass das neueste Treiberpaket installiert wird, sodass Treiber für neuere Betriebssysteme und neuere Geräte verfügbar sind.
- Bereitstellungskonsole, Anwendung oder geeignete Scripts, die WS-MAN-Webdienstanforderungen und Methodenaufrufe senden können.

Installieren Sie ein Betriebssystem unter Verwendung der Treiber, die über den Lifecycle-Controller lokal mit dem Server verbunden sind.

So führen Sie eine Remote-Bereitstellung des Betriebssystems durch:



ANMERKUNG: Erstellen Sie zur Verwendung eines benutzerdefinierten Betriebssystems das benutzerdefinierte Betriebssystem-Image (.iso-Format) und geben Sie es im Netzwerk frei oder erstellen Sie ein ISO-Image auf einer DVD.

1. Rufen Sie die Methode **GetDriverPackInfo()** auf, um die auf dem Server unterstützten Betriebssysteme und die auf dem Lifecycle-Controller installierte Treiberpaketversion aufzuführen.
2. Rufen Sie die Methode **UnpackAndAttach()** auf, um die Treiber für das gewählte Betriebssystem vom Lifecycle-Controller auf ein internes, mit OEMDRV bezeichnetes USB-basiertes Laufwerk zu kopieren, das mit dem Server verbunden ist.
Standarmäßig wird dieses OEMDRV-Laufwerk dem Server gegenüber für etwa 18 Stunden angezeigt und danach automatisch getrennt. Allerdings können Sie zur Angabe der Dauer (zwischen 1 Minute und 18 Stunden), während der das Laufwerk auf dem Server vorhanden sein muss den optionalen Parameter **ExposeDuration** verwenden.
3. Verwenden Sie abhängig davon, wo das Betriebssystemimage gehostet wird, eine der folgenden Methoden, um das ISO mit dem lokalen Server zu verbinden und ihn sofort neu zu starten.
 - **BootToNetworkISO()** — Wenn das Betriebssystemimage (.iso-Format) auf einer Netzwerkfreigabe (NFS oder CIFS) gehostet wird, dann verwenden Sie diese Methode, um das Netzwerk-ISO als virtuelles USB CD-ROM-Gerät mit dem Server zu verbinden und starten Sie sofort von dort aus, um die Betriebssysteminstallation zu starten.
 - **BootToISOFromVFlash()** — Wenn das Betriebssystemimage (.iso-Format) auf der vFlash SD-Karte gehostet wird, dann verwenden Sie diese Methode, um das Image als lokales USB CD-ROM-Gerät zu verbinden und starten Sie sofort von dort aus, um die Betriebssysteminstallation zu starten.
-  **ANMERKUNG:** Sie müssen als Vorbedingung vor dem Ausführen von **BootToISOFromVFlash()** zum Kopieren des .iso-Images von NFS, CIFS, oder einer TFTP-Freigabe auf vFlash die Methode **DownloadISOtoVFlash()** verwenden, damit es später für den Start verwendet werden kann. Wenn die vFlash-SD-Karte jedoch installiert ist und nicht formatiert wurde, formatiert diese Methode die Karte und lädt anschließend das ISO-Image herunter.
 - **BootToPXE()** — Wenn das Betriebssystem in PXE gehostet wird, dann verwenden Sie diese Methode, um den Server neu zu starten und zum Initiieren der OS-Installation in PXE zu starten.
4. Verwenden Sie nach Abschluss der Betriebssysteminstallation basierend auf der Art der Anbindung des ISOs eine der Methoden, um das ISO vom Hostserver zu trennen.
 - **DetachISOImage()** — Wenn das ISO unter Verwendung von **BootToNetworkISO()** angebunden wurde, dann verwenden Sie diese Methode, um das ISO vom Hostserver zu trennen.
 - **DetachISOFromVFlash()** — Wenn das ISO unter Verwendung von **BootToISOFromVFlash()** angebunden wurde, dann verwenden Sie diese Methode, um das ISO vom Hostserver zu trennen. Anschließend kann die Methode **DeleteISOFromVFlash()** verwendet werden, um das ISO vom vFlash zu löschen, wenn das ISO nicht mehr benötigt wird.
5. Rufen Sie die Methode **DetachDrivers()** auf, um das OEMDRV-Laufwerk zu trennen, das die Betriebssystemtreiber enthält.
-  **ANMERKUNG:** Während der OS-Installation installiert das systemeigene OS-Installationsprogramm automatisch die auf dem OEMDRV-Gerät vorhandenen Treiber.

Referenzen für die Betriebssystembereitstellung

 **ANMERKUNG:** Die in dieser Tabelle referenzierten Abschnitte enthalten ausschließlich allgemeine Beispiele.

Tabelle 4. Schrittnummer und Speicherort

Schrittnummer	Speicherort der Speicherrichtlinie für Lifecycle-Controller-Webdienste (Windows oder Linux)
Schritt 1.	11.3.1 — Abrufen von Treiberpaketinformationen
Schritt 2.	11.3.2 — Entpacken ausgewählter Treiber und Verbindung mit dem Host-OS als USB-Gerät
Schritt 3.	11.3.6 — Start auf Netzwerk-ISO 11.3.11 — Start auf ISO von VFlash

Schrittnummer	Speicherort der Speicherrichtlinie für Lifecycle-Controller-Webdienste (Windows oder Linux)
---------------	---

11.3.8 — Start in PXE

[Schritt 4.](#)

11.3.7 — Netzwerk-ISO USB-Gerät trennen

11.3.13 — ISO von VFlash trennen

[Schritt 5.](#)

11.3.3 — Emuliertes USB-Gerät mit Treibern trennen

Profil

DCIM_OSDeployment Profile

MOFs

- DCIM_OSDeploymentService.mof
- DCIM_OSConcreteJob.mof
- DCIM_LCElementConformsToProfile.mof
- DCIM_LCRegisteredProfile.mof

Kopieren der BS-Treiber auf eine Netzwerkfreigabe

So kopieren Sie die Betriebssystemtreiber vom Lifecycle-Controller auf eine Netzwerkfreigabe:

1. Rufen Sie die Methode **GetDriverPackInfo()** auf, um die auf dem Server unterstützten Betriebssysteme und die auf dem Lifecycle-Controller installierte Treiberpaketversion aufzuführen.
2. Rufen Sie die Methode **UnpackAndShare()** auf, um die Treiber für das ausgewählte Betriebssystem vom Lifecycle-Controller auf eine Netzwerkfreigabe (CIFS oder NFS) zu kopieren.

Referenzen für die Betriebssystembereitstellung



ANMERKUNG: Die in dieser Tabelle referenzierten Abschnitte enthalten ausschließlich allgemeine Beispiele.

Tabelle 5. Schrittnummer und Speicherort

Schrittnummer	Speicherort der Speicherrichtlinie für Lifecycle-Controller-Webdienste (Windows oder Linux)
---------------	---

[Schritt 1.](#)

11.3.1 — Abruf von Treiberpaketinformationen

[Schritt 2.](#)

11.3.2 — Ausgewählte Treiber entpacken und als USB-Gerät mit Host-OS verbinden

Profil

DCIM_OSDeployment Profile

MOFs

- DCIM_OSDeploymentService.mof
- DCIM_OSConcreteJob.mof
- DCIM_LCElementConformsToProfile.mof
- DCIM_LCRegisteredProfile.mof

Remote-Dateifreigabe verwenden

Für eine erfolgreiche Ausführung von Remoteaufgaben auf dem Server müssen Sie sicherstellen, dass die unter [Allgemeine Voraussetzungen vor der Verwendung der Remote-Services](#) bereitgestellten Vorbedingungen erfüllt sind:

So stellen Sie das Betriebssystem unter Verwendung einer Remote-Dateifreigabe bereit:

1. Rufen Sie die Methode **ConnectRFSISOImage()** auf, die das ISO auf der Remote-Dateifreigabe (RFS), die für den Server als ein lokales CD-ROM-Gerät emuliert wird, verbindet. Stellen Sie sicher, dass RFS unter Verwendung der iDRAC GUI oder RACADM angebunden wird, oder stellen Sie das iDRAC-Attribut `AttachMode` über Web-Services auf `Attach` ein.
2. Rufen Sie die Methode **GetRFSISOImageConnectionInfo()** auf, um die RFS-Verbindungsinformationen zu erhalten.
3. Rufen Sie die Methode **DisconnectRFSISOImage()** auf, um das ISO-Image vom Server zu trennen.

Referenzen für die Verwendung einer Remote-Dateifreigabe



ANMERKUNG: Die in dieser Tabelle referenzierten Abschnitte enthalten ausschließlich allgemeine Beispiele.

Tabelle 6. Schrittnummer und Speicherort

Schrittnummer	Speicherort der Speicherrichtlinie für Lifecycle-Controller-Webdienste (Windows oder Linux)
Schritt 1	11.3.18 - Verbinden Sie sich mit einem RFS ISO-Image
Schritt 2	11.3.20 - Rufen Sie die RFS ISO-Image Verbindungsinformationen ab
Schritt 3	11.3.19 - Trennen Sie das RFS ISO-Image

Profile

DCIM_OSDeployment Profile

MOFs

- DCIM_OSDeploymentService.mof
- DCIM_OSConcreteJob.mof
- DCIM_LCElementConformsToProfile.mof
- DCIM_LCRegisteredProfile.mof


Start auf ISO während der Serverwartung

Stellen Sie für das erfolgreiche Durchführen von Remote-Vorgängen auf dem Server sicher, dass die im Abschnitt [Allgemeine Vorbereitungen vor der Verwendung der Remote-Services](#) enthaltenen Vorbereitungen erfüllt sind.

In Datenzentren und Unternehmensumgebungen werden physikalische Server normalerweise dazu verwendet, um virtuelle Computer und Arbeitslasten zu hosten. Wenn der Server Wartung benötigt (Hardware-Austausch, Konfigurationsänderungen, Aktualisierungen, usw.), werden die Arbeitslasten auf andere physikalische Systeme migriert und der ursprüngliche Server geht in den Wartungsmodus. In diesem Modus startet der Server in eine Umgebung vor Laden des Betriebssystems (in der Regel ein ISO), die über eine Netzwerkfreigabe mehrere Male verbunden wird, bis alle Probleme behoben wurden. Unter Verwendung des OS-Bereitstellungsprofils können die folgenden Methoden verwendet werden, um dies effizienter möglich zu machen.

So starten Sie während der Server-Wartung in ein ISO:

1. Rufen Sie die Methode **ConnectNetworkISOImage()** auf, um das ISO einer Netzwerkfreigabe (CIFS oder NFS) für den Server als virtuelles CD-ROM-Gerät verfügbar zu machen. Immer dann, wenn das verwaltete System während der Wartung neu gestartet wird, startet das System jedes Mal ungeachtet der Startreihenfolge in dieses ISO, bis das ISO unter Verwendung der Methode **DisconnectNetworkISOImage()** getrennt wird.

-  **ANMERKUNG:** Das ISO wird neu verbunden, wenn iDRAC zurückgesetzt wird, oder wenn die Stromzufuhr unterbrochen wird.
2. Rufen Sie die Methode **GetNetworkISOImageConnectionInfo()** auf, um die Details hinsichtlich des Netzwerk-ISOs abzurufen, das unter Verwendung der Methode **ConnectNetworkISOImage()** verbunden wird. Diese weist auch darauf hin, ob das ISO vom System aus gestartet wird oder nicht. Lesen Sie für weitere Informationen *OS-Bereitstellungsprofil* und die zugehörigen MOFs.
 3. Rufen Sie die Methode **DisconnectNetworkISOImage()** auf, um das ISO-Image vom Server zu trennen.
 4. Rufen Sie die Methode **SkipISOImageBoot()** auf, sodass das System (unter Verwendung der Methode **ConnectNetworkISOImage()**) während des nächsten Serverstarts keine einmalige Startsequenz auf das verbundene ISO ausführt. Bei anschließenden Neustarts fährt das BIOS damit fort, auf das ISO zu starten, bis zum Trennen des ISOs die Methode **DisconnectNetworkISOImage()** verwendet wird.

Referenzen für das Starten auf ISO während der Server-Wartung


 **ANMERKUNG:** Die in dieser Tabelle referenzierten Abschnitte enthalten ausschließlich allgemeine Beispiele.

Tabelle 7. Schrittnummer und Speicherort

Schrittnummer	Speicherort der Speicherrichtlinie für Lifecycle-Controller-Webdienste (Windows oder Linux)
Schritt 1.	11.3.14 — Netzwerk-ISO-Image verbinden 11.3.15 — Netzwerk-ISO-Image trennen
Schritt 2.	11.3.17 — Netzwerk-ISO-Image Verbindungsinformationen abrufen
Schritt 3.	11.3.15 — Netzwerk-ISO-Image trennen
Schritt 4.	11.3.16 — ISO-Image-Start überspringen

Profile

DCIM_OSDeployment Profile




MOFs

- DCIM_OSDeploymentService.mof
- DCIM_OSConcreteJob.mof
- DCIM_LCElementConformsToProfile.mof
- DCIM_LCRegisteredProfile.mof

Auf ISO starten - Methodenvergleich

Tabelle 8. . Auf ISO starten - Methoden

Schritte	BootToNetworkISO	BootToISOFromVFlash	ConnectNetworkISOImage	ConnectRFSISO
Herstellen einer Verbindung zu einem Netzwerk-ISO und dieses Netzwerk-ISO als virtuelles CD-ROM-Gerät verbinden	Ja	-	Ja	Ja
Herstellen einer Verbindung zu einem ISO auf einer vFlash SD-Karte und dieses ISO als virtuelles CD-ROM-Gerät verbinden	-	Ja	-	-
Hostserver automatisch neu starten	Ja	Ja	-	-
Sofort auf ISO-Image starten	Ja	Ja	-	-
Einmaliger Start	Ja	Ja	-	-
Für 18 Stunden (oder eine festgelegte Dauer) mit einem Hostserver verbunden	Ja	Ja	-	-
Kann andere Aufgaben durchführen, wie z.B. Aktualisierungen. Konfiguration nach Ausführen dieser Methode unter Verwendung von Webdiensten.	-	-	-	Ja

Schritte	BootToNetworkISO	BootToISOFromVFlash	ConnectNetworkISOIm age	ConnectRFSISO
	<p> ANMERKUNG: Bei nachfolgenden Neustarts des Hosts erfolgt der Start nur dann auf das ISO-Image, wenn das Gerät (ISOIMG) als erstes Gerät in der BIOS-Startgerätereihefolge definiert ist. Dies ist nur dann anwendbar, wenn das ISO verbunden ist und die Zeit nicht abgelaufen ist, oder wenn das ISO nicht explizit getrennt wurde.</p>	<p> ANMERKUNG: Bei jedem Neustart des Host-Systems, startet das BIOS ungeachtet der Startreihenfolge auf dieses Gerät (ISOIMG).</p>	<p> ANMERKUNG: Wenn das RFS-Gerät das erste Gerät in der BIOS-Startliste ist und der Server neu startet, dann startet das BIOS jedes Mal auf das verbundene ISO.</p>	

Einmalige Startsequenz

Verwenden Sie die Methoden für die einmalige Startsequenz, um den Server sofort neu zu starten und anschließend in das ISO, die Festplatte oder die PXE zu starten. Verwenden Sie diese Methoden, um während der Durchführung der Server-Wartung, dem Einleiten einer Betriebssysteminstallation, dem Starten auf die Festplatte, oder dem Starten in PXE eine einmalige Startsequenz auf ein ISO vor dem Laden des Betriebssystems durchzuführen.

Führen Sie dazu folgende Schritte durch:

- **BootToPXE()** — Rufen Sie diese Methode auf, um den Server sofort neu zu starten und ungeachtet der Startreihenfolge der Startliste in PXE zu starten.
- **BootToHD()** — Rufen Sie diese Methode auf, um den Server sofort neu zu starten und ungeachtet der Startreihenfolge der Startliste auf dem ersten Laufwerk des Servers zu starten.

 **ANMERKUNG:** Verwenden Sie für die einmalige Startsequenz alternativ dazu BIOS-Methoden wie z.B. **ChangeBootOrderByInstanceID()** oder **SetAttribute()**.

Verhalten der Methode „BootToHD“

Im folgenden werden einige der Instanzen aufgeführt, in denen die Methode möglicherweise nicht korrekt funktioniert:

- Wenn das System mehr als ein Laufwerk hat, dann wählt es das erste Laufwerk in der Startreihenfolge aus.
- Wenn die Startreihenfolge ein anderes Gerät als erstes Gerät hat (zum Beispiel ein USB-Flash-Laufwerk), dann startet es in dieses Gerät.
- Wenn sich das System im UEFI-Startmodus befindet, muss das Laufwerk mit dem Betriebssystem ebenfalls im UEFI-Startmodus installiert sein. Der einmalige Start auf einem Laufwerk, auf der das Betriebssystem im BIOS-Startmodus installiert wurde, funktioniert nicht.
- Wenn auf dem System kein Laufwerk installiert ist, wird die Methode ausgeführt. Stellen Sie daher sicher, dass ein unterstütztes Laufwerk installiert ist, bevor Sie die Methode ausführen.

Info - Aufgabenkennungen

Einige in diesem Dokument beschriebene Methoden geben Aufgabenkennungen als Ausgabeparameter zurück. Die Aufgaben sind bei der Verfolgung einer angeforderten Aktion hilfreich, die nicht sofort durchgeführt werden kann und, aufgrund zugrundeliegender technologischer Einschränkungen, eine längere Zeit in Anspruch nimmt, die die standardmäßigen Zeitüberschreitungen für die Reaktion auf Webdienstanfragen übersteigt. Die zurückgegebene Aufgabenkennung kann anschließend bei WS-MAN „Enumerate“ oder „Get“-Anfragen zur Einholung von Aufgabenobjektinstanzen verwendet werden. Aufgabenobjektinstanzen enthalten eine Aufgabenstatuseigenschaft, die überprüft werden kann, um den derzeitigen Status der Aufgabe abzulesen, und ob diese erfolgreich abgeschlossen wurde oder auf ein Problem gestoßen und fehlgeschlagen ist. Wenn ein Aufgabenfehler auftritt, enthält die Aufgabeninstanz außerdem eine Fehlermeldungseigenschaft, die detaillierte Informationen zur Art des Fehlers bereitstellt. Andere Eigenschaften enthalten andere Informationen für die Fehleridentifikation, die zur Lokalisierung der Fehlermeldung in die unterstützten Sprachen und zum Erhalt detaillierterer Beschreibungen und Beschreibungen empfohlener Antwortmaßnahmen verwendet werden können.

Alle in diesem Dokument beschriebenen Methoden, die mit `DCIM_OSDeploymentService` in Zusammenhang stehen, geben Fehlercodes zurück, die anzeigen ob die Methode erfolgreich ausgeführt wurde, ob ein Fehler aufgetreten ist, oder eine Aufgabe erstellt wurde. Die Aufgabenerstellung findet dann statt, wenn die gerade in der Methode durchgeführte Aufgabe nicht sofort abgeschlossen werden kann. Darüberhinaus geben die Methoden auch Ausgabeparameter zurück, die eine Fehlermeldung (auf Englisch) und andere Fehlerkennungen enthalten, die zur Lokalisierung des Fehlers in die unterstützten Sprachen verwendet werden können. Die Fehlerkennungen können zur Indizierung und Verarbeitung von Dell Message Registry XML-Dateien verwendet werden. Die Dell Message Registry-Dateien sind in den sechs unterstützten Sprachen vorhanden, eine Datei pro Sprache. Zusätzlich zu den übersetzten Fehlermeldungen enthalten die Message Registry (Fehlermeldungsregistrierungs)-Dateien zusätzliche detaillierte Fehlerbeschreibungen und empfohlene Antwortmaßnahmen für jeden Fehler, der von der Remote-Services-Webdienstschnittstelle des Lifecycle-Controllers zurückgegeben wird. Gehen Sie zum Download der Dell Message Registry XML-Dateien auf delltechcenter.com/page/Lifecycle+Controller/.

Dies sind die Methoden, die konkrete Aufgabeninstanzen zurückgeben:

- `UnpackAndAttach()`
- `UnpackAndShare()`
- `BootToNetworkISO`
- `DownloadISOToVFlash()`
- `BootToISOFromVFlash`
- `ConnectNetworkISOImage`
- `ConnectRFSISOImage()`

Die Methoden, die nur Ausgabeparameter und keine Aufgabeninstanzen zurückgeben sind:

- `GetDriverPackInfo()`
- `DetachDrivers()`
- `DetachISOImage()`
- `BootToPXE()`
- `BootToHD()`
- `GetHostMACInfo()`
- `DetachISOFromVFlash()`
- `DeleteISOFromVFlash()`
- `DisconnectNetworkISOImage()`
- `GetNetworkISOImageConnectionInfo()`

- SkipISOImageBoot()
- DisconnectRFSISOImage()
- GetRFSISOImageConnectionInfo()

Verwalten von Aufgaben

Remote-Services stellt die folgenden Funktionalitäten für die Verwaltung von Lifecycle-Controller-Aufgaben bereit:

- Aufgaben erstellen — Erstellen Sie spezifische Aufgabentypen zum Übernehmen von Konfigurationen.
- Zeitliche Planung von Aufgaben und Aufgabenwarteschlangen - Führen Sie innerhalb eines einzigen Neustarts mehrere Aufgaben aus, indem Sie die Methode **SetupJobQueue()** in der Klasse `DCIM_JobService` verwenden. Wenn Sie einen Auftrag unter Verwendung der Methode **CreateTargetedConfigJob()** erstellen, ohne die Startzeit einzustellen, dann verwenden Sie die Methode **SetupJobQueue()** zum Festlegen des Zeitplans und der Ausführungsreihenfolge. Wenn die Startzeit in der Methode **CreateTargetedConfigJob()** eingestellt wurde, kann er nicht mit anderen Aufgaben gebündelt werden und die Aufgabe wird für die Ausführung zur angegebenen Zeit eingerichtet.
- Aufgaben löschen – Löschen Sie einen spezifizierten bestehenden Auftrag, indem Sie die Methode **DeleteJobQueue()** in der Klasse `DCIM_JobService` verwenden.
- Alle Aufgaben melden – Listen Sie die Klasse `DCIM_LifecycleJob` auf, um alle Aufgaben zu melden.
- Eing geplante Aufgaben melden – Listen Sie die Klasse `DCIM_LifecycleJob` mit dem Auswahlfilter `JobStatus=Scheduled` auf, um einen Bericht mit allen zeitlich eing geplanten Aufgaben zu erstellen.

Weitere Informationen über die Auftragssteuerung finden Sie im Abschnitt [Auftragssteuerungsprofil](#).

Aufgabentypen

Es gibt zwei Aufgabentypen, systemerstellte Aufgaben (implizit) und benutzererstellte Aufgaben (explizit):


- Systemerstellte Aufgaben werden beim Ausführen spezifischer Remote-Services-Aufgaben erstellt. Beispielsweise erstellen Remote-Services-Funktionen, wie z.B. das Exportieren der Hardware-Bestandsliste, Exportieren von Lizenzen, Erstellen einer persistenten Speicherpartition usw. eine Aufgabe und geben die Aufgabenkennung zurück. Das Abfragen des Aufgabenstatus bestimmt den Fertigstellungsstatus der Aufgabe.
- Benutzererstellte Aufgaben, wie z.B. `CreateTargetedConfigJob`, `CreateRebootJob` und `InstallFromURI` werden zum Übernehmen von Benutzerkonfigurationen für RAID, NIC, BIOS usw. verwendet. Sie können für die sofortige Ausführung oder die Ausführung zu einem bestimmten Zeitpunkt eing geplant werden.


Systemerstellte Aufgaben	Benutzererstellte Aufgaben
vFlash (Initialisieren)	RAID-Konfiguration
vFlash (Partition erstellen)	BIOS-Konfiguration
vFlash (Partition formatieren)	NIC-Konfiguration
vFlash (Partition verbinden)	iDRAC-Konfiguration
vFlash (Partition trennen)	Systemkonfiguration
vFlash (Daten aus Partition exportieren)	Softwareaktualisierung von (BIOS, NIC, RAID, usw.)
vFlash (Partition unter Verwendung von Image erstellen)	Neustarten
Das Lebensdauerprotokoll exportieren.	
Hardwarebestandsliste exportieren	
Werkskonfiguration exportieren	

Benutzererstellte Aufgaben

Im folgenden werden benutzererstellte Aufgaben aufgeführt:

- **CreateTargetedConfigJob** — Diese Methode wird beim Konfigurieren von RAID, NIC, BIOS, iDRAC und dem System verwendet. Verwenden Sie diese Methode, um die Konfigurationsänderungen auszuführen und eine Aufgabe zum Anwenden der Konfigurationsänderungen zu erstellen.
- **CreateRebootJob** — Diese Methode wird zum Erstellen von Neustartaufgaben verwendet.
- **InstallFromURI** — Diese Methode wird verwendet, um die Firmware von BIOS, RAID, NIC, iDRAC, PSU, Lifecycle-Controller, BS-Treiberpakete und Diagnoseprogramme zu aktualisieren. Bei Erfolg gibt diese Methode eine Aufgabenkennung (Job-ID) zurück. Diese Aufgabenkennung führt auf dieser Entität die Softwareaktualisierung durch.

 **ANMERKUNG:** Wenn zum Aktualisieren der BIOS-, RAID-, NIC-, iDRAC- und PSU-Firmware die Methode **InstallFromURI()** verwendet wird, dann verwenden Sie für die zeitliche Planung der Aufgabenkennung die Methode **SetupJobQueue()**.

 **ANMERKUNG:** Wenn die Methode **InstallFromURI()** zum Aktualisieren des Lifecycle-Controllers, Treiberpakets und Diagnoseprogramms verwendet wird, dann planen Sie keine Aufgabe ein.

Aufgaben-Zeitplan

Die Aufgaben können zeitlich für Aufgabenkennungen eingeplant werden, die unter Verwendung einer der Aufgaben-Erstellungsmethoden zurückgegeben werden.

SetupJobQueue — Diese Methode wird nur für diejenigen Aufgabenkennungen verwendet, die von einer der Aufgaben-Erstellungsmethoden zurückgegeben werden und noch nicht eingeplant wurden.


Löschen einer Aufgabe

Durch das Verwenden der **JID_CLEARALL()** Methode, können alle aktuellen Aufgaben im System gelöscht werden. Als Alternative können Sie eine spezifische Aufgabe durch Verwendung seiner Aufgabenkennung löschen.

Zeitliche Planung separater Aufgaben für mehrere Aktionen

So planen Sie separate Aufgaben für mehrere Aktionen (im folgenden Beispiel: BIOS- und NIC-Aktualisierung und NIC-Konfiguration):

1. Rufen Sie die Methode **InstallFromURI()** für die BIOS- und NIC-Firmwareaktualisierungspakete auf. Die Methode lädt die BIOS- und NIC-Aktualisierungen herunter und erstellt eine Aufgabenkennung für jeden Geräteaktualisierungsauftrag.
2. Stellen Sie für eine NIC (z.B. integrierter NIC 1) die NIC-Attribute ein und erstellen Sie einen Zielauftrag für diesen Satz. Die Methode gibt eine Aufgabenkennung zurück.
3. Verwenden Sie diese Aufgabenkennungen und die Methode **SetupJobQueue()**, um diese Aufgaben zeitlich so zu planen, dass Sie in der zur spezifizierten Startzeit spezifizierten Reihenfolge ausgeführt werden.

 **ANMERKUNG:** Um den iDRAC das System automatisch zur geplanten Zeit neu starten zu lassen, erstellen Sie einen Neustartauftrag (wobei Sie den Neustarttyp spezifizieren – ordnungsgemäß oder Aus- und Wiedereinschalten), und fügen Sie die Neustartaufgabenkennung in die Liste der beim Methodenaufruf **SetupJobQueue()** spezifizierten Aufgaben ein. Wenn ein Neustartauftrag nicht in der eingerichteten Aufgabenwarteschlange enthalten ist, stehen die Aufgaben für eine Durchführung zur geplanten Startzeit bereit, sind jedoch hinsichtlich des Neustarts des Systems und zum Starten der Aufgabendurchführung auf eine externe Aktion angewiesen.

Mehrere Zielaufgaben durchführen

Durchführung mehrerer Zielaufgaben (z.B. Einstellen von NIC-Attributen auf mehreren NICs) zur gleichen Zeit:



ANMERKUNG: Sie können Zielaufgaben während des POSTs oder System-Setups erstellen. Die Aufgaben werden nicht ausgeführt, bis das System den POST abschließt oder das System-Setup beendet.

1. Konfiguration der integrierten NIC 1: Legen Sie die NIC-Attribute für Integrated NIC 1 (integrierte NIC 1) fest und erstellen Sie eine angezielte Konfigurationsaufgabe für Integrated NIC 1 mit einer geplanten Zeit von TIME_NOW, stellen Sie dabei jedoch sicher, dass Sie keinen Neustart einplanen.
2. Konfiguration der integrierten NIC 2: Legen Sie die NIC-Attribute für Integrated NIC 2 (integrierte NIC 2) fest und erstellen Sie eine angezielte Konfigurationsaufgabe für Integrated NIC 1 mit einer geplanten Zeit von TIME_NOW, stellen Sie dabei jedoch sicher, dass Sie keinen Neustart einplanen.
3. Stellen Sie die NIC-Attribute für integrierte NIC 3 ein, erstellen Sie eine angezielte Aufgabe für integrierte NIC 3 mit einer geplanten Startzeit von TIME_NOW und spezifizieren Sie außerdem einen Neustarttyp.

Der iDRAC startet das System gemäß der durch den Neustarttyp definierten Methode und alle Aufgaben werden gleichzeitig ausgeführt.

Spezifizieren der Startzeit und Endzeit

Die Methoden **CreateTargetedConfigJob()** und **SetupJobQueue()** akzeptieren die Startzeitenparameter, wie z.B. `ScheduledStartTime`, `StartTimeInterval` und `UntilTime`. Wenn der Parameter `StartTime` (Startzeit) null ist, wird die Aktion nicht gestartet. Der date-time Datentyp wird über das folgende Format YYYYMMDDhhmmss definiert:

- yyyy für das Jahr steht
- MM für den Monat steht
- DD für den Tag steht
- hh für die Stunden steht
- mm für die Minuten steht
- ss für die Sekunden steht

Z. B. 20090930112030 – Geben Sie in diesem Format das Datum und die Uhrzeit für alle Lifecycle Controller-Aktualisierungen, eingestellten Attribute und Methoden der Art **CreateTargetedConfigJob()** in verschiedenen Dienstklassen ein. „TIME_NOW“ ist ein spezieller Wert, der für die unverzügliche Ausführung der Aufgaben steht.

Automatisches Löschen von Aufgaben

Aufgaben werden automatisch gelöscht, wenn die Anzahl der Aufgaben im System höher als der Wert der Eigenschaft `StartAutoDeleteAtThreshold` der Klasse `DCIM_JobService` ist. Alle Aufgaben, die länger als der Wert `DeleteOnCompletionTimeout` der Klasse `DCIM_JobService` fertiggestellt werden (entweder erfolgreich oder nicht), werden vom System gelöscht.



ANMERKUNG: Der Wert `DeleteOnCompletionTimeout` wird unter Verwendung der Methode `SetDeleteOnCompletionTimeout` geändert.

Alle Aufgaben löschen

Verwenden Sie die **DeleteJobQueue()-Methode** zusammen mit dem **Stichwort** `JID_CLEARALL` für die Aufgaben-ID, um alle Aufgaben und alle ausstehenden Konfigurationsdaten, die den Aufgaben zugeordnet wurden zu löschen.

Verwalten der RAID-Konfiguration

Verwenden Sie die RAID-Konfigurationsfunktion, um die Eigenschaften des RAID-Controllers, der physischen Laufwerke und der an das System angebotenen Gehäuse zu erhalten. Sie können unter Verwendung der zur Verfügung stehenden Methoden verschiedene Attribute der physischen und virtuellen Laufwerke konfigurieren.

RAID-Controller anzeigen

- Führen Sie den Auflistungsvorgang in der Klasse `DCIM_ControllerView` durch, um die Instanzeigenschaften aller an das System angebotenen RAID-Controller anzuzeigen.
- Führen Sie den „Get“ (Einholen)- Vorgang in der Klasse `DCIM_ControllerView` unter Verwendung der richtigen Instanzkennungen der benötigten RAID-Controller durch, um die zugehörigen Eigenschaften anzuzeigen.

Erstellen aufgeteilter (sliced) virtueller Laufwerke

So erstellen Sie aufgeteilte (sliced) virtuelle Laufwerke:

1. Finden Sie heraus, welches die RAID-Konfigurationen des Systems sind, indem Sie die Methode **GetRAIDLevels()** (RAID-Ebenen einholen) in der Klasse `DCIM_RAIDService` verwenden.
2. Wählen Sie das/die physikalische(n) Laufwerk(e), auf denen Sie das virtuelle Laufwerk erstellen wollen auf Basis der Kennungen aus, die Sie unter Verwendung der Methode **GetAvailableDisks()** in der Klasse `DCIM_RAIDService` gewonnen haben.
3. Überprüfen Sie die verfügbaren Größen und standardmäßigen virtuellen Laufwerksparameter für die gewünschte RAID-Ebene und das physikalische Laufwerk, indem Sie die Methode **CheckVDValues()** in der Klasse `DCIM_RAIDService` verwenden.
4. Erstellen Sie die Eingabeparameter, bevor Sie die Methode **CreateVirtualDisk()** aufrufen.
5. Rufen Sie die Methode **CreateVirtualDisk()** auf.
6. Überprüfen Sie die Ausgabeparameter (Rückgabecodewerte) für die gewählte Methode. Die Instanzkennung des ausstehenden virtuellen Laufwerks ist ein Ausgabeparameter und es wird der Rückgabecodewert rückgegeben, wenn die Methode erfolgreich war. Beispielsweise wird der Code 0 rückgegeben, wenn die Methode erfolgreich war.
7. Erstellen Sie vor dem Aufrufen der Methode **CreateTargetedConfigJob()** die Eingabeparameter (z.B. „Ziel“, „RebootType“, „ScheduledStartTime“, „UntilTime“, usw.) und verwenden Sie den richtigen FQDD (Fully Qualified Device Descriptor) für den Controller.
8. Rufen Sie die Methode **CreateTargetedConfigJob()** auf, um die ausstehenden Werte anzuwenden.
9. Fragen Sie den Status des Auftragskennungsabgabewertes ab, indem Sie die Methoden des Auftragssteuerungsprofils verwenden.
10. Listen Sie die Klasse `DCIM_VirtualDiskView` auf, um das erstellte virtuelle Laufwerk anzuzeigen.

RAID-Konfiguration

Für eine erfolgreiche Ausführung von Remoteaufgaben auf dem Server müssen Sie sicherstellen, dass die folgenden Vorbedingungen erfüllt sind:

- [Allgemeine Voraussetzungen vor der Verwendung der Remote-Services](#)
- PERC-Controller und Firmware unterstützen das Local Key Management (LKM, Verwaltung lokaler Schlüssel)
- SED-Laufwerke

Einrichten und Konfigurieren eines RAID mit den folgenden Hardware-Ressourcen:

- Speicher-Controller – PERC
- physische Laufwerke (SEDs) – 4
- Größe jedes physischen Laufwerks – 1 TB

Erstellen Sie die folgende RAID-Konfiguration:




- Größe jedes virtuellen Laufwerks 10 GB (10.240 MB)
- Anzahl der virtuellen Laufwerke – 10
- RAID-Stufe – 5
- Dediziertes Hotspare – 1
- Verschlüsselung auf dem Controller aktivieren und einen lokalen Schlüssel erstellen

So konfigurieren Sie RAID:



1. Rufen Sie die Liste der mit dem System verbundenen Speicher-Controller und deren Eigenschaften ab. Überprüfen und notieren Sie den Status der folgenden Controller-Parameter für die spätere Verwendung:
 - FQDD (Fully Qualified Device Descriptor) des Controllers
 - Sicherheitsstatus
 - Verschlüsselungsmodus
 - Schlüssel-ID
2. Rufen Sie die FQDDs und die Werte für die physischen Laufwerke ab, die mit dem Controller verknüpft sind.
3. Führen Sie das Verfahren **CreateVirtualDisk()** aus, nachdem Sie die in der folgenden Tabelle angezeigten korrekten Werte definiert haben:

Tabelle 9. Werte für das RAID-Setup

Parameter	Wert
FQDD	FQDD des Controllers und der verknüpften physischen Laufwerke
RAID-Stufe	Legen Sie die RAID-Stufe auf 5 fest. RAID-5 organisiert Daten in Stripes über die physischen Laufwerke hinweg und verwendet Paritätsinformationen zum Aufführen redundanter Daten. Wenn ein physisches Laufwerk ausfällt, werden die Daten unter Verwendung der Paritätsinformationen wieder aufgebaut. RAID 5 bietet gute Leseleistung und langsamere Schreibleistung mit guter Datenredundanz.
Span-Tiefe	Setzen Sie den Wert auf 1.
Span-Länge	Setzen Sie den Wert auf 3. Der Wert der Span-Länge bezieht sich auf die Anzahl physischer Laufwerke, die in den einzelnen Spans enthalten sind. Die Berechnung erfolgt durch das Teilen der Anzahl an physischen Laufwerke durch den Wert der Span-Tiefe.
Größe	Definieren Sie 10.240 MB für jedes virtuelle Laufwerk.
Start-LBA	Berechnen Sie die Start-LBA auf der Basis der bereits vorhandenen virtuellen Laufwerke. Verwenden Sie zur Berechnung der nächsten Start-LBA in Blöcken mit 512 Byte die folgenden Formeln:

Parameter	Wert
	<p> ANMERKUNG: Dies ist nur bei Vorhandensein von segmentierten virtuellen Laufwerken erforderlich.</p> <ul style="list-style-type: none"> – RAID0 – Vorherige Start-LBA + ((Größe / Anzahl der Laufwerke) / 512) – RAID1 – Vorherige Start-LBA + (Größe / 512) – RAID5 – Vorherige Start-LBA + ((Größe / (Anzahl der Laufwerke - 1)) / 512) – RAID6 – Vorherige Start-LBA + ((Größe / (Anzahl der Laufwerke - 2)) / 512) – RAID10 – Vorherige Start-LBA + ((Größe / 2) / 512) – RAID50 – Vorherige Start-LBA + ((Größe / (Anzahl der Laufwerke pro Span - 1)) / 512) – RAID60 – Vorherige Start-LBA + ((Größe / (Anzahl der Laufwerke pro Span - 2)) / 512) <p> ANMERKUNG: Setzen Sie alternativ dazu den Starting LBA auf "0xFFFFFFFFFFFFFFFF", dann wird der Startpunkt des Segments automatisch so berechnet, dass er sich direkt nach dem Ende des letzten Segments befindet.</p>
Stripe-Größe	<p>Die Größe des Stripe-Elements entspricht der Menge von Laufwerksspeicherplatz, den ein Stripe auf den einzelnen physischen Laufwerken im Stripe in Anspruch nimmt. Sie können die folgenden Werte in Bits festlegen:</p> <p> ANMERKUNG: Die S110 und H310Controller unterstützen nur eine Stripe-Größe von 64KB.</p> <ul style="list-style-type: none"> – 64KB = 128 – 128KB = 256 – 256KB = 512 – 512KB = 1024 – 1MB = 2048
Leseregel	<ul style="list-style-type: none"> – Kein Vorauslesen – Vorauslesen – Adaptives Read-Ahead
Schreibverfahren	<ul style="list-style-type: none"> – Durchschreiben – Rückschreiben – Rückschreiben erzwingen
Festplatten-Cache-Regel	<ul style="list-style-type: none"> – Aktiviert – Deaktiviert
Name des virtuellen Laufwerks	<p>Sie können optional einen Namen für das virtuelle Laufwerk vergeben. Für diesen Namen sind maximal 115 alphanumerische Zeichen verfügbar.</p>

4. Führen Sie die Methode zum Erstellen von 10 virtuellen Laufwerken noch 9mal mit denselben Werten aus, die oben in der Tabelle aufgeführt sind.
5. Überprüfen Sie, ob die virtuellen Laufwerke erstellt wurden.
6. Legen Sie die folgenden Werte fest, und rufen Sie die Methode **EnableControllerEncryption()** auf:
 - FQDD (Fully Qualified Device Descriptor) des Controllers
 - Verschlüsselungsmethode – Verschlüsselung über lokalen Schlüssel

- Schlüssel-ID
 - Passphrase – Eine gültige Passphrase enthält 8 bis 32 Zeichen. Sie muss eine Kombination aus Groß- und Kleinbuchstaben, Zahlen und Symbolen enthalten und darf keine Leerzeichen enthalten.
7. Verwenden Sie den FQDD für die physische Festplatte, die als Ersatzlaufwerk verwendet wird, und rufen Sie die Methode **AssignSpare()** auf.
-  **ANMERKUNG:** Wenn Sie ein dediziertes Ersatzlaufwerk benötigen, dann verwenden Sie den FQDD des zugehörigen virtuellen Laufwerks als Ziel anstelle den FQDD des Controllers.
8. Konstruieren Sie die Eingabeparameter (z.B., Target, RebootType, ScheduledStartTime, usw) für die Methode **CreateTargetedConfigJob()**. Lesen Sie das Dokument „RAID-Profil“ auf delltechcenter.com/page/DCIM.Library, um die Liste aller unterstützten Eingabeparameter anzuzeigen.
9. Rufen Sie die Methode **CreateTargetedConfigJob()** auf, um die ausstehenden Werte anzuwenden. Wenn diese Methode erfolgreich ist, muss das System eine Aufgabenkennung für die von Ihnen erstellte Konfigurationsaufgabe rückgeben.
-  **ANMERKUNG:** Das System muss neu gestartet werden, um die Aufgaben auszuführen.

Szenario nach der Konfiguration des RAID-Setups

1. Rufen Sie den Aufgabenstatus mithilfe der zu einem früheren Zeitpunkt erstellten Aufgabenkennung ab.
2. Um zu überprüfen, ob die RAID-Konfiguration und die auf einem lokalen Schlüssel basierende Verschlüsselung erfolgreich sind, müssen Sie verifizieren, dass das System automatisch auf den Lifecycle-Controller startet und die Änderung der RAID-Konfiguration und des lokalen Schlüssels übernimmt.
3. Rufen Sie den Aufgabenstatus über die zu einem früheren Zeitpunkt generierte Aufgabenkennung ab. Für diese Aufgabenkennung wird die Statusmeldung `Aufgabe erfolgreich abgeschlossen` ausgegeben.
4. Wiederholen Sie [Schritt 1](#) und [Schritt 2](#), und überprüfen Sie, ob die Änderungen erfolgreich waren.

Referenzen zur Konfiguration von RAID


 **ANMERKUNG:** Die in dieser Tabelle referenzierten Abschnitte enthalten ausschließlich allgemeine Beispiele.

Tabelle 10. Schrittnummer und Speicherort

Schrittnummer	Speicherort der Speicherrichtlinie für Lifecycle-Controller-Webdienste (Windows oder Linux)
Schritt 1	16.7 – Auflisten der RAID-Bestandsklasse - ControllerView Class
Schritt 2	16.9 – Auflisten der RAID-Bestandsklasse - PhysicalDiskView Class
Schritt 3	16.18.5 – Erstellen einer aufgeteilten (sliced) virtuellen Festplatte – CreateVirtualDisk
Schritt 4	16.18.5 – Erstellen einer aufgeteilten (sliced) virtuellen Festplatte – CreateVirtualDisk
Schritt 5	16.10 – Auflisten des RAID-Bestands - VirtualDiskView
Schritt 6	16.17.3 – Sperren des Controllers über einen Schlüssel - EnableControllerEncryption
Schritt 7	16.16.2 – Zuweisen des Hotspares - AssignSpare
Schritt 8	16.14 – Anwenden der noch offenen Werte für das RAID - CreateTargetedConfigJob

Schrittnummer	Speicherort der Speicherrichtlinie für Lifecycle-Controller-Webdienste (Windows oder Linux)
Schritt 9	16.14 – Anwenden der noch offenen Werte für das RAID - CreateTargetedConfigJob

Profile

DCIM-SimpleRAIDProfile

MOFs

- DCIM_ControllerView.mof
- DCIM_EnclosureView.mof
- DCIM_PhysicalDiskView.mof
- DCIM_RAIDAttribute.mof
- DCIM_RAIDEnumeration.mof
- DCIM_RAIDInteger.mof
- DCIM_RAIDService.mof
- DCIM_RAIDString.mof
- DCIM_VirtualDiskView.mof

Konvertieren eines SATA-Laufwerks vom RAID-Modus in einen Nicht-RAID-Zustand

Für eine erfolgreiche Ausführung von Remoteaufgaben auf dem Server müssen Sie sicherstellen, dass die folgenden Vorbedingungen erfüllt sind:

- [Allgemeine Vorbedingungen vor Verwendung der Remote-Services.](#)
- PERC S110 oder H310-Controller, der den Nicht-RAID-Modus unterstützt.
- SATA- oder SSD-Festplatten

So konvertieren Sie das RAID-Laufwerk in ein Nicht-RAID SATA-Laufwerk:

1. Rufen Sie die Liste der mit dem System verbundenen Speicher-Controller und deren Eigenschaften ab.
2. Rufen Sie die FQDDs, die Werte für den Controller sowie für die physischen Festplatten ab, die mit dem Controller verknüpft sind.
3. Rufen Sie die Methode **ConvertToNonRAID()** zum Einleiten der Konvertierung auf.
4. Rufen Sie die Methode **CreateTargetedConfigJob()** auf, um die ausstehenden Werte anzuwenden. Wenn diese Methode erfolgreich ist, muss das System eine Auftragskennung für die von Ihnen erstellte Konfigurationsaufgabe rückgeben.

Referenzen für das Konvertieren eines SATA-Laufwerks

 **ANMERKUNG:** Die in dieser Tabelle referenzierten Abschnitte enthalten ausschließlich allgemeine Beispiele.

Tabelle 11. Schrittnummer und Speicherort

Schrittnummer	Speicherort der Speicherrichtlinie für Lifecycle-Controller-Webdienste (Windows oder Linux)
Schritt 1	16.7 – Auflisten der RAID-Bestandsklasse - ControllerView Class
Schritt 2	16.9 – Auflisten der RAID-Bestandsklasse - PhysicalDiskView Class

Schrittnummer	Speicherort der Speicherrichtlinie für Lifecycle-Controller-Webdienste (Windows oder Linux)
Schritt 3	16.21 Konvertieren physikalischer Laufwerke in Nicht-RAID-Laufwerke - ConvertToNonRAID()
Schritt 4	16.14 – Anwenden der noch offenen Werte für das RAID - CreateTargetedConfigJob

Profile

DCIM-SimpleRAIDProfile

MOFs

- DCIM_ControllerView.mof
- DCIM_EnclosureView.mof
- DCIM_PhysicalDiskView.mof
- DCIM_RAIDAttribute.mof
- DCIM_RAIDEnumeration.mof
- DCIM_RAIDInteger.mof
- DCIM_RAIDService.mof
- DCIM_RAIDString.mof
- DCIM_VirtualDiskView.mof

Verwalten von Netzwerkgeräten

Verwenden Sie die Netzwerkverwaltungsfunktion, um eine detaillierte Liste der folgenden im System vorhandenen Netzwerkgeräte abzurufen und ihre Attribute festzulegen:

- Netzwerkschnittstellenkarten (NICs)
- Konvergente Netzwerkadapter (CNAs)
- LAN On Motherboards (LOMs)
- Netzwerktochterkarten (NDCs)
- Mezzanine-Karten (nur bei Blade-Servern)

Beziehen Sie sich für weitere Informationen über das **Einfache NIC**-Profil auf [Einfaches NIC-Profil](#).

Anzeigen der Netzwerkgerät-Bestandsliste

- Führen Sie den Auflistungsvorgang in der Klasse `DCIM_NICView` durch, um die Instanzeigenschaften aller im System integrierten Netzwerkgeräte (Broadcom und Intel) anzuzeigen.
- Führen Sie den Vorgang „Get“ (Abrufen) in der Klasse unter Verwendung der richtigen Instanzkennungen der benötigten Netzwerkgeräte durch, um die zugehörigen Eigenschaften anzuzeigen.

Anzeigen der Netzwerkgerät-Attribute


- Führen Sie den Auflistungsvorgang in einer der `DCIM_NICAttribute` Klassen (`DCIM_NICEnumeration`, `DCIM_NICInteger` und `DCIM_NICString`) durch, um alle zur Verfügung stehenden Attribute und möglichen Werte aller im System integrierten Netzwerkgeräte anzuzeigen.
- Führen Sie den Vorgang „Get“ (Abrufen) in einer der `DCIM_NICAttribute`-Klassen aus, um die Netzwerkgerät-Attribute anzuzeigen. Verwenden Sie für spezifische Subklassen-Attributinformationen die richtige Instanzkennung gemeinsam mit dem in der Subklasse aufgeführten Attributnamen.

Festlegen der Netzwerkgerät-Attribute

Einstellen der Attribute:

1. Identifizieren Sie die entsprechende Instanz-ID, und notieren Sie die Instanzinformationen.
2. Versichern Sie sich, dass das Feld `IsReadOnly` auf „Falsch“ eingestellt ist.
3. Verwenden Sie die Instanzinformationen für die Vorbereitung der Eingabeparameter.
4. Rufen Sie die `SetAttribute()` bzw. `SetAttributes()`-Methode auf.
5. Führen Sie den Befehl „Get“ (Abrufen) für das Attribut aus, um den aktualisierten Wert im Feld „Ausstehend“ anzuzeigen.
6. Erstellen Sie vor dem Aufrufen der Methode `CreateTargetedConfigJob()` die Eingabeparameter (z.B. `Target`, `RebootType`, `ScheduledStartTime`, `UntilTime`, usw.) und verwenden Sie den richtigen FQDD (Fully Qualified Device Descriptor) des Netzwerkgeräts für das Ziel. Lesen Sie das Dokument Simple NIC Profile auf delltechcenter.com/page/DCIM.Library um die Liste aller unterstützten Eingabeparameter anzuzeigen.

7. Rufen Sie die Methode **CreateTargetedConfigJob()** auf, um die ausstehenden Werte anzuwenden. Wenn diese Methode erfolgreich ist, muss das System eine Aufgabenkennung für die von Ihnen erstellte Konfigurationsaufgabe rückgeben.


 **ANMERKUNG:** Das System muss neu gestartet werden, um die Aufgabe des Einstellens des Attributs bzw. der Attribute ausführen zu können.

8. Fragen Sie den Status des Aufgabenkennungsangabewertes ab, indem Sie die Methoden des Aufgabensteuerungsprofils verwenden.
9. Wiederholen Sie Schritt 5, um die erfolgreiche Ausführung der Methode zu bestätigen.

Löschen der ausstehenden Werte


Zum Löschen der ausstehenden Werte:

1. Erstellen Sie vor dem Aufrufen der Methode **DeletePendingConfiguration()** in der Klasse `DCIM_JobService` die Eingabeparameter, und verwenden Sie den richtigen FQDD (Fully Qualified Device Descriptor) des Netzwerkgeräts.

 **ANMERKUNG:** Ausstehende Daten können nur vor der Erstellung einer Zielaufgabe gelöscht werden. Nachdem die Zielaufgabe erstellt wurde, können Sie diese Methode nicht ausführen. Falls erforderlich, können Sie die Methode **DeleteJobQueue()** zum Löschen der Aufgabe und der ausstehenden Werte aufrufen. Die Methode funktioniert jedoch nicht, wenn das System neu gestartet wurde und die Aufgabe die Ausführung begonnen hat.


2. Rufen Sie die Methode **DeletePendingConfiguration()** auf.
3. Sie können die Tilgung auf Basis des rückgegebenen Codewertes der Methode bestätigen.

Aktivieren oder Deaktivieren der Partition auf der CNA

 **ANMERKUNG:** Selbst wenn Sie die Eigenschaft „NicPartitioning“ oder die Eigenschaft „PartitionState“ deaktivieren, kann die Partition 1 nicht deaktiviert werden.

So aktivieren oder deaktivieren Sie eine Partition auf der CNA:

1. Listen Sie die Klasse `DCIM_NICEnumeration` auf, und identifizieren Sie den aktuellen Wert der Instanzen der Klasse mit `NicMode`, `iScsiOffloadMode` und `FCoEOffloadMode` und deren FQDD-Eigenschaften.
2. Verwenden Sie für die identifizierte Partition die FQDD-Eigenschaft, und rufen Sie die Methode **SetAttribute()** auf, um die Partition zu aktivieren oder zu deaktivieren.


 **ANMERKUNG:** Die Partition ist auch dann aktiviert, wenn einer der Modi aktiv sind.

3. Führen Sie den Befehl „Get“ für das Attribut aus, um den aktualisierten Wert im Feld „Pending“ anzuzeigen.


4. Erstellen Sie vor dem Aufrufen der Methode **CreateTargetedConfigJob()** die Eingabeparameter („Target“, „RebootJobType“, „ScheduledStartTime“, „UntilTime“ usw.).

Wenn auf mehr als einer Partition auf einer Schnittstelle eine Konfigurationsänderung vorgenommen wurde, definieren Sie „RebootJobType“ und „ScheduledStartTime“ nicht. Planen Sie die Aufgabe über die Methoden des Aufgabensteuerungsprofils. Lesen Sie das Dokument „Simple NIC Profile“ auf delltechcenter.com/page/DCIM.Library um die Liste aller unterstützten Eingabeparameter anzuzeigen.

5. Rufen Sie die Methode **CreateTargetedConfigJob()** auf, um die ausstehenden Werte anzuwenden. Wenn diese Methode erfolgreich ist, gibt das System eine Aufgabenkennung für die erstellte Konfigurationsaufgabe aus.

 **ANMERKUNG:** Starten Sie das System neu, um die Aufgabe zur Erstellung des Attributs bzw. der Attribute auszuführen.

6. Erstellen Sie mithilfe von **CreateRebootJob()** eine Neustartaufgabe, und planen Sie alle Partitionsaufgaben und die Neustartaufgabe mithilfe von **SetupJobQueue()**.

 **ANMERKUNG:** Noch offene Änderungen auf den Partitionen gehen verloren, wenn Partitionsaufgaben nicht für die gemeinsame Ausführung geplant werden.

7. Fragen Sie den Status des Auftragkennungsausgabewertes ab, indem Sie die Methoden des Aufgabensteuerungsprofils verwenden.
8. Wiederholen Sie Schritt 1, um die erfolgreiche Ausführung der Methode zu bestätigen.

Ändern der Merkmale und der Bandbreite einer Partition für einen CNA

Für eine erfolgreiche Ausführung von Remoteaufgaben auf dem Server müssen Sie sicherstellen, dass die folgenden Vorbedingungen, die unter [Allgemeine Voraussetzungen vor der Verwendung der Remote-Services](#) zur Verfügung stehen, erfüllt sind:

Partitionieren Sie eine Schnittstelle, und weisen Sie das Merkmal und die Bandbreite auf einer Converged Network Adapter-Karte mit einem 10-GB-Ethernet-Link mit Unterstützung für mehrere Merkmale zu.


Die folgenden Merkmale und der Bandbreite müssen festgelegt werden:

Tabelle 12. Merkmale und Bandbreite

Anzahl der Merkmale	2
Merkmale für jede Partition	Bandbreite
iSCSI	50
FCoE	50

So ändern Sie die Merkmale und legen Bandbreite für eine Partition in einem CNA fest:

1. Listen Sie die Klasse `DCIM_NICenumeration` auf, und identifizieren Sie den aktuellen Wert der Instanzen der Klasse mit „AttributeName=NicMode/FCoEOffloadMode/iScsiOffloadMode“ und deren FQDD-Eigenschaften.
2. Verwenden Sie für die identifizierte Partition die FQDD-Eigenschaft, und rufen Sie die Methode **SetAttribute()** auf, um das spezifische Merkmal zu aktivieren und die anderen Merkmale zu deaktivieren.

 **ANMERKUNG:** Da auf einer Partition mehrere Merkmale unterstützt werden, können Sie mehrere Merkmale gleichzeitig aktivieren und deaktivieren. Weitere Informationen zu Einschränkungen in Bezug auf die Einstellungen der Merkmale auf verschiedenen CNA-Karten finden Sie unter *iDRAC7 version 1.00.00 Readme* oder im Dokument „Einfaches NIC-Profil“ unter delltechcenter.com/page/DCIM.Library.

3. Gehen Sie zu *Schritt 6*, um die verbleibenden Schritte abzuschließen.
4. Listen Sie die Klasse `DCIM_NICInteger` auf, und identifizieren Sie den aktuellen Wert der Instanzen der Klasse mit „AttributeName=MaxBandwidth“ oder „MinBandwidth“ und deren FQDD-Eigenschaften. Die Höchst- und Mindestbandbreitenwerten.
 - 20 - 30
 - 30 - 40
 - 25 - 35

Weitere Informationen zu Einschränkungen in Bezug auf die Bandbreite bei verschiedenen CNA-Karten finden Sie unter *iDRAC7 version 1.00.00 Readme* oder im Dokument „Einfaches NIC-Profil“ unter delltechcenter.com/page/DCIM.Library.

5. Verwenden Sie die FQDD für die identifizierte Partition, und rufen Sie die Methode **SetAttribute()** auf, um die Bandbreite zu ändern.
6. Überprüfen Sie den aktualisierten Wert im offenen Feld für das Attribut.
7. Erstellen Sie vor dem Aufrufen der Methode **CreateTargetedConfigJob()** die Eingabeparameter (Target, RebootJobType, ScheduledStartTime, UntilTime usw.).

Wenn auf mehr als einer Partition auf einer Schnittstelle eine Konfigurationsänderung vorgenommen wurde, definieren Sie `RebootJobType` und `ScheduledStartTime` nicht. Planen Sie die Aufgabe über die Methoden des Aufgabensteuerungsprofils. Gehen Sie zu *Schritt 9*, um die Aufgaben zu erstellen. Lesen Sie das Dokument „Simple NIC Profile“ auf delltechcenter.com/page/DCIM.Library um die Liste aller unterstützten Eingabeparameter anzuzeigen.

8. Rufen Sie die Methode **CreateTargetedConfigJob()** auf, um die ausstehenden Werte anzuwenden. Wenn diese Methode erfolgreich ist, muss das System eine Aufgabekennung für die von Ihnen erstellte Konfigurationsaufgabe zurückgeben.

 **ANMERKUNG:** Das System muss neu gestartet werden, um die Aufgabe des Einstellens des Attributs bzw. der Attribute ausführen zu können.

9. Erstellen Sie mithilfe von **CreateRebootJob()** eine Neustartaufgabe, und planen Sie alle Partitionsaufgaben und die Neustartaufgabe mithilfe von **SetupJobQueue()**. Noch offene Änderungen auf den Partitionen gehen verloren, wenn sie nicht für die gemeinsame Ausführung geplant werden.
10. Sie können den Status des Aufgabekennungsabgabewertes abfragen, indem Sie die Methoden des Aufgabesteuerungsprofils verwenden.
11. Wiederholen Sie den Abschnitt unter *Schritt 4*, um die erfolgreiche Ausführung der Methode zu bestätigen.

Referenzen zum Ändern der Merkmale

 **ANMERKUNG:** Die in dieser Tabelle referenzierten Abschnitte enthalten ausschließlich allgemeine Beispiele.

Tabelle 13. Schrittnummer und Speicherort

Schrittnummer	Speicherort der Speicherrichtlinie für Lifecycle-Controller-Webdienste (Windows oder Linux)
Schritt 1.	15.1 – Auflisten der Aufzählungsklasse für den CNA-Bestand
Schritt 2.	15.14 – Festlegen von CNA-LAN-Modi
Schritt 4.	15.3 – Auflisten der Ganzzahlenklasse für den CNA-Bestand
Schritt 5.	15.11 – Festlegen des Attributs „MaxBandwidth“
Schritt 6.	15.3 – Auflisten der Ganzzahlenklasse für den CNA-Bestand
Schritt 7.	16.7 – Anwenden der noch offenen Werte für das CNA – CreateTargetedConfigJob()
Schritt 8.	16.14 – Anwenden der noch offenen Werte für das CNA – CreateTargetedConfigJob()
Schritt 9.	7.8 — CreateRebootJob() 10.2.1 — Aufgabewarteschlange einzurichten
Schritt 10.	10.2.3 – Auflisten von Aufgaben im Aufgabenspeicher

Profile

Dokument „Einfaches NIC-Profil“ unter delltechcenter.com/page/DCIM.Library


MOFs

- DCIM_NICView
- DCIM_NICString
- DCIM_NICEnumeration
- DCIM_NICInteger
- DCIM_NICAttribute
- DCIM_NICService

Einrichten der virtuellen Adressattribute

Für eine erfolgreiche Ausführung von Remoteaufgaben auf dem Server müssen Sie sicherstellen, dass die folgenden Vorbedingungen, die im Abschnitt [Allgemeine Voraussetzungen vor der Verwendung der Remote-Services](#) zur Verfügung stehen, erfüllt sind:

Ändern Sie die virtuellen Adressattribute auf einer CNA-Karte.

 **ANMERKUNG:** Alle virtuellen Adressattribute werden auf den Standardwert zurückgesetzt, wenn das System von der Netzstromversorgung getrennt wird.

Legen Sie die entsprechenden Werte für jede der folgenden virtuellen Adressattribute fest:

- VirtMacAddr
- VirtIscsiMacAddr
- VirtFIPMacAddr
- VirtWWN
- VirtWWPN

Referenzen zu virtuellen Adressattributen


 **ANMERKUNG:** Die in dieser Tabelle referenzierten Abschnitte enthalten ausschließlich allgemeine Beispiele.

Tabelle 14. Schrittnummer und Speicherort

Schrittnummer	Speicherort der Speicherrichtlinie für Lifecycle-Controller-Webdienste (Windows oder Linux)
-	15.12 – Einrichten des Attributs „VirtMacAddr“
Profile	
DCIM_SimpleNIC Profile	
MOFs	
<ul style="list-style-type: none">• DCIM_NICView• DCIM_NICString• DCIM_NICEnumeration• DCIM_NICInteger• DCIM_NICAattribute• DCIM_NICService	

Einrichten der Attribute „Boot Target-ISCSI“ und „FCoE“

Für eine erfolgreiche Ausführung von Remoteaufgaben auf dem Server müssen Sie sicherstellen, dass die folgenden Vorbedingungen, die unter [Allgemeine Voraussetzungen vor der Verwendung der Remote-Services](#) zur Verfügung stehen, erfüllt sind:

Ändern Sie die Attribute „iSCSI“ und „FCoE“ auf einer CNA-Karte.

So ändern Sie iSCSI- und FCoE-Attribute:

- Legen Sie zum Festlegen der iSCSI-Initiator-Attribute die entsprechenden Werte für die folgenden Entitäten fest:

- IscsilInitiatorIpAddr
- IscsilInitiatorSubnet
- IscsilInitiatorSubnetPrefix
- IscsilInitiatorGateway
- IscsilInitiatorPrimDns
- IscsilInitiatorSecDns
- iscsilInitiatorName
- IscsilInitiatorChapId
- IscsilInitiatorChapPwd
- Um das erste iSCSI-Ziel einzurichten, legen Sie die entsprechenden Werte für die folgenden Entitäten fest:
 - ConnectFirstTgt
 - FirstTgtIpAddress
 - FirstTgtTcpPort
 - FirstTgtBootLun
 - FirstTgtIscsiName
 - FirstTgtChapId
 - FirstTgtChapPwd
- Um das FCoE-Startziel zu konfigurieren, legen Sie die entsprechenden Werte für die folgenden Entitäten fest:
 - MTUParams
 - ConnectFirstFCoETarget
 - FirstFCoEWWPNTarget
 - FirstFCoEBootTargetLUN
 - FirstFCoEFCVLANID

Bestandsliste und Protokolle

Verwenden Sie die Bestandslisten- und Protokollfunktionen, um:

- Aktuelle und werkseitige Bestandsliste abrufen und exportieren
- Lebensdauerprotokoll abrufen und exportieren
- Reset des Systems

Abruf des Hardwarebestandes

Unter Verwendung der Remotedienste können Sie die Hardwarebestandsliste eines Systems sofort abrufen. Die Bestandsliste führt alle auf dem System installierten Hardware-Geräte auf.

Die Informationen zur Hardware-Bestandsliste werden auf dem persistenten Speicher des Lifecycle-Controllers zwischengespeichert und stehen iDRAC- und UEFI-Anwendungen zur Verfügung.


Sie müssen zum Abruf der Hardware-Bestandsliste die Ansichtsklassen von unterschiedlicher Systemhardware auflisten, wie z.B. von Lüftern, Netzteilen, iDRAC, Videokarten, CPU, DIMMs und PCI/PCIe, um deren Eigenschaften anzuzeigen.

Lesen Sie für weitere Informationen zu verschiedenen Hardwareprofilen den Abschnitt unter [Hardware-Bestandslistenprofile](#).

Weitere Informationen zu den einfach zu verwendenden Bezeichnungen der Hardwarekomponenten finden Sie unter [Leicht zu verwendende Systemkomponentenbezeichnungen](#).

Exportieren der aktuellen Hardware-Bestandsliste


- Rufen Sie zum Exportieren der aktuellen Hardware-Bestandsliste als XML-Datei die Methode **ExportHWInventory()** in der Klasse `DCIM_LCService` auf.
- Rufen Sie zum Speichern einer Kopie der Werkseinstellungen eines verwalteten Knotens die Methode **ExportFactoryConfiguration()** in der Klasse `DCIM_LCService` auf.

 **ANMERKUNG:** Speichern Sie die XML-Datei auf einem USB-Gerät oder einer Netzwerkreigabe, oder in beiden Speicherorten.


Lifecycle-Protokoll

Lifecycle-Protokoll zeigt die folgenden Informationen auf:

- iDRAC-Konfigurationsänderungen
- Protokolle aller Remote-Schreibvorgängen und Benutzerauthentifizierungsfehler
- Firmware-Aktualisierungsverlauf, basierend auf Gerät, Version und Datum.
- BIOS- und NIC-Konfigurationsänderungen.
- RAID Konfigurationsänderungen.
- Fehlermeldungskennungen. Lesen Sie für weitere Informationen das Verzeichnis der Fehlermeldungen auf support.dell.com/manuals.
- Ereignisse (nur Aktualisierung und Konfiguration) basierend auf Schweregrad, Kategorie und Datum.

 **ANMERKUNG:** Die Einzelheiten der Konfigurationsänderungen werden nicht angezeigt.

- Kundenkommentare basierend auf dem Datum.

 **ANMERKUNG:** Das Lifecycle-Protokoll steht sogar dann zur Verfügung, wenn das OS nicht auf dem System installiert ist und ist unabhängig vom Energiezustand des Systems.


Exportieren des Lifecycle-Protokolls


Verwenden Sie diese Funktion zum Exportieren der Lifecycle-Protokollinformationen in eine XML-Datei. Speichern Sie die XML-Datei auf einem USB-Gerät oder einer Netzwerfreigabe, oder in beiden Speicherorten.

Rufen Sie zum Exportieren des Lifecycle-Protokolls die Methode **ExportLCLog()** in der Klasse `DCIM_LCService` auf. Nähere Informationen finden Sie unter [Lifecycle Protokoll-Schema](#).

Löschen der Konfiguration und Zurücksetzen auf die Standardeinstellungen

Verwenden Sie diese Funktion zum Löschen jeglicher sensibler Daten und konfigurationsbezogener Informationen, wenn Sie einen verwalteten Knoten aus dem Betrieb nehmen, einen verwalteten Knoten für eine andere Anwendung wiederverwenden, oder einen verwalteten Knoten auf einen nicht-sicheren Speicherort verschieben müssen.


 **VORSICHT:** Diese Funktion setzt den iDRAC auf die Werkseinstellungen zurück und löscht sämtliche iDRAC-Benutzeranmeldeinformationen und IP-Adressen-Konfigurationseinstellungen. Sie löscht außerdem Lifecycle-Protokolle, die Verlaufsdaten aller Änderungsereignisse, Firmwareaktualisierungen und Benutzerkommentare, Zertifikate, ExportFactoryConfiguration-Informationen und Firmware Rollback-Dateien enthalten. Es wird empfohlen, dass Sie das Lifecycle-Protokoll auf einen sicheren Speicherort exportieren, bevor Sie diese Funktion verwenden. Fahren Sie nach dem Vorgang das System manuell herunter und schalten Sie es dann wieder ein.

 **ANMERKUNG:** Sichern Sie das Lifecycle-Protokoll und die „ExportedFactoryConfiguration“, bevor Sie die Konfiguration löschen.

Rufen Sie zum Löschen der Konfiguration und Zurücksetzen auf die Werkseinstellungen die Methode **LCWipe()** in der Klasse `DCIM_LCService` auf.

Anzeigen und Exportieren der Hardwarebestandsliste nach dem Zurücksetzen des Lifecycle-Controllers:

Nach dem Durchführen des Zurücksetzens von Lifecycle-Controller werden inkorrekte Bestandsdaten angezeigt oder (in eine XML-Datei) exportiert. Zum Anzeigen oder Exportieren der korrekten Hardwarebestandslistendaten nach dem Zurücksetzen des Lifecycle-Controllers:

 **ANMERKUNG:** Nach dem Durchführen des Zurücksetzens von Lifecycle-Controller fahren Sie manuell das System herunter.

1. Schalten Sie das System ein und warten Sie ein paar Minuten, bis der iDRAC den Betrieb aufnimmt.
2. Trennen Sie das Stromkabel und warten Sie 30 Sekunden.
3. Schließen Sie das Stromkabel wieder an und starten Sie das System und rufen Sie die **ExporthWInventory()**-Methode auf der `DCIM_LCService`-Klasse auf.

Remote-Aktualisierungen

Verwenden Sie die Remote-Aktualisierungs- und Firmware-Bestandslistenfunktion, um Diagnose, Aktualisierung und den Abruf der Firmware-Bestandsliste durchzuführen.

Verwendung von Remote-Aktualisierung


Remote-Aktualisierung, auch als bandexterne Aktualisierung oder betriebssystemunabhängige Plattformaktualisierung bekannt, erlaubt Ihnen, das System unabhängig vom Betriebssystemzustand zu aktualisieren. Sie können die Firmware ungeachtet dessen initialisieren, ob sich die Systemstromversorgung im ein- oder ausgeschalteten Status befindet.


Bei einer betriebssystemunabhängigen Plattformaktualisierung ist es nicht erforderlich, dass auf dem System ein Betriebssystem ausgeführt wird. Mehrfachaktualisierungen können zusammen mit einem ordentlichen Neustart bzw. einem Neustart durch Aus- und Einschalten des Lifecycle-Controllers geplant werden, um die Aktualisierungen auszuführen. Obgleich für die Aktualisierungen zwischenzeitliche BIOS-Neustarts erforderlich sein könnten, handhabt sie der Lifecycle-Controller automatisch, bis die Aktualisierungen abgeschlossen sind.

Diese Funktion unterstützt zwei Methoden zum Ausführen von Aktualisierungen:

- **Installation über den Uniform Resource Identifier (URI):** Diese Methode erlaubt einer WS-MAN-Anforderung, Software unter Verwendung eines URI auf einer Host-Plattform zu installieren oder aktualisieren. Der URI besteht aus einer Zeichenkette, die zum Identifizieren oder Benennen einer Ressource auf dem Netzwerk verwendet wird. Der URI wird zur Angabe des Speicherorts des Dell Update Package-Abbildes auf dem Netzwerk verwendet, das auf den Lifecycle-Controller heruntergeladen und dann installiert werden kann.
- **Installation über die Softwareidentität:** Diese Methode erlaubt die Aktualisierung bzw. den Rollback auf eine Version, die auf dem Lifecycle-Controller bereits verfügbar ist.

Sie können eine WS-MAN-fähige Anwendung oder ein WS-MAN-fähiges Script oder Befehlszeilendienstprogramm verwenden, um eine Remote-Aktualisierung auszuführen. Die Anwendung bzw. das Script führt die Aufforderung der WS-MAN-Aufrufungsmethode unter Verwendung einer der Remote-Aktualisierungsschnittstellen-Methoden durch. Der iDRAC lädt anschließend die Firmware vom Netzwerkfreigabe-URI (lokale Netzwerkfreigabe, CIFS, NFS, FTP, TFTP, http) herunter und bereitet die Aktualisierungen so vor, dass sie zum festgelegten Zeitpunkt und unter Verwendung der festgelegten Typen des Systemneustarts, „graceful“ (ordentlich), „power cycle“ (aus- und einschalten) oder „force“ (erzwingen), durchgeführt werden.

 **ANMERKUNG:** Wenn Sie auf dem Treiberpaket für das System eine Remote-Aktualisierung ausführen, wird das aktuelle Treiberpaket ersetzt. Das ersetzte Treiberpaket steht dann nicht mehr zur Verfügung.

 **ANMERKUNG:** Es werden nur alphanumerische Pfadnamen unterstützt.

Unterstützte Geräte

Remote-Aktualisierung wird für die folgenden Geräte und Komponenten unterstützt:

- iDRAC7
- RAID-Serie 6 und 7
- NICs, LOMs, NDCs und CNAs (Broadcom, Intel und QLogic)
- Netzteile




- BIOS
- BS-Treiberpaket
- Lifecycle-Controller
- Diagnose

Remote-Aktualisierung über den URI

So führen Sie Remote-Aktualisierung über den URI aus:

1. Verwenden Sie den entsprechenden WS-MAN-Client, um eine Methodenaufruf-Aufforderung an die iDRAC-IP-Adresse zu senden. Der WS-MAN-Befehl schließt die Methode **UpdateFromURI()** auf dem `DCIM_SoftwareInstallationService` sowie den Speicherort ein, von dem aus der iDRAC das Dell Update Package (DUP) herunterladen soll. Die unterstützten Download-Protokolle sind FTP, HTTP, CIFS, NFS und TFTP.

Wenn der Befehl erfolgreich aufgerufen wird, wird eine Auftrags-ID ausgegeben.

-  **ANMERKUNG:** Zusätzliche Aufrufungsaufforderungen der Methode **UpdateFromURI()** können unter Verwendung von WS-MAN zur Erstellung anderer Aktualisierungsaufgaben gesendet werden.
- 2. Rufen Sie die Methode **CreateRebootJob()** auf dem `DCIM_SoftwareInstallationService` auf und legen Sie den gewünschten Neustartyp (Ordentlicher Neustart ohne erzwungenes Herunterfahren, Aus- und Einschalten und ordentlicher Neustart mit erzwungenem Herunterfahren) fest.
- 3. Unter Verwendung der Aktualisierungs- und Neustartaufgaben-Kennungen können Sie das Dell Job Control-Profil (Dell Aufgabensteuerungsprofil) verwenden, um diese Aufgaben so zu planen, dass sie entweder sofort oder zu einem zukünftigen Datum bzw. einer zukünftigen Uhrzeit ausgeführt werden. Sie können die Aufgabenkennung auch verwenden, um den Status einer Aufgabe abzufragen oder eine Aufgabe abubrechen.
- 4. Alle Aufgaben werden als erfolgreich gekennzeichnet. Falls während des Downloads oder der Aktualisierung ein Fehler auftrat, werden die Aufgaben als fehlgeschlagen gekennzeichnet. Bei fehlgeschlagenen Aufgaben stehen die Fehlermeldung und die Fehlermeldungs-ID in den Auftragsinformationen zur Verfügung.
-  **ANMERKUNG:** Nachdem das DUP erfolgreich heruntergeladen und extrahiert wurde, aktualisiert der Downloader den Auftragsstatus als `Heruntergeladen`, worauf der Auftrag zeitlich geplant werden kann. Wenn die Signatur ungültig oder der Download oder die Extrahierung fehlgeschlagen ist, wird der Auftragsstatus zusammen mit einem entsprechenden Fehlercode als `Fehlgeschlagen` angegeben.
-  **ANMERKUNG:** Um die aktualisierte Firmware-Versionen anzuzeigen, listen Sie Firmware-Bestandsliste auf, nachdem die Firmware-Aktualisierungsaufgaben abgeschlossen wurden.


Remote-Aktualisierung planen

Sie können Firmware-Aktualisierungen jetzt oder in Zukunft planen oder vorbereiten. Sie können Aktualisierungen von Diagnoseprogramm, Lifecycle-Controller und Betriebssystemtreiberpaket direkt und ohne jegliche Vorbereitungen durchführen. Diese Aktualisierungen werden angewendet, sobald sie heruntergeladen worden sind; sie benötigen den Job Scheduler nicht. Bei allen anderen Remote-Aktualisierungen handelt es sich um vorbereitete Aktualisierungen, die unter Verwendung verschiedener Planungsoptionen geplant werden müssen. Die DUPs werden auf den Lifecycle-Controller heruntergeladen und vorbereitet, und die eigentliche Aktualisierung wird durchgeführt, indem ein Neustart des Systems in den UEFI-Lifecycle-Controller durchgeführt wird.


Es stehen mehrere Optionen zum Einplanen von Aktualisierungen zur Verfügung:

- Ausführen von Aktualisierungen gewünschter Komponenten zum gewünschten Zeitpunkt.
- Ausführen des Neustartbefehls, um eine Neustart-Aufgabenkennung abzurufen.
- Überprüfen des Status beliebiger Aufgaben, indem Sie `DCIM_SoftUpdateConcreteJob`-Instanzen auflisten und den Wert der Eigenschaft `JobStatus` überprüfen.

- Planen der Aufgaben unter Verwendung der Methode **SetupJobQueue()** des `DCIM_JobService`.


 **ANMERKUNG:** Für Remote-Aktualisierungen der Remotedienste in der Version 1.3 können Sie nur die Methode **SetupJobQueue()** verwenden.

- Löschen vorhandener Aufgaben unter Verwendung der Methode **DeleteJobQueue()** des `DCIM_JobService`.

 **ANMERKUNG:** Wenn Sie das System herunterfahren oder es bei geplantem Aktualisierungsaufgabe für mehr als 15 Minuten in heruntergefahrenem Zustand lassen, dann wird empfohlen, dass Sie die geplante Aufgabe löschen.

Zurücksetzen auf vorhergehende Versionen


Verwenden Sie die Methode **InstallFromSoftwareIdentity()**, um mittels vorheriger Versionen der im Lifecycle-Controller gespeicherten Firmware neu zu installieren. Anstatt das DUP herunterzuladen, erstellt **InstallFromSoftwareIdentity()** eine Aufgabe und gibt die Aufgabekennung zurück.

 **ANMERKUNG:** Aktualisierungen für Lifecycle-Controller, Diagnose und Treiberpakete können nicht zurückgesetzt werden.

Verwenden der Remote-Firmware-Bestandsaufnahme

Die Funktion für die Remote-Firmware-Bestandsaufnahme ruft eine Bestandsliste der derzeit auf verschiedenen Geräten im verwalteten System installierten Firmware ab. Sie ruft außerdem die für ein Rollback zur Verfügung stehenden Versionen ab (N und N-1-Versionen).

Mit der Funktion für die Remote-Firmware-Bestandsaufnahme können Sie eine Bestandsaufnahme unabhängig vom Systemstatus und Status des Betriebssystems ausführen. Sie können eine Liste der Firmware für installierte Geräte sowie der für Rollback und Neuinstallation verfügbaren Firmware abrufen.

 **ANMERKUNG:** Die iDRAC-Benutzeranmeldeinformationen, die für die WS-MAN-Aufforderungsauthentifizierung verwendet werden, erfordern Anmeldeberechtigungen zum Anfordern der Bestandsaufnahme von Firmware und integrierter Software. Sie sind jedoch nicht auf Administratoren beschränkt.

Unterstützte Geräte

Die sofortige Firmware-Bestandsaufnahme wird für diese Geräte und Komponenten unterstützt:


- iDRAC7
- Speicher-Controller (RAID-Serie 7 und 8)
- NICs und LOMs (Broadcom, Intel und QLogic)
- Netzteile
- BIOS
- OS-Treiberpaket
- Life Cycle Controller
- Diagnose
- Complex Programmable Logic Device (CPLD, komplex programmierbares Logikgerät)
- Physische Laufwerke
- Gehäuse

Die Klasse der sofortigen Firmware-Bestandsaufnahme bietet Firmware-Bestandsaufnahmeinformationen zu:

- Der auf den unterstützten Geräten installierten Firmware
- Den Firmware-Versionen, die auf den einzelnen Geräten zur Installation verfügbar sind.

Abruf des Firmwarebestandes


Das DCIM_SoftwareInventory-Profil definiert die Erweiterungen der Dell-CIM-Datenmodelle, die installierte Versionen und zur Installation verfügbare Versionen von Firmware und integrierter Software auf dem Server repräsentieren. Sie können unter Verwendung des WS-MAN-Webdienstprotokolls auf die Firmware-Bestandsaufnahme zugreifen.


 **ANMERKUNG:** Es ist möglich, dass Instanzen der Art `DCIM_SoftwareIdentity` für Hardware, die zuvor installiert und dann entfernt wurde. Solche Instanzen werden in der Bestandsliste als `verfügbar` aufgeführt, wenn CSIOR nicht durchgeführt wird.

Sie rufen eine Firmwarebestandsaufnahme unter Verwendung von Windows WS-MAN ab:

1. Listen Sie die Klasse `DCIM_SoftwareIdentity` auf, um die Bestandsliste des Systems abzurufen.


Die Bestandsaufnahmen werden als installierte und verfügbare CIM-Instanzen zusammengetragen.

 **ANMERKUNG:** Benutzer mit Administratorrechten oder Berechtigungen zum Ausführen von Serverbefehlen können die Bestandsaufnahme der Firmware und integrierten Software des Systems abrufen.

 **ANMERKUNG:** Bestandsaufnahmeinstanzen werden sowohl im ausgeschalteten als auch im eingeschalteten Zustand des Systems vom System abgerufen.

- Die derzeit auf der Komponente installierte Software ist als Instanz der installierten Software aufgeführt. Der Statuswert dieser Instanz wird als `Installiert` dargestellt.
- Die verfügbare Software im beständigen Speicher wird als Instanz der verfügbaren Software aufgeführt. Der Schlüsseleigenschaftswert dieser Instanz, Instanz-ID, wird als `DCIM: INSTALLED :<COMPONENTTYPE> :<COMPONENTID> :<Version>` (`DCIM: AVAILABLE :<KOMPONENTENTYP> :<KOMPONENTEN-ID>:<Version>`) dargestellt, und der Statuswert dieser Instanz wird als „Available“ (Verfügbar) dargestellt. Instanzen aktuell installierter Software werden auch als Instanzen verfügbarer Software dargestellt.

2. Bestandsaufnahmeinstanzen bieten Eingabewerte für die Aktualisierungs- und Rollback-Vorgänge. Suchen Sie zum Ausführen des Aktualisierungsvorgangs den Instanz-ID-Wert aus der installierten Instanz, `DCIM: INSTALLED :<comptype> :< compid> :< version>` (`DCIM: INSTALLIERT:<CompTyp>:<Comp-ID>:<Version>`), aus. Suchen Sie für den Rollback-Vorgang den Instanz-ID-Wert aus der verfügbaren Instanz, `DCIM:AVAILABLE:<comptype>:<compid>:<version>` (`DCIM: VERFÜGBAR:<CompTyp>:<Comp-ID>:<Version>`), aus. Instanz-ID-Werte können nicht bearbeitet werden.

 **ANMERKUNG:** Wenn der Eigenschaftswert `Versionszeichenkette` von Instanz verfügbarer Software der Instanz installierter Software gleich ist, darf der Instanz-ID-Wert dieser Instanz verfügbarer Software nicht für den Rollback-Vorgang verwendet werden.

Typen der Remote-Planung

Es gibt zwei Methoden für Planung:

- Sofortige Aktualisierung
- Geplante Aktualisierung

Sofortige Aktualisierung

Planen Sie zum sofortigen Aktualisieren von Komponenten-Firmware die Aktualisierungs- und Neustartaufgaben mit einer Startzeit von **TIME_NOW**. Das Planen eines Neustarts oder einer Aktualisierung ist für Aktualisierungen der Lifecycle-Controller-Komponenten (z.B. Lifecycle-Controller, Diagnose und BS-Treiberpakete) nicht erforderlich. Die Aktualisierungen für diese Komponenten erfolgen sofort.

Geplante Aktualisierung

Das Festlegen einer eingeplanten Startzeit für einen oder mehrere Aufgaben unter Verwendung der Methode **SetupJobQueue()** erfordert das Festlegen eines Datum-/Uhrzeitwerts für den Parameter `StartTimeInterval`. Optional kann auch für den Parameter `UntilTime` ein Datum-/Uhrzeitwert festgelegt werden.

Durch das Festlegen eines Parameters des Typs `UntilTime` wird ein Wartungsfenster zum zeitlich gebundenen Ausführen der Aktualisierungen definiert. Wenn das Zeitfenster abläuft und die Aktualisierungen nicht abgeschlossen werden konnten, werden alle derzeit ausgeführten Aktualisierungsaufgaben abgeschlossen. Nicht bearbeitete Aufgaben deren geplante Startzeit begonnen hat, schlagen jedoch fehl.

Zeitplanungs-Neustartverhalten einrichten

Die Methode **CreateRebootJob()** wählt einen der folgenden Neustarttypen als Eingabeparameter, und eine Neustartaufgabenkennung wird als Ausgabeparameter ausgegeben. Die Neustartaufgabenkennung wird als letzte Aufgabenkennung im Parameter `JobArray` der Methode **SetupJobQueue()** zusammen mit anderen Aufgabenkennungen verwendet.


- **Neustart 1 Aus- und Einschalten** — Führt das Aus- und Wiedereinschalten des verwalteten Servers durch, wodurch das System herunter- und wieder hochgefahren wird. Dies erfolgt nicht in Form eines ordentlichen Neustarts. Das System schaltet das System aus, ohne eine Herunterfahren-Aufforderung an ein Betriebssystem zu senden. Nur Neustarttyp 1 fährt das System hoch, wenn sich das System im Zustand „Aus“ befindet, während jedoch weiterhin Wechselstrom zugeführt wird.
- **Neustart 2 - Ordentlicher Neustart ohne erzwungenes Herunterfahren** – Führt den Befehl des ordentlichen Herunterfahrens des verwalteten Servers aus. Wenn das System außerdem während der Wartezeit bei Aus- und Wiedereinschalten heruntergefahren wird, wird das System wieder hochgefahren und der Neustartaufgabe wird als **Reboot Completed** gekennzeichnet. Wenn das System nicht während der `WaitTime` beim `PowerCycle` heruntergefahren wird, wird der Neustartauftrag als fehlgeschlagen gekennzeichnet.
- **Neustart 2 - Ordentlicher Neustart mit erzwungenem Herunterfahren** – Führt den Befehl des ordentlichen Herunterfahrens des verwalteten Servers aus. Wenn das System außerdem während der Wartezeit bei Aus- und Wiedereinschalten heruntergefahren wird, wird das System wieder hochgefahren und der Neustartaufgabe wird als **Reboot Completed** gekennzeichnet. Wenn das System nicht während der `WaitTime` beim `PowerCycle` heruntergefahren wird, wird das System aus- und wieder eingeschaltet.

Verwaltung der Teilersetzung

Die Teilersetzungsfunktion stellt für eine gerade ausgetauschte Komponente, wie z.B. einem RAID-Controller, einer NIC oder Stromversorgung, die automatische Aktualisierung der Firmware, bzw. der Konfiguration, oder beidem bereit, um zum ursprünglichen Teil zu passen. Dies ist eine lizenzpflichtige Funktion, die bei installierter iDRAC7 Enterprise-Lizenz verfügbar ist. Wenn eine Komponente ersetzt und die Funktion der Teilersetzung aktiviert ist, werden die Lifecycle Controlle-Maßnahmen lokal auf dem Systemmonitor angezeigt.

Sie können auf die Teilersetzung bezogene Eigenschaften unter Verwendung verschiedener WS-Management fähiger Dienstprogramme konfigurieren. Weitere Informationen finden Sie unter *Lifecycle-Controller Web Services – Schnittstellenrichtlinie – Windows und Linux Version*. DCIM-Profilspezifizierung und zugehörige MOF-Dateien stehen im Dell TechCenter-Wiki im Bereich der DCIM Extension Library zur Verfügung (www.DellTechCenter.com).

 **ANMERKUNG:** Für eine SAS-Karte wird nur die Firmware-Aktualisierung unterstützt. Konfigurationsaktualisierung wird nicht unterstützt, da die Attribute auf einer SAS-Karte nicht konfigurierbar sind.

 **ANMERKUNG:** Teilersetzung wird von verschiedenen Herstellern für viele Serverkomponenten unterstützt. Beziehen Sie sich für eine umfassende Liste auf die *iDRAC7 Version 1.00.00 Infodatei*, die auf support.dell.com/manuals verfügbar ist.

Bezug/Einstellung von Teile-Firmware- und Konfigurationsaktualisierungsattributen

Um die aktuellen Eigenschaftswerte **Teile-Firmware-Aktualisierung** und **Systembestandsaufnahme nach Neustart** unter Verwendung von WS-MAN abzurufen, kann eine Auflistungsbefehlaufforderung gesendet werden, um Instanzen der Klasse `DCIM_LCEnumeration` abzurufen. Ein `DCIM_LCEnumeration` Instanzobjekt, das die einzelnen Attribute repräsentiert, wird pro Attribut zurückgesendet, wobei die `AttributeName`-Zeichenketteneigenschaft des Objekts den Namen der mit der Teilersetzung in Verbindung stehenden Eigenschaft, wie **Teile-Firmware-Aktualisierung** enthält. Die Eigenschaft `Aktueller Wert` enthält die aktuelle Einstellung der Eigenschaft. Bestimmte Attributnamen und -werte finden Sie in der Spezifikation zum Verwaltungsprofil des Dell Lifecycle-Controllers. Eine davon sind:

- `AttributeName` - „Teile-Konfigurationsaktualisierung“
- `PossibleValues` - Deaktiviert, Immer anwenden, Nur bei Firmware-Übereinstimmung anwenden
- `AttributeName` - Teile-Firmwareaktualisierung
- `PossibleValues` - Deaktivieren, Nur Versionserweiterung zulassen, Firmware des ersetzten Teils angleichen

Zum Konfigurieren eines mit einer Teilersetzung in Verbindung stehenden Eigenschaftswerts werden Maßnahmen zum Einrichten und Anwenden unter Verwendung des WS-MAN-Webdienstprotokolls angefordert.

Rufen Sie die Methode **SetAttribute()** in der Klasse `DCIM_LCService` auf, um die Attribute festzulegen. Die Methode **SetAttribute()** verwendet Eigenschaftsnamen und -werte als Eingabeparameter. Die Tabelle führt die Werte der Teile-Firmware und der Konfigurationsaktualisierung auf.

Optionen	Werte
Teile-Firmware-Aktualisierung	
Nur Versionserweiterung zulassen	Wenn die Eingabe für den „CurrentValue“, „Nur Versionserweiterung zulassen“ lautet, wird die Firmware-Aktualisierung auf ersetzten Teilen ausgeführt, wenn die Firmware-Version des neuen Teils niedriger ist als die des Originalteils.
Firmware des ersetzten Teils angleichen	Wenn die Eingabe für den „Aktuellen Wert“, „Firmware des ersetzten Teils angleichen“ lautet, wird die Firmware des neuen Teils auf die Version des Originalteils aktualisiert.
Deaktivieren	Wenn die Eingabe „Deaktivieren“ lautet, finden die Firmware-Erweiterungsmaßnahmen nicht statt.
Aktualisierung der Teilekonfiguration	
Immer anwenden	Die aktuelle Konfiguration wird angewendet, wenn ein Teil ersetzt wird.
Nur bei Übereinstimmung der Firmware anwenden	Die aktuelle Konfiguration wird nur dann angewendet, wenn die aktuelle Firmware mit der Firmware eines ersetzten Teils übereinstimmt.
Deaktiviert	Die aktuelle Konfiguration wird nicht angewendet, wenn ein Teil ersetzt wird.

Rufen Sie die Methode **CreateConfigJob()** in der Klasse `DCIM_LCService` auf, um die Werte anzuwenden. Die Methode **CreateConfigJob()** verwendet die geplante Startzeit als Parameter (der `TIME_NOW` sein kann) und, falls erforderlich, einen Neustart. Eine Aufgabenkennung wird als Parameter ausgegeben und kann verwendet werden, um den Status der sich in Ausführung befindenden Aufgabe zu überprüfen.

Sichern und Wiederherstellen

Verwenden Sie die Export- und Importfunktion zum Sichern, Exportieren oder Wiederherstellen eines Serverprofils.

Exportieren von Serverprofilen auf die iDRAC vFlash-Karte oder die Netzwerkfreigabe

Für eine erfolgreiche Ausführung von Remoteaufgaben auf dem Server müssen Sie sicherstellen, dass die folgenden Vorbedingungen erfüllt sind:

- [Allgemeine Voraussetzungen vor der Verwendung der Remote-Services](#)
- iDRAC7 Enterprise-Lizenz wurde installiert.cccc
- Server weist eine gültige Service-Tag-Nummer mit sieben Zeichen auf.
- Der Zielspeicherort hat Lese- oder Schreibzugriff.
- iDRAC vFlash-Karte:
 - Installiert, aktiviert und initialisiert.
 - Mindestens 384 MB freier Speicherplatz.
- Netzwerkressource
 - Für den iDRAC werden Berechtigungen und Firewall-Einstellungen bereitgestellt, um mit dem System zu kommunizieren, auf dem die Netzwerkfreigabe definiert ist.
 - Es wurde die richtige Funktionslizenz installiert.
 - Mindestens 384 MB freier Speicherplatz.

 **ANMERKUNG:** Durch das Aufrufen der Methode **BackupImage()** wird eine Backup-Image-Datei auf der Netzwerkfreigabe erstellt; die Größe variiert dabei abhängig von der Systemkonfiguration von 30 MB bis 384 MB.

- Auf dem iDRAC sind Berechtigungen zum Ausführen von Serverbefehlen vorhanden.

Erstellen Sie ein Backup der Server-Firmware und der Konfiguration, und exportieren Sie das Backup auf die iDRAC vFlash-Karte oder auf eine Netzwerkfreigabe. Die Backup-Datei wird mit einer Passphrase gesichert.

So sichern Sie Folgendes:

- Hardware- und Firmware-Bestand, wie z. B. BIOS, LOMs, durch Lifecycle-Controller unterstützte Add-in-NIC-Karten und Speicher-Controller (RAID-Stufe, virtuelle Festplatte und Controller-Attribute).
- Systeminformationen wie z. B. Service-Tag-Nummer, System-Type usw.
- Images für die Lifecycle-Controller-Firmware, Systemkonfiguration sowie Firmware und Konfiguration für iDRAC.

Wichtige Hinweise

- Stellen Sie während des Exports sicher, dass Aufgaben wie z. B. die Firmware-Aktualisierung, die Betriebssystembereitstellung und Firmware-Konfigurationen nicht ausgeführt werden. Wenn eine Betriebssystembereitstellung mithilfe des Lifecycle-Controllers durchgeführt wird, setzen Sie iDRAC zurück, oder brechen Sie den Lifecycle-Controller ab, bevor Sie den Export fortsetzen können.
- Nach der Bereitstellung eines Betriebssystems mithilfe des Lifecycle-Controllers ist OEMDRV für 18 Stunden geöffnet, da der Lifecycle-Controller nicht auf den Status der Betriebssysteminstallation zugreifen kann. Wenn Sie nach der Betriebssystembereitstellung Aufgaben wie Aktualisierung, Konfiguration oder Wiederherstellung


durchführen müssen, müssen Sie die OEMDRV-Partition entfernen. Setzen Sie zum Entfernen der Partition iDRAC zurück, oder brechen Sie den Lifecycle-Controller ab.

- Planen Sie keine Remotedienst-Aufgaben, z. B. BIOS-Aktualisierungen oder Einstellungen von NIC-Attributen.
- Wenn Sie den Parameter `ScheduledStartTime` nicht verwenden, wird eine Aufgabekennung ausgegeben, die Aufgabe wird jedoch nicht geplant. Rufen Sie zum Planen der Aufgabe die Methode **SetupJobQueue()** des `DCIM_JobService` auf.
- Sie können eine Exportaufgabe mithilfe der Methode **DeleteJobQueue()** in der Klasse `DCIM_JobService` vor dem Ausführungsbeginn abbrechen. Nachdem die Ausführung der Aufgabe begonnen hat, drücken Sie F2 während des Einschalt-Selbsttests (POST) und wählen Sie die Option `Lifecycle-Controller` abbrechen. Dadurch wird der Wiederherstellungsprozess gestartet und setzt das System in einen bereits bekannten Status zurück. Die Wiederherstellung erfolgt innerhalb von 5 Minuten. Zur Überprüfung, ob die Wiederherstellung erfolgreich durchgeführt wurde, fragen Sie die Exportaufgabe über die WS-Verwaltungsbefehle ab, oder überprüfen Sie die iDRAC RAC- oder Lifecycle-Protokolle.
- Beim Export auf eine Netzwerkfreigabe über die WS-Verwaltung sind nur 64 Zeichen in der Bezeichnung des Images zulässig.
- Stellen Sie sicher, dass die Backup-Datei während des Exports oder Imports nicht beschädigt wird.

So exportieren Sie das Systemprofil:

1. Bauen Sie die Eingabeparameter in Abhängigkeit davon auf, wo die Backup-Image-Datei gespeichert wird: auf der iDRAC vFlash-Karte oder auf der Netzwerkfreigabe (CIFS oder NFS).
2. Rufen Sie die Methode **BackupImage()** auf `DCIM_LCService`. Auf dem Bildschirm wird eine Aufgabekennung ausgegeben (z. B. `JID_001291194119`).
3. Zum Abrufen des Aufgabenstatus oder des prozentualen Aufgabenfortschritts führen Sie den entsprechenden WS-Verwaltungsbefehl für die Aufgabekennung aus.

Überprüfen Sie neben der Abfrage der Aufgabekennung mithilfe verschiedener Skripting-Sprachen die iDRAC-Protokolle, um den Fortschritt der Aufgabe abzurufen. Wenn für den Aufgabenstatus `Abgeschlossen` angezeigt wird, überprüfen Sie die Lifecycle-Protokolle für alle Exporteinträge. Exportieren Sie zum Anzeigen des Protokolls das Protokoll mithilfe der Methode **ExportLCLog()** (LC-Protokoll exportieren) auf der `DCIM_LCService`-Klasse, oder zeigen Sie das Protokoll auf der Benutzeroberfläche für Unified Server Configurator–Lifecycle-Controller Enabled an.

 **ANMERKUNG:** Wenn der Export fehlschlägt, wird der Aufgabenstatus als fehlgeschlagen gekennzeichnet, außerdem wird eine Meldung angezeigt, die den Grund für den fehlgeschlagenen Export angibt. Weitere Informationen zu den Fehlermeldungskennungen und den empfohlenen Maßnahmen finden Sie in der *Dell Lifecycle-Controller Remote Services-Liste mit Fehlermeldungen und Fehlerbehebungen* unter support.dell.com/manuals.

Funktion oder Systemverhalten zum Exportieren des Server-Profiles

- Während des Exports ist der Lifecycle-Controller nicht verfügbar.
- Während des Exports wird eine der folgenden Aktivitäten ausgeführt:
 - Eine Partition mit dem Kennzeichnungsamen `SRVCNF` wird automatisch auf der iDRAC vFlash-Karte erstellt, und die Backup-Datei wird in dieser Partition erstellt und gespeichert. Wenn eine Partition mit einem Kennzeichnungsamen `SRVCNF` auf der iDRAC vFlash-Karte bereits vorhanden ist, wird diese überschrieben.
 - Die Backup-Datei wird erstellt und auf einer Netzwerkfreigabe gespeichert.
- Der Export dauert je nach Serverkonfiguration bis zu 45 Minuten.
- Während des Exports werden alle unterstützten Komponenten in einem Arbeitsgang gesichert. Es ist nicht möglich, eine einzelne Komponente zu sichern (z. B. können Sie nicht ausschließlich die LOM-Firmware und -Konfiguration sichern.)
- Während des Exports werden keine Treiberpakete oder Diagnosepaketinformationen gesichert.

- Sichern Sie für zusätzliche Sicherheit die Backup-Image-Datei mit einer Passphrase.
- Wenn Sie keinen Wert für die Variable `ShareType` eingeben, wird dieser Wert durch die Remotedienste als 0 eingelesen. Außerdem versuchen die Remotedienste, das Image auf der NFS-Freigabe zu sichern.
- Während des Exports werden nur die aktuellen Firmware-Versionen für von Lifecycle-Controller unterstützten Geräten (BIOS, iDRAC, NIC und Speicher-Controller) gesichert, eine Sicherung der Rollback-Firmware-Versionen erfolgt nicht.

Beispiel: Die derzeit installierte BIOS-Firmware-Version lautet 2.1, die Version 2.0 ist die Rollback-Version (2.0 war die Version vor der Installation von Version 2.1). Nach dem Export wird die derzeit installierte BIOS-Firmware-Version 2.1 gesichert.

Referenzen zum Exportieren des Serverprofils


 **ANMERKUNG:** Die in dieser Tabelle referenzierten Abschnitte enthalten ausschließlich allgemeine Beispiele.

Tabelle 15. Schrittnummer und Speicherort


Schrittnummer	Speicherort der Speicherrichtlinie für Lifecycle-Controller-Webdienste (Windows oder Linux)
Schritt 1.	18.1 – Serverprofil exportieren
Schritt 2.	18.1.1 – Serverprofil nach iDRAC vFlash Card exportieren - BackupImage() 18.1.2 – Serverprofil auf NFS-Freigabe exportieren - BackupImage() 18.1.2 – Serverprofil auf CIFS-Freigabe exportieren - BackupImage()
Schritt 3.	18.1.4 – Exportstatus überwachen
Profile	
DCIM-LCManagementProfile	
MOFs	
DCIM_LCService.mof	

Importieren des Serverprofils von einer iDRAC vFlash-Karte oder einer Netzwerkfreigabe

Für eine erfolgreiche Ausführung von Remoteaufgaben auf dem Server müssen Sie sicherstellen, dass die folgenden Vorbedingungen erfüllt sind:

- [Allgemeine Voraussetzungen vor der Verwendung der Remote-Services.](#)
- iDRAC7 Enterprise-Lizenz wurde installiert.
- Die Service-Tag-Nummer des Servers ist entweder leer oder identisch mit der Nummer zum Zeitpunkt der Erstellung des Backups.
- iDRAC vFlash-Karte:
 - Ist installiert, aktiviert und weist die SRVCNF-Partition auf.
 - Mindestens 384 MB freier Speicherplatz steht zur Verfügung.
- Wenn das Backup von einer iDRAC vFlash-Karte importiert werden soll, stellen Sie sicher, dass die Karte installiert ist und das Backup-Image auf der SRVCNF-Partition enthält. Dieses Image stammt von der gleichen Plattform, die Sie importieren.
- Wenn Sie das Backup von einer Netzwerkfreigabe importieren, stellen Sie sicher, dass die Netzwerkfreigabe, auf der die Backup-Datei gespeichert ist, weiterhin zugänglich ist.
- Wenn die Hauptplatine ersetzt wird, bevor der Import durchgeführt wird, stellen Sie sicher, dass die Hauptplatine mit den aktuellen iDRAC- und BIOS-Versionen installiert ist.


Importieren Sie das Backup für die Firmware und die Konfiguration (Server und Firmware), und stellen Sie es auf dem gleichen System wieder her, auf dem das Backup erstellt wurde.

 **ANMERKUNG:** Wenn Sie die Hauptplatine austauschen, stellen Sie sicher, dass Sie die Hardware am gleichen Standort neu installieren. Montieren Sie beispielsweise die NIC PCI-Karte auf dem gleichen PCI-Steckplatz, der vor dem Backup verwendet wurde.

Optional können Sie die Konfiguration der aktuellen virtuellen Festplatte löschen und die Konfiguration aus der Backup-Image-Datei wiederherstellen.


Wichtige Hinweise

- Benutzerdaten sind in der Backup-Image-Datei nicht vorhanden. Durch das Löschen der Konfiguration werden auch die Benutzerdaten gelöscht.
- Stellen Sie während des Imports sicher, dass Aufgaben wie z. B. die Firmware-Aktualisierung, die Betriebssystembereitstellung und Firmware-Konfigurationen nicht ausgeführt werden. Wenn die Betriebssystembereitstellung mithilfe des Lifecycle-Controllers ausgeführt wird, müssen Sie iDRAC zurücksetzen oder den System-Service vor der Ausführung des Imports abbrechen.
- Nach der Bereitstellung des Betriebssystems mithilfe des Lifecycle-Controllers ist OEMDRV für 18 Stunden zugänglich. Wenn Sie nach der Betriebssystembereitstellung weitere Aktivitäten ausführen möchten, z. B. Aktualisierung, Konfiguration oder Import, müssen Sie OEMDRV-Partition entfernen. Setzen Sie zum Entfernen der Partition iDRAC zurück, oder brechen Sie den Lifecycle-Controller ab.
- Wenn Sie bei den WS-Verwaltungsbefehlen nicht den Parameter `ScheduledStartTime` verwenden, wird eine Aufgabenkennung ausgegeben, es erfolgt jedoch keine Planung. Rufen Sie zum Planen einer Aufgabe die Methode **SetupJobQueue()** auf.
- Sie können eine Import-Aufgabe mithilfe der Methode **DeleteJobQueue()** vor dem Ausführungsbeginn abbrechen. Nachdem die Ausführung der Aufgabe begonnen hat, drücken Sie während des Einschalt-Selbsttests (POST) die Taste F2 und gehen Sie zu **iDRAC-Einstellungen** → **Lifecycle-Controller** und wählen Sie **Ja** für **Lifecycle-Controller-Maßnahmen abbrechen**, oder setzen Sie iDRAC zurück. Dadurch wird der Wiederherstellungsprozess eingeleitet, der das System in einen bekannten, funktionsfähigen Betriebsstatus zurücksetzt. Der Wiederherstellungsprozess darf nicht mehr als fünf Minuten in Anspruch nehmen. Zur Überprüfung, ob der Wiederherstellungsprozess erfolgreich durchgeführt wurde, fragen Sie die Importaufgabe über die WS-Verwaltungsbefehle ab, oder überprüfen Sie die iDRAC RAC- oder Lifecycle-Protokolle.
- Wenn Sie die Hauptplatine vor dem Start des Importprozesses ausgetauscht haben, drücken Sie während des Einschalt-Selbsttests (POST) die Tastenkombination „STRG+E“, und legen Sie eine IP-Adresse auf dem Netzwerk fest, so dass Sie die Methode **RestoreImage()** aufrufen können. Nachdem Sie diese Methode aufgerufen haben, wird die Service-Tag-Nummer aus der Backup-Image-Datei wiederhergestellt.

 **ANMERKUNG:** Die Netzteil-Firmware wird während des Importvorgangs nicht aktualisiert. Während der Netzteilfirmwareaktualisierung wird die Stromzufuhr zur PSU getrennt. Die Firmware ist nach Abschluss des Importvorgangs verfügbar und kann angewendet werden, falls erforderlich.

So importieren Sie das Systemprofil:


1. Bauen Sie die Eingabeparameter in Abhängigkeit davon auf, wo die Backup-Image-Datei gespeichert wird: auf der iDRAC vFlash-Karte oder auf der Netzwerkgreifgabe (CIFS oder NFS).
2. Rufen Sie die Methode **RestoreImage()** auf. Auf dem Bildschirm wird eine Aufgabenkennung ausgegeben (z. B. `JID_001291194119`).
3. Führen Sie zum Abrufen des Aufgabenstatus oder des prozentualen Aufgabenfortschritts den erforderlichen Befehl für die Aufgabenkennung aus.
Überprüfen Sie neben der Abfrage der Aufgabenkennung mithilfe verschiedener Skripting-Sprachen die iDRAC-Protokolle, um den Fortschritt der Aufgabe abzurufen. Wenn für den Aufgabenstatus **Abgeschlossen** angezeigt wird, überprüfen Sie die Lifecycle-Protokolle auf alle Backup-Einträge. Exportieren Sie zum Anzeigen des Protokolls das Protokoll mithilfe der Methode **ExportLCLog()** (Lifecycle-Protokoll exportieren) auf der `DCIM_LCService`-Klasse, oder zeigen Sie das Protokoll auf der Benutzeroberfläche für Lifecycle-Controller an.

 **ANMERKUNG:** Wenn der Import fehlschlägt, wird der Aufgabenstatus als fehlgeschlagen gekennzeichnet, außerdem wird eine Meldung angezeigt, warum dieser Fehler aufgetreten ist. Weitere Informationen zu den Fehlermeldungskennungen und den empfohlenen Maßnahmen finden Sie in der *Dell Lifecycle-Controller Remote Services-Liste mit Fehlermeldungen und Fehlerbehebungen* unter support.dell.com/manuals.

Szenario nach der Wiederherstellung

- Es werden die folgenden Aufgaben ausgeführt:
 - Das System schaltet sich aus, wenn es eingeschaltet ist. Wenn das Betriebssystem ausgeführt wird, wird versucht, das System ordnungsgemäß herunterzufahren. Schlägt dieser Versuch fehl, wird das Herunterfahren des Systems nach 15 Minuten erzwungen.
 - Das System stellt die gesamten Lifecycle-Controller-Inhalte wieder her.
 - Das System wird eingeschaltet und startet den Lifecycle-Controller, der Aufgaben zur Wiederherstellung der Firmware für unterstützte Geräte (BIOS, Speicher-Controller und Add-in-NIC-Karten) durchführt.
 - Das System wird neu gestartet und ruft den Lifecycle-Controller auf, die Aufgaben zur Firmware-Überprüfung, zur Wiederherstellung der Konfiguration für unterstützte Geräte (BIOS, Storage-Controller und Add-in-NIC-Karten) und zur abschließenden Überprüfung durchführen, ob alle Aufgaben ordnungsgemäß ausgeführt wurden.
 - Das System schaltet sich aus und führt die iDRAC-Konfiguration und Firmware-Wiederherstellung durch. Nach Abschluss setzt sich der iDRAC zurück und das System wird eingeschaltet.
 - Das System schaltet sich ein und der Wiederherstellungsvorgang wurde abgeschlossen. Überprüfen Sie die iDRAC die Lifecycle-Protokolle auf Einträge, die auf einen abgeschlossenen Wiederherstellungsprozess hinweisen.
- Überprüfen Sie nach dem Import die Lifecycle-Protokolle. Verwenden Sie dazu entweder die Lifecycle-Controller-Benutzeroberfläche, oder exportieren Sie die LC-Protokolle mithilfe der WS-Verwaltung auf eine Netzwerkreigabe. Die Protokolle enthalten Einträge für Konfigurations- und Firmware-Aktualisierungen des BIOS, der Speicher-Controller, der LOMs und der Add-in-NIC-Karten - falls unterstützt. Wenn es mehrere Einträge für jedes dieser Geräte gibt, ist die Anzahl der Einträge identisch mit der Häufigkeit, mit der die Remotedienste versucht haben, die Wiederherstellung umzusetzen.

System- bzw. Funktionsverhalten für Szenario nach der Wiederherstellung

- Während des Imports ist Lifecycle-Controller nicht verfügbar.
 - Während des Imports werden alle gesicherten Komponenten wiederhergestellt.
 - Der Import kann je nach Serverkonfiguration bis zu 60 Minuten dauern.
 - Während des Imports werden keine Diagnose- oder Treiberpaketinformationen wiederhergestellt.
 - Der Importprozess behält standardmäßig die aktuelle Konfiguration der virtuellen Festplatte bei.
-  **ANMERKUNG:** Wenn Sie die aktuelle Konfiguration des virtuellen Laufwerks löschen und die Konfiguration aus einer Backup-Image-Datei wiederherstellen möchten, verwenden Sie den Parameter `PreserveVDConfig` mit dem Wert `0`. In diesem Fall werden die Inhalte auf dem virtuellen Laufwerk während des Backups nicht wiederhergestellt (z. B. das Betriebssystem), sondern es wird nur ein leeres virtuelles Laufwerk erstellt, außerdem werden die Attribute festgelegt.
- Während der Ausführung der Aufgabe werden zusätzliche Neustarts durchgeführt, das das System versucht, die Konfiguration für ein Gerät festzulegen, das versucht, die Aufgabe erneut auszuführen. Überprüfen Sie die Protokolle auf Informationen zu fehlgeschlagenen Ereignissen.
 - Zum Aufrufen der Methode **RestoreImage()** muss der iDRAC-Benutzer über Execute Server Command (Ausführen von Serverbefehlen)-Berechtigungen verfügen.
 - Der Controller ermöglicht selbst dann die Erstellung von globalen Hotspares, wenn keine virtuellen Laufwerke vorhanden sind und entfernt diese, nachdem das System neu gestartet wurde. Wenn ein Hotspare ohne virtuelle Laufwerke erstellt wird, wird versucht, den Wiederherstellungsprozess auf dem SAS-Controller auszuführen. Wenn die Wiederherstellung nicht erfolgreich ausgeführt werden kann, wird eine Fehlermeldung ausgegeben.

- Nach dem Import des Serverprofils wird die derzeit installierte Firmware-Version zur Rollback-Version.
 Beispiel 1: Die derzeit installierte BIOS-Firmware-Version lautet 2.2, und Version 2.1 wurde während des Exports installiert. Nach dem Import ist Version 2.1 die installierte Version, und Version 2.1 ist die Rollback-Version.
 Beispiel 2: Die derzeit installierte BIOS-Firmware-Version lautet 2.1, und Version 2.1 wurde während des Exports installiert. Nach dem Import ist Version 2.1 die installierte Version, und Version 2.1 ist die Rollback-Version.

Referenzen zum Importieren des Server-Profiles

 **ANMERKUNG:** Die in dieser Tabelle referenzierten Abschnitte enthalten ausschließlich allgemeine Beispiele.

Tabelle 16. Schrittnummer und Speicherort

Schrittnummer	Speicherort der Speicherrichtlinie für Lifecycle-Controller-Webdienste (Windows oder Linux)
Schritt 1	18.2 – Serverprofil importieren
Schritt 2	18.2.1 – Serverprofil von iDRAC vFlash-Karte importieren - RestoreImage() 18.2.2 – Serverprofil von iNFS vFlash-Freigabe importieren - RestoreImage() 18.2.3 – Serverprofil von iNFS vFlash-Freigabe importieren - RestoreImage()
Schritt 3	18.2.4 – Importstatus überwachen
Profile	
Dell_LCManagement Profile	
MOFs	
DCIM_LCService.mof	

Verwalten der vFlash SD-Karte

vFlash-Dienst ist eine lizenzpflichtige Funktion. Die vFlash SD-Karte ist eine SD (Secure Digital)-Karte, die in den vFlash SD-Kartensteckplatz des verwalteten System eingesteckt wird. Sie können Karten mit maximal 16GB Kapazität verwenden. Nach Einlegen der Karte müssen Sie außerdem den vFlash-Dienst aktivieren, um Partitionen zu erstellen und zu verwalten.

Beziehen Sie sich für weitere Informationen zur **vFlash SD-Karte** auf das [Profil für beständigen Speicher](#).

Anzeige der Bestandsliste der vFlash SD-Karte

Führen Sie in der `DCIM_VFlashView`-Klasse den Auflistungsvorgang („Enumerate“) aus, um alle Eigenschaften der vFlash SD-Karte anzuzeigen, wie z.B.:

- Verfügbare Größe
- Kapazität
- Lizenziert
- Funktionszustand
- Zustand „Aktivieren oder Deaktivieren“
- Zustand „Initialisiert“
- Zustand „Schreibgeschützt“.

Anzeige der Partitionen auf der vFlash SD-Karte

Führen Sie den Auflistungsvorgang in der Klasse `DCIM_OpaqueManagementData` durch, um alle Partitionen und deren Eigenschaften anzuzeigen; z.B. Partitionskennung, Größe und Datenformat.

Erstellen und Modifizieren einer Partition auf einer vFlash SD Card

So erstellen und modifizieren Sie Partitionen auf einer vFlash SD-Karte:

1. Führen Sie den Auflistungsvorgang in der Klasse `DCIM_OpaqueManagementData` aus, um die Liste der derzeitigen Partitionen zu erhalten.
2. Erstellen Sie die Eingabeparameter, bevor Sie die Methode **CreatePartition()** oder **CreatePartitionUsingImage()** in der Klasse `DCIM_PersistentStorageService` aufrufen.
3. Rufen Sie die Methode **CreatePartitionUsingImage()** auf, um eine startfähige Imagedatei zu bilden. Dadurch wird aus dem auf Serverfreigaben wie NFS, CIFS und FTP gespeicherten Speicherabbild eine startfähige Partition erstellt. Rufen Sie alternativ dazu **CreatePartitionUsingImage()** auf, um eine startfähige Partition von einem ISO-Image aus zu erstellen.
Code 4096 wird rückgegeben, wenn eine Aufgabe erfolgreich erstellt wurde.
4. Fragen Sie den Status des Aufgabekennungsausgabewertes ab, indem Sie die Methoden des Aufgabensteuerungsprofils verwenden.
5. Wiederholen Sie Schritt 1, um die erfolgreiche Ausführung der Methode zu bestätigen.

6. Rufen Sie die Methode **ModifyPartition()** auf, um den Zugriffstyp der Partition auf „Read-Only“ (schreibgeschützt) oder „Read-Write“ (Lese-/Schreibzugriff) zu ändern.

iDRAC-Konfigurationen

Verwenden Sie die Funktion zum Konfigurieren von iDRAC-Attributen.

Abrufen und Festlegen der iDRAC-Attribute

Für eine erfolgreiche Ausführung von Remoteaufgaben auf dem Server müssen Sie sicherstellen, dass die folgenden Vorbedingungen, die im Abschnitt [Allgemeine Voraussetzungen vor der Verwendung der Remote-Services](#) zur Verfügung stehen, erfüllt sind:

So rufen Sie iDRAC-Attribute ab und legen dieselbe fest:



ANMERKUNG: Nach der Einrichtung der iDRAC-Konfiguration ist kein Neustart erforderlich.

1. Listen Sie die Klasse `DCIM_iDRACCardAttribute` auf, um alle Instanzen dieser Klasse zu identifizieren (also sämtliche Attribute für die iDRAC-Konfiguration).
2. Verwenden Sie zum Abrufen der erforderlichen Attribute die Eigenschaft „InstanceID“ sowie die Klassenbezeichnung, um die erforderliche Instanz abzurufen.
3. Rufen Sie die Methode **ApplyAttributes()** in der Klasse `DCIM_iDRACCardService` auf, um die Attribute mithilfe der FQDD-Eigenschaft, mithilfe von `AttributeName` und `AttributeValue` festzulegen.
Auf dem Bildschirm wird eine Aufgabenkennung ausgegeben (z. B. `JID_001291194119`).
4. Führen Sie zum Abrufen des Aufgabenstatus oder des prozentualen Aufgabenfortschritts den erforderlichen Befehl für die Aufgabenkennung aus.
5. Verwenden Sie zum Überprüfen der Änderungen die Eigenschaft „InstanceID“ des Attributs, rufen Sie so die Instanz ab, und überprüfen Sie den Attributwert, um zu gewährleisten, dass Sie diesen Wert festgelegt haben.

Referenzen zum Abrufen und Festlegen der iDRAC-Attribute



ANMERKUNG: Die in dieser Tabelle referenzierten Abschnitte enthalten ausschließlich allgemeine Beispiele.

Tabelle 17. Schrittnummer und Speicherort

Schrittnummer	Speicherort der Speicherrichtlinie für Lifecycle-Controller-Webdienste (Windows oder Linux)
Schritt 1	19.1 – Auflisten der iDRAC-Kartenbestandsklasse - Enumeration Class 19.1 – Auflisten der iDRAC-Kartenbestandsklasse - Integer Class 19.1 – Auflisten der iDRAC-Kartenbestandsklasse - String Class
Schritt 2	19.2 – Auflisten einer iDRAC-Karteninstanz - Enumeration
Schritt 3	19.4.1 – Ändern der iDRAC-Werte - ApplyAttributes() (sofort)
Schritt 4	19.4.2 – Abfragen des Aufgabefertigstellungsstatus
Schritt 5	19.4.3 – Definieren der Attributüberprüfung
Profile	
DCIM_iDRACCardProfile	

Schrittnummer	Speicherort der Speicherrichtlinie für Lifecycle-Controller-Webdienste (Windows oder Linux)
---------------	---

MOFs

- DCIM_iDRACCardEnumeration.mof
- DCIM_iDRACCardInteger.mof
- DCIM_iDRACCardService.mof
- DCIM_iDRACCardString.mof
- DCIM_iDRACCardView.mof

iDRAC-Attribute ()

Mithilfe der Remotedienste können Sie die in den folgenden Tabellen aufgeführten iDRAC-Attribute festlegen.

Tabelle 18. LAN-Attribute

Attribut	Beschreibung	Werte
VLAN aktiviert	Der VLAN-Betriebsmodus und die entsprechenden Parameter. Wenn VLAN aktiviert wird, wird nur übereinstimmender VLAN-ID-Datenverkehr akzeptiert. Wenn deaktiviert, sind VLAN-ID und VLAN-Priorität nicht verfügbar, und alle für diese Parameter vorhandenen Werte werden außer Acht gelassen.	Aktivieren oder Deaktivieren
VLAN ID	Legt den VLAN-ID-Wert fest. Die zulässigen Werte werden durch die IEEE 801.11g-Spezifikation vorgegeben.	1 bis 4094
VLAN-Priorität	Legt den VLAN-ID-Prioritätswert fest. Die zulässigen Werte werden durch die IEEE 801.11g-Spezifikation vorgegeben.	0 bis 7
Automatische Verhandlung	Wenn die Funktion der automatischen Verhandlung eingeschaltet ist, bestimmt sie, ob der iDRAC die Werte Duplexmodus und Netzwerkgeschwindigkeit durch Kommunikation mit dem nächstgelegenen Router oder Hub automatisch festlegt. Wenn die Funktion der automatischen Verhandlung ausgeschaltet ist, müssen die Werte Duplexmodus und Netzwerkgeschwindigkeit manuell eingestellt werden.	Ein oder Aus
LAN-Geschwindigkeit	Konfiguriert die Netzwerkgeschwindigkeit, um sich der Netzwerkumgebung des Benutzers anzupassen. Diese Option ist nicht verfügbar, wenn Automatische Verhandlung auf Ein eingestellt ist.	10 MB oder 100 MB
LAN Duplex	Konfiguriert den Duplexmodus, um sich der Netzwerkumgebung des Benutzers anzupassen. Diese Option ist nicht verfügbar, wenn Automatische Verhandlung auf Ein eingestellt ist.	Voll oder Halb

Tabelle 19. LAN-Benutzerkonfiguration

Attribut	Beschreibung	Wert
Auto-Ermittlung	Automatische Ermittlung der Server.	Aktivieren oder Deaktivieren
Adresse des Bereitstellungsservers	Geben Sie die Adresse des Bereitstellungsservers ein.	IPV4 oder IPV6 oder Hostname
Kontozugriff	Durch das Deaktivieren des Kontozugriffs werden alle anderen Felder auf dem Bildschirm LAN-Benutzerkonfiguration deaktiviert.	Aktivieren oder Deaktivieren
Kontobenzutzername	Aktiviert die Änderung eines iDRAC-Benutzernamens.	Höchstens 16 druckbare ASCII-Zeichen
Kennwort	Ermöglicht dem Administrator das Festlegen oder die Bearbeitung des (verschlüsselten) Kennworts des iDRAC-Benutzers.	Maximal 20 Zeichen
Kennwort bestätigen	Geben Sie zur Bestätigung das iDRAC-Kennwort des Benutzers erneut ein.	Maximal 20 Zeichen
Kontoberechtigung	Weist der Benutzergruppe die maximalen Benutzerberechtigungen für den IPMI LAN-Kanal zu.	Admin, Operator, Benutzer, oder Kein Zugriff
Smart Card-Authentifizierung	Smart-Card-Authentifizierung für die iDRAC-Anmeldung. Wenn aktiviert, muss für den Zugriff auf den iDRAC eine Smart Card installiert sein.	Aktivieren, deaktivieren oder mit RACADM aktivieren

Tabelle 20. Verbindungsmodus für virtuelle Laufwerksgeräte

Modus	Beschreibung
Verbunden	Die virtuellen Laufwerksgeräte stehen in der aktuellen Betriebssystemumgebung zur Verfügung. Das virtuelle Laufwerk macht ein Floppy-Image, Floppy-Laufwerk oder CD/DVD-Laufwerk Ihres Systems auf der Konsole des verwalteten Systems verfügbar, als wäre das Floppy-Image oder -Laufwerk auf dem lokalen System vorhanden (angeschlossen oder verbunden).
Nicht angeschlossen	Die virtuellen Datenträgergeräte stehen nicht zur Verfügung.
Automatisch Verbunden	Die virtuellen Datenträgergeräte werden automatisch jedesmal dem Server zugeordnet, wenn der Benutzer einen Datenträger physisch anschließt.

Tabelle 21. IPv4-Konfiguration

Attribut	Beschreibung	Werte
IPv4	iDRAC NIC IPv4-Protokollunterstützung. Durch das Deaktivieren von IPv4 werden die Steuerelemente deaktiviert.	Aktivieren oder Deaktivieren
Verschlüsselungsschlüssel RMCP+	Konfigurierung des RMCP+-Verschlüsselungsschlüssels (keine Leerschritte zulässig). Die Standardeinstellung besteht ausschließlich aus Nullen (0).	0 bis 40 Hexadezimalzahlen
IP-Adressen-Quelle	Die Fähigkeit des iDRAC-NIC, eine IPv4-Adresse vom DHCP-Server zu erhalten.	Aktivieren oder Deaktivieren

Attribut	Beschreibung	Werte
	Wenn Sie IP-Adressen-Quelle deaktivieren, werden auch Ethernet-IP-Adresse und andere benutzerkonfigurierte Steuerungen deaktiviert.	
DNS-Server von DHCP abrufen	iDRAC ruft die DNS vom Server für das DHCP (Dynamic Host Configuration Protocol [Dynamisches Host-Konfigurationsprotokoll]) ab.	Ja oder Nein
DNS Server 1 (Primärer DNS-Server)	iDRAC ruft die IP-Adresse für DNS Server 1 vom Server für das DHCP (Dynamic Host Configuration Protocol [Dynamisches Host-Konfigurationsprotokoll]) ab.	Der Maximalwert lautet 255.255.255.255.
DNS Server 2 (Sekundärer DNS-Server)	iDRAC ruft die IP-Adresse für DNS Server 2 vom Server für das DHCP (Dynamic Host Configuration Protocol [Dynamisches Host-Konfigurationsprotokoll]) ab.	Der Maximalwert lautet 255.255.255.255.

Tabelle 22. IP-Konfigurationsattribute

Attribut	Beschreibung	Werte
iDRAC-Name registrieren	Erfassen Sie den iDRAC-Namen im DNS (Domain Name System [Domänennamensystem]).	Ja oder Nein
iDRAC-Name	Ermöglicht das Anzeigen und Bearbeiten des iDRAC-Namens, der für die Erfassung des DNS verwendet wird. Die Zeichenkette des Namens kann bis zu 63 druckbare ASCII-Zeichen enthalten. Sie können die Zeichenkette des Namens bearbeiten, wenn die Einstellung für iDRAC-Namen registrieren Nein lautet.	Aktivieren oder Deaktivieren
Domänenname von DHCP	iDRAC ruft den Domänennamen vom DHCP-Server ab. Wenn die Einstellung Nein lautet, muss der Domänenname manuell eingegeben werden.	Ja oder Nein
Domänenname	Ermöglicht das Anzeigen oder Bearbeiten des iDRAC-Domänennamens, der verwendet wird, wenn er nicht vom DHCP abgerufen wird. Sie können einen Domänennamen festlegen, wenn Domänenname von DHCP auf Nein eingestellt ist.	Aktivieren oder Deaktivieren
Zeichenkette des Host-Namens	Ermöglicht die Definition oder Bearbeitung des Hostnamens, der mit iDRAC verknüpft ist. Die Zeichenkette des Host-Namens kann bis zu 62 druckbare ASCII-Zeichen enthalten.	Aktivieren oder Deaktivieren

Abrufen und Festlegen von iDRAC-Benutzern und -Rollen

Für eine erfolgreiche Ausführung von Remoteaufgaben auf dem Server müssen Sie sicherstellen, dass die folgenden Vorbedingungen erfüllt sind:

- [Allgemeine Voraussetzungen vor der Verwendung der Remote-Services](#)
- [Abrufen und Festlegen der iDRAC-Attribute](#)

Legen Sie die Benutzernamen und Kennwörter für iDRAC fest, und weisen Sie den Benutzern Rollen zu.

So rufen Sie iDRAC-Benutzer und Rollen ab und legen diese fest:

1. Listen Sie `DCIM_iDRACCardAttribute` auf und identifizieren Sie ein Attribut, das Sie ändern wollen.
2. Rufen Sie die Eigenschaften der folgenden Attribute ab:
 - FQDD (zum Beispiel: iDRAC.Embedded.1)
 - GroupID (zum Beispiel: Users.3)
 - AttributeName (zum Beispiel: UserName, Privilege, IpmiSerialPrivilege or IpmiLanPrivilege)
3. Rufen Sie die Methode **ApplyAttributes()** in der Klasse `DCIM_iDRACCardService` auf, um die Attribute mithilfe der FQDD-Eigenschaft, mithilfe von AttributeName und AttributeValue festzulegen.
 - Target — Wert der FQDD-Eigenschaft
 - AttributeName[] — Werte der GroupID-Eigenschaft und AttributeName-Eigenschaft - GroupID#AttributeName (z.B. Users.3#UserName or Users.3#Password)
 - AttributeValue[] — Für die Attribute festzulegende Werte

Auf dem Bildschirm wird eine Aufgabenkennung ausgegeben (z. B. JID_001291194119).

4. Überprüfen Sie den neuen Wert des Administratorbenutzernamens („CurrentValue“ wird in den neuen Wert geändert.)

Referenzen zum Abrufen und Festlegen von iDRAC-Benutzern und -Rollen

 **ANMERKUNG:** Die in dieser Tabelle referenzierten Abschnitte enthalten ausschließlich allgemeine Beispiele.

Tabelle 23. Schrittnummer und Speicherort

Schrittnummer	Speicherort der Speicherrichtlinie für Lifecycle-Controller-Webdienste (Windows oder Linux)
Schritt 2.	5.2.1 Konto und Funktionen (unter Verwendung von iDRAC-Attributen)
Schritt 3.	5.3.1 Ändern des Benutzernamens (unter Verwendung von iDRAC-Attributen)
Schritt 4.	5.2.1 Konto und Funktionen (unter Verwendung von iDRAC-Attributen)

Profile

DCIM_iDRACCardProfile

MOFs

- DCIM_iDRACCardEnumeration.mof
- DCIM_iDRACCardInteger.mof
- DCIM_iDRACCardService.mof
- DCIM_iDRACCardString.mof
- DCIM_iDRACCardView.mof

Weiterleiten von Änderungen an der iDRAC-IP-Adresse

Für eine erfolgreiche Ausführung von Remoteaufgaben auf dem Server müssen Sie sicherstellen, dass die folgenden Vorbedingungen, die im Abschnitt [Allgemeine Voraussetzungen vor der Verwendung der Remote-Services](#) zur Verfügung stehen, erfüllt sind:

Ermöglicht das Weiterleiten von Änderungen an der IP-Adresse von iDRAC an SCCM. Es wird eine SOAP-Meldung (Simple Object Access Protocol-Meldung) gesendet, um auf die Änderung der iDRAC-IP-Adresse hinzuweisen. Über diese Funktion werden die Bereitstellungsserver darüber informiert, dass sich die iDRAC-IP-Adresse für das mit der Service-Tag-Nummer verknüpfte System geändert hat.

Um eine Änderung an der iDRAC IP-Adresse zu melden, definieren Sie mithilfe des Administratorkontos das Attribut „IPChangeNotification“. Legen Sie optional die Adresse des Bereitstellungsservers fest.

Es werden die folgenden Schritte ausgeführt, wenn sich die IP-Adresse des iDRAC aufgrund eines manuellen Eingriffs oder des Ablaufs der DHCP-Lizenz ändert, benachrichtigt iDRAC die Bereitstellungsserver über die Service-Tag-Nummer des Servers und über die iDRAC-IP-Adresse. Der Bereitstellungsserver ermittelt dann anhand der Service-Tag-Nummer den alten Eintrag des Servers und führt eine Aktualisierung durch.

Wenn sich die iDRAC-IP-Adresse ändert und keine Benachrichtigung eingeht, verliert der Bereitstellungsserver die Kontrolle über den Server.

Funktion oder Systemverhalten zum Weiterleiten von Änderungen an der iDRAC-IP-Adresse

- Wenn das iDRAC-Attribut für den Bereitstellungsserver definiert wurde, wird der Attributwert verwendet, ansonsten wird der Bereitstellungsserver mithilfe einer der folgenden Optionen bestimmt: DHCP-Anbieter, DNS SRV-Datensatz oder standardmäßiger Hostname des Bereitstellungsservers.
- Diese Funktion ist standardmäßig deaktiviert.
- Über diese Funktion werden die Bereitstellungsserver darüber informiert, dass eine Änderung an der IP-Adresse auch dann vorgenommen wurde, wenn Auto-Ermittlung deaktiviert ist.
- Der Bereitstellungsserver muss die Benachrichtigung zu Änderungen an der IP-Adresse anfragen.
- Unterstützt die Benachrichtigung mehrerer Bereitstellungsserver.

Referenzen zum Weiterleiten von Änderungen an der iDRAC-IP-Adresse

 **ANMERKUNG:** Die in dieser Tabelle referenzierten Abschnitte enthalten ausschließlich allgemeine Beispiele.

Tabelle 24. Schrittnummer und Speicherort

Schrittnummer	Speicherort der Speicherrichtlinie für Lifecycle-Controller-Webdienste (Windows oder Linux)
-	19.9.1 – Abrufen des aktuellen Status der iDRAC-IP-Adressänderung 19.9.2 – Festlegen der Benachrichtigung über die iDRAC-IP-Adressänderung - SetAttribute()

Profile

DCIM_iDRACCardProfile

MOFs

- DCIM_iDRACCardEnumeration.mof
- DCIM_iDRACCardInteger.mof

Schrittnummer	Speicherort der Speicherrichtlinie für Lifecycle-Controller-Webdienste (Windows oder Linux)
<ul style="list-style-type: none">• DCIM_iDRACCardService.mof• DCIM_iDRACCardString.mof• DCIM_iDRACCardView.mof	

Verwaltung der BIOS- und Startkonfiguration


Verwenden Sie zum Konfigurieren der BIOS-Eigenschaften und zum Durchführen von Vorgängen wie z.B. dem Ändern der Startquelle und der Startreihenfolge die Funktion für die BIOS- und Startkonfiguration. Weitere Informationen finden Sie im [Profil „BIOS- und Startverwaltung“](#).

Anzeigen der Bestandsliste der BIOS-Attribute

Führen Sie den Auflistungsvorgang in einer der Klassen `DCIM_BIOSInteger`, `DCIM_BIOSEnumeration`, `DCIM_BIOSPassword` und `DCIM_BIOSString` durch, um alle verfügbaren Instanzen der BIOS-Attribute eines Systems anzuzeigen.

Einstellen der BIOS-Attribute


Einstellen der Attribute:

1. Identifizieren Sie das Zielattribut über `AttributeName`.
 2. Versichern Sie sich, dass das Feld `IsReadOnly` auf „Falsch“ eingestellt ist.
 3. Notieren Sie sich die vor dem Aufruf der **`SetAttribute()`** bzw. **`SetAttributes()`**-Methode die Instanzinformationen, die Sie in Schritt 1 erhalten haben und bereiten Sie die Eingabeparameter vor.
 4. Rufen Sie die **`SetAttribute()`** bzw. **`SetAttributes()`**-Methode auf.
 5. Überprüfen der Ausgabeparameter.
 6. Bereiten Sie vor dem Aufruf der Methode **`CreateTargetedConfigJob()`** Eingabeparameter vor (z.B. `RebootJobType`, `ScheduledStartTime`, `UntilTime`, `Job`, usw.) und verwenden Sie den richtigen BIOS FQDD.
 7. Rufen Sie die Methode **`CreateTargetedConfigJob()`** auf.
-  **ANMERKUNG:** Das System muss neu gestartet werden, um die Aufgabe des Einstellens des Attributs bzw. der Attribute ausführen zu können.
8. Fragen Sie den Status des Aufgabekennungsausgabewertes ab, indem Sie die Methoden des Auftragssteuerungsprofils verwenden.
 9. Wiederholen Sie den Abschnitt in Schritt, um die erfolgreiche Ausführung der Methode zu bestätigen.

Einmalige Startsequenz

Verwenden Sie die Startverwaltungsmethoden, um den einmaligen Start von einem BIOS-Startgerät aus durchzuführen. Wenn Sie versuchen, die einmalige Startsequenz von einer vFlash-Partition aus durchzuführen, die nicht eingebunden ist, binden die Remotedienste diese automatisch ein und geben eine Aufgabekennung zurück. Sie können die Aufgabe unter Verwendung dieser Kennung abfragen.

Einstellen der einmaligen Startsequenz:

1. Führen Sie den Auflistungsvorgang in der Klasse `DCIM_BootConfigSetting` durch, und identifizieren Sie das Feld `ElementName`, das die „BootSeq“ (Startsequenz) und die zugehörige „InstanceID“ enthält.
 2. Führen Sie den Auflistungsvorgang in der Klasse `DCIM_BootSourceSetting` durch und machen Sie die Instanzkennung der Startquelle ausfindig. Das Attribut „CurrentEnabledStatus“ jeder Instanz kennzeichnet, ob diese aktiviert oder deaktiviert ist.
 3. Notieren Sie sich die vor dem Aufruf der **ChangeBootOrderByInstanceID()** die Instanzinformationen, die Sie im Schritt 1 und Schritt 2 erhalten haben und bereiten Sie die Eingabeparameter vor.
 4. Rufen Sie die Methode **ChangeBootOrderByInstanceID()** auf.
 5. Überprüfen der Ausgabeparameter.
 6. Bereiten Sie vor dem Aufruf der Methode **CreateTargetedConfigJob()** Eingabeparameter vor (z.B. `RebootJobType`, `ScheduledStartTime`, `UntilTime`, `Job`, usw.) und verwenden Sie den richtigen BIOS FQDD.
 7. Rufen Sie die Methode **CreateTargetedConfigJob()** auf.
-  **ANMERKUNG:** Das System muss neu gestartet werden, um die Aufgabe des Einstellens des Attributs bzw. der Attribute ausführen zu können.
8. Fragen Sie den Status des Aufgabenkennungsabgabewertes ab, indem Sie die Methoden des Auftragssteuerungsprofils verwenden.
 9. Wiederholen Sie Schritt 2, um die erfolgreiche Ausführung der Methode zu bestätigen.

Festlegen, Ändern und Löschen des BIOS-Kennworts



Für eine erfolgreiche Ausführung von Remoteaufgaben auf dem Server müssen Sie sicherstellen, dass die folgenden Vorbedingungen erfüllt sind:

- [Allgemeine Voraussetzungen vor der Verwendung der Remote-Services](#)
- Administratorberechtigungen für iDRAC
- Aktuelles BIOS-Kennwort ist lokal vorhanden
- Status des Kennwortes muss „gesperrt“ (locked) sein.

So legen Sie das BIOS-Kennwort fest, ändern und löschen es:

1. Listen Sie die Klasse `DCIM_BIOSPassword` auf, um den Kennwortstatus zu überprüfen. Mögliche Werte des Kennwortstatus sind:
 - 0–Status nicht verfügbar
 - 2–Kein Kennwort festgelegt
 - 3–Kennwort wurde NICHT festgelegt
 - 4–Kennwort wurde unter Verwendung eines Jumpers deaktiviert
2. Rufen Sie die Methode **ChangePassword()** in der Klasse `DCIM_BIOSService` mit den entsprechenden Parametern für die folgenden Aktivitäten auf:
 - Festlegen des Kennworts
 - Ändern des Kennworts
 - Löschen des Kennworts

Zum Ändern des Kennworts müssen Sie das korrekte alte Kennwort gemeinsam mit dem neuen Kennwort verwenden. Wenn Sie ein falsches Kennwort verwenden, werden die Aufgaben zum Festlegen und Erstellen einer Zielaufgabe zwar weiterhin ausgeführt, die Aufgabe schlägt jedoch fehl, und das Kennwort kann nicht geändert oder gelöscht werden.

-  **ANMERKUNG:** Zum Ändern oder Löschen des Setup-Kennworts muss das alte Setup-Kennwort verwendet werden. Zum Ändern oder Löschen des Systemkennworts können aber sowohl das alte Systemkennwort wie auch das Setup-Kennwort verwendet werden.
3. Bereiten Sie vor dem Aufruf der Methode **CreateTargetedConfigJob()** Eingabeparameter vor (z.B. RebootJobType, ScheduledStartTime, UntilTime, Job, usw.) und verwenden Sie den richtigen BIOS FQDD.
-  **ANMERKUNG:** Das System muss neu gestartet werden, um die Aufgabe des Einstellens des Attributs bzw. der Attribute ausführen zu können.
4. Rufen Sie die Methode **CreateTargetedConfigJob()** auf.
 5. Führen Sie zum Abrufen des Aufgabenstatus oder des prozentualen Aufgabenfortschritts den erforderlichen Befehl für die Aufgabenkennung aus.
 6. Überprüfen Sie, ob sich das BIOS-Kennwort lokal auf dem System befindet.

Referenzen zum Festlegen, Ändern und Löschen des BIOS-Kennworts

 **ANMERKUNG:** Die in dieser Tabelle referenzierten Abschnitte enthalten ausschließlich allgemeine Beispiele.

Tabelle 25. Schrittnummer und Speicherort

Schrittnummer	Speicherort der Speicherrichtlinie für Lifecycle-Controller-Webdienste (Windows oder Linux)
Schritt 1.	17.10 Auflisten der Aufzählungsklasse für den CNA-Bestand
Schritt 3 und Schritt 4	17.9.2 – Erstellen der Konfigurationsaufgabe auf dem Ziel
Schritt 5.	17.9.3 – Überwachen des Status für das festgelegte BIOS-Kennwort
Profile	
Dell_BIOSandBootManagement Profile	
MOFs	
DCIM_BIOSService.mof	

Andere Anwendungsfall-Szenarios

Dieser Abschnitt enthält einige unterschiedliche Anwendungsfälle.

Abrufen des Remotedienststatus

Für eine erfolgreiche Ausführung von Remoteaufgaben auf dem Server müssen Sie sicherstellen, dass die folgenden Vorbedingungen, die im Abschnitt [Allgemeine Voraussetzungen vor der Verwendung der Remote-Services](#) zur Verfügung stehen, erfüllt sind:

Bevor Sie Remotedienst-Aktivitäten ausführen (z. B. NICs verwalten, RAID-Konfigurationen oder Bestand verwalten usw.), müssen Sie sicherstellen, dass die Remotedienste ausgeführt werden, auf dem aktuellen Stand sind und Daten senden können. Verwenden Sie die Funktion „Status für Remotedienste abrufen“, um die folgenden Aktivitäten auszuführen:

- Aktuellen Status der Remotedienste abrufen, z. B. `Bereit`, `Nicht bereit` oder `Wird neu geladen`.
- Abrufaktivität fortsetzen, um zu bestimmen, ob die Remotedienste in den Status „Bereit“ übergehen.

So rufen Sie den Remotedienststatus ab:

1. Rufen Sie die Methode **GetRSStatus()** auf.
Daraufhin werden ein Status sowie `Meldung`, `MessageID` und `ReturnValue` ausgegeben.
2. Setzen Sie die Ausführung dieser Methode so lange fort, bis der Status `Bereit` ausgegeben wird.
Der Status `Bereit` zeigt an, dass Lifecycle-Controller bereit ist, Aktivitäten auszuführen.

Referenzen zum Abrufen des Remotedienststatus

 **ANMERKUNG:** Die in dieser Tabelle referenzierten Abschnitte enthalten ausschließlich allgemeine Beispiele.

Tabelle 26. Schrittnummer und Speicherort

Schrittnummer	Speicherort der Speicherrichtlinie für Lifecycle Controller-Webdienste (Windows oder Linux)
Schritt 1.	20.1 – Abrufen des Status für den Remotedienst
Profile	
DCIM-LCManagementProfile	
MOFs	
DCIM_LCService.mof	

Remote Services-Profile

Dieser Abschnitt enthält allgemeine Informationen zu den einzelnen Profilen und ihren Klassen und Methoden.

Lesen Sie für weitere Informationen zu den Profilen und den zugehörigen MOFs unter delltechcenter.com/page/DCIM.Library nach.

Lesen Sie für Beispiele zu den WinRM- und WS-Management Befehlszeilenaufrufe den Abschnitt:

- delltechcenter.com/page/Lifecycle+Controller
- *Lifecycle-Controller-Webdienste – Schnittstellenrichtlinie - Windows und Linux*

Profil „Betriebssystembereitstellung“

Die folgende Tabelle führt die Klassen, Funktionen, Vorgänge und Methoden des Profils „Betriebssystembereitstellung“ auf.

Tabelle 27. . Profil „Betriebssystembereitstellung“

Klassenname	Vorgänge	Methoden
DCIM_OSDeploymentService	„Aufzählung erhalten“ aufrufen	Siehe Betriebssystembereitstellung - Methoden
DCIM OSDConcreteJob	Aufzählung erhalten	–

Betriebssystembereitstellung - Methoden

- Die Methode **GetDriverPackInfo()** (Informationen zum Treiberpaket abrufen) gibt eine Liste mit Betriebssystemen zurück, die Sie auf dem Server installieren können, indem Sie die im Dell Lifecycle Controller vorhandenen integrierten Gerätetreiber verwenden.
- Die Methode **UnpackAndAttach()** extrahiert die Treiber für das ausgewählte Betriebssystem auf ein für die angegebene Zeitspanne lokal an den Server angebundenes USB-Gerät.
- Die Methode **DetachDrivers()** trennt das die Treiber enthaltende USB-Gerät vom Host-Server.
- Die Methode **UnpackAndShare()** extrahiert die Treiber für das gewählte Betriebssystem und kopiert sie auf die angegebene Netzwerkebene.
- Die Methode **BootToNetworkISO()** wird zum Starten des Systems mittels eines auf einer CIFS- oder NFS-Netzwerkebene liegenden ISO-Speicherabbildes verwendet.
- Die Methode **DetachISOImage()** trennt das ISO-Speicherabbild vom Host-Server.
- Die Methode **BootToPXE()** wird zum Starten des Servers unter Verwendung des PXE (Preboot Execution Environment)-Mechanismus verwendet.
- Die Methode **DownloadISOTOVFlash()** wird zum Herunterladen des (pre-OS) ISO-Speicherabbildes auf die vFlash SD-Karte verwendet.
- Die Methode **BootToISOFromVFlash()** wird zum Starten des bereits heruntergeladenen vFlash- (pre-OS) Speicherabbildes verwendet.
- Die Methode **DetachISOFromVFlash()** trennt das ISO-Speicherabbild vom Host-Server.
- Die Methode **DeleteISOFromVFlash()** löscht das ISO-Speicherabbild von der vFlash SD-Karte.

Profil „Lifecycle-Controller-Management“

Die folgende Tabelle führt die Klassen, Funktionen, Vorgänge und Methoden des Profils „Lifecycle-Controller-Management“ auf.

Tabelle 28. Profil „Lifecycle-Controller-Management“

Klassenname	Vorgänge	Methoden
DCIM_LCService	„Aufzählung erhalten“ aufrufen	SetAttribute() SetAttributes() GetRemoteServicesAPIStatus() Siehe auch Auto-Ermittlung – Methoden , Lifecycle-Protokoll – Methoden und Hardware-Bestandsliste – Methoden .
DCIM_LCString	Aufzählung erhalten	–
DCIM_LCEnumeration	Aufzählung erhalten	–

LC Service-Methoden

Die folgenden Methoden werden verwendet, um Attribute zu definieren, die mit der Auto-Erkennung, der Teilersetzung und der E/A-Identität in Verbindung stehen.

- Die Methode **SetAttribute()** wird zum Festlegen des Wertes eines einzelnen Attributs verwendet.
- Die Methode **SetAttributes()** wird zum Festlegen des Wertes mehrerer Attribute verwendet.
- Die Methode **CreateConfigJob()** wird zum Übernehmen der durch die Methoden **SetAttribute()** und **SetAttributes()** festgelegten, noch ausstehenden Werte verwendet.
- Die Methode **GetRemoteServicesAPIStatus()** wird verwendet um zu erfahren, ob Lifecycle Controller-Remotedienste bereit für die Annahme von Webdienstanfragen sind.

Methoden zur automatischen Erkennung

- Die Methode **ReInitiateDHS()** wird zur erneuten Initialisierung der Bereitstellungsserver-Erkennung und Handshakes verwendet.
- Die Methode **ClearProvisioningServer()** wird zum Löschen der Bereitstellungsserverwerte verwendet.
- Die Methode **DownloadServerPublicKey()** wird zum Herunterladen des öffentlichen Server-Schlüssels auf den Lifecycle Controller (LC) verwendet.
- Die Methode **DownloadClientCerts()** wird zum Herunterladen des privaten Client-Zertifikates, Kennworts und Root-Zertifikates auf den LC verwendet.
- Die Methode **DeleteAutoDiscoveryClientCerts()** wird zum Löschen der zuvor heruntergeladenen Client-Zertifikate für die automatische Ermittlung und der privaten Schlüssel verwendet.
- Die Methode **SetCertificateAndPrivateKey()** wird unter Verwendung des Inhalts einer PKCS#12 Datei zum Aktualisieren des iDRAC-Zertifikates und der privaten Schlüsselpaare verwendet.
- Die Methode **SetPublicCertificate()** wird zum Aktualisieren eines öffentlichen SSL-Zertifikates auf dem iDRAC verwendet.
- Die Methode **DeleteAutoDiscoveryServerPublicKey()** wird zum Löschen der zuvor heruntergeladenen öffentlichen Serverschlüssel für die automatische Ermittlung verwendet.

Export- und Importmethoden

- Die Methode **BackupImage()** führt Sicherungen oder Exporte der Firmware, des Firmware-Bestands und der Konfiguration der Serverkomponenten auf der vFlash SD-Karte oder Netzwerkfreigabe durch.
- Die Methode **RestoreImage()** importiert die Serverprofile und setzt den Server auf eine frühere Konfiguration zurück.
- Die Methode **GetRSStatus()** wird verwendet, um den Status der Remotedienste abzurufen.
- Die Methode **GetRemoteServicesAPIStatus()** ruft den Status des Host-Servers ab, den Lifecycle-Controller-Status und den Gesamtstatus bezüglich der Durchführbarkeit der Bereitstellungsaufgaben zu gegebenem Zeitpunkt.

Lifecycle Protokollierungsmethoden

- Die Methode **LCWipe()** wird zum Löschen sämtlicher Konfigurationen auf dem Lifecycle-Controller verwendet, bevor das System außer Dienst gestellt wird.
- Die Methode **ExportLCLog()** wird zum Exportieren des Protokolls des Lifecycle-Controllers in eine auf einer Remotefreigabe liegende Datei verwendet.
- Die Methode **InsertCommentInLCLog()** wird zum Hinzufügen zusätzlicher Benutzerkommentare in das Lifecycle-Controller-Protokoll verwendet.

Methode für die Hardware-Bestandsliste

- Die Methode **ExportHWInventory()** wird zum Exportieren der Hardware-Bestandsliste des Lifecycle-Controllers in eine auf einer Remotefreigabe liegende Datei verwendet.
- Die Methode **ExportFactoryConfiguration()** wird zum Exportieren der Hardware-Bestandsliste des Lifecycle-Controllers in eine auf einer Remotefreigabe liegende Datei verwendet.

Profil „Einfaches NIC“

Die folgende Tabelle führt die Klassen, Funktionen, Vorgänge und Methoden des einfachen NIC-Profiles auf.

Tabelle 29. . Einfaches NIC-Profil

Klassenname	Funktionen	Vorgänge	Methoden
DCIM_NICService	Dies ist die zentrale Klasse. Sie wird aufgerufen, um die NIC-, FCOE- und iSCSI-Attribute abzurufen.	„Aufzählung erhalten“ aufrufen	Siehe Simple NIC – Methoden
DCIM_NICView	Verwenden Sie diese Klasse zum Anzeigen der Instanz-IDs und anderer Eigenschaften der im System vorhandenen LOMs und Add-in-NICs und -CNAs.	Aufzählung erhalten	–
DCIM_NICAttribute — Diese Klasse zeigt den Ausgangswert für die folgenden BIOS-Subklassen an:			
• DCIM_NICEnumeration	Verwenden Sie diese Subklasse, um die Eigenschaften von NIC-	Aufzählung erhalten	SetAttribute() SetAttributes()

Klassenname	Funktionen	Vorgänge	Methoden
	Enumerationsinstanzen anzuzeigen.		
• DCIM_NICInteger	Verwenden Sie diese Subklasse, um die Eigenschaften von NIC-Integerinstanzen anzuzeigen.	Aufzählung erhalten	SetAttribute() SetAttributes()
• DCIM_NICString	Verwenden Sie diese Subklasse, um die Eigenschaften von NIC-Zeichenketteninstanzen anzuzeigen.	Aufzählung erhalten	SetAttribute() SetAttributes()

„Einfaches NIC“ - Methoden

Diese Methoden werden verwendet, um NIC-, FCOE- und iSCSI-Attribute auf das LAN auf Hauptplatinen, Add-in-NICs und -CNAs im System anzuwenden. Jede Methode hat ihren eigenen Satz an Eingangs- und Ausgangsparametern. Die Methoden haben spezifische Rückgabecodewerte. In der NIC-Serviceklasse sind vier unterschiedliche Methoden enthalten:

- Die Methode **SetAttribute()** wird zum Festlegen oder Ändern des Wertes eines Attributs verwendet.
- Die Methode **SetAttributes()** wird zum Festlegen der Werte einer Gruppe von Attributen verwendet.
- Die Methode **CreateTargetedConfigJob()** wird zum Übernehmen der durch die Methoden SetAttribute() und SetAttributes() erstellten, noch ausstehenden Werte verwendet. Die erfolgreiche Ausführung dieser Methode erstellt eine Aufgabe zum Übernehmen ausstehender Attributwerte.



ANMERKUNG: Nachfolgende Aufrufe der Methode **CreateTargetedConfigJob()** nach der ersten **CreateTargetedConfigJob()** Methode ergeben einen Fehler, bis die erste Aufgabe vollständig abgeschlossen wurde. Wenn Sie die Methode **CreateTargetedConfigJob()** mehrmals aufrufen, werden ältere Anfragen überschrieben bzw. gehen verloren.

- Die Methode **DeletePendingConfiguration()** bricht die ausstehenden Änderungen der Konfiguration (erstellt unter Verwendung der Methoden „SetAttribute“ und „SetAttributes“) ab, bevor die Konfigurationsaufgabe mittels **CreateTargetedConfigJob()** erstellt wird.

Profil „BIOS- und Startverwaltung“

Die folgende Tabelle führt die Klassen, Funktionen, Vorgänge und Methoden des Profils „BIOS- und Startverwaltung“ auf.

Tabelle 30. . Profil „BIOS- und Startverwaltung“

Klassenname	Funktionen	Vorgänge	Methoden
BIOS Management			
DCIM_BIOSService	Verwenden Sie diese zentrale Klasse zum Modifizieren der BIOS-Attribute.	„Aufzählung erhalten“ aufrufen	Siehe BIOS- und Startverwaltung-Methoden
DCIM_BIOSEnumeration	Verwenden Sie diese Subklasse, um die Eigenschaften von BIOS-	Aufzählung erhalten	SetAttribute() SetAttributes()

Klassenname	Funktionen	Vorgänge	Methoden
	Enumerationsinstanzen anzeigen.		
DCIM_BIOSInteger	Verwenden Sie diese Subklasse, um die Eigenschaften von BIOS-Zeichenketteninstanzen anzeigen.	Aufzählung erhalten	SetAttribute() SetAttributes()
DCIM_BIOSString	Verwenden Sie diese Subklasse, um die Eigenschaften von BIOS-Integerinstanzen anzeigen.	Aufzählung erhalten	SetAttribute() SetAttributes()
DCIM_BIOSPassword	Verwenden Sie diese Subklasse, um die BIOS-Kennworte zu verwalten.	Aufzählung erhalten	ChangePassword()
DCIM_BootConfigSetting	Diese Klasse hat die folgenden Startlisteninstanzen: <ul style="list-style-type: none"> • IPL • BCV • UEFI • vFlash • OneTime 	„Aufzählung erhalten“ aufrufen	ChangeBootSourceState() ChangeBootOrderByInstanceID()


Boot Management

DCIM_BootSourceSetting	Verwenden Sie diese Klasse, um die Startquelle und die Startreihenfolge der zugehörigen Geräte zu ändern.	Aufzählung erhalten	–
------------------------	---	---------------------	---

BIOS- und Startverwaltung - Methoden

Die BIOS and Boot Management-Methoden werden zum Übernehmen von Attributen und zum Ändern der im System enthaltenen Startkonfigurationen verwendet. Jede Methode hat ihren eigenen Satz an Eingangs- und Ausgangsparametern. Die Methoden haben spezifische Rückgabecodewerte. Die folgenden Methoden werden in der BIOS- und Startverwaltung verwendet:

- Die Methode **SetAttribute()** wird zum Festlegen oder Ändern des Wertes eines BIOS-Attributs verwendet.
- Die Methode **SetAttributes()** wird zum Festlegen oder Ändern der Werte einer Gruppe von Attributen verwendet.
- Die Methode **ChangeBootSourceState()** wird zum Ändern des „EnabledState“ einer Startquelle von „deaktiviert“ auf „aktiviert“ oder „aktiviert“ auf „deaktiviert“ verwendet.
- Die Methode **ChangeBootOrderByInstanceID()** wird zum Ändern der Startreihenfolge der Startquellen aus den Startlisteninstanzen (IPL, BCV, UEFI) verwendet. Diese Methode erwartet Startquelleninstanzen aus nur einer Liste. Rufen Sie diese Methode deshalb bei Instanzen aus unterschiedlichen Startlisten mehrmals auf, um die Startreihenfolge von mehreren Instanzen zu ändern.
- Die Methode **CreateTargetedConfigJob()** wird zum Übernehmen der durch die Methoden **SetAttribute()** und **SetAttributes()** erstellten, noch ausstehenden Werte verwendet. Die erfolgreiche Ausführung dieser Methode erstellt eine Aufgabe zum Übernehmen ausstehender Attributwerte. Diese Methode wird auch zum Festlegen der Startreihenfolge, des Quellenstatus und des einmaligen Startgerätes verwendet.

 **ANMERKUNG:** Nachfolgende Aufrufe der Methode **CreateTargetedConfigJob()** nach der ersten **CreateTargetedConfigJob()** Methode ergeben einen Fehler, bis die erste Aufgabe vollständig abgeschlossen wurde. Sie können jedoch die aktuelle Aufgabe löschen und eine neue aufgabe erstellen, indem Sie **CreateTargetedConfigJob()** verwenden.

- Die Methode **DeletePendingConfiguration()** bricht die ausstehenden Änderungen der Konfiguration (erstellt unter Verwendung der Methoden „SetAttribute“ und „SetAttributes“) ab, bevor die Konfigurationsaufgabe mittels **CreateTargetedConfigJob()** erstellt wird.
- Die Methode **ChangePassword()** bewirkt die Änderung des BIOS-Kennworts.

Profil „Persistenter Speicher“

Die folgende Tabelle führt die Klassen, Funktionen, Vorgänge und Methoden des Profils „Persistenter Speicher“ auf.

Tabelle 31. . Profil „Persistenter Speicher“

Klassenname	Funktionen	Vorgänge	Methoden
DCIM_PersistentStorage Service	Verwenden Sie diese zentrale Klasse zum Definieren der extrinsischen Methoden.	„Aufzählung erhalten“ aufrufen	Siehe vFlash SD-Karte – Methoden
DCIM_VFlashView	Verwenden Sie diese Klasse, um die verschiedenen Instanz-Kennungen und zugehörigen Eigenschaften aller an ein System angebundener vFlash SD-Karten anzuzeigen.	Aufzählung erhalten	–
DCIM_OpaqueManagementData	Verwenden Sie diese Unterklasse, um die auf einer bestimmten vFlash SD-Karte verfügbaren Partitionen anzuzeigen.	Aufzählung erhalten	–

vFlash SD Card Methods

- Die Methode **InitializeMedia()** wird zum Formatieren der vFlash SD-Karte verwendet.
- Die Methode **VFlashStateChange()** wird zum Aktivieren oder Deaktivieren der vFlash SD-Karte verwendet.
- Die Methode **CreatePartition()** wird zum Erstellen einer neuen Partition auf einer vFlash SD-Karte verwendet.
- Die Methode **CreatePartitionUsingImage()** wird zum Erstellen einer neuen Partition unter Verwendung einer Speicherabbilddatei verwendet (die im **.img** oder **.iso**-Format vorhanden ist).
- Die Methode **DeletePartition()** wird zum Löschen einer Partition einer vFlash SD-Karte verwendet.
- Die Methode **FormatPartition()** wird zum Formatieren der ausgewählten Partition der vFlash SD-Karte verwendet.
- Die Methode **ModifyPartition()** wird zum Ändern der Partitionen auf der vFlash verwendet. Dies hängt vom Partitionstyp ab - Floppy, Festplatte oder CD.
- Die Methode **AttachPartition()** wird zur Anbindung einer oder mehrerer Partitionen als virtuelles USB-Massenspeichergerät verwendet.
- Die Methode **DetachPartition()** wird zum Trennen einer oder mehrerer Partionen verwendet, die als virtuelles Massenspeichergerät verwendet werden.
- Die Methode **ExportDataFromPartition()** wird zum Kopieren oder Exportieren der Inhalte einer vFlash SD-Kartenpartition auf einen lokalen oder Remote-Speicherort unter Verwendung einer Speicherabbilddatei in den Formaten **.img** und **.iso** verwendet.

Profil „RAID“

Die folgende Tabelle führt die Klassen, Funktionen, Vorgänge und Methoden des RAID-Profiles auf.

Tabelle 32. Profil „RAID“


Klassenname	Funktionen	Vorgänge	Methoden
DCIM_RAIDService	Dies ist die zentrale Klasse. Sie definiert die extrinsischen Methoden.	„Aufzählung erhalten“ aufrufen	Siehe RAID-Methoden
DCIM_ControllerView	Verwenden Sie diese Klasse, um die verschiedenen Instanz-Kennungen und zugehörigen Eigenschaften der an ein System angebundenen Controller anzuzeigen.	Aufzählung erhalten	–
DCIM_PhysicalDiskView	Verwenden Sie diese Klasse, um die verschiedenen Instanz-Kennungen und zugehörigen Eigenschaften der an ein System angebundenen physischen Festplatten anzuzeigen.	Aufzählung erhalten	–
DCIM_VirtualDiskView	Verwenden Sie diese Klasse, um die verschiedenen Instanz-Kennungen und zugehörigen Eigenschaften der erstellten virtuellen Laufwerke anzuzeigen.	Aufzählung erhalten	–
DCIM_EnclosureView	Verwenden Sie diese Klasse, um die verschiedenen Instanz-Kennungen und zugehörigen Eigenschaften der an ein System angebundenen Gehäuse anzuzeigen.	Aufzählung erhalten	–
DCIM_ControllerBattery View	Verwenden Sie diese Subklasse, um die Eigenschaften des Controller-Akkus anzuzeigen.	Aufzählung erhalten	–
DCIM_EnclosureEMMView	Verwenden Sie diese Klasse, um die verschiedenen Instanz-Kennungen und zugehörigen Eigenschaften der Gehäuse mit EMM-Firmware anzuzeigen.	Aufzählung erhalten	–
DCIM_EnclosurePSUView	Verwenden Sie diese Klasse, um die verschiedenen Instanz-Kennungen und zugehörigen Eigenschaften des Gehäusenetzteils anzuzeigen.	Aufzählung erhalten	–

Klassenname	Funktionen	Vorgänge	Methoden
DCIM_EnclosureFanSensor	Verwenden Sie diese Klasse, um die verschiedenen Instanz-Kennungen und zugehörigen Eigenschaften des Gehäuselüfters anzuzeigen.	Aufzählung erhalten	–
DCIM_EnclosureTemperatureSensor	Verwenden Sie diese Klasse, um die verschiedenen Instanz-Kennungen und zugehörigen Eigenschaften des Gehäuselüfters anzuzeigen.	Aufzählung erhalten	–


RAID-Methoden

Die RAID-Methoden werden zum Anwenden von Attributen auf unterschiedliche RAID-Komponenten verwendet. Jede Methode hat ihren eigenen Satz an Eingangs- und Ausgangsparametern. Die Methoden haben spezifische Rückgabecodewerte. Die verschiedenen Methoden der RAID-Dienstklasse sind:

- Die Methode **AssignSpare()** wird für die Zuweisung eines physischen Laufwerks zu einem virtuellen Laufwerks als dediziertes Ersatzlaufwerk, oder als globales Ersatzlaufwerk verwendet.
- Die Methode **ResetConfig()** wird zum Löschen sämtlicher virtueller Laufwerke und zum Aufheben der Zuweisung aller physikalischen Ersatzlaufwerke verwendet. Sämtliche Daten auf den vorhandenen virtuellen Laufwerken gehen dabei verloren.

 **ANMERKUNG:** Die virtuellen Laufwerke (auf den physikalischen Fremdlaufwerken), die nicht importiert werden, werden nicht gelöscht.

- Die Methode **ClearForeignConfig()** wird zur Vorbereitung jeglicher physikalischer Fremdlaufwerke für die Aufnahme in die lokale Konfiguration verwendet.

 **ANMERKUNG:** Sämtliche Daten auf den physischen Fremdlaufwerken gehen dabei verloren.

- Die Methode **DeleteVirtualDisk()** wird zum Löschen eines einzelnen virtuellen Laufwerks vom Zielcontroller verwendet. Das erfolgreiche Ausführen dieser Methode resultiert in der Markierung dieses virtuellen Laufwerks für das Löschen.
- Die Methode **CreateVirtualDisk()** wird zum Erstellen eines einzelnen virtuellen Laufwerks auf dem Zielcontroller verwendet. Das erfolgreiche Ausführen dieser Methode resultiert in einem ausstehenden, aber noch nicht erstellten virtuellen Laufwerk.
- Die Methode **GetHSDisks()** wird verwendet, um die mögliche Laufwerksauswahl herauszufinden, die als ein dediziertes Ersatzlaufwerk für das identifizierte virtuelle Laufwerk verwendet werden können.
- Die Methode **GetRAIDLevels()** wird verwendet, um die mögliche RAID-Ebenenauswahl zur Erstellung virtueller Laufwerke herauszufinden. Wird die Liste mit physikalischen Laufwerken nicht bereitgestellt, wirkt sich diese Methode auf alle verbundenen Laufwerke aus.
- Die Methode **GetAvailableDisks()** wird verwendet, um die mögliche Laufwerksauswahl zur Erstellung virtueller Laufwerke herauszufinden.
- Die Methode **CheckVDValues()** wird verwendet, um die Größe der virtuellen Laufwerke und der Standardeinstellungen für eine gegebene RAID-Ebene und einen gegebenen Laufwerkssatz herauszufinden.
- Die Methode **SetControllerKey()** legt den Schlüssel auf Controllern fest, die Laufwerksverschlüsselung unterstützen.
- Die Methode **LockVirtualDisk()** verschlüsselt das identifizierte virtuelle Laufwerk. Das virtuelle Laufwerk muss sich auf physikalischen Laufwerken befinden, die die Verschlüsselung unterstützen, wobei die Verschlüsselung auf ihnen aktiviert sein muss.

- Die Methode **CreateTargetedConfigJob()** wird verwendet, um die durch andere Methoden erstellten, ausstehenden Werte zu übernehmen. Die erfolgreiche Ausführung dieser Methode erstellt eine Aufgabe zum Übernehmen ausstehender Attributwerte.

 **ANMERKUNG:** Nachfolgende Aufrufe der Methode **CreateTargetedConfigJob()** nach der ersten **CreateTargetedConfigJob()** Methode ergeben einen Fehler, bis die erste Aufgabe vollständig abgeschlossen wurde.

- Die Methode **DeletePendingConfiguration()** bricht die ausstehenden Änderungen der Konfiguration (erstellt unter Verwendung der anderen Methoden) ab, bevor die Konfigurationsaufgabe mittels **CreateTargetedConfigJob()** erstellt wird.
- Die Methode **RemoveControllerKey()** (Controller-Schlüssel entfernen) löscht den Verschlüsselungsschlüssel auf dem Controller. Alle verschlüsselten virtuellen Laufwerke und die verknüpften Daten werden gelöscht.
- Die Methode **ReKey()** (Schlüsselneuerstellung) wird zum Ändern des Verschlüsselungsschlüssels für die lokale Schlüsselverwaltung auf dem Zielcontroller verwendet.
- Die Methode **EnableControllerEncryption()** (Controller-Verschlüsselung aktivieren) wendet die Verschlüsselung mit lokalen Schlüsseln (Local Key Encryption, LKM) auf Controller an.
- Die Methode **SetAttribute()** (Attribut festlegen) wird zum Festlegen oder Ändern des Wertes eines RAID-Attributs verwendet.
- Die Methode **SetAttributes()** wird zum Festlegen oder Ändern der Werte einer Gruppe von Attributen verwendet.
- Die Methode **CreateVirtualDisk()** wird zum Erstellen eines virtuellen Laufwerks auf dem Zielcontroller verwendet. Diese Methode kann auch dazu verwendet werden, um Folgendes zu tun:
 - Erstellen aufgeteilter (sliced) virtueller Festplatten. Eine aufgeteilte virtuelle Festplatte wird erstellt, wenn der Wert des Eingabeparameters **CreateVirtualDisk()** (Virtuelle Festplatte erstellen) geringer als die Gesamtgröße des Satzes mit physischen Festplatten ist. Sie können mit dem gleichen Satz an physischen Festplatten und der gleichen RAID-Stufe, die Sie für die Erstellung der ersten virtuellen Festplatte verwendet haben, zusätzliche aufgeteilte (sliced) virtuelle Festplatten erstellen.
 - Erstellen einer virtuellen Festplatte der Art „CacheCade“ auf dem Zielcontroller. Bei diesem Verfahren wird intern eine virtuelle Festplatte auf der RAID-Stufe 0 erstellt. Dieses Erstellungsverfahren ist identisch mit dem Verfahren zur Erstellung einer aufgeteilten (sliced) virtuellen Festplatte.
- Die Methode **UnassignSpares()** (Zuweisung für Spares aufheben) wird für die Rücknahme der Zuweisung einer physischen Festplatte zu einer virtuellen Festplatte als dediziertes Hotspare oder als globales Hotspare verwendet.

Profile „Hardware-Bestandslisten“

Die folgende Tabelle führt die Klassen, Funktionen, Vorgänge und Methoden für unterschiedliche Hardware auf dem verwalteten Knoten auf.

Tabelle 33. Profile „Hardware-Bestandslisten“

Klassenname	Funktionen	Vorgänge	Methoden
Profil „CPU“			
DCIM_CPUView	Verwenden Sie diese Klasse, um die Instanzinformationen von allen im System vorhandenen CPUs und zugehörigem Cache zu erhalten.	Aufzählung erhalten	–
Profil „Lüfter“			
DCIM_FanView	Verwenden Sie diese Klasse, um die Instanzinformationen von allen im System	Aufzählung erhalten	–

Klassenname	Funktionen	Vorgänge	Methoden
	vorhandenen Lüftern zu erhalten.		
Profil „iDRAC“			
DCIM_IDRACCardView	Verwenden Sie diese Klasse, um die Instanzinformationen von allen im System vorhandenen iDRAC-Karten zu erhalten.	Aufzählung erhalten	–
Profil „Speicher“			
DCIM_MemoryView	Verwenden Sie diese Klasse, um die Instanzinformationen von allen im System vorhandenen Speichermodulen zu erhalten.	Aufzählung erhalten	–
Profil „PCI“			
DCIM_PCIDeviceView	Verwenden Sie diese Klasse, um die Instanzinformationen von allen im System vorhandenen PCI-Geräten zu erhalten.	Aufzählung erhalten	–
Profil „Video“			
DCIM_VideoView	Verwenden Sie diese Klasse, um die Instanzinformationen von allen im System vorhandenen Videocontrollern zu erhalten.	Aufzählung erhalten	–
Profil „Netzteil“			
DCIM_PowerSupplyView	Verwenden Sie diese Klasse, um die Instanzinformationen von allen im System vorhandenen Netzteilen zu erhalten.	Aufzählung erhalten	–
Profil „Systemansicht“			
DCIM_SystemView	Verwenden Sie diese Klasse, um allgemeine Einzelheiten über das System, wie z.B. Systemhersteller, Modell, Service-Tag-Nummer, Gesamtspeicher, BIOS-Version, Systemkennung, Systemkennnummer, Energiestatus usw. zu erhalten.	Aufzählung erhalten	–

Profil „Aufgabensteuerung“

Die folgende Tabelle führt die Klassen, Funktionen, Vorgänge und Methoden des Profils „Aufgabensteuerung“ auf.

Tabelle 34. Profil „Aufgabensteuerung“

Klassenname	Vorgänge	Methoden
DCIM_JobControlService	Aufzählung erhalten	Siehe Aufgabensteuerung – Methoden
DCIM_LifecycleJob	Aufzählung erhalten	–

„Aufgabensteuerung“ - Methoden

Die Methoden werden verwendet, um die Aufgabenwarteschlange einzurichten und die Aufgaben aus der Aufgabenwarteschlange zu löschen.

- Die Methode **SetupJobQueue()** wird zum Erstellen einer Aufgabenwarteschlange verwendet, die eine oder mehr Aufgaben enthält, die in einer bestimmten Reihenfolge innerhalb der Warteschlange abgearbeitet werden.
- Die Methode **DeleteJobQueue()** wird zum Löschen von Aufgaben aus der Warteschlange verwendet.

Profil „Netzteil“

Die folgende Tabelle führt die Klassen, Funktionen, Vorgänge und Methoden des Profils „Netzteil“ auf.

Tabelle 35. Profil „Netzteil“

Klassenname	Vorgänge	Methoden
DCIM_PowerSupplyView	Aufzählung erhalten	–
DCIM_PowerSupply	Aufzählung erhalten	–
DCIM_PowerRedundancySet	Aufzählung erhalten	–

Profil zur Stromzustandsverwaltung

Die folgende Tabelle führt die Klassen, Funktionen, Vorgänge und Methoden des Profils zur Stromzustandsverwaltung auf.

Tabelle 36. Profil zur Stromzustandsverwaltung

Klassenname	Vorgänge	Methoden
DCIM_CSPowerManagementService	„Aufzählung erhalten“ aufrufen	Siehe Profil zur Stromzustandsverwaltung – Methode
DCIM_CSPowerManagementCapabilities	Aufzählung erhalten	–
DCIM_CSAssociatedPowerManagementService	Aufzählung erhalten	–

Profil zur Stromzustandsverwaltung – Methoden

Die Methode wird zum Abrufen des Status der Änderung des Stromzustands verwendet.

- Die Methode **RequestPowerStateChange()** wird zum Abrufen der ausstehenden Änderung des Stromzustands aufgerufen.

Profil zum Datensatzprotokoll

Die folgende Tabelle führt die Klassen, Funktionen, Vorgänge und Methoden des Profils zum Datensatzprotokoll auf.

Tabelle 37. Profil zum Datensatzprotokoll

Klassenname	Vorgänge	Methoden
DCIM_LCRecordLog	„Aufzählung erhalten“ aufrufen	Siehe Profil zum Datensatzprotokoll – Methode
DCIM_LCRecordLogCapabilities	Aufzählung erhalten	–
DCIM_LCLogEntry	„Aufzählung erhalten“ festlegen	–
DCIM_SELRecordLog	„Aufzählung erhalten“ aufrufen	–
DCIM_SELRecordLogCapabilities	Aufzählung erhalten	–
DCIM_SELLogEntry	„Aufzählung erhalten“ festlegen	–

Profil zum Datensatzprotokoll-Methoden

Die Methoden werden zum Verwalten der in einem System erstellten Protokolle verwendet.

- Die Methode **ClearLog()** wird zum Löschen aller Einträge im SEL-Protokoll verwendet. Der Rückgabecode Null zeigt an, dass die Protokolleinträge erfolgreich gelöscht wurden.
- Die Methode **GetConfigResults()** bietet die Möglichkeit die Konfigurationsergebnisse abzurufen, die mit einem bestimmten protokollierten Eintrag verbunden sind.

Profil zur rollenbasierten Autorisierung

Die folgende Tabelle führt die Klassen, Funktionen, Vorgänge und Methoden des Profils „Rollenbasierte Authentifizierung“ auf.

Tabelle 38. Profil zur rollenbasierten Autorisierung

Klassenname	Vorgänge	Methoden
DCIM_LocalRolePrivilege	„Aufzählung erhalten“ festlegen	–
DCIM_CLPPrivilege	Aufzählung erhalten	–
DCIM_Role	Aufzählung erhalten	–
DCIM_IPMIRole	Aufzählung erhalten	–
DCIM_IPMISOLRole	Aufzählung erhalten	–
DCIM_CLPRole	Aufzählung erhalten	–
DCIM_LocalRoleBasedAuthorizationService	Aufzählung erhalten	–
DCIM_IPMIRoleBasedAuthorizationService	Aufzählung erhalten	Siehe Profil zur rollenbasierten Autorisierung – Methoden
DCIM_CLPRoleBasedAuthorizationService	Aufzählung erhalten	Siehe Profil zur rollenbasierten Autorisierung – Methoden
DCIM_LocalRoleBasedManagementCapabilities	Aufzählung erhalten	–

Klassenname	Vorgänge	Methoden
DCIM_IPMIRoleBasedManagementCapabilities	Aufzählung erhalten	–
DCIM_CLPRoleBasedManagementCapabilities	Aufzählung erhalten	–

Profil zur rollenbasierten Autorisierung – Methoden

Die Methoden werden zur Verwaltung des rollenbasierten Zugriffs auf ein System verwendet.

- Die Methode **AssignRoles()** der Klasse DCIM_IPMIRoleBasedAuthorizationService wird zur Zuweisung eines Sicherheitsprinzips, das durch eine Instanz von DCIM_IPMIIdentity repräsentiert wird, auf null oder mehr Rollen verwendet, die durch Instanzen von DCIM_IPMIRole repräsentiert werden.
- Die Methode **AssignRoles()** der Klasse DCIM_CLPRoleBasedAuthorizationService wird zur Zuweisung eines Sicherheitsprinzips, das durch eine Instanz von DCIM_CLPIdentity repräsentiert wird, auf null oder mehr Rollen verwendet, die durch Instanzen von DCIM_CLPRole repräsentiert werden.

Profil zu Sensoren

Die folgende Tabelle führt die Klassen, Funktionen, Vorgänge und Methoden des Sensoren-Profiles auf.

Tabelle 39. Profil zu Sensoren

Klassenname	Vorgänge	Methoden
DCIM_PSNumericSensor	„Aufzählung erhalten“ festlegen	–
DCIM_NumericSensor	„Aufzählung erhalten“ festlegen	–
DCIM_Sensor	Aufzählung erhalten	–

Profil zum Serviceprozessor

Die folgende Tabelle führt die Klassen, Funktionen, Vorgänge und Methoden des Profil zum Serviceprozessor auf.

Tabelle 40. Profil zum Serviceprozessor

Klassenname	Vorgänge	Methoden
DCIM_SPCoordinatorSystem	„Aufzählung erhalten“ aufrufen	Siehe Profil zum Serviceprozessor-Methoden
DCIM_TimeService	„Aufzählung erhalten“ aufrufen	Siehe Profil zum Serviceprozessor-Methoden

Dienstprozessorprofil - Methoden

Die Methoden werden zum Verwalten des Dienstprozessors verwendet.

- Die Methode **RequestStateChange()** wird zum Zurücksetzen des iDRAC-Status auf den im Parameter RequestedState spezifizierten Wert verwendet.
- Es wird die Methode **ManageTime()** verwendet, um die Dienstprozessorzeit abzufragen.

Ereignisfilterprofil

Die folgende Tabelle führt die Klassen, Funktionen, Vorgänge und Methoden des Ereignisfilterprofils auf.

Tabelle 41. Ereignisfilterprofil

Klassenname	Vorgänge	Methoden
DCIM_EFConfigurationService	„Aufzählung erhalten“ aufrufen, festlegen (nach Kategorie)	Sie Ereignisfilterprofil – Methoden
DCIM_EventFilter	Aufzählung erhalten	–

Ereignisfilterprofil - Methoden

Die Methoden werden zur Verwaltung von Ereignisfiltern verwendet.

- Die Methode **SetEventFilterByCategory()** wird verwendet, um die Aktion und Benachrichtigungen für alle Ereignisfilter festzulegen, die zu einer bestimmten Kategorie, Unterkategorie und Schweregrad gehören.
- Die Methode **SetEventFilterByInstanceIDs()** wird verwendet, um die Aktion und Benachrichtigungen für alle Ereignisfilter festzulegen, die zu einem bestimmten Satz von Instanzkennungen gehören.

Lizenz-Verwaltungsprofil

Die folgende Tabelle führt die Klassen, Funktionen, Vorgänge und Methoden des Lizenz-Verwaltungsprofils auf.

Tabelle 42. Lizenz-Verwaltungsprofil

Klassenname	Vorgänge	Methoden
DCIM_LicenseManagementService	„Aufzählung erhalten“ aufrufen	Siehe Lizenz-Verwaltungsprofil – Methoden
DCIM_LicensableDevice	Aufzählung erhalten	–
DCIM_License	Aufzählung erhalten	–

Lizenzverwaltungsprofil - Methoden

Die Methoden werden zum Verwalten der Lizenzen verwendet.

- Die Methode **ImportLicense()** wird zum Importieren von Lizenzdateien in den Lizenzmanager verwendet.
- Die Methode **ImportLicenseFromNetworkShare()** wird zum Importieren der im Speicherort der Freigabe angegebenen Lizenz verwendet.
- Die Methode **DeleteLicense()** wird zum Löschen zugewiesener Lizenzen verwendet.
- Die Methode **ExportLicense()** wird zum Exportieren von Lizenzdateien vom iDRAC verwendet.
- Die Methode **ExportLicenseByDevice()** wird zum Exportieren von Lizenzdateien des iDRACs verwendet.
- Die Methode **ExportLicenseToNetworkShare()** wird zum Exportieren von Lizenzdateien des iDRACs verwendet.
- Die Methode **ExportLicenseByDeviceToNetworkShare()** wird zum Exportieren von Lizenzdateien von einem Gerät auf einen externen Speicherort verwendet.
- Die Methode **ReplaceLicense()** wird zum Ersetzen von Lizenzdateien im Lizenzmanager verwendet.

Profil der iDRAC-Karte

Die folgende Tabelle führt die Klassen, Funktionen, Vorgänge und Methoden des Profils „iDRAC-Karte“ auf.

Tabelle 43. Profil der iDRAC-Karte

Klassenname	Vorgänge	Methoden
DCIM_IDRACCardView	Aufzählung erhalten	–
DCIM_IDRACCardEnumeration	Aufzählung erhalten	–
DCIM_IDRACCardString	Aufzählung erhalten	–
DCIM_IDRACCardInteger	Aufzählung erhalten	–
DCIM_IDRACCardService	„Aufzählung erhalten“ aufrufen	Siehe Profil der iDRAC-Karte – Methoden

Profil der iDRAC-Karte – Methoden

Die Methoden werden zum Verwalten von iDRAC verwendet.

- Die Methode **SetAttribute()** wird zum Festlegen oder Ändern des Wertes eines iDRAC-Attributs verwendet.
- Die Methode **SetAttributes()** wird zum Festlegen oder Ändern der Werte einer Gruppe von iDRAC-Attributen verwendet.
- Die Methode **CreateTargetedConfigJob()** wird zum Übernehmen der durch die Methoden SetAttribute() und SetAttributes() erstellten, noch ausstehenden Werte verwendet.
- Die Methode **DeletePendingConfiguration()** wird zum Abbrechen der durch die Methoden SetAttribute() und SetAttributes() erstellten, noch ausstehenden Werte verwendet.
- Die Methode **ApplyAttributes()** wird zum Festlegen oder Ändern des Wertes eines iDRAC-Attributs verwendet.
- Die Methode **SendTestEmailAlert()** wird zum Senden von Test-E-Mail-Warnungen verwendet.

Basisserver und Profil zum physischen Bestand

Die folgende Tabelle führt die Klassen, Funktionen, Vorgänge und Methoden des Profils Basisserver und Profil zum physischen Bestand auf.

Tabelle 44. Basisserver und Profil zum physischen Bestand

Klassenname	Vorgänge	Methoden
DCIM_ComputerSystem	„Aufzählung erhalten“ aufrufen	Siehe Basisserver und Profil zum physischen Bestand – Methoden
DCIM_ComputerSystemPackage	Aufzählung erhalten	–
DCIM_CSEnabledLogicalElementCapabilities	Aufzählung erhalten	–
DCIM_Chassis	Aufzählung erhalten	–

Profil für Basis-Server und physische Anlagen - Methoden

Die Methoden werden zum Durchführen grundlegender Serververwaltungsaufgaben verwendet.

- Die Methode **RequestStateChange()** wird zum Ändern des Status einer Komponente auf einen dieser Werte verwendet: Aktiviert, Deaktiviert, Zurücksetzen.

Systeminfoprofil

Die folgende Tabelle führt die Klassen, Funktionen, Vorgänge und Methoden des Systeminfoprofils auf.

Tabelle 45. Systeminfoprofil

Klassenname	Vorgänge	Methoden
DCIM_SystemEnumeration	Aufzählung erhalten	–
DCIM_SystemString	Aufzählung erhalten	–
DCIM_SystemInteger	Aufzählung erhalten	–
DCIM_SystemManagementService	Aufzählung erhalten Aufrufen	Siehe System-Info-Methoden

Systeminfo-Methoden

Die Methoden werden zum Abrufen von grundlegenden Systeminformationen verwendet.

- Die Methode **SetAttribute()** wird zum Festlegen oder Ändern des Wertes eines System-Attributs verwendet.
- Die Methode **SetAttributes()** wird zum Festlegen oder Ändern der Werte einer Gruppe von Attributen verwendet.
- Die Methode **CreateTargetedConfigJob()** wird zum Übernehmen der durch die Methoden SetAttribute() und SetAttributes() erstellten, noch ausstehenden Werte verwendet.
- Die Methode **DeletePendingConfiguration()** wird zum Abbrechen der durch die Methoden SetAttribute() und SetAttributes() erstellten, noch ausstehenden Werte verwendet.
- **ShowErrorsOnLCD()** Methode wird zum Aus- und Einblenden von LCD-Fehlern verwendet.
- **IdentifyChassis()** Methode wird zum Ein- und Ausschalten von LEDs auf dem Gehäuse verwendet, um es identifizieren zu können.

Profil zur einfachen Identitätsverwaltung

Die folgende Tabelle führt die Klassen, Funktionen, Vorgänge und Methoden des Profils zur einfachen Identitätsverwaltung auf.

Tabelle 46. Profil zur einfachen Identitätsverwaltung

Klassenname	Vorgänge	Methoden
DCIM_Account	„Aufzählung erhalten“ festlegen, aufrufen	Siehe Einfache Identität – Methoden
DCIM_EnabledLogicalElementCapabilities	Aufzählung erhalten	–
DCIM_LocalUserIdentity	Aufzählung erhalten	–
DCIM_LANIdentity	Aufzählung erhalten	–

Klassenname	Vorgänge	Methoden
DCIM_SerialIdentity	Aufzählung erhalten	–
DCIM_CLPIdentity	Aufzählung erhalten	–
DCIM_LocalUserAccountManagementService	Aufzählung erhalten	–
DCIM_IPMIAccountManagementService	Aufzählung erhalten	–
DCIM_CLPAccountManagementService	Aufzählung erhalten	–
DCIM_LocalUserAccountManagementCapabilities	Aufzählung erhalten	–
DCIM_IPMICLPAccountManagementCapabilities	Aufzählung erhalten	–
DCIM_RegisteredProfile	Aufzählung erhalten	–
DCIM_LCRegisteredProfile	Aufzählung erhalten	–

Einfache Identität - Methoden

Die Methode **RequestStateChange()** wird verwendet, um das durch die Instanz DCIM_Account repräsentierte Konto zu aktivieren oder zu deaktivieren.

Fehlerbehebung und häufig gestellte Fragen

Fehlermeldungen

Weitere Informationen zu den Fehlermeldungskennungen und den empfohlenen Maßnahmen finden Sie in der „Dell Lifecycle-Controller Remote Services-Liste mit Fehlermeldungen und Fehlerbehebungen“ unter support.dell.com/manuals. Wählen Sie zum Anzeigen der Fehlermeldung und zugehörigen Informationen die **Fehlermeldungskennung** aus der Drop-Down-Liste Fehlermeldungskennung aus. Darüberhinaus können Sie das detaillierte Fehlermeldungsregister unter delltechcenter.com/page/Lifecycle+Controller herunterladen.

Automatische Ermittlung - LCD Meldungen

Die folgende Tabelle führt die LCD-Meldungen auf, die während der Durchführung von Vorgängen der automatischen Ermittlung angezeigt werden.

Tabelle 47. Automatische Ermittlung - Meldungen

Meldung 1	Meldung 2
Angehalten	–
Durchführen	siehe Auto-Ermittlung Fehlermeldungen und Lösungen
Unterbrochen	siehe Auto-Ermittlung Fehlermeldungen und Lösungen
Abgeschlossen	–

In der folgenden Tabelle werden die LCD-Fehlermeldungen und -Lösungen aufgelistet. Diese Meldungen werden in Kombination mit den Meldungen angezeigt, die in aufgeführt werden. Wenn z.B. ein [Vorgang der automatischen Ermittlung](#) läuft und ein Verwaltungskonto aktiviert wurde, werden die Meldungen `Wird ausgeführt und Blockiert` und `Administratorkonto aktiviert` auf dem Frontblendenbildschirm angezeigt.

Tabelle 48. Auto-Ermittlung Fehlermeldungen und Lösungen

Meldung 2	Lösungen
Angehalten (Standard)	k.A.
Gestartet	k.A.
Automatische Ermittlung deaktiviert	Aktivieren Sie die automatische Ermittlung.
Blockiertes Admin-Konto aktiviert	Deaktivieren Sie alle administrativen Konten.
Blockiertes Active Directory aktiviert	Deaktivieren Sie das aktive Verzeichnis.
Blockiertes IPv6 aktiviert	Deaktivieren Sie IPv6.
Blockiertes No IP auf NIC	Aktivieren Sie die NIC.
Kein Bereitstellungsserver gefunden	Überprüfen Sie den Wert von psinfo im BIOS. Wenn psinfo nicht im BIOS konfiguriert wurde, dann überprüfen Sie, ob die DHCP-Option aktiviert und/oder die DNS-Serverkonfiguration gültig ist.

Meldung 2	Lösungen
Blockierter Bereitstellungsserver nicht erreichbar/Ungültige Adresse	Überprüfen Sie den Wert von psinfo im BIOS.
Keine Service-Tag-Nummer	Starten Sie den Server. Falls das Problem weiterhin besteht, kontaktieren Sie den technischen Support.
SSL-Verbindung fehlgeschlagen, kein Dienst an IP/Port	Überprüfen Sie den Wert von psinfo im BIOS, oder die Anbieteroption auf dem DHCP-Server.
SSL-Verbindung abgelehnt	Überprüfen Sie den Wert von psinfo im BIOS, oder die Anbieteroption auf dem DHCP-Server.
SSL-Verbindung fehlgeschlagen (Serverauthentifizierung)	Das Server-Zertifikat ist ungültig oder wurde nicht mit dem auf dem iDRAC installierten Trusted Server CA-Zertifikat signiert. Tauschen Sie entweder das Zertifikat des Bereitstellungsservers aus, oder laden Sie einen neuen iDRAC-zertifizierten Server hoch.
SSL-Verbindung fehlgeschlagen (Clientauthentifizierung)	iDRAC Client-Zertifikat wurde nicht durch eine Zertifizierungsstelle signiert, der der Bereitstellungsserver vertraut. Fügen Sie entweder die iDRAC-Zertifizierungsstelle zur Liste vertrauenswürdiger Zertifizierungsstellen hinzu oder generieren Sie auf dem iDRAC ein neues Zertifikat.
Sonstige SSL-Verbindung fehlgeschlagen	Aktivieren Sie ein Root-Konto durch das BIOS, um das iDRAC-TraceLog abzurufen. Falls das Problem weiterhin besteht, kontaktieren Sie den technischen Support.
SOAP-Fehler	Der Bereitstellungsserver unterstützt den SOAP-Aufruf getCredentials() nicht. Überprüfen Sie, dass der Server automatische Ermittlung unterstützt und dass die Bereitstellungsserverinformationen ordnungsgemäß in der DHCP-Anbieteroption, dem DNS SRV-Eintrag oder dem BIOS eingestellt sind.
Keine Anmeldeinformationen zurückgegeben	Überprüfen Sie, dass die Service-Tag-Nummer auf dem Bereitstellungsserver in der Liste der bekannten Server enthalten ist.
Kontenerstellung fehlgeschlagen	Stellen Sie sicher, dass nicht bereits alle der 16 iDRAC-Konten verwendet werden.

Häufig gestellte Fragen (FAQs)

Dieser Abschnitt beantwortet von Benutzern der Remote-Services häufig gestellte Fragen.

1. Was ist Lifecycle-Controller?

Lifecycle-Controller ist eine integrierte Systemverwaltungslösung für die Unterstützung von Kunden bei der Durchführung von Diagnosen, Betriebssystembereitstellung (OS-Bereitstellung), Firmwareaktualisierungen und Konfiguration. Remote-Services“ ist ein allgemeiner Begriff, der sich auf die Möglichkeit bezieht, Nutzer in die Lage zu versetzen, sich per Remote-Verbindung mit den Zielservers zu verbinden und Script-basierte Systemverwaltungsvorgänge durchzuführen.

2. Wie kann ich die Verbindung zwischen dem Client und dem verwalteten Server unter Verwendung der Remotedienste überprüfen?

Verwenden Sie das Ping-Dienstprogramm, um die Verbindung zwischen Client und verwaltetem Server zu überprüfen. Stellen Sie anschließend sicher, dass der Client und das Netzwerk die HTTP- und SSL-Protokolle zulassen.

3. Was ist Teilersetzung?

Die Teilersetzungs-Funktion ermöglicht dem System, für eine installierte oder ausgetauschte Hardwarekomponente automatisch die Firmware zu aktualisieren, oder Konfiguration, oder beides.

4. Was ist CSIOR und warum ist er aktiviert?

CSIOR ist Collect System Inventory on Restart (Systembestand bei Neustart erfassen). Es ermöglicht das automatische Aktualisieren der Firmware und Hardwarebestandsliste während des Systemstarts. Das System wird ab Werk mit deaktiviertem CSIOR geliefert.

5. Wie kann ich die Systembestandsinformationen auf dem neuesten Stand halten, wenn an BIOS-, RAID- oder NIC-Attributen lokale Änderungen vorgenommen werden?

Drücken Sie entweder manuell <F10> während des Systemstarts oder setzen Sie das CSIOR-Attribut auf „enabled“ (aktiviert), um bei jedem Systemstart die Systembestandsliste und Konfigurationsattributinformationen zu sammeln.

Listen Sie die Klasse `DCIM_SystemView` auf, um den Wert unter Eigenschaften `LastSystemInventoryTime` und „LastUpdateTime“ einer bestimmten Komponente anzuzeigen.

6. Wie aktualisiere ich das verwaltete System unter Verwendung des Lifecycle-Controller oder der Remote-Services?

Drücken Sie für den Lifecycle-Controller während des Systemstarts <F10>. Klicken Sie auf der Lifecycle-Controller-Benutzeroberfläche auf **Plattformaktualisierung** und wählen Sie **Zu aktualisierende Geräte** aus. Weitere Informationen zu Remotediensten finden Sie unter Lifecycle-Controller Web Services Interface Guide–Windows and Linux version (Lifecycle-Controller-Webdienste – Schnittstellenrichtlinie - Windows und Linux).

7. Was soll ich tun, wenn ein schwerwiegender Fehler auftritt, gefolgt von einem roten Bildschirm?

Führen Sie einen Kaltneustart (Aus- und Einschaltvorgang) durch, wenn der rote Bildschirm angezeigt wird.

8. Muss ich ein Betriebssystem (BS) installieren, um auf den Lifecycle-Controller oder die Remote-Services zuzugreifen?

Ein Betriebssystem wird für den Zugriff auf den Lifecycle-Controller oder die Remote-Services nicht benötigt.

9. Welche UEFI-Version wird unterstützt: 32-Bit oder 64-Bit?

UEFI unterstützt 64-Bit.

10. Warum wird in der NIC-Bestandsliste nichts zurückgegeben, obwohl das System Broadcom oder INTEL NICs verwendet?

Die auf dem System installierten NICs werden von Dell nicht unterstützt.

11. Kann ich auf dem System unter Verwendung der WS-Management-Funktionen einen Remote-Neustart durchführen?

Ja, das System kann unter Verwendung der Methode `RequestStateChange()` in der Klasse `DCIM_ComputerSystem` neu gestartet werden. Ein Neustart kann zeitlich eingeplant werden, indem eine Neustartaufgabe unter Verwendung der Methode `CreateRebootJob()` in der Klasse `DCIM_JobService` erstellt wird und anschließend die Neustartaufgabe unter Verwendung der Methode `SetupJobQueue()` des Aufgabensteuerungsdienstes zeitlich eingeplant wird.

12. Warum ändert sich LastUpdateTime nicht, wenn ich ein DIMM austausche?

Wenn ein DIMM entfernt und erneut im gleichen Steckplatz installiert wird, ändert sich `LastUpdateTime` in der Ansicht nicht.

13. Gibt es Möglichkeiten zur Verbesserung der Reaktionszeit für das Einholen der `DCIM_iDracCardAttribute` unter Verwendung von WinRM?

Ja. Das Einstellen der WinRM-Konfiguration durch Ausführen des folgenden Befehls reduziert die Zeit, die durch die `PCIDeviceView`-Auflistung in Anspruch genommen wird.

```
#winrm set winrm/config @{MaxBatchItems="75"}
```

14. Wie lösche ich Aufgaben?

Listen Sie `DCIM_LifecycleJob` auf, um alle Aufgaben im Lifecycle-Controller aufzuführen und verwenden Sie die Methode `DeleteJobQueue()`, um einzelne Aufgaben zu löschen.

15. Wie lösche ich alle Aufgaben?

Rufen Sie die Methode `DeleteJobQueue()` mit einer Aufgabenkennung von `JID_CLEARALL` auf.

16. Wann können wir die durch das WS-Management widergespiegelten Änderungen erkennen, wenn die Änderungen lokal in HII vorgenommen werden?

Nach dem Verlassen des USC aktualisiert die Lifecycle-Controller-Management-Schnittstelle die verfügbaren Informationen innerhalb von etwa zwei Minuten.

17. Was muss der Systemstatus sein, um die Methode `CreateTargetedConfigJob()` erfolgreich aufrufen zu können?

Das System muss entweder ausgeschaltet sein, oder den BIOS POST durchlaufen haben (z.B. BIOS oder UEFI Startverwaltung), oder das OS gestartet haben, damit die Methode `CreateTargetedConfigJob()` erfolgreich ist. Die Aufgaben werden jedoch nicht ausgeführt, bis das System den POST abgeschlossen, bzw. das **System-Setup** beendet hat.

18. Anleitung zum Löschen einer Aufgabe, die mithilfe der Methode „`CreateTargetedConfigJob()`“ (Zielkonfigurationsaufgaben erstellen) erstellt wurde

Beim Aufrufen der Methode `CreateTargetedConfigJob()` wird eine zusätzliche Neustartaufgabe erstellt, die es dem System ermöglicht, einen Neustart auf Lifecycle-Controller auszuführen und damit die Aufgabe auszuführen. Wenn Sie diese Aufgabe löschen möchten, muss die Neustartaufgabe ebenfalls gelöscht werden. Sie können entweder alle Aufgaben auflisten und die relevanten Aufgaben zum Löschen auswählen, oder Sie können „`JID_CLEARALL`“ verwenden, um alle Aufgaben zu löschen.

19. Worin unterscheidet sich die `ProcCore`-Einstellung bei Quad Core-Prozessoren?

Bei Quad-Core-Prozessoren wird der aktuelle Wert auf `ALL` eingestellt, wenn der Wert des Attributs „`ProcCore`“ auf 4 eingestellt wird.

20. Warum werden alle „NIC LED-Blinken Attribute“ immer auf NULL gesetzt, nachdem die Aufgabe abgeschlossen wurde?

„NIC LED-Blinken Attribute“ ist eine einmalige Einstellung. Nach Abschluss der SSIB-Aufgabe setzt sie aber den derzeitigen Wert auf Null. Der Zweck dieses Attributs ist es, die NIC-LEDs für eine bestimmte Zeitspanne (in Sekunden) blinken zu lassen.

21. Wie viele Attribute kann ich durch die Methode „`SetAttribute()`“ einstellen?

Durch die Methode `SetAttribute()` können Sie nur ein Attribut einstellen. Um zwei oder mehr Attribute mit einem Methodenaufruf einzustellen, verwenden Sie die Methode `SetAttributes()` für die „Dienste“ der gerade konfigurierten Komponente.

22. Warum werden einige andere Attribute eingestellt, während gerade ein unterschiedliches Attribut eingestellt wird?

Im BIOS und auf der NIC sind eine Attribute vorhanden, die Abhängigkeiten voneinander aufweisen. Bei der Einstellung eines bestimmten Attributs, werden alle abhängigen Attribute auf Basis ihrer Abhängigkeiten modifiziert. Dies ist ein erwartetes Verhalten.

- BIOS-Abhängigkeiten — TPM, Energieverwaltung, Netzstromwiederherstellung und Integrierte NIC.
- NIC-Abhängigkeiten — VLAN-Modus und WakeONLAN-Attribute.

23. Kann ich „`VlanMode`“ und „`VlanID`“ in der gleichen Aufgabe einstellen?

Sie können die `VlanMode`- und `VlanID`-Attribute, die Abhängigkeiten beinhalten, nicht in der gleichen Aufgabe einstellen. Sie müssen das übergeordnete Attribut (`VlanMode`) als ersten Einstellvorgang einstellen, das untergeordnete Attribut (`VlanID`) in einem zweiten Einstellvorgang und anschließend die Aufgabe mit „`commit`“ übergeben.

Schema

In diesem Abschnitt wird ein typisches Schema für das Lifecycle-Potokoll angezeigt.

Lifecycle Protokoll-Schema

```
<?xml version="1,0" encoding="UTF-8"?>
<?xml version="1.0" encoding="UTF-8"?> <xs:schema xmlns:xs="http://www.w3.org/
2001/XMLSchema" xmlns:dm="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified" attributeFormDefault="unqualified"> <xs:element
name="Description" type="xs:string"/> <xs:element name="MessageID"
type="xs:string"/> <xs:element name="Arg" type="xs:string"/> <xs:element
name="MessageArguments"> <xs:complexType> <xs:sequence minOccurs="0">
<xs:element ref="dm:Arg" minOccurs="0"/> </xs:sequence> </xs:complexType> </
xs:element> <xs:element name="Event"> <xs:complexType> <xs:sequence
minOccurs="0"> <xs:element ref="dm:Description"minOccurs="0"/> <xs:element
ref="dm:MessageID" minOccurs="0"/> <xs:element
ref="dm:MessageArguments" minOccurs="0"/> </xs:sequence> <xs:attribute
name="TimeStamp" type="xs:string" use="required"/> <xs:attribute name="AgentID"
type="xs:integer" use="required"/> <xs:attribute name="Severity"
type="xs:integer" use="required"/> <xs:attribute name="s"
type="xs:string" use="required"/> </xs:complexType> </xs:element> <xs:element
name="Events"> <xs:complexType> <xs:sequence minOccurs="0"> <xs:element
ref="dm:Event" minOccurs="0" maxOccurs="unbounded"/> </xs:sequence>
<xs:attribute name="lang" type="xs:string" use="optional"/> <xs:attribute
name="schemaVersion" type="xs:string" use="optional"/> <xs:attribute
name="timeStamp" type="xs:dateTime" use="optional"/> </xs:complexType> </
xs:element> </xs:schema>
```


Leicht zu verwendende Systemkomponentenbezeichnungen

Die folgende Tabelle enthält den FQDD (Fully Qualified Device Descriptor) der Systemkomponenten und die entsprechenden einfach zu verwendenden Bezeichnungen.

FQDD der Bezeichnung der Systemkomponente	Leicht zu verwendende Bezeichnung ("Easy-To-Use")
RAID.Integrated.1	Integrierter RAID-Controller
RAID.Embedded.1-1	Integrierter S110 RAID-Controller
RAID.Slot.1-1	RAID-Controller in Steckplatz 1
NIC.Mezzanine.1B-1	NIC in Mezzanine
NIC.Mezzanine.1C-1	
NIC.Mezzanine.1C-2	
NIC.Mezzanine.3C-2	
NIC.Integrated.1	Integrierter NIC 1
NIC.Integrated.2	Integrierter NIC 2
NIC.Integrated.1-1	Integrierter NIC 1 Port 1
NIC.Integrated.1-1	Integrierter NIC 1 Port 1 Partition 1
NIC.Slot.1-1	NIC in Steckplatz1 Port 1
NIC.Slot.1-2	NIC in Steckplatz1 Port 2
Video.Embedded.1-1	Integrierter Grafikkontroller
HostBridge.Embedded.1-1	Integrierte Host-Bridge 1
ISABridge.Embedded.1-1	Integrierte ISA-Bridge 2
P2PBridge.Embedded.1-1	Integrierte P2P-Bridge 3
P2PBridge.Mezzanine.2B-1	Integrierte Host-Bridge in Mezzanin 1 (Architektur B)
USBUHCI.Embedded.1-1	Integrierte USB UHCI 1
USBOHCI.Embedded.1-1	Integrierte USB OHCI 1
USBEHCI.Embedded.1-1	Integrierte USB EHCI 1
Disk.SATAEmbedded.A-1	Laufwerk auf integriertem SATA-Port A
Optical.SATAEmbedded.B-1	Optisches Laufwerk auf integriertem SATA-Port B
TBU.SATAExternal.C-1	Bandsicherung auf externem SATA-Port C
Disk.USBFront.1-1	Mit Front-USB 1 verbundenes Laufwerk
Floppy.USBBack.2-1	Mit hinterem USB 2 verbundenes Floppy-Laufwerk
Optical.USBFront.1-1	Mit vorderem USB 1 verbundenes optisches Laufwerk
Disk.USBInternal.1	Mit internem USB 1 verbundenes Laufwerk

FQDD der Bezeichnung der Systemkomponente	Leicht zu verwendende Bezeichnung ("Easy-To-Use")
Optical.iDRACVirtual.1-1	Virtuell verbundenes optisches Laufwerk
Floppy.iDRACVirtual.1-1	Virtuell verbundenes Floppy-Laufwerk
Disk.iDRACVirtual.1-1	Virtuell verbundenes Laufwerk
Floppy.vFlash.<string>	vFlash SD-Kartenpartition 2
Disk.vFlash.<string>	vFlash SD-Kartenpartition 3
iDRAC.Embedded.1-1	iDRAC
System.Embedded.1-1	System
HardDisk.List.1-1	Laufwerk C:
BIOS.Embedded.1-1	System-BIOS
BIOS.Setup.1-1	System BIOS-Setup
PSU.Slot.1	Netzteil 1
Fan.Embedded.1	Lüfter 1
Fan.Embedded.2	Lüfter 2
System.Chassis.1	Blade-Gehäuse
LCD.Chassis.1	LCD
Fan.Slot. 1	Lüfter 1
Fan.Slot. 2	Lüfter 2
...	...
Fan.Slot. 9	Lüfter 9
MC.Chassis.1	Gehäuseverwaltungs-Controller 1
MC.Chassis.2	Gehäuseverwaltungs-Controller 2
KVM.Chassis.1	KVM
IOM.Slot.1	E/A-Modul 1
...	...
IOM.Slot.6	E/A-Modul 6
PSU.Slot.1	Netzteil 1
...	...
PSU.Slot.6	Netzteil 6
CPU.Socket.1	CPU 1
System.Modular.2	Blade 2
DIMM.Socket.A1	DIMM A1