Dell Chassis Management Controller Version 3.10 für Dell EMC PowerEdge VRTX

Benutzerhandbuch

DELL EMC

Anmerkungen, Vorsichtshinweise und Warnungen

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

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

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

2018 - 06

Rev. A01

Inhaltsverzeichnis

1

Übersicht

Der Dell Chassis Management Controller (CMC) für Dell EMC PowerEdge VRTX ist eine Systemverwaltungs-Hardware- und -Softwarelösung zur Verwaltung des **PowerEdge VRTX**-Gehäuses. Der CMC verfügt über einen eigenen Mikroprozessor und Speicher und wird von dem modularen Gehäuse, an das er angeschlossen ist, mit Strom versorgt.

Der CMC ermöglicht IT-Administratoren das:

- Anzeigen der Bestandsliste
- Durchführen der Konfiguration und Überwachung
- Remote-Einstellen zum Aktivieren oder Deaktivieren von Gehäusen und Servern
- Aktivieren von Warnungen für Ereignisse auf Servern und Komponenten im Servermodul
- Anzeigen von Speichercontrollern und Festplattenlaufwerken im VRTX-Gehäuse
- Verwalten des PCIe-Untersystems im VRTX-Gehäuse
- Bereitstellen einer Eins-zu-Vielen-Verwaltungsschnittstelle zu den iDRACs und E/A-Modulen im Gehäuse

Sie können das PowerEdge VRTX-Gehäuse entweder mit einem einzelnen CMC oder mit redundanten CMCs konfigurieren. In redundanten CMC-Konfigurationen übernimmt der Standby-CMC die Gehäuseverwaltung, falls der primäre CMC die Kommunikation mit dem Gehäuse oder dem Verwaltungsnetzwerk verliert.

Der CMC bietet verschiedene Systemverwaltungsfunktionen für Server. Die Energie- und Temperaturverwaltung stellen die Hauptfunktionen des CMC dar, die im Folgenden aufgeführt sind:

- Automatische Energie- und Temperaturverwaltung in Echtzeit für das gesamte Gehäuse.
  - Der CMC überwacht den Strombedarf des Systems und unterstützt den optionalen Dynamic Power Supply Engagement (DPSE)-Modus. Dieser Modus ermöglicht es dem CMC, die Energieeffizienz zu verbessern, indem die Netzteile eingestellt werden können, während sich der Server im Standby-Modus befindet, und die Last- und Redundanzanforderungen dynamisch verwaltet werden.
  - CMC meldet den Leistungsbedarf in Echtzeit und zeichnet Hoch- und Tiefpunkte mit Zeitstempel auf.
  - Der CMC ermöglicht das Einrichten einer optionalen maximalen Gehäusestromobergrenze (Systemeingangsstromobergrenze), die warnt und Maßnahmen wie die Beschränkung des Stromverbrauchs der Server ausführt und/oder das Einschalten von neuen Servern verhindert, um das Gehäuse unter der festgelegten Stromgrenze zu halten.
  - CMC überwacht und steuert automatisch die Funktionen der Kühlungslüfter und Gebläse auf Grundlage tatsächlicher Messwerte von Umgebungs- und internen Temperaturwerten.
  - Der CMC stellt umfassende Informationen zu den Komponenten im Gehäuseinneren sowie Status- und Fehlerberichte bereit.
- CMC bietet einen Mechanismus für die zentrale Konfiguration der folgenden Elemente:
  - Netzwerk- und Sicherheitseinstellungen auf den Dell PowerEdge VRTX-Geräten.
  - Einstellungen der Stromredundanz und der Obergrenze für den Stromverbrauch.
  - E/A-Switches und iDRAC-Netzwerkeinstellungen.
  - Das erste Startgerät auf den Serverblades.
  - Konsistenzprüfungen für die E/A-Struktur zwischen dem E/A-Modul und Servern. Der CMC deaktiviert gegebenenfalls auch Komponenten, um die Systemhardware zu schützen.
  - Sicherheitsmerkmale für den Benutzerzugriff.
  - Speicherkomponenten, einschließlich des Fehlertoleranzmodus für den Speicher-Controller.
  - PCIe-Steckplätze.

Sie können den CMC so konfigurieren, dass E-Mail-Warnungen oder SNMP-Trap-Warnungen versendet werden, wenn Warnungen oder Fehler wie Temperaturen, Hardwarefehlkonfigurationen, Stromausfällen, Lüftergeschwindigkeiten und Lüfter vorliegen.

Themen:

Was ist neu in dieser Version?

Diese Version von CMC für Dell EMC PowerEdge VRTX unterstützt:

- Aktualisieren des Linux-Kernel-OpenSource-Pakets auf Version 9.4.31.
- Aktivieren der Windows-Dateifreigabeprotokollversion SMBv2 und SMBv3.
- Aktualisieren des OpenSSH-OpenSource-Pakets auf Version 7.6p1. Die für SSH erforderliche Mindestschlüssellänge beträgt 1.024 Bit.
- Steckplatznamen mit einer Länge von 24 Zeichen zur Identifizierung einzelner Server.
- Aktivieren von SNMP-Trap für die Warnung TMP8501.
- Erweitern der Struktur-FlexAddress-Konfigurationsunterstützung in der **.xml**-Gehäuseprofildatei.
- 128-Bit-Sitzungskennungen.
- 140-2-konforme Kryptographie nach Federal Information Processing Standards (FIPS).
- Firmware- und Treiber-Aktualisierung von COMMs-Karten auf Dell PowerEdge-Servern der 14. Generation.

Wichtige Funktionen

Die CMC-Funktionen werden in Verwaltungs- und Sicherheitsfunktionen eingeteilt.

Verwaltungsfunktionen

Der CMC enthält die folgenden Verwaltungsfunktionen:

- Redundante CMC-Umgebung.
- Registrierung des dynamischen Domänennamensystems (DDNS) für IPv4 und IPv6.
- Anmeldungsverwaltung und Konfiguration für lokale Benutzer, Active Directory und LDAP
- Erweiterte Kühloptionen, wie z. B. „ECM“ (Erweiterter Abkühlmodus) und „Lüfter-Offset“ können aktiviert werden, um für eine Verbesserung der Leistung eine zusätzliche Kühlung zu gewährleisten.
- Remote-Systemverwaltung und -überwachung über SNMP, eine Webschnittstelle, ein iKVM, eine Telnet- oder eine SSH-Verbindung.
- Überwachung - Zugriff auf Systeminformationen und Komponentenstatus.
- Zugriff auf Systemereignisprotokolle – Bietet Zugriff auf das Hardwareprotokoll und das Gehäuse-Protokoll.
- Firmware-Aktualisierungen für verschiedene Gehäusekomponenten – Damit können Sie die Firmware für CMC, iDRAC auf Servern, Gehäuse-Infrastruktur und Gehäusespeichern aktualisieren.

- Firmware-Aktualisierung von Server-Komponenten, wie z. B. BIOS, Netzwerk-Controller, Speicher-Controller, usw. auf mehreren Servern im Gehäuse mithilfe des Lifecycle Controller.
- Dell OpenManage Software Integration – Ermöglicht es Ihnen, die CMC-Web-Schnittstelle vom Dell OpenManage Server Administrator oder OpenManage Essentials (OME) 1.2 zu starten.
- CMC-Warnung – Warnt Sie anhand einer Remote syslog-E-Mail-Benachrichtigung oder eines SNMP-Traps über potenzielle Probleme mit verwalteten Knoten.
- Remote-Stromverwaltung – Bietet Remote-Stromverwaltungsfunktionen wie z. B. Ausschalten und Reset einer beliebigen Gehäusekomponente von einer Verwaltungskonsole aus.
- Stromverbrauchsberichte.
- SSL-Verschlüsselung (Secure Sockets Layer) – Bietet sichere Remote-Systemverwaltung über die Webschnittstelle.
- Startpunkt für die Web-Schnittstelle des Integrated Dell Remote Access Controller (iDRAC).
- Unterstützung für WS-Management.
- FlexAddress-Funktion – Ersetzt die werkseitig zugewiesenen WWN/MAC-Kennungen (World Wide Name / Media Access Control) durch gehäuseseitig zugewiesene WWN/MAC-Kennungen für einen bestimmten Steckplatz.
- Unterstützung der iDRAC-E/A-Kennungsfunktion für erweitertes WWN/MAC-Adress Inventory.
- Grafische Anzeige des Gehäusekomponentenstatus und des Funktionszustandes.
- Unterstützung für Einfach- und Mehrfach-Steckplatzserver.
- LCD-iDRAC-Konfigurationsassistent unterstützt iDRAC-Netzwerkkonfiguration.
- Einfache iDRAC-Anmeldung.
- Network Time Protocol (NTP)-Unterstützung.
- Verbesserte Server-Übersichts-, Stromberichts- und Stromsteuerungsseiten
- Erzwungenes CMC-Failover und virtuelles Neueinsetzen von Servern.
- Multi-Gehäuseverwaltung, wodurch bis zu acht weitere Gehäuse vom Hauptgehäuse aus sichtbar sind.
- Speicherkomponenten im Gehäuse konfigurieren
- Ordnet den Servern und deren Identifikation Steckplätze zu.

Sicherheitsfunktionen

Der CMC bietet die folgenden Sicherheitsfunktionen:

- Sicherheitsverwaltung auf Kennwortebene – Verhindert den unberechtigten Zugriff auf ein Remote-System.
- Zentralisierte Benutzerauthentifizierung durch:
  - Verwendung des Active Directory-Standardschemas oder eines erweiterten Schemas (optional).
  - Hardware-gespeicherte Benutzer-IDs und Kennwörter.
- Rollenbasierte Autorität – Ermöglicht es einem Administrator, spezifische Berechtigungen für jeden Benutzer zu konfigurieren.
- Benutzer-ID- und Kennwort-Konfiguration über die Web-Schnittstelle. Die Web-Schnittstelle unterstützt 128-Bit-SSL 3.0-Verschlüsselung und 40-Bit-SSL 3.0-Verschlüsselung (für Länder, in denen 128-Bit nicht zulässig ist).

  ANMERKUNG: Telnet unterstützt keine SSL-Verschlüsselung.
- Konfigurierbare IP-Schnittstellen (falls zutreffend).
- Beschränkung der Anmeldungsfehlversuche pro IP-Adresse, mit Anmeldungsblockierung der IP-Adresse, wenn die Grenze überschritten wird.
- Konfigurierbare automatische Sitzungszeitüberschreitung und mehrere gleichzeitige Sitzungen.
- Beschränkter IP-Adressenbereich für Clients, die an den CMC angeschlossen werden.
- Secure Shell (SSH), die eine verschlüsselte Schicht für höhere Sicherheit verwendet.
- Einfache Anmeldung, Zweifaktor-Authentifizierung und Authentifizierung mit öffentlichem Schlüssel.

Gehäuseübersicht

Die Abbildung hier zeigt eine Ansicht der CMC-Verbindungen.

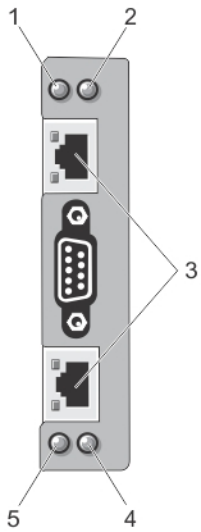


Abbildung 1. CMC-Verbindungen und LEDs

Tabelle 1. CMC-Verbindungen und LEDs

Element	Anzeige, Taste oder Anschluss
1	Status-/Identifikationsanzeiger (CMC 1)
2	Stromanzeiger (CMC 1)
3	CMC-Verbindungsschnitstellen (2)
4	Stromanzeiger (CMC 2)
5	Status-/Identifikationsanzeiger (CMC 2)

Hier wird eine Rückansicht des Gehäuses mit einer Tabelle angezeigt, die die Teile und Geräte, die im CMC verfügbar sind, auflistet.

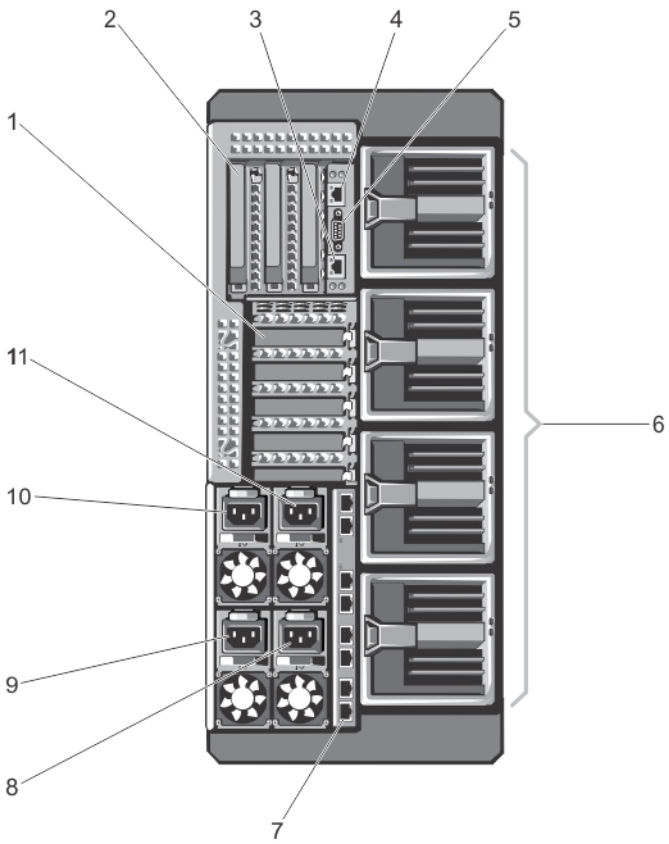


Abbildung 2. CMC-Rückseite

Tabelle 2. CMC-Rückseite – Teile

Element	Anzeige, Taste oder Anschluss
1	PCIe-Erweiterungskartensteckplätze (niedriges Profil) (5)
2	PCIe-Erweiterungskartensteckplätze mit voller Bauhöhe (3)
3	CMC GB Ethernet-Port (CMC-2)
4	CMC GB Ethernet-Port (CMC-1)
5	Serieller Konnektor
6	Lüftermodule (4)
7	E/A-Modulschnittstellen
8	Netzteil 4
9	Netzteil 3
10	Netzteil 1
11	Netzteil 2

Hier wird eine Vorderansicht des Gehäuses mit einer Tabelle angezeigt, die die Teile und Geräte, die im CMC verfügbar sind, auflistet.

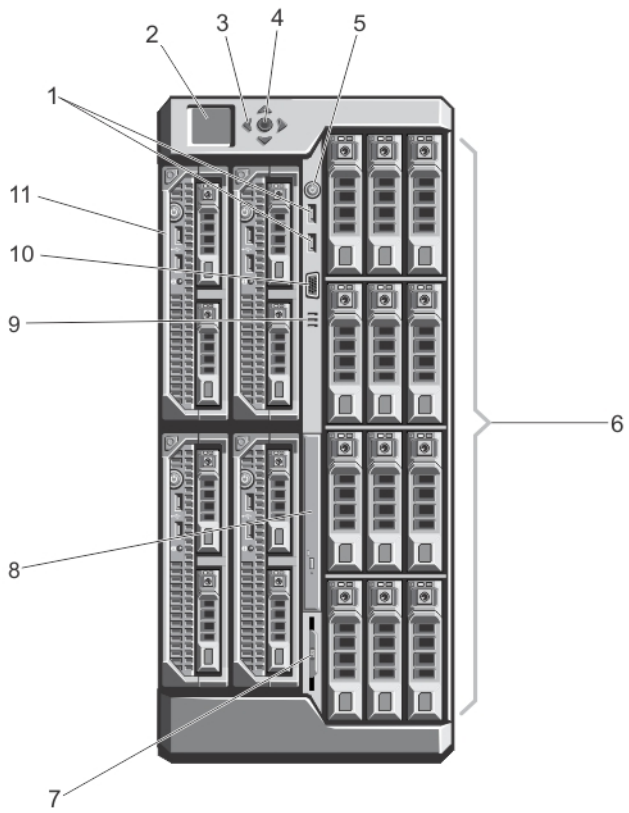


Abbildung 3. Merkmale und Anzeigen auf der Vorderseite – Gehäuse für 3,5-Zoll-Festplattenlaufwerke

Tabelle 3. Vorderseite – Funktionen und Anzeigen

Element	Anzeige, Taste oder Anschluss	Beschreibung
1	USB-Anschlüsse (2)	Ermöglichen das Anschließen von Tastatur und Maus am System.
2	LCD-Display	Zeigt Systeminformationen sowie Status- und Fehlermeldungen an, die darüber informieren, ob das System ordnungsgemäß funktioniert oder überprüft werden muss.
3	LCD-Menü Scrolltasten (4)	Bewegt den Cursor schrittweise vorwärts.
4	Auswahlschaltfläche zum Markieren	Wählt und speichert ein Element auf dem LCD-Bildschirm und wechselt zum nächsten Bildschirm.
5	Betriebsanzeige, Netzschalter des Gehäuses	Die Betriebsanzeige leuchtet, wenn das Gehäuse eingeschaltet ist. Der Betriebsschalter steuert die Ausgabe des Netzteils an das System.
6	Festplattenlaufwerke (HDD)	**2,5-Zoll-Festplattenlaufwerksgehäuse**: Bis zu 25 hot-swap-fähige 2,5-Zoll-Festplattenlaufwerke. **3,5-Zoll-Festplattenlaufwerksgehäuse**: Bis zu zwölf hot-swap-fähige 3,5-Zoll-Festplattenlaufwerke.
7	Informationsbereich	Ein ausziehbares Etikettenfeld, auf dem Sie nach Bedarf Systeminformationen wie die Service-Tag-Nummer, NIC, MAC-Adresse, Angaben zum elektrischen Verbrauch des Systems und Markierungen der Worldwide-Zulassungsbehörde verzeichnen können.
8	Optisches Laufwerk (optional)	Ein optionales SATA-DVD-ROM-Laufwerk oder -DVD+/-RW-Laufwerk

Element	Anzeige, Taste oder Anschluss	Beschreibung
9	Belüftungsöffnungen	Belüftungsöffnungen für die Temperatursensoren. **ANMERKUNG: Um eine ordnungsgemäße Kühlung zu gewährleisten, stellen Sie sicher, dass die Belüftungsöffnungen nicht blockiert sind.**
10	Bildschirmanschluss	Ermöglicht das Anschließen eines Bildschirms am System.
11	Servermodule	Bis zu vier PowerEdge M520-, M620-, M630- oder M640-Servermodule oder zwei M820-Servermodule, die speziell für das Gehäuse konfiguriert wurden.

Minimale CMC-Version

Die folgende Tabelle listet die minimal erforderliche CMC-Version zur Aktivierung der aufgelisteten Servermodule auf.

Tabelle 4. Minimale CMC-Version für Servermodule

Server	Minimale Version von CMC
PowerEdge M520	CMC 1.36
PowerEdge M620	CMC 1.36
PowerEdge M820	CMC 1.36
PowerEdge M630	CMC 2.00
PowerEdge M830	CMC 2.00
PowerEdge M640	CMC 3.00

Die folgende Tabelle listet die minimal erforderliche CMC-Version zur Aktivierung der aufgelisteten E/A-Module auf.

Tabelle 5. Minimale CMC-Version für E/A-Module

EAM-Switches	Minimale Version von CMC
R1 VRTX 1 GB-Passthrough	CMC 1.20
1-GbE-Switch R1-2401 VRTX	CMC 1.20
10-GB-Switch R1-2210 VRTX	CMC 2.00

Unterstützte Remote-Zugriffsverbindungen

Die folgende Tabelle führt die unterstützten Remote Access Controller auf.

Tabelle 6. Unterstützte Remote-Zugriffsverbindungen

Verbindung	Funktionen
CMC-Netzwerkschnittstellen	• GB-Schnittstelle: Dedizierte Netzwerkschnittstelle für die CMC-Webschnittstelle. • DHCP-Unterstützung. • SNMP-Traps und E-Mail-Ereignisbenachrichtigung. • Netzwerkschnittstelle für den iDRAC und E/A-Module (EAMs)

Verbindung	Funktionen
	• Unterstützung für die Telnet/SSH-Befehlskonsole und RACADM CLI-Befehle einschließlich Systemstart-,Reset-, Hochfahren-, und Herunterfahren-Befehle.
Serielle Schnittstelle	• Unterstützung für serielle Konsolen- und RACADM-CLI-Befehle einschließlich Systemstart-, Reset-, Hochfahren- und Herunterfahren-Befehle. • Unterstützung für binären Austausch für Anwendungen, die speziell dafür vorgesehen sind, über ein Binärprotokoll mit einem bestimmten Typ von E/A-Modulen zu kommunizieren. • Die serielle Schnittstelle kann mit dem Befehl connect (oder racadm connect) intern an die serielle Konsole eines Servers oder E/A-Moduls angeschlossen werden. • Ermöglicht Zugriff nur auf das aktive CMC.

Unterstützte Plattformen

CMC unterstützt modulare Server, die für die PowerEdge VRTX-Plattform konzipiert sind. Informationen zur Kompatibilität von CMC finden Sie in der Dokumentation Ihres Geräts.

Informationen über die derzeit unterstützten Plattformen finden Sie in den *Dell Chassis Management Controller (CMC) Version 3.0 for Dell PowerEdge VRTX Release Notes* (Versionshinweisen zu Dell Chassis Management Controller (CMC) Version 3.0 für Dell PowerEdge VRTX), die unter **dell.com/support/manuals** verfügbar sind.

Unterstützte Web-Browser

Die folgenden Webbrowser werden für Dell PowerEdge VRTX unterstützt:

- Microsoft Internet Explorer 11
- Microsoft EDGE
- Safari Version 8.0.8
- Safari Version 9.0.3
- Mozilla Firefox 57
- Mozilla Firefox 58
- Google Chrome 62
- Google Chrome 63

ANMERKUNG: TLS 1.1 und TLS 1.2 werden in dieser Version standardmäßig unterstützt. Um jedoch TLS 1.0 zu aktivieren, müssen Sie den folgenden racadm-Befehl verwenden:

```
$ racadm config -g cfgRacTuning -o cfgRacTuneTLSProtocolVersionEnable TLSv1.0+
```

Lizenzenverwaltung

Die CMC-Funktionen richten sich nach der erworbenen Lizenz (CMC Express oder CMC Enterprise). Über die Schnittstellen können Sie nur auf lizenzierte Funktionen zugreifen, über die Sie CMC konfigurieren oder verwenden können. Dazu gehören z. B. die CMC-Web-Schnittstelle, RACADM, WS-MAN, usw. Die Lizenzverwaltung und die Firmware-Aktualisierungsfunktion unter CMC können immer über die CMC-Web-Schnittstelle und RACADM aufgerufen werden.

Lizenztypen

Die folgenden Lizenztypen sind verfügbar:

- 30-Tage-Testversion und Verlängerung – Diese Lizenz läuft nach 30 Tagen ab und kann um 30 weitere Tage verlängert werden. Evaluierungslizenzen sind zeitlich begrenzt. Die Zeit, die für die Evaluierung zur Verfügung steht, reduziert sich sukzessive, wenn das System eingeschaltet ist.
- Dauerlizenz – Die Lizenz ist an die Service-Tag-Nummer gebunden und damit dauerhaft.

Lizenzen anfordern

Verwenden Sie zum Anfordern von Lizenzen eines der folgenden Verfahren:

- E-Mail – Die Lizenz ist an eine E-Mail angehängt, die nach der Anforderung der Lizenz durch das technische Support Center versendet wird.
- Selbstbedienungs-Portal – In CMC wird ein Link zum Selbstbedienungs-Portal angezeigt. Klicken Sie auf diesen Link, um das internetbasierte Selbstbedienungs-Portal für die Lizenzierung aufzurufen. Hier können Sie die gewünschten Lizenzen erwerben. Weitere Informationen finden Sie in der Online-Hilfe für das Selbstbedienungs-Portal.
- Point-of-sale – Die Lizenz wird im Rahmen der Systembestellung angefordert.

Lizenzvorgänge

Bevor Sie die Lizenzverwaltungsschritte ausführen, müssen Sie sicherstellen, dass Sie die erforderlichen Lizenzen besitzen. Weitere Informationen finden Sie unter Überblicks- und Funktionshandbuch unter support.dell.com.

Sie können die folgenden Lizenzvorgänge unter Verwendung von CMC, RACADM und WS-MAN für eine 1-zu-1-Lizenzverwaltung und unter Verwendung von Dell License Manager für eine 1-zu-n-Lizenzverwaltung ausführen:

ANMERKUNG: Sollten Sie ein System erworben haben, auf dem sämtliche Lizenzen bereits vorinstalliert sind, ist eine Lizenzverwaltung nicht erforderlich.

- Ansicht – Zeigen Sie die aktuellen Lizenzinformationen an.
- Importieren – Nachdem Sie die Lizenz erhalten haben, speichern Sie die Lizenz auf einen lokalen Speicher, und importieren Sie sie über eine unterstützte Schnittstelle nach CMC. Die Lizenz wird importiert, wenn Sie die Validierungsprüfungen bestanden hat.

  ANMERKUNG: Bei einigen neuen Funktionen ist für die Aktivierung dieser Funktionen ein CMC-Neustart erforderlich.
- Exportieren – Exportieren Sie die installierte Lizenz zu Sicherungszwecken oder für eine spätere Neuinstallation nach einem Austausch eines Service-Teils auf ein externes Speichergerät. Der Dateiname und das Format der exportieren Lizenz lauten wie folgt: <EntitlementID>.xml.
- Löschen – Löschen Sie die Lizenz, die mit einer Komponente verknüpft ist, wenn diese Komponente nicht vorhanden ist. Nach dem Löschen der Lizenz wird diese nicht mehr auf CMC gespeichert, und die Basisproduktfunktionen werden aktiviert.
- Ersetzen – Ersetzen Sie die Lizenz, um eine Evaluierungslizenz zu verlängern, um einen Lizenztyp zu ändern, z. B. eine Evaluierungslizenz in eine erworbene Lizenz, oder um eine abgelaufene Lizenz zu verlängern.
- Eine Evaluierungslizenz kann durch eine umfangreichere Evaluierungslizenz oder eine erworbene Lizenz ersetzt werden.
- Eine erworbene Lizenz kann durch eine aktualisierte Lizenz oder durch eine umfangreichere Lizenz ersetzt werden. Für weitere Informationen zu Lizenzen klicken Sie auf Dell Software License Management Portal.
- Weitere Informationen – Hier finden Sie weitere Informationen zur installierten Lizenz oder zu den Lizenzen, die für eine auf dem Server installierte Komponente verfügbar sind.

  ANMERKUNG: Damit die Option „Weitere Informationen“ die korrekte Seite anzeigt, stellen Sie sicher, dass Sie *.dell.com zur Liste der vertrauenswürdigen Sites in den Sicherheitseinstellungen hinterlegen. Weitere Informationen finden Sie in der Internet Explorer-Online-Dokumentation.

Status und Zustand von Lizenzkomponenten und verfügbare Optionen

In der folgenden Tabelle wird die Liste der verfügbaren Lizenzvorgänge auf der Basis des Status oder des Zustands der Lizenz angezeigt.

Tabelle 7. Lizenzvorgänge auf der Basis des Status oder des Zustands

Status oder Zustand von Lizenz/Komponente	Importieren	Exportieren	„Löschen“	Ersetzen	Mehr erfahren
Nicht-Administrator-Anmeldung	Nein	Ja	Nein	Nein	Ja
Aktive Lizenz	Ja	Ja	Ja	Ja	Ja
Abgelaufene Lizenz	Nein	Ja	Ja	Ja	Ja
Lizenz installiert, jedoch fehlt Komponente	Nein	Ja	Ja	Nein	Ja

Lizenzen über die CMC-Webschnittstelle verwalten

Um Lizenzen über die iDRAC7-Webschnittstelle zu verwalten, gehen Sie zu **Gehäuseübersicht** > **Setup** > **Lizenzen**.

Stellen Sie vor dem Importieren einer Lizenz sicher, dass Sie eine gültige Lizenzdatei auf dem lokalen System bzw. auf einer Netzwerkfreigabe, die für den CMC zugänglich ist, gespeichert haben. Die Lizenz ist entweder integriert oder wird Ihnen per E-Mail vom **Selbstbedienungs-Internetportal** oder über das Tool für die Lizenzschlüsselverwaltung zugestellt.

Daraufhin werden auf der Seite **Lizenzen** die Lizenzen angezeigt, die mit den Geräten verknüpft sind, oder jene Lizenzen, die zwar installiert sind, für die das entsprechende Gerät im System jedoch nicht vorhanden ist. Weitere Informationen zum Importieren, Exportieren, Löschen oder Ersetzen einer Lizenz finden Sie in der *Online-Hilfe*.

Lizenzen über RACADM verwalten

Um Lizenzen under der Verwendung von RACADM-Befehlen zu verwalten, verwenden Sie den folgenden Lizenz-Unterbefehl.

```
racadm license <Lizenzbefehltyp>
```

Weitere Informationen zu RACADM-Befehlen finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX), verfügbar unter dell.com/support/manuals.

Lizenzierbare Funktionen in CMC

Eine Liste der CMC-Funktionen, die aufgrund Ihrer Lizenz aktiviert wurden, wird in dieser Tabelle angegeben.

Tabelle 8. Lizenzierbare Funktionen

Funktion	Express	Enterprise	Anmerkungen
CMC-Netzwerk	Ja	Ja	
Serielle CMC-Schnittstelle	Ja	Ja	
RACADM (SSH, Lokal und Remote)	Ja	Ja	
CMC-Setup-Backup	Nein	Ja	
CMC-Setup-Wiederherstellung	Ja	Ja	
WS-MAN	Ja	Ja	
SNMP	Ja	Ja	
Telnet	Ja	Ja	
SSH	Ja	Ja	
Internet-basierte Schnittstelle	Ja	Ja	
E-Mail-Warnungen	Ja	Ja	
LCD-Bereitstellung	Ja	Ja	
Erweiterte iDRAC-Verwaltung	Ja	Ja	
Remote-Syslog	Nein	Ja	
Verzeichnisdienste	Nein*	Ja	*Für Nicht-Standardverzeichnisdiensteinstellungen ist nur „Verzeichnisdienste zurücksetzen“ mit Express-Lizenz erlaubt. „Verzeichnisdienste zurücksetzen“ setzt die Verzeichnisdienste auf Werkseinstellung zurück.
Einfache iDRAC-Anmeldung.	Nein	Ja	
Zweifaktor-Authentifizierung	Nein	Ja	
PK-Authentifizierung	Nein	Ja	
Remote-Dateifreigabe	Ja	Ja	
Steckplatz-Resourcen-Verwaltung	Nein	Ja	
Gehäuseebenen-Stromobergrenzen	Nein*	Ja	*Für Nicht-Standard-Stromobergrenzeneinstellungen ist nur „Stromobergrenzen zurücksetzen“ mit der Express-Lizenz erlaubt. „Stromobergrenzen zurücksetzen“ setzt die Stromobergrenzen auf die Werkseinstellungen zurück.
Dynamische Netzteil-Einsatzfähigkeit	Nein*	Ja	*Für Nicht-Standard-DPSE-Einstellungen ist nur „DPSE zurücksetzen“ mit einer Express-Lizenz erlaubt. „DPSE zurücksetzen“ setzt DPSE auf die Werkseinstellungen zurück.

Funktion	Express	Enterprise	Anmerkungen
Verwaltung von mehreren Gehäusen	Nein	Ja	
Erweiterte Konfiguration	Nein	Ja	
Gehäuse-Ebenen-Backup	Nein	Ja	
FlexAddress-Aktivierung	Nein*	Ja	*Für Nicht-Standard-FlexAddress-Einstellungen ist nur „Standardeinstellung zurücksetzen“ mit der Express-Lizenz erlaubt. „Standardeinstellung zurücksetzen“ setzt die FlexAddress-Einstellungen auf die Werkseinstellungen zurück.
PCIe-Adapter-Zuordnungen	Ja*	Ja	*Maximal zwei PCIe-Adapter können pro Server mit einer Express-Lizenz zugewiesen werden.
Virtueller Adapter zu Steckplatz-Zuordnung	Nein*	Ja	*Für Nicht-Standard-Zuordnung von Virtual Adaptern ist nur die Standardzuordnung mit einer Express-Lizenz erlaubt. „Standardeinstellung zurücksetzen“ setzt die Zuordnung des virtuellen Adapters auf die Werkseinstellungen zurück.
Virtueller Adapter zu Steckplatz-Zuordnung aufheben	Ja	Ja	
Erstellen von Server-Klonen	Nein	Ja	
Eins-zu-viele-Server-Firmware-Aktualisierungen	Nein	Ja	
Eins-zu-viele-Konfiguration für iDRAC	Nein	Ja	
Startidentität	Nein	Ja	
Gehäuseprofil	Nein	Ja	
Quick Deploy	Nein	Ja	

Lokalisierte Versionen der CMC-Webschnittstelle anzeigen

Um lokalisierte Versionen der CMC-Webschnittstelle anzuzeigen, lesen Sie sich die Dokumentation Ihres Web-Browsers durch.

Unterstützte Verwaltungskonsolenanwendungen

CMC unterstützt die Integration mit Dell OpenManage-Konsole. Weitere Informationen finden Sie in der Dokumentation der OpenManage-Konsole unter **dell.com/support/manuals**.

Verwendung dieses Handbuchs

Der Inhalt dieses Benutzerhandbuchs ermöglicht es Ihnen, die Tasks auszuführen, indem Sie Folgendes verwenden:

- Die Webschnittstelle: Hier erhalten Sie nur aufgabenbezogene Informationen. Weitere Informationen zu den Feldern und Optionen finden Sie in der *CMC for Dell PowerEdge VRTX Online Help* (Online-Hilfe für den CMC für Dell PowerEdge VRTX), die Sie über die Webschnittstelle öffnen können.

- Die RACADM-Befehle: Hier finden Sie den RACADM-Befehl oder das Objekt, den bzw. das Sie verwenden müssen. Weitere Informationen zu einem RACADM-Befehl finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX), das unter **dell.com/cmcmanuals** verfügbar ist.

Weitere nützliche Dokumente

So greifen Sie auf die Dokumente der Dell Support-Website zu: Zusammen mit diesem Referenzhandbuch können Sie auf die folgenden Anleitungen zugreifen, die unter **dell.com/support/manuals** zur Verfügung stehen.

- Die *VRTX CMC-Online-Hilfe* enthält Informationen zur Verwendung der Webschnittstelle. Klicken Sie für den Zugriff auf die Online-Hilfe in der CMC-Webschnittstelle auf **Hilfe**.
- Im *Chassis Management Controller Version 3.0 for Dell PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller Version 3.0 für PowerEdge VRTX) finden Sie Informationen zur Verwendung der RACADM-Funktionen, die mit VRTX in Beziehung stehen.
- Die *Versionshinweise zu Dell Chassis Management Controller (CMC) für Dell PowerEdge VRTX Version 3.0*, verfügbar unter **dell.com/cmcmanuals**, enthalten den letzten Stand der Änderungen am System oder an der Dokumentation bzw. erweitertes technisches Referenzmaterial für erfahrene Benutzer oder Techniker.
- Im *Integrated Dell Remote Access Controller (iDRAC)*-Benutzerhandbuch finden Sie Informationen zur Installation, Konfiguration und Wartung des iDRACs auf verwalteten Systemen.
- Die *Dell PowerEdge VRTX-Speicher-Subsystem-Kompatibilitäts-Matrix* bietet Informationen über die Baseline-Versionen für das PowerEdge VRTX-Speichersubsystem. Dieses Dokument ist online unter **dell.com/support/manuals** verfügbar.
- Das *Dell OpenManage Server Administrator-Benutzerhandbuch* enthält Informationen über die Installation und Anwendung von Server Administrator.
- Das *Dell OpenManage SNMP-Referenzhandbuch für iDRAC und Chassis Management Controller* enthält Informationen über SNMP-MIBs.
- Das *Benutzerhandbuch zu den Dell Update Packages* enthält Informationen über das Abrufen und Verwenden von Dell Update Packages als Teil Ihrer Systemaktualisierungsstrategie.
- Das *Dell Shared PowerEdge RAID Controller (PERC) 8 User's Guide* (Dell freigegebene PowerEdge-Benutzerhandbuch für RAID-Controller (PERC) 8) enthält Informationen zur Bereitstellung der freigegebenen PERC 8-Karte und zur Verwaltung des Speicheruntersystems. Dieses Dokument steht online unter **dell.com/storagecontrollermanuals** zur Verfügung.
- Die Dokumentation zur Dell-Systemverwaltungsanwendung enthält Informationen über das Installieren und Verwenden der Systemverwaltungssoftware.

Die folgenden Systemdokumente enthalten weitere Informationen über das System, auf dem VRTX CMC installiert ist:

- 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.
- Das *Dell PowerEdge VRTX Getting Started Guide* – Dell PowerEdge VRTX-Handbuch zum Einstieg), das mit Ihrem System geliefert wurde, enthält eine Übersicht über die Systemfunktionen, die Einrichtung des Systems und technische Daten.
- Das Setup-Platzset, das mit Ihrem System geliefert wurde, enthält Informationen über die Systemersteinrichtung und Konfiguration.
- Das Owner's Manual (Benutzerhandbuch) des Servermoduls gibt Informationen über die Funktionen des Servermoduls an, beschreibt den Fehlerbehebungsvorgang für das Servermodul und das Installieren oder Austauschen der Komponenten des Servermoduls. Dieses Dokument steht online unter **dell.com/poweredgemanuals** zur Verfügung.
- In der zusammen mit der Rack-Lösung gelieferten Rack-Dokumentation ist beschrieben, wie das System in einem Rack installiert wird.
- Die vollständigen Namen der in diesem Dokument verwendeten Abkürzungen und Akronyme finden Sie im Glossar unter **dell.com/support/manuals**.
- In der Dokumentation zur Systemverwaltungssoftware sind die Merkmale, die Anforderungen, die Installation und die grundlegende Funktion der Software beschrieben.
- Die Dokumentation für alle separat erworbenen Komponenten enthält Informationen zur Konfiguration und zur Installation dieser Optionen.
- Alle im Lieferumfang des Systems enthaltenen Medien mit Dokumentationen und Hilfsmitteln zur Konfiguration und Verwaltung des Systems, insbesondere in Bezug auf Betriebssystem, Systemverwaltungssoftware, System-Updates und mit dem System erworbene Komponenten. Weitere Informationen über das System finden Sie über den Quick Resource Locator (QRL) auf Ihrem System und in der System-Setup-Übersicht, die im Lieferumfang Ihres Systems enthalten ist. Laden Sie die QRL-Anwendung von Ihrer mobilen Plattform herunter, um die Anwendung auf Ihrem mobilen Gerät zu aktivieren.

Zugriff auf Dokumente von der Dell EMC Support-Website

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

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

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

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

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

2

Installation und Setup des CMC

Dieser Abschnitt enthält Informationen darüber, wie die CMC-Hardware installiert, der Zugriff auf den CMC eingerichtet und die Verwaltungsumgebung zur Verwendung des CMC konfiguriert wird und führt Sie durch die Tasks zum Konfigurieren eines CMC:

- Anfänglichen Zugriff auf den CMC einrichten.
- Über ein Netzwerk auf den CMC zugreifen.
- CMC-Benutzer hinzufügen und konfigurieren.
- Aktualisieren der CMC-Firmware

Weitere Informationen zur Installation und Einrichtung redundanter CMC-Umgebungen finden Sie unter Redundante CMC-Umgebung verstehen.

Themen:

Bevor Sie beginnen

Laden Sie die neueste Version der CMC-Firmware für PowerEdge VRTX von **dell.com/support/** herunter, bevor Sie die CMC-Umgebung einrichten.

Stellen Sie zudem sicher, dass Sie die DVD *Dell Systems Management Tools and Documentation* haben, die zum Lieferumfang Ihres Systems gehört.

Installieren der CMC-Hardware

Der CMC ist in Ihrem Gehäuse vorinstalliert und es ist demzufolge keine Installation erforderlich. Sie können einen zweiten CMC installieren und diesen als Standby-CMC zum aktiven CMC ausführen.

Prüfliste zur Gehäusegruppen-Einrichtung

Mit den folgenden Tasks können Sie das Gehäuse korrekt einrichten:

1 Der für den CMC und die Management Station verwendete Browser muss sich in demselben Netzwerk befinden, das als das Verwaltungsnetzwerk bezeichnet wird. Verbinden Sie ein Ethernet-Netzwerkkabel von der aktiven CMC-Schnittstelle mit dem Verwaltungsnetzwerk.

2 Installieren Sie das E/A-Modul in das Gehäuse und verbinden Sie das Netzwerkkabel mit dem Gehäuse.

3 Schieben Sie die Server in das Gehäuse ein.

4 Schließen Sie das Gehäuse an der Stromquelle an.

5 Betätigen Sie den Netzschalter oder schalten Sie das Gehäuse von der CMC-Webschnittstelle an, nachdem Sie den Task in Schritt 7 abgeschlossen haben.

ANMERKUNG: Schalten Sie die Server nicht ein.

6 Navigieren Sie unter Verwendung des LCD-Bereichs zur IP-Übersicht, und klicken Sie zur Auswahl auf die Schaltfläche zum Markieren. Verwenden Sie die IP-Adresse für den CMC im Browser des Verwaltungssystems (IE, Chrome oder Mozilla). Um DHCP für CMC einzurichten, verwenden Sie den LCD-Bereich, um auf **Hauptmenü** > **Einstellungen** > **Netzwerkeinstellungen** zu klicken.

7 Stellen Sie unter Verwendung des Webbrowsers eine Verbindung mit der CMC-IP-Adresse her, indem Sie den Standardbenutzernamen (root) und das Kennwort (calvin) verwenden.

8 Geben Sie jedem iDRAC eine IP-Adresse in der CMC-Webschnittstelle und aktivieren Sie die LAN- und IPMI-Schnittstelle.

ANMERKUNG: Auf manchen Servern ist die iDRAC-LAN-Schnittstelle standardmäßig deaktiviert. Diese Information kann auf der CMC-Webschnittstelle unter Server-Übersicht > Setup gefunden werden. Dies könnte eine erweiterte Lizenzoption sein, in welchem Falle Sie die Setup-Funktion für jeden Server verwenden müssen.

9 Geben Sie dem E/A-Modul in der CMC-Webschnittstelle eine IP-Adresse. Sie können die IP-Adresse durch Klicken auf **E/A-Modulübersicht** und dann auf **Setup** erhalten.

10 Stellen Sie über den Webbrowser eine Verbindung mit jedem iDRAC her und nehmen Sie die endgültige Konfiguration des iDRAC vor. Der Standardbenutzername ist `root` und das Kennwort lautet `calvin`.

11 Stellen Sie unter Verwendung des Webbrowsers eine Verbindung mit jedem E/A-Modul her und nehmen Sie die endgültige Konfiguration der E/A-Module vor.

12 Schalten Sie die Server ein und installieren Sie das Betriebssystem.

ANMERKUNG: Der CMC wird neu gestartet, wenn das Bedienfeld nicht ordnungsgemäß am Gehäuse installiert ist.

CMC-Basisnetzwerkverbindung

Um eine höchstmögliche Redundanz zu erzielen, verbinden Sie jeden verfügbaren CMC mit dem Verwaltungsnetzwerk.

Remote-Zugriffssoftware auf einer Management Station installieren

Sie können von einer Management Station aus mithilfe von Remote-Zugriffssoftware, wie z. B. Telnet, Secure Shell (SSH), über betriebssystemseitig bereitgestellte serielle Konsolendienstprogramme oder über die Webschnittstelle auf den CMC zugreifen.

Um Remote-RACADM von Ihrer Management Station zu verwenden, installieren Sie Remote-RACADM unter Verwendung der DVD *Dell Systems Management Tools and Documentation*, die für Ihr System erhältlich ist. Diese DVD enthält die folgenden Dell OpenManage-Komponenten:

- DVD-Stammverzeichnis - Enthält das Dell Systems Build- und Update-Hilfsprogramm.
- SYSMGMT – Enthält die Systems Management-Softwareprodukte einschließlich Dell OpenManage Server Administrator.
- Docs – Enthält Dokumentation für Systeme, Systems Management Softwareprodukte, Peripheriegeräte und RAID-Controller.

- SERVICE – Enthält die Hilfsprogramme, die Sie benötigen, um das System zu konfigurieren, und die neuesten Diagnosehilfsmittel und Dell-optimierte Treiber für das System.

Informationen zur Installation von Dell OpenManage-Softwarekomponenten finden Sie im auf der DVD verfügbaren *Dell OpenManage Installation and Security User's Guide* (Dell OpenManage-Installation und Sicherheit-Benutzerhandbuch) oder unter **dell.com/support/manuals**. Sie können die neueste Version der Dell DRAC Tools unter **support.dell.com** herunterladen.

RACADM auf einer Linux-Management Station installieren

1 Melden Sie sich als „root“ bei einem System unter dem Red Hat Enterprise Linux- oder SUSE Linux Enterprise Server-Betriebssystem an, auf dem Sie die Komponenten des verwalteten Systems installieren möchten.

2 Legen Sie die DVD *Dell Systems Management Tools and Documentation* in das DVD-Laufwerk ein.

3 Um die DVD am erforderlichen Standort bereitzustellen, verwenden Sie den Befehl mount oder einen ähnlichen Befehl.

ANMERKUNG: Auf dem Red Hat Enterprise Linux 5-Betriebssystem werden DVDs automatisch mit der Ladeoption –`noexec mount` geladen. Diese Option erlaubt Ihnen nicht, beliebige ausführbare Datei von der DVD auszuführen. Sie müssen die DVD-ROM manuell laden und dann die Befehle ausführen.

4 Navigieren Sie zum Verzeichnis **SYSMGMT/ManagementStation/linux/rac**. Geben Sie den folgenden Befehl ein, um die RAC-Software zu installieren:

```
rpm -ivh *.rpm
```

5 Um Hilfe zum RACADM-Befehl zu erhalten, geben Sie nach der Eingabe der vorherigen Befehle `racadm help` ein. Weitere Informationen über RACADM finden Sie im *Chassis Management Controller for Dell PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

ANMERKUNG: Wenn Sie die RACADM-Remote-Fähigkeit verwenden, müssen Sie über Schreibberechtigung in den Ordnern verfügen, in denen Sie die RACADM-Unterbefehle verwenden, die sich auf Dateivorgänge beziehen, z.B.: `racadm getconfig -f <file name>`

RACADM von einer Linux Management Station deinstallieren

1 Melden Sie sich als `root` beim System an, auf dem die Funktionen der Management Station deinstalliert werden sollen.

2 Führen Sie den rpm-Abfragebefehl aus, um zu bestimmen, welche Version der DRAC-Hilfsprogramme installiert ist:

```
rpm -qa | grep mgmtst-racadm
```

3 Überprüfen Sie die zu deinstallierende Paketversion und deinstallieren Sie die Funktion unter Verwendung des Befehls `rpm -e rpm -qa | grep mgmtst-racadm`.

Einen Webbrowser konfigurieren

Sie können den CMC und die im Gehäuse installierten Server und Module über einen Webbrowser konfigurieren und verwalten. Lesen Sie den Abschnitt „Unterstützte Webbrowser“ in der *Dell Systems Software Support Matrix* unter **dell.com/support/manuals**.

Der für den CMC und die Management Station verwendete Browser muss sich in demselben Netzwerk befinden, das als das *Verwaltungsnetzwerk* bezeichnet wird. Basierend auf Ihren Sicherheitsanforderungen kann das Verwaltungsnetzwerk ein eigenständiges Hochsicherheitsnetzwerk sein.

ANMERKUNG: Sie müssen sicherstellen, dass Sicherheitsmaßnahmen im Verwaltungsnetzwerk, wie Firewalls und Proxyserver, den Webbrowser nicht daran hindern, auf CMC zuzugreifen.

Bedenken Sie auch, dass Browserfunktionen die Konnektivität oder Leistung beeinträchtigen können, insbesondere dann, wenn das Verwaltungsnetzwerk keinen Internetzugang hat. Wenn auf der Management Station ein Windows-Betriebssystem ausgeführt wird, gibt es Internet Explorer-Einstellungen, die die Konnektivität beeinträchtigen können, selbst wenn Sie für den Zugriff auf das Verwaltungsnetzwerk eine Befehlszeilenschnittstelle verwenden.

ANMERKUNG: Um Sicherheitsrisiken zu beheben, überwacht Microsoft Internet Explorer streng die Zeit bei seiner Cookieverwaltung. Um dies zu unterstützen, muss die Computerzeit, die auf dem Internet Explorer ausgeführt wird, mit der Zeit auf dem CMC synchronisiert werden.

Proxy-Server

Um einen Proxy-Server zu durchsuchen, der keinen Zugriff auf das Verwaltungsnetzwerk hat, können Sie die Verwaltungsnetzwerkadresse zur Ausnahmenliste des Browsers hinzufügen. Dies weist den Browser an, den Proxy-Server beim Zugriff auf das Verwaltungsnetzwerk zu umgehen.

Internet Explorer

So bearbeiten Sie die Ausnahmeliste in Internet Explorer:

1 Starten Sie den Internet Explorer.
2 Klicken Sie auf **Tools** > **Internet-Optionen** > **Verbindungen**.
3 Klicken Sie im Abschnitt **LAN-Einstellungen** auf **LAN-Einstellungen.**
4 Wählen Sie unter **Proxy-Server** die Option **Proxy-Server für Ihr LAN verwenden (Diese Einstellungen gelten nicht für DFÜ- oder VPN-Verbindungen)** aus und klicken Sie dann auf **Erweitert**.
5 Fügen Sie im Abschnitt **Ausnahmen** die Adressen für die CMCs und iDRACs im Verwaltungsnetzwerk unter Verwendung des Semikolons als Trennzeichen zur Liste hinzu. Sie können DNS-Namen und Platzhalter in Ihren Einträgen verwenden.

Mozilla Firefox

So bearbeiten Sie die Ausnahmeliste in Mozilla Firefox Version 19.0:

1 Mozilla Firefox starten.
2 Klicken Sie auf **Tools** > **Optionen** (für Systeme, die Windows ausführen) oder klicken Sie auf **Bearbeiten** > **Einstellungen** (für Systeme, die Linux ausführen).
3 Klicken Sie auf **Erweitert** und dann auf das Register **Netzwerk**.
4 Klicken Sie auf **Einstellungen**.
5 Wählen Sie **Manuelle Proxy-Konfiguration.**
6 Geben Sie im Feld **Kein Proxy für** die Adressen für die CMCs und iDRACs im Verwaltungsnetzwerk ein; verwenden Sie dazu die kommagetrennte Liste. Sie können DNS-Namen und Platzhalter in Ihren Einträgen verwenden.

Microsoft Phishing-Filter

Wenn in Ihrem Verwaltungssystem der Microsoft Phishing-Filter in Internet Explorer aktiviert ist und Ihr CMC keinen Zugang zum Internet hat, dann kann es sein, dass der Zugriff auf den CMC ein paar Sekunden verzögert wird. Diese Verzögerung kann eintreten, wenn Sie den Browser oder eine andere Schnittstelle wie beispielsweise Remote-RACADM verwenden. So deaktivieren Sie den Phishing-Filter:

1 Starten Sie den Internet Explorer.
2 Klicken Sie auf **Extras** > **Phishing-Filter** und dann auf **Phishing-Filter**-Einstellungen.
3 Wählen Sie die Option **Phishing-Filter deaktivieren** aus und klicken Sie auf **OK**.

Abrufen der Zertifikatsperrliste (CRL)

Wenn der CMC nicht über einen Internetzugang verfügt, deaktivieren Sie in Internet Explorer die Abruffunktion für die Zertifikatsperrliste (CRL). Diese Funktion testet, ob ein Server wie etwa der CMC Web Server ein Zertifikat verwendet, das sich auf einer Liste widerrufener

Zertifikate befindet, die aus dem Internet abgerufen wurde. Wenn kein Zugriff auf das Internet möglich ist, kann diese Funktion zu Verzögerungen von mehreren Sekunden führen, wenn Sie mit dem Browser oder einer Befehlszeilenschnittstelle, z. B. Remote-RACADM, auf den CMC zugreifen.

So deaktivieren Sie das Abrufen der Zertifikatsperrliste:

1 Starten Sie den Internet Explorer.
2 Klicken Sie auf **Tools** > **Internetoptionen** und klicken Sie dann auf **Erweitert**.
3 Gehen Sie zum Abschnitt „Sicherheit“, deaktivieren Sie die Option **Auf gesperrte Zertifikate von Herausgebern überprüfen** und klicken Sie auf **OK**.

Dateien mit dem Internet Explorer vom CMC herunterladen

Wenn Sie zum Herunterladen von Dateien vom CMC den Internet Explorer verwenden, kann es zu Problemen kommen, wenn die Option **Verschlüsselte Seiten nicht auf der Festplatte speichern** nicht aktiviert ist.

So aktivieren Sie die Option **Verschlüsselte Seiten nicht auf der Festplatte speichern**:

1 Starten Sie den Internet Explorer.
2 Klicken Sie auf **Tools** > **Internetoptionen Erweitert**.
3 Wählen Sie im Abschnitt **Sicherheit** die Option **Verschlüsselte Seiten nicht auf der Festplatte speichern** aus.

CMCNoble_Animationen im Internet Explorer erlauben

Wenn Sie Dateien über die Webschnittstelle herunter- oder hochladen, dreht sich ein Dateiübertragungssymbol und zeigt damit an, dass eine Übertragungsaktivität stattfindet. Wenn Sie Internet Explorer verwenden, muss der Browser so konfiguriert sein, dass Animationen wiedergegeben werden können.

So konfigurieren Sie Internet Explorer zum Abspielen von Animationen:

1 Starten Sie den Internet Explorer.
2 Klicken Sie auf **Tools** > **Internetoptionen** und klicken Sie dann auf **Erweitert**.
3 Gehen Sie zum Abschnitt **Multimedia** und wählen Sie die Option **Animationen auf Webseiten wiedergeben** aus.

Einrichtung des Erstzugriffs auf den CMC

Um den CMC im Remote-Zugriff zu verwalten, verbinden Sie den CMC mit dem Verwaltungsnetzwerk und konfigurieren Sie dann die CMC-Netzwerkeinstellungen.

ANMERKUNG: Um die PowerEdge VRTX-Lösung zu verwalten, muss sie mit Ihrem Verwaltungsnetzwerk verbunden sein.

Weitere Informationen über die Konfiguration der CMC-Netzwerkeinstellungen finden Sie unter Die anfängliche Netzwerkkonfiguration des CMC. Diese Erstkonfiguration weist die TCP/IP-Netzwerkbetriebsparameter zu, die den Zugriff auf den CMC aktivieren.

Der CMC und der iDRAC auf jedem Server und die Netzwerkverwaltungsschnittstellen für alle Switch-E/A-Module sind mit einem gemeinsamen integrierten Netzwerk im PowerEdge VRTX-Gehäuse verbunden. Damit kann das Verwaltungsnetzwerk vom Serverdatennetzwerk getrennt werden. Es ist wichtig, diesen Datenverkehr zu trennen, um ununterbrochenen Zugriff auf die Gehäuseverwaltung zu haben.

Der CMC ist mit dem Verwaltungsnetzwerk verbunden. Alle externen Zugriffe auf den CMC und die iDRACs werden über den CMC erreicht. Umgekehrt erfolgt der Zugriff auf die verwalteten Server über Netzwerkverbindungen zum E/A-Modul (EAM). Dies ermöglicht, dass Anwendungsnetzwerk und Verwaltungsnetzwerk voneinander getrennt sind.

Es wird empfohlen, dass Sie die Gehäuseverwaltung vom Datennetzwerk isolieren. Wegen des möglichen Datenverkehrs auf dem Datennetzwerk können die Verwaltungsschnittstellen auf dem internen Verwaltungsnetzwerk vom für Server bestimmten Datenverkehr

überlasten. Dies führt zu Verzögerungen in der CMC- und iDRAC-Kommunikation. Diese Verzögerungen können zu einem unvorhersagbaren Gehäuseverhalten führen, wie etwa die Anzeige von CMC durch iDRAC als offline, obwohl es arbeitet, was wiederum weiteres unerwünschtes Verhalten verursacht. Falls es unmöglich ist, das Verwaltungsnetzwerk physisch zu isolieren, besteht noch die Möglichkeit, den CMC- und iDRAC-Datenverkehr auf ein separates VLAN umzuleiten. Die CMC- und einzelnen iDRAC-Netzwerkschnittstellen können für die Verwendung eines VLAN konfiguriert werden.

CMC-Netzwerk anfänglich konfigurieren

ANMERKUNG: Durch Ändern der CMC-Netzwerkeinstellungen wird möglicherweise die aktuelle Netzwerkverbindung getrennt.

Sie können die anfängliche Netzwerkkonfiguration des CMC durchführen, bevor oder nachdem der CMC eine IP-Adresse erhält. Die Konfiguration der anfänglichen CMC-Netzwerkeinstellungen, bevor eine IP-Adresse zugeteilt ist, kann über eine der folgenden Schnittstellen erfolgen:

- Das LCD-Bedienfeld an der Gehäusevorderseite
- Die serielle Dell-CMC-Konsole

Die Konfiguration der ursprünglichen Netzwerkeinstellungen, nachdem der CMC über eine IP-Adresse verfügt, kann über eine der folgenden Optionen erfolgen:

- Befehlszeilenschnittstellen (CLIs), wie z. B. eine serielle Konsole, Telnet, SSH oder die Dell-CMC-Konsole über iKVM.
- Remote-RACADM
- CMC-Webschnittstelle
- LCD-Schnittstelle

CMC unterstützt sowohl IPv4- als auch IPv6-Adressierungsmodi. Die Konfigurationseinstellungen für IPv4 und IPv6 sind voneinander unabhängig.

CMC-Netzwerke über die LCD-Bedienfeld-Schnittstelle konfigurieren

Sie können mit der LCD-Bedienfeldschnittstelle das CMC-Netzwerk einrichten.

ANMERKUNG: Sie können die Ausrichtung eines LCD-Displays (für Rack- oder Tower-Modus) anpassen, indem sie die Schaltflächen „Nach oben“ und „Nach unten“ für zwei Sekunden gedrückt halten. Alternativ können Sie auch die Schaltflächen „Nach rechts“ und „Nach links“ verwenden. Weitere Informationen über die Schaltflächen auf dem LCD-Bedienfeld eines CMC finden Sie unter LCD-Navigation.

1 So starten Sie die CMC-Konfiguration:
   - Bei einem Gehäuse, das zuvor noch nicht konfiguriert wurde, wird der Bereich **LCD-Sprache** angezeigt. Wechseln Sie im Bereich **LCD-Sprache** mithilfe der Pfeilschaltflächen zur gewünschten Sprache. Wenn die gewünschte Sprache markiert ist, wählen Sie die Sprache aus, indem Sie auf die mittlere Schaltfläche drücken. Der Bereich **Netzwerkeinstellungen** wird angezeigt.
   - Bei einem Gehäuse, das zuvor konfiguriert wurde, wird der Bereich **Hauptmenü** angezeigt. Wählen Sie im **Hauptmenü** zuerst **Einstellungen** und dann **Netzwerkeinstellungen** aus.

2 Wählen Sie im Bereich **Netzwerkeinstellungen** den gewünschten Einrichtungsmodus aus:
   - **Setup-Kurzanleitung (DHCP)** – Wählen Sie diesen Modus aus, um den CMC schnell mit DHCP-Adressen einzurichten. Weitere Informationen zur CMC-Konfiguration mit diesem Modus finden Sie unter **Konfiguration von CMC mit Setup-Kurzanleitung (DHCP)**.
   - **Erweitertes Setup** – Wählen Sie diesen Modus aus, um den CMC für erweiterte Konfigurationen einzurichten. Weitere Informationen zur CMC-Konfiguration mit diesem Modus finden Sie unter **CMC unter Verwendung von erweitertem Setup konfigurieren**.

Konfiguration von CMC mit Setup-Kurzanleitung (DHCP)

So richten Sie ein Netzwerk unter Verwendung der LCD-Schnittstelle ein:

1 Wählen Sie im Bereich **Netzwerkeinstellungen** die Option **Setup-Kurzanleitung (DHCP)** aus. In dem Bereich wird die folgende Meldung angezeigt:

```
About to get DHCP addresses. Ensure CMC network cable is connected.
```

2 Drücken Sie auf die mittlere Schaltfläche, um die Akzeptieren-Schaltfläche zu markieren. Drücken Sie erneut auf die mittlere Schaltfläche, um die Einstellungen zu übernehmen, oder navigieren Sie zur Pfeil-zurück-Schaltfläche und drücken Sie dann auf die mittlere Schaltfläche, um zurückzugehen und die Einstellungen zu ändern.

CMC unter Verwendung von erweitertem Setup konfigurieren

1 Wenn Sie im Bereich **Netzwerkeinstellungen Erweitertes Setup** auswählen, wird die folgende Meldung angezeigt, um zu bestätigen, dass Sie CMC konfigurieren möchten:

```
Configure CMC?
```

2 Klicken Sie für die CMC-Konfiguration über die erweiterten Setup-Eigenschaften auf die Schaltfläche in der Mitte, und aktivieren Sie das Kontrollkästchen.

ANMERKUNG: Um die CMC-Konfiguration zu übergehen, navigieren Sie zum „X“ -Symbol, und drücken Sie dann die Schaltfläche in der Mitte.

3 Wenn Sie dazu aufgefordert werden, eine entsprechende Netzwerkgeschwindigkeit auszuwählen, wählen sie eine Netzwerkgeschwindigkeit (**Autom. (1GB)**, **10MB**, oder **100MB**) unter Verwendung der entsprechenden Schaltflächen aus.

Die Einstellung der Netzwerkgeschwindigkeit muss mit Ihrer Netzwerkkonfiguration übereinstimmen, damit ein effektiver Netzwerkdurchsatz gewährleistet ist. Wenn die Netzwerkgeschwindigkeit geringer eingestellt wird als die Taktrate Ihrer Netzwerkkonfiguration, steigt der Verbrauch der Bandbreite und die Netzwerkkommunikation wird verlangsamt. Ermitteln Sie, ob Ihr Netzwerk die oben angegebenen Netzwerkgeschwindigkeiten unterstützt, und legen Sie sie entsprechend fest. Wenn Ihre Netzwerkkonfiguration keinem dieser Werte entspricht, wird empfohlen, dass Sie die Option **Autom. (1 GB)** aktivieren oder die Benutzerdokumentation Ihres Netzwerkgeräteherstellers lesen.

4 Führen Sie einen der folgenden Schritte aus:

- Wählen Sie **Autom. (1 GB)** aus, indem Sie auf die mittlere Schaltfläche drücken. Drücken Sie anschließend erneut auf die mittlere Schaltfläche. Daraufhin wird der Bereich **Protokoll** angezeigt. Fahren Sie mit Schritt 6 fort.
- Wählen Sie **10 Mb** oder **100 Mb** aus. Der Bereich **Duplex**

  angezeigt wird. Fahren Sie mit Schritt 5 fort.

Drücken Sie ansonsten

5 Wählen Sie im Bereich **Duplex** den Duplexmodus (**Voll** oder **Halb**) der Ihrer Netzwerkumgebung angepasst ist, drücken Sie auf die Schaltfläche in der Mitte, und drücken Sie erneut auf die mittlere Schaltfläche. Daraufhin wird der Bereich **Protokoll** angezeigt.

ANMERKUNG: Die Einstellungen für Netzwerkgeschwindigkeit und Duplexmodus sind nicht verfügbar, wenn Automatische Verhandlung auf Ein gesetzt oder 1000 MB (1 Gbit/s) ausgewählt ist. Wenn die automatische Verhandlung für das eine Gerät aktiviert ist, jedoch nicht für das andere, kann das Gerät, das die automatische Verhandlung verwendet, zwar die Netzwerkgeschwindigkeit, jedoch nicht den Duplexmodus des anderen Geräts bestimmen. In diesem Fall wird während der automatischen Verhandlung Halbduplex als Duplexmodus ausgewählt. Ein derartiger Duplex-Übereinstimmungsfehler führt zu einer langsamen Netzwerkverbindung.

6 Wählen Sie im Bereich **Protokoll** ein Internet-Protokoll (**nur IPv4**, **nur IPv6**, oder **Beide**) aus, das Sie für CMC verwenden wollen, drücken Sie dann auf die mittlere Schaltfläche und drücken Sie erneut auf die mittlere Schaltfläche.

7
- Wenn Sie die Option **IPv4** oder **Beide** auswählen, wählen Sie den Modus **DHCP** oder **Statisch** aus. Fahren Sie mit Schritt 8 fort..
- Wenn Sie jedoch **IPv6** auswählen, wird der Bereich **iDRAC konfigurieren** angezeigt. Fahren Sie später in dieser Prozedur mit Schritt 11 fort.

8 Wählen Sie im Bereich **Modus** den Modus aus, in dem der CMC die IP-Adressen der NICs abrufen soll: Wenn Sie „DHCP“ auswählen, ruft der CMC von einem DHCP-Server in Ihrem Netzwerk automatisch Informationen zur IP-Konfiguration (IP-Adresse, Subnetzmaske und Gateway) ab. Dem CMC wird in Ihrem Netzwerk eine eindeutige IP-Adresse zugewiesen. Wenn Sie **DHCP** auswählen, drücken Sie auf die mittlere Schaltfläche, und drücken Sie dann erneut auf die mittlere Schaltfläche. Daraufhin wird der Bereich **iDRAC konfigurieren** angezeigt. Fahren Sie später in dieser Prozedur mit Schritt 11 fort.

9 Wenn Sie **Statisch** auswählen, geben Sie die IP-Adresse, Gateway, und die Subnet-Maske ein, indem Sie den Anweisungen im LCD-Bereich folgen.

Die eingegebenen IP-Informationen werden angezeigt. Drücken Sie auf die mittlere Schaltfläche, und drücken Sie dann erneut auf die mittlere Schaltfläche. Im Bildschirm **CMC-Konfiguration** werden die Einstellungen für **Statische IP-Adresse**, **Subnetzmaske** und

Gateway aufgeführt, die Sie eingegeben haben. Überprüfen Sie die Einstellungen auf Richtigkeit. Um eine Einstellung zu korrigieren, drücken Sie auf die entsprechenden Schaltflächen. Drücken Sie auf die mittlere Schaltfläche, und drücken Sie dann erneut auf die mittlere Schaltfläche. Der Bereich **DNS registrieren?** wird angezeigt.

10 Wählen Sie zur Registrierung das Kontrollkästchen-Symbol aus, und drücken Sie dann auf die mittlere Schaltfläche. Legen Sie die IP-Adresse des DNS-Servers fest, wählen Sie das Kontrollkästchen-Symbol aus, und drücken Sie dann die mittlere Schaltfläche. Wenn eine DNS-Registrierung nicht erforderlich ist, wählen Sie das „X"-Symbol aus, und drücken Sie auf die mittlere Schaltfläche.

11 Geben Sie an, ob Sie einen iDRAC konfigurieren möchten:

- **Nein**: Wählen Sie das „X"-Symbol aus, und drücken Sie dann auf die Schaltfläche in der Mitte. Fahren Sie später in dieser Prozedur mit Schritt 17 fort.
- **Ja**: Wählen Sie das Kontrollkästchen-Symbol aus, und drücken Sie dann auf die Schaltfläche in der Mitte.

Sie können iDRAC auch über die CMC-Web-Schnittstelle konfigurieren.

12 Wählen Sie im Feld **Protokoll** die IP-Adresse aus, die Sie für die Server verwenden möchten:

- **IPv4** – Die Optionen von **DHCP** oder **Statisch** werden angezeigt.
- **Beide**

  – Die Optionen **DHCP** oder **Statisch** werden angezeigt.
- **IPv6**

  – Der Bereich **iDRAC-Konfiguration** wird angezeigt. Fahren Sie mit Schritt 15 fort.

13 Wählen Sie **DHCP** oder **Statisch** aus.

Tabelle 9. Netzwerkmodus

Dynamic Host Configuration Protocol (DHCP)	iDRAC ruft von einem DHCP-Server auf dem Netzwerk automatisch Informationen zur IP-Konfiguration (IP-Adresse, Subnetzmaske und Gateway) ab. Dem iDRAC wird in Ihrem Netzwerk eine eindeutige IP-Adresse zugewiesen. Drücken Sie auf die mittlere Schaltfläche. Der Bereich **IPMI-über-LAN** wird angezeigt.

Statisch	Wenn Sie **Statisch** ausgewählt haben, geben Sie die IP-Adresse, Gateway, und die Subnet-Maske manuell ein, indem Sie den Anweisungen im LCD-Bereich folgen.
	Wenn Sie die Option **Statisch** ausgewählt haben, drücken Sie auf die mittlere Schaltfläche, und fahren Sie dann mit Folgendem fort:
	a Die folgende Meldung fragt, of Sie die IPs unter Verwendung des IP von Steckplatz-1 automatisch erhöhen wollen.
	`IPs will auto-increment by slot number.`
	Klicken Sie auf die mittlere Schaltfläche. Die folgende Meldung fordert Sie auf, die Steckplatz–1 IP-Nummer einzugeben.
	`Enter slot 1 (starting) IP`
	Geben Sie die Steckplatz–1 IP-Nummer ein und drücken Sie dann auf die Schaltfläche in der Mitte.
	b Bestimmen Sie die Subnetzmaske und drücken Sie dann auf die Schaltfläche in der Mitte.
	c Bestimmen Sie den Gateway und drücken Sie dann die Schaltfläche in der Mitte.
	d Im Bildschirm **Netzwerkübersicht** werden die Einstellungen für **Statische IP-Adresse**, **Subnetzmaske** und **Gateway** aufgeführt, die Sie eingegeben haben. Überprüfen Sie die Einstellungen auf Richtigkeit. Um eine Einstellung zu korrigieren, drücken Sie auf die entsprechenden Schaltflächen, und drücken Sie dann auf die mittlere Schaltfläche.
	e Wenn Sie die Richtigkeit der von Ihnen eingegebenen Einstellungen bestätigt haben, fahren Sie mit Schritt 10 fort.
	Der Bereich **IPMI-über-LAN** wird angezeigt.

14 Wählen Sie im Bereich **IPMI-über-LAN** die Option **Aktivieren** oder **Deaktivieren** aus, um IPMI-über-LAN zu aktivieren oder zu deaktivieren. Drücken Sie auf die mittlere Schaltfläche, um fortzufahren.

15 Die folgende Meldung wird im Bereich **iDRAC-Konfiguration** angezeigt.

`Apply settings to installed servers?`

Um alle iDRAC-Netzwerkeinstellungen für die installierten Server zu übernehmen, wählen Sie das Kontrollkästchen-Symbol aus, und drücken Sie dann auf die mittlere Schaltfläche. Wählen Sie andernfalls das „X"-Symbol aus, und drücken Sie auf die mittlere Schaltfläche.

16 Die folgende Meldung wird im nächsten Fensterbereich **iDRAC-Konfiguration** angezeigt.

```
Auto-Apply settings to newly-inserted servers?
```

Um alle iDRAC-Netzwerkeinstellungen für die neu installierten Server zu übernehmen, wählen Sie das Kontrollkästchen-Symbol aus, und drücken Sie auf die mittlere Schaltfläche. Wenn ein neuer Server in das Gehäuse eingesetzt wird, werden Sie auf dem LCD-Display gefragt, ob der Server automatisch mit den zuvor konfigurierten Netzwerkeinstellungen und Richtlinien bereitgestellt werden soll. Wenn Sie die iDRAC-Netzwerkeinstellungen nicht für die neu installierten Servern übernehmen möchten, wählen Sie das „X"-Symbol aus, und drücken Sie auf die mittlere Schaltfläche. Wenn ein neuer Server in das Gehäuse eingesetzt wird, werden die iDRAC-Netzwerkeinstellungen nicht konfiguriert.

17 Die folgende Meldung wird im Bereich **iDRAC-Konfiguration** angezeigt.

```
Apply All Enclosure Settings?
```

Um alle Gehäuseeinstellungen zu übernehmen, wählen Sie das Kontrollkästchen-Symbol aus, und drücken Sie auf die mittlere Schaltfläche. Wählen Sie andernfalls das „X"-Symbol aus, und drücken Sie auf die mittlere Schaltfläche.

18 Nach einer Wartezeit von 30 Sekunden können Sie im Bereich **IP-Zusammenfassung** die von Ihnen bereitgestellten IP-Adressen überprüfen, um sicherzustellen, dass die Adressen korrekt sind. Um eine Einstellung zu korrigieren, drücken Sie auf das Pfeil-nach-links-Symbol, und drücken Sie dann auf die mittlere Schaltfläche, um zum Bildschirm für diese Einstellung zurückzukehren. Nachdem Sie eine IP-Adresse korrigiert haben, drücken Sie auf die mittlere Schaltfläche.

Wenn Sie die von Ihnen eingegebenen Einstellungen als korrekt bestätigt haben, klicken Sie auf die mittlere Schaltfläche und klicken Sie dann erneut auf die mittlere Schaltfläche. Daraufhin wird der Bereich **Hauptmenü** angezeigt.

Der CMC und die iDRACs sind jetzt im Netzwerk verfügbar. Sie können über die Webschnittstelle oder Befehlszeilenschnittstellen, wie etwa eine serielle Konsole, Telnet und SSH, unter der zugewiesenen IP-Adresse auf den CMC zugreifen.

Schnittstellen und Protokoll für den Zugriff auf CMC

Nachdem Sie die CMC-Netzwerkeinstellungen konfiguriert haben, können Sie über verschiedene Schnittstellen im Remote-Zugriff auf den CMC zugreifen. Die folgenden Tabelle listet die Schnittstellen auf, die Sie für den Remote-Zugriff auf CMC verwenden können.

ANMERKUNG: Da Telnet nicht so sicher wie die anderen Schnittstellen ist, ist es standardmäßig deaktiviert. Sie können Telnet mithilfe von Web, SSH oder Remote-RACADM aktivieren.

ANMERKUNG: Die gleichzeitige Verwendung von mehr als einer Schnittstelle kann zu unerwarteten Ergebnissen führen.

Tabelle 10. CMC-Schnittstellen

Schnittstelle	Beschreibung
Webschnittstelle	Ermöglicht Remote-Zugriff auf den CMC über eine grafische Benutzeroberfläche. Die Webschnittstelle ist in die CMC-Firmware integriert und der Zugriff erfolgt von einem unterstützten Webbrowser auf der Management Station über die NIC-Schnittstelle. Eine Liste der unterstützten Webbrowser finden Sie im Abschnitt „Unterstützte Webbrowser" in der *Dell Systems Software Support Matrix* unter **dell.com/support/manuals**.
Remote-RACADM-Befehlszeilenschnittstelle	Verwenden Sie dieses Befehlszeilen-Dienstprogramm, um CMC und dessen Komponenten zu verwalten. Sie können Remote- oder Firmware-RACADM verwenden: • Remote-RACADM ist ein Client-Dienstprogramm, das auf einer Management Station ausgeführt wird. Es verwendet die bandexterne Netzwerkschnittstelle, um die RACADM-Befehle auf dem Managed System auszuführen, außerdem wird der HTTPs-Kanal verwendet. Die Option `-r` führt den RACADM-Befehl über ein Netzwerk aus. • Zugriff auf Firmware RACADM ist möglich durch die Anmeldung am CMC mittels SSH oder Telnet. Sie können die Firmware RACADM-Befehle ausführen, ohne die CMC IP, den Benutzernamen oder das Kennwort festzulegen. Sie können nach der RACADM-Eingabeaufforderung die Befehle ohne das racadm-Präfix direkt ausführen.
Gehäuse-LCD-Bedienfeld	Verwenden Sie die LCD auf der Frontblende, um die folgenden Aktivitäten auszuführen:

Schnittstelle	Beschreibung
	• Warnungen und CMC-IP-Adresse anzeigen • DHCP festlegen • Statische IP-Einstellungen für CMC konfigurieren • Anzeigen der CMC-MAC-Adresse für den aktiven CMC. • Anzeigen der an das Ende der CMC-IP angehängten CMC-VLAN-ID, wenn VLAN bereits konfiguriert ist.
Telnet	Ermöglicht Befehlszeilenzugriff auf den CMC über das Netzwerk. Die RACADM-Befehlszeilenschnittstelle und der `connect`-Befehl, der zum Herstellen einer Verbindung zur seriellen Konsole eines Servers oder E/A-Moduls verwendet wird, sind über die CMC-Befehlszeile verfügbar. **ANMERKUNG: Telnet ist kein sicheres Protokoll und wird standardmäßig angezeigt. Telnet überträgt alle Daten, einschließlich Kennwörter, im Textformat. Bei der Übertragung von vertraulichen Informationen verwenden Sie die SSH-Schnittstelle.**
SSH	Verwenden Sie SSH, um RACADM-Befehle auszuführen. Sie bietet dieselben Fähigkeiten wie die Telnet-Konsole und verwendet eine verschlüsselte Transportschicht für höhere Sicherheit. Der SSH-Dienst ist standardmäßig auf CMC aktiviert und kann deaktiviert werden.
WSMan	Die WSMAN-Services basieren auf dem Web Services for Management (WSMAN)-Protokoll für 1-zu-n-Verwaltungsaufgaben. Sie können einen WS-MAN-Client verwenden, z. B. den WinRM-Client (Windows) oder den OpenWSMAN-Client (Linux), um die CMC-Services-Funktion zu verwenden. Sie können außerdem Power Shell- und Python-Skript verwenden, um auf die WSMAN-Schnittstelle zu schreiben. WSMAN ist ein SOAP-basiertes (Simple Object Access Protocol) Protokoll, das für die Systemverwaltung verwendet wird. CMC verwendet WS-Management zum Übermitteln von DMTF-CIM-basierten Verwaltungsinformationen (DMTF = Distributed Management Task Force; CIM = Common Information Model). Die CIM-Informationen definieren die Semantik- und Informationstypen, die in einem verwalteten System geändert werden können. Die CMC-WSMAN-Implementierung verwendet SSL auf Schnittstelle 443 für Transportsicherheit und unterstützt Standardauthentifizierung. Die durch WS-Management zur Verfügung gestellten Daten werden durch die CMC-Instrumentierungsschnittstelle bereitgestellt, die den DMTF-Profilen und den Erweiterungsprofilen zugeordnet ist. Für weitere Informationen, siehe: • MOFs und Profile – **delltechcenter.com/page/DCIM.Library** • DTMF-Website – **www.dmtf.org/standards/profiles/** • WSMan-Versionshinweisdatei. • **www.wbemsolutions.com/ws_management.html** • DMTF WSManagement-Spezifikationen: **www.dmtf.org/standards/wbem/wsman** Web Services-Schnittstellen können durch wirksames Einsetzen der Client-Infrastruktur genutzt werden, beispielsweise Windows WinRM und Powershell CLI, Open Source-Dienstprogramme wie WSManCLI und Anwendungsprogrammierungsumgebungen wie Microsoft .NET. Das Tool WinRM stellt eine standardmäßige Reaktionszeitüberschreitung von 60 Sekunden für alle von ihm ausgesendeten WSMAN-Befehle ein. WinRM lässt keine Änderung dieses Zeitüberschreitungsintervalls zu. Aufgrund eines Fehlers im Tool WinRM wird mit dem Befehl „winrm set winrm/config @{MaxTimeoutms ="80000"}“ die Zeitüberschreitungseinstellung nicht geändert. Daher wird empfohlen, WinRM nicht für Befehle zu verwenden, deren Ausführung möglicherweise länger als eine Minute dauert.

Schnittstelle	Beschreibung
	Es wird empfohlen, Bibliotheken zu verwenden, die SOAP-XML-Pakete erstellen, da Benutzer mithilfe dieser Bibliotheken die Dauer der Zeitüberschreitung konfigurieren können. Für Client-Verbindungen mithilfe von Microsoft WinRM ist mindestens die Version 2.0 erforderlich. Weitere Informationen dazu finden Sie im Microsoft-Artikel, <**support.microsoft.com/kb/968929**>.

ANMERKUNG: Der Standardbenutzername für das CMC-Modul ist `root` und das Standardkennwort lautet `calvin`.

Starten von CMC mit anderen Systems Management Tools

Sie können CMC auch vom Dell Server Administrator oder Dell OpenManage Essentials starten.

Um mit dem Dell Server Administrator auf die CMC-Schnittstelle zuzugreifen, starten Sie Server Administrator auf der Management Station. Klicken Sie in der Systemstruktur im linken Fensterbereich der Server Administrator-Startseite auf **System** > **Hauptsystemgehäuse** > **Remote-Access-Controller**. Weitere Informationen finden Sie im *Dell Server Administrator User's Guide* (Dell Server Administrator-Benutzerhandbuch) unter **dell.com/support/manuals**.

Herunterladen und Aktualisieren der CMC-Firmware

Um die CMC-Firmware herunterzuladen, gehen Sie zu Herunterladen der CMC-Firmware.

Um die CMC-Firmware aktualisieren, gehen Sie zu Aktualisieren der CMC-Firmware.

Einrichten des physischen Standorts und des Namens für das Gehäuse

Sie können den Gehäusestandort in einem Rechenzentrum und den Gehäusenamen durch das Ermitteln des Gehäuses im Netzwerk einrichten (der Standardname lautet **Dell Rack System**). Beispiel: Eine SNMP-Anfrage für den Gehäusenamen gibt den von Ihnen konfigurierten Namen aus.

Einrichten des physischen Standorts und des Namens für das Gehäuse über die Webschnittstelle

So richten Sie den Standort und den Namen für ein Gehäuse über die Webschnittstelle ein:

1 Wählen Sie im rechten Fensterbereich **Gehäuseübersicht** aus und klicken Sie auf **Setup**.

2 Geben Sie auf der Seite **Allgemeine Gehäuseeinstellungen** den physischen Standort und den Gehäusenamen ein. Weitere Informationen zum Festlegen der Gehäuseeigenschaften finden Sie in der *Online Hilfe*.

ANMERKUNG: Das Feld Gehäusestandort ist optional. Es wird empfohlen, die Felder Rechenzentrum, Gang, Rack und Rack-Steckplatz zu verwenden, um den physischen Standort des Gehäuses anzuzeigen.

3 Klicken Sie auf **Anwenden**. Die Einstellungen werden gespeichert.

Einrichten des physischen Standorts und des Namens für das Gehäuse über RACADM

Um den Namen, den Standort, das Datum und die Uhrzeit für das Gehäuse über die Befehlszeilenschnittstelle einzurichten, gehen Sie zu den Befehlen **setsysinfo** und **setchassisname**. Weitere Informationen finden Sie unter *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

Datum und Uhrzeit auf dem CMC einstellen

Stellen Sie Datum und Uhrzeit manuell ein oder synchronisieren Sie Datum und Uhrzeit mit einem Network Time Protocol (NTP)-Server.

Datum und Uhrzeit auf dem CMC unter Verwendung der CMC-Webschnittstelle einstellen

So stellen Sie das Datum und die Uhrzeit auf dem CMC ein:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Setup** > **Datum/Uhrzeit**.

2 Datum und Uhrzeit können mit einem NTP-Server (Network Time Protocol) auf der Seite **Datum/Uhrzeit** synchronisiert werden, indem Sie **NTP aktivieren** auswählen und bis zu drei NTP-Server festlegen. Für die manuelle Einstellung von Datum und Uhrzeit deaktivieren Sie die Option **NTP aktivieren** und bearbeiten Sie dann die Felder **Datum** und **Zeit**.

3 Wählen Sie im Drop-Down-Menü **Zeitzone** aus und klicken dann auf **Anwenden**.

Datum und Uhrzeit auf dem CMC mittels RACADM einstellen

Anleitungen zum Einstellen von Datum und Uhrzeit mit der Befehlszeilenschnittstelle finden Sie im **config-Befehl** und `cfgRemoteHosts`-Datenbankeigenschaftengruppen im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX), der unter **dell.com/support/manuals** verfügbar ist.

LEDs zum Identifizieren von Komponenten im Gehäuse konfigurieren

Sie können die LEDs von Komponenten (Gehäuse, Server, physische Festplattenlaufwerke, virtuelle Festplatten, und E/A Module) zum Blinken aktivieren, damit Sie die Komponenten auf dem Gehäuse identifizieren können.

ANMERKUNG: Zum Modifizieren dieser Einstellungen müssen Sie die Berechtigung als Gehäusekonfigurations-Administrator besitzen.

Konfigurieren von LED-Blinken über die CMC-Webschnittstelle

Blinken von LEDs für eine, mehrere oder alle Komponenten aktivieren:

- Gehen Sie im linken Fensterbereich zu einer der folgenden Seiten:
  - **Gehäuseübersicht** > **Fehlerbehebung**.
  - **Gehäuseübersicht** > **Gehäuse-Controller** > **Fehlerbehebung** .

– **Gehäuse-Übersicht** > **Server-Übersicht** > **Fehlerbehebung**.

ANMERKUNG: Auf dieser Seite können nur Server ausgewählt werden.

– **Gehäuse-Übersicht** > **E/A-Modulübersicht** > **Fehlerbehebung** .

– **Speicher** > **Fehlerbehebung** > **Identifizieren**.

ANMERKUNG: Physische Festplatte pro Gehäuse, virtuelle Festplatten pro Gehäuse und externe Speicherkomponenten-LED können auf dieser Seite ausgewählt werden.

Um den Blinkvorgang für eine Komponenten-LED zu starten, wählen Sie Option **Alle auswählen/Alle abwählen** für die entsprechende physische Festplatte oder virtuelle Festplatte oder Gehäuse und klicken Sie dann auf **Blinken**. Zur Deaktivierung des Blinkens einer Komponenten-LED, löschen Sie die Option **Alle auswählen/Alle abwählen** für die entsprechende LED und klicken Sie dann auf **Blinken beenden**.

LED-Blinken mittels RACADM konfigurieren

Öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC, melden Sie sich an und geben Sie Folgendes ein:

`racadm setled -m <module> [-l <ledState>]`, wobei *<module>* das Modul bezeichnet, dessen LED Sie konfigurieren möchten. Konfigurationsoptionen:

- `server-n` wobei *n* = 1-4
- `switch-1`
- `cmc-active`

und *<ledState>* gibt an, ob die LED blinken soll. Konfigurationsoptionen:

- 0 - Nicht blinken (Standardeinstellung)
- 1 - Blinken

`racadm raid <operation> <component FQDD>`, wobei der Wert *Vorgang* `blink` oder `unblink` ist und der FQDD für das physische Festplattenlaufwerk, die virtuelle Festplatte und Gehäuse der Komponente ist.

CMC-Eigenschaften konfigurieren

Sie können CMC-Eigenschaften, wie z. B. Strombudget, Netzwerkeinstellungen, Benutzer sowie SNMP- und E-Mail-Warnungen über die Webschnittstelle oder RACACM-Befehle konfigurieren.

Konfiguration des iDRAC-Startverfahrens über die CMC-Webschnittstelle

So konfigurieren Sie das iDRAC-Startverfahren über die Seite **Allgemeine Gehäuseeinstellungen**:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Setup**.
Die Seite **Allgemeine Gehäuseeinstellungen** wird angezeigt.

2 Wählen Sie im Drop-Down-Menü für die Eigenschaft **iDRAC-Startverfahren IP-Adresse** oder **DNS**.

3 Klicken Sie auf **Anwenden**.

ANMERKUNG: Ein DNS-basierter Start wird nur in folgenden Fällen für iDRACs verwendet:

- Die Gehäuseeinstellung ist DNS.
- Der CMC hat erkannt, dass der entsprechende iDRAC mit einem DNS-Namen konfiguriert wurde.

Konfiguration des iDRAC-Startverfahrens mit RACADM

Um die CMC-Firmware mit RACADM zu aktualisieren, verwenden Sie den Unterbefehl `cfgRacTuneIdracDNSLaunchEnable`. Weitere Informationen finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX) unter **dell.com/support/manuals**.

Konfiguration von Richtlinienattributen für Anmeldesperrung über die CMC-Webschnittstelle

ANMERKUNG: Um die folgenden Aufgaben auszuführen, müssen Sie die Berechtigung als Gehäusekonfigurations-Administrator besitzen.

Mit der **Anmeldesicherheit** können Sie die IP-Bereichsattribute für die CMC-Anmeldung über die CMC-Webschnittstelle konfigurieren. So konfigurieren Sie die IP-Bereichsattribute über die CMC-Webschnittstelle:

1. Wählen Sie im linken Fensterbereich **Gehäuseübersicht** aus und klicken Sie auf **Netzwerk** > **Netzwerk**.
   Die Seite **Netzwerkkonfiguration** wird angezeigt.
2. Klicken Sie im Abschnitt „IPv4-Einstellungen“ auf **Erweiterte Einstellungen**. Alternativ können Sie auf die Seite **Anmeldesicherheit** zugreifen, indem Sie im linken Fensterbereich **Gehäuseübersicht** wählen und auf **Sicherheit** > **Anmeldung** klicken.
   Die Seite **Anmeldesicherheit** wird angezeigt.
3. Um die Funktion Benutzer blockieren bzw. IP blockieren im Abschnitt **Richtlinie für Anmeldesperrung** zu aktivieren, wählen Sie **Sperrung durch Benutzernamen** bzw. **Sperrung durch IP-Adresse (IPv4)**.
   Die Optionen zum Einstellen der anderen Attribute zur Anmeldesperrung sind aktiviert.
4. Geben Sie die erforderlichen Werte für die Richtlinienattribute der Anmeldesperrung in die aktivierten Felder – **Sperrung Fehlerzähler**, **Sperrungsausfallfenster** und **Sperrung durch Zeitüberschreitung** – ein. Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.
5. Klicken Sie auf **Anwenden**, um diese Einstellungen zu speichern.

Konfiguration von Richtlinienattributen für Anmeldesperrung mit RACADM

Sie können RACADM nutzen, um für folgende Funktionen Richtlinienattribute für die Anmeldesperrung zu konfigurieren:

- Blockieren von Benutzern
- Blockieren von IP-Adressen
- Anzahl der erlaubten Anmeldeversuche
- Zeitspanne, bis der Fehlerzähler für die Sperrung erscheint
- Sperrungsdauer

- So aktivieren Sie die Funktion zum Blockieren von Benutzern:
  ```
  racadm config -g cfgRacTuning -o cfgRacTuneUserBlkEnable <0|1>
  ```
- So aktivieren Sie die Funktion zum Blockieren von IP-Adressen:
  ```
  racadm config -g cfgRacTuning -o cfgRacTuneIPBlkEnable <0|1>
  ```
- So legen Sie die Anzahl der erlaubten Anmeldeversuche fest:
  ```
  racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount
  ```
- So legen Sie die Zeitspanne fest, in der der Fehlerzähler für die Sperrung erscheinen muss:
  ```
  racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow
  ```
- So legen Sie einen Wert für die Sperrungsdauer fest:
  ```
  racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime
  ```

Weitere Informationen über diese Objekte finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX) unter **dell.com/support/manuals**.

Die redundante CMC-Umgebung verstehen

Sie können einen Standby-CMC installieren, der aktiviert wird, wenn der aktive CMC ausfällt. Der redundante CMC kann vorinstalliert sein oder zu einem späteren Zeitpunkt hinzugefügt werden. Um volle Redundanz bzw. optimale Leistung zu gewährleisten, achten Sie darauf, dass das CMC-Netzwerk korrekt verkabelt ist.

Failover-Ereignisse können auftreten, wenn:

- Führen Sie den RACADM-Befehl `cmcchangeover` aus. Lesen Sie den Abschnitt `cmcchangeover`-Befehl im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX), verfügbar unter dell.com/support/manuals.
- Führen Sie den RACADM-Befehl `racreset` aus. Lesen Sie den Abschnitt `racreset`-Befehl im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX), verfügbar unter dell.com/support/manuals.
- Der aktive CMC wird über die Webschnittstelle zurückgesetzt. Mehr über die Option `Reset CMC` für **Power Control Operations** finden Sie unter Durchführen von Stromsteuerungsvorgänge an einem Server.
- Das Netzwerkkabel vom aktiven CMC entfernt wird.
- Der aktive CMC vom Gehäuse entfernt wird.
- Ein CMC-Firmware-Flash auf dem aktiven CMC initiiert wird.
- Ein aktiver CMC nicht mehr funktioniert.

ANMERKUNG: Im Falle eines CMC-Failovers werden alle iDRAC-Verbindungen und alle aktiven CMC-Sitzungen abgemeldet. Benutzer mit abgemeldeten Sitzungen müssen sich erneut mit dem aktiven CMC verbinden.

Info zum Standby-CMC

Der Standby-CMC ist mit dem aktiven CMC identisch und spiegelt diesen stets wider. Sowohl der aktive als auch der Standby-CMC müssen mit derselben Firmware-Revision installiert sein. Bei unterschiedlichen Firmware-Revisionen meldet das System „Redundanzherabsetzung".

Der Standby-CMC nimmt die Einstellungen und Eigenschaften des aktiven CMCs an. Sie müssen darauf achten, dass stets dieselbe Firmware-Version auf beiden CMCs unterhalten wird. Konfigurationseinstellungen müssen auf dem Standby-CMC jedoch nicht dupliziert werden.

ANMERKUNG: Weitere Informationen zur Installation eines CMC finden Sie im *VRTX Owner's Manual* (VRTX-Benutzerhandbuch). Für Anleitungen zur Installation der CMC-Firmware auf Ihrem Standby-CMC, lesen Sie Aktualisierung der Firmware.

Ausfallsicherer CMC-Modus

Das PowerEdge VRTX-Gehäuse aktiviert den ausfallsicheren Modus zum Schutz von Servern und E/A-Modulen vor Ausfällen. Der ausfallsichere Modus wird aktiviert, wenn das Gehäuse nicht von einem CMC kontrolliert wird. Während des CMC-Failover-Zeitraums oder während eines einzelnen Verlusts der CMC-Verwaltung:

- können Sie die neu-installierten Server nicht einschalten.
- können Sie nicht per Remote auf vorhandene Server zugreifen.
- wird die Server-Leistung reduziert, um den Stromverbrauch zu begrenzen, bis die Verwaltung durch den CMC wiederhergestellt wird.

Im Folgenden werden einige der Bedingungen aufgeführt, die zum Verlust der CMC-Verwaltung führen können:

- CMC-Entfernung — Die Gehäuseverwaltung wird nach Ersatz des CMC wieder aufgenommen oder nach der Ausfallsicherung eines Standby-CMCs.
- Entfernen eines CMC-Netzwerkkabels oder Verlust der Netzwerkverbindung — Die Gehäuseverwaltung wird wieder aufgenommen, nachdem das Gehäuse zum Standby-CMC gesichert wird. Die Netzwerkausfallsicherung wird nur im redundanten CMC-Modus aktiviert.
- Zurücksetzen des CMC – Die Gehäuseverwaltung wird wieder aufgenommen, nachdem der CMC neu gestartet oder das Gehäuse auf den Standby-CMC umgeschaltet wurde.
- CMC-Ausfallsicherungsbefehl gegeben — Die Gehäuseverwaltung wird wieder aufgenommen, nachdem das Gehäuse zum Standby-CMC gesichert wird.
- CMC-Firmware-Aktualisierung – Die Gehäuseverwaltung wird wieder aufgenommen, nachdem der CMC neu gestartet oder das Gehäuse auf den Standby-CMC umgeschaltet wurde. Es wird empfohlen, zunächst den Standby-CMC zu aktualisieren, so dass nur ein Failover-Ereignis auftreten kann.
- CMC-Fehlererkennung und -behebung – Die Gehäuseverwaltung wird wieder aufgenommen, nachdem der CMC zurückgesetzt oder das Gehäuse auf den Standby-CMC umgeschaltet wurde.

ANMERKUNG: Sie können das Gehäuse entweder mit einem einzelnen CMC oder mit redundanten CMCs konfigurieren. In redundanten CMC-Konfigurationen übernimmt das Standby-CMC die Gehäuseverwaltung, falls das primäre CMC die Kommunikation mit dem Gehäuse oder dem Verwaltungsnetzwerk verliert.

Aktiver CMC – Auswahlprozess

Die beiden CMC-Steckplätze unterscheiden sich nicht; das bedeutet, dass der Steckplatz alleine keine Vorrangfunktion bestimmt. Stattdessen übernimmt der zuerst installierte und gestartete CMC die Rolle des aktiven CMC. Wenn bei zwei installierten CMCs der Netzstrom eingeschaltet wird, übernimmt normalerweise der im Gehäusesteckplatz 1 installierte CMC die aktive Rolle. Die blaue LED zeigt den aktiven CMC an.

Wenn zwei CMCs in einem Gehäuse eingesetzt werden, das bereits eingeschaltet ist, kann die automatische Aktiv oder Standby-Verhandlung bis zu zwei Minuten dauern. Der normale Gehäusebetrieb wird wieder aufgenommen, wenn die Verhandlung abgeschlossen ist.

Funktionszustand eines redundanten CMC abrufen

Sie können den Funktionszustand eines Standby-CMC über die Webschnittstelle anzeigen. Weitere Informationen über den Zugriff auf den CMC-Funktionszustand über die Webschnittstelle finden Sie unter Anzeigen zu Gehäuseinformationen und Funktionszustandsüberwachung von Gehäuse und Komponenten.

Frontblende konfigurieren

Sie können Folgendes konfigurieren:

- Netzschalter
- LCD
- DVD-Laufwerk

Netzschalter konfigurieren

So gehen Sie for, um den Netzschalter zu konfigurieren

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Frontblende** > **Setup**.

2 Wählen Sie auf der Seite **Frontblendenkonfiguration** im Abschnitt **Netzschalterkonfiguration** die Option **Netzschalter des Gehäuses deaktivieren** und klicken Sie dann auf **Anwenden**.

Der Gehäusenetzschalter ist deaktiviert.

Konfigurieren von LCD

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Frontblende** > **Setup** .

2 Auf der Seite **Eigenschaften**, im Abschnitt **LCD-Konfiguration**:

- Wählen Sie die Option **LCD-Bedienfeld sperren** aus, um sämtliche Konfigurationen, die Sie unter Verwendung der LCD-Schnittstelle ausführen können, zu deaktivieren.
- Wählen Sie aus dem Dropdown-Menü **LCD-Sprache** die erforderliche Sprache aus.
- Wählen Sie aus dem Dropdown-Menü **LCD-Ausrichtung** den erforderlichen Modus – **Tower-Modus** oder **Rack-Modus** aus.

ANMERKUNG: **Wenn Sie das Gehäuse unter Verwendung des LCD-Assistenten konfigurieren und wenn Sie die Option Einstellungen automatisch zu neu eingefügten Servern anwenden auswählen, können sie die Funktion Einstellungen automatisch zu neu eingefügten Servern anwenden unter Verwendung einer Basic-Lizenz nicht deaktivieren. Wenn Sie nicht möchten, das diese Funktion wirksam wird, ignorieren Sie entweder die Meldung, die auf dem LCD angezeigt wird und die automatisch verschwindet; oder drücken Sie auf die Schaltfläche Nicht akzeptieren auf dem LCD und drücken Sie dann auf die mittlere Schaltfläche.**

3 Klicken Sie auf **Anwenden**.

Zugriff auf einen Server unter Verwendung von KVM

Um den KVM einem Server zuzuordnen und den Zugriff auf die Remote-Konsole durch die KVM-Schnittstelle zu aktivieren, können Sie die CMC-Webschnittstelle, RACADM oder die LCD-Scnittstelle verwenden.

Einen Server dem KVM under Verwendung der CMC-Webschnittstelle zuordnen

Stellen Sie sicher, dass die KVM-Konsole am Gehäuse angeschlossen ist.
So ordnen Sie einen Server einem KVM zu:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Frontblende** > **Setup** .

2 Wählen Sie auf der Seite **Frontblendenkonfiguration**, im Abschnitt **KVM-Konfiguration,** aus der Liste **KVM zugeordnet** den Steckplatz aus, der einem KVM zugeordnet werden muss, und klicken Sie dann auf **Anwenden**.

ANMERKUNG: **Der KVM ermöglicht die Zuordnung zu allen Serversteckplätzen. Wenn Sie einen Server mit voller Höhe einsetzen oder einen Server mit halber Höhe durch einem Server mit voller Höhe austauschen, wird das Server-Zuordnungsverhalten nicht geändert. Wenn der KVM jedoch einem unteren Steckplatz zugeordnet wird und der Steckplatz über einen Server mit voller Höhe verfügt, ist der KVM nur über den oberen Steckplatz verfügbar. Sie müssen den KVM den oberen Steckplätzen neu zuordnen.**

Einen Server under Verwendung von LCD einem KVM zuordnen

Stellen Sie sicher, dass die KVM-Konsole am Gehäuse angeschlossen ist.
So ordnen Sie einen Server under Verwendung von LCD einem KVM zu – Gehen Sie vom **Hauptmenü**-Bildschirm auf dem LCD zu **KVM-Zuordnung**, wählen Sie den Server, der zugeordnet werden muss und drücken Sie auf OK.

Einen Server einem DVD-Laufwerk zuordnen

So ordnen Sie den Server dem Gehäuse -DVD-Laufwerk zu:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Frontblende** > **Setup** .

2 Auf der Seite **Frontblendenkonfiguration** im Abschnitt **DVD-Laufwerkskonfiguration**:

Wählen Sie im Drop-Down-Menü **DVD zugeordnet** einen der Server aus. Wählen Sie die Server aus, für die Zugriff zum Gehäuse -DVD-Laufwerk erforderlich ist.

3 Klicken Sie auf **Anwenden**.

Die DVD ermöglicht die Zuordnung zu allen Serversteckplätzen. Wenn Sie einen Server mit voller Höhe einsetzen oder einen Server mit halber Höhe durch einem Server mit voller Höhe austauschen, wird das Server-Zuordnungsverhalten nicht geändert. Wenn die DVD jedoch einem unteren Steckplatz zugeordnet wird und der Steckplatz über einen Server mit voller Höhe verfügt, ist die DVD nur über den oberen Steckplatz verfügbar. Sie müssen die DVD den oberen Steckplätzen neu zuordnen.

3

Anmeldung beim CMC

Sie können sich beim CMC als CMC-Lokalbenutzer, als Microsoft Active Directory-Benutzer oder als LDAP-Benutzer anmelden. Der Standardbenutzername lautet `root`, und das Standardkennwort lautet `calvin`. Sie können sich auch über die einmalige Anmeldung (SSO) oder eine Smart Card anmelden.

ANMERKUNG: CMC unterstützt nicht die folgenden Sonderzeichen als Benutzername oder Kennwort vom Gehäuseprofil unter Verwendung von XML:

" , ! , #, $, %, ^, &, *, (,), -, _, +, =, ?, {, }, +, &, >, |, .., ', [

Themen:

Auf die CMC-Webschnittstelle zugreifen

Stellen Sie vor der Anmeldung bei CMC über die Webschnittstelle sicher, dass Sie einen unterstützten Web-Browser (Internet Explorer oder Firefox) konfiguriert haben und dass das Benutzerkonto mit den erforderlichen Berechtigungen erstellt wurde.

ANMERKUNG: Wenn Sie Microsoft Internet Explorer verwenden, die Verbindung über einen Proxy herstellen und der Fehler `The XML page cannot be displayed` angezeigt wird, müssen Sie den Proxy deaktivieren, um fortzufahren.

So greifen Sie auf die CMC-Webschnittstelle zu:

1. Öffnen Sie einen auf Ihrem System unterstützten Webbrowser.

   Die neuesten Informationen über unterstützte Webbrowser finden Sie in der *Dell Systems Software Support Matrix* unter **dell.com/support/manuals**.
2. Geben Sie in das Feld **Adresse** die folgende URL ein und drücken Sie die Eingabetaste:
   - Um mit einer IPv4-Adresse auf CMC zuzugreifen, geben Sie `https://<CMC IP-Adresse>` ein.

     Wenn die Standard-HTTPS-Anschlussnummer, Anschluss 443, geändert wurde, geben Sie Folgendes ein: `https://<CMC IP address>:<port number>`
   - Um mit einer IPv6-Adresse auf CMC zuzugreifen, geben Sie `https://[<CMC IP address>]` ein.

     Wenn die standardmäßige HTTPS-Schnittstellennummer (Schnittstelle 443) geändert wird, geben Sie Folgendes ein: `https://[<CMC IP address>]:<port number>`, wobei *<CMC-IP-Adresse>* für die CMC-IP-Adresse und *<Schnittstellennummer>* für die HTTPS-Schnittstellennummer steht.

Die Seite **CMC-Anmeldung** wird angezeigt.

ANMERKUNG: Bei Verwendung von IPv6 muss die <CMC-IP-Adresse> in eckige Klammern ([ ]) eingeschlossen werden.

Anmelden bei CMC als lokaler Benutzer, Active Directory-Benutzer oder LDAP-Benutzer

Um sich am CMC anzumelden, müssen Sie ein CMC-Konto mit der Berechtigung zum **Anmelden am CMC** besitzen. Der Standardbenutzername für das CMC-Modul ist root und das Standardkennwort lautet calvin. Das Konto „root“ ist das werkseitig voreingestellte Verwaltungskonto des CMC.

ANMERKUNG:

- Um die Sicherheit zu erhöhen, empfiehlt Dell dringend, das Standardkennwort des Root-Kontos bei der Ersteinrichtung zu ändern.
- Wenn die Zertifikatüberprüfung aktiviert ist, müssen Sie die FQDN des Systems angeben. Wenn die Zertifikatüberprüfung aktiviert und die IP-Adresse für den Domänen-Controller angegeben ist, schlägt die Anmeldung fehl.

CMC unterstützt keine erweiterten ASCII-Zeichen, wie ß, å, é, ü oder andere in nicht-englischen Sprachen verwendete Sonderzeichen.

So melden Sie sich als lokaler Benutzer, Active Directory-Benutzer oder LDAP-Benutzer an.

1 Geben Sie im Feld **Benutzername** Ihren Benutzernamen ein:
   - CMC-Benutzername: <Benutzername>
   - Active Directory-Benutzername: <Domäne>\<Benutzername>, <Domäne>/<Benutzername> oder <Benutzer>@<Domäne>.
   - LDAP-Benutzername: <Benutzername>

   ANMERKUNG: Dieses Feld unterscheidet Groß- und Kleinschreibung.
2 Geben Sie im Feld **Kennwort** das Benutzerkennwort ein.

   ANMERKUNG: Für Active Directory-Benutzer ist das Feld Benutzername abhängig von Groß-/Kleinschreibung.
3 Wählen Sie im Drop-Down-Menü des Felds **Domäne** die gewünschte Domäne aus.
4 Optional können Sie eine Sitzungszeitüberschreitung wählen. Dies ist die Dauer, die Sie ohne Aktivität angemeldet bleiben können, bevor Sie automatisch abgemeldet werden. Der Standardwert ist die **Web Service-Leerlaufzeitüberschreitung**.
5 Klicken Sie auf **OK**.

   Sie sind bei CMC mit den erforderlichen Berechtigungen angemeldet.

   Sie können sich auf einer einzelnen Workstation nicht mit verschiedenen Benutzernamen in mehreren Browserfenstern an der Webschnittstelle anmelden.

ANMERKUNG: Wenn die LDAP-Authentifizierung aktiviert ist und Sie versuchen, sich bei CMC mit den lokalen Anmeldeinformationen anzumelden, werden die Anmeldeinformationen zunächst im LDAP-Server und dann im CMC geprüft.

Anmeldung beim CMC mit Smart Card

Um diese Funktion zu verwenden, müssen Sie über eine Enterprise-Lizenz verfügen. Sie können sich über eine Smart Card bei CMC anmelden. Smart Cards verfügen über eine Zweifaktor-Authentifizierung (TFA) mit Sicherheit auf zwei Ebenen:

- Physisches Smart Card-Gerät.
- Geheimcode, z. B. ein Kennwort oder eine PIN.

Benutzer müssen ihre Anmeldeinformationen über die Smart Card und die PIN überprüfen.

ANMERKUNG: Sie können bei einer Smart Card-CMC-Anmeldung nicht die IP-Adresse verwenden. Kerberos überprüft Ihre Anmeldeinformationen gegenüber dem vollständig qualifizierten Domänennamen (FQDN).

Bevor Sie sich über eine Smart Card als Active Directory-Benutzer anmelden, müssen Sie die folgenden Schritte ausführen:

- Laden Sie ein vertrauenswürdiges Zertifikat einer Zertifizierungsstelle (ein von einer Zertifizierungsstelle signiertes Active Directory-Zertifikat) nach CMC hoch
- Konfigurieren Sie den DNS-Server.
- Aktivieren Sie die Active Directory-Anmeldung.
- Smart Card-Anmeldung aktivieren.

So melden Sie sich über eine Smart Card als Active Directory-Benutzer bei CMC an:

1 Melden Sie sich beim CMC unter Verwendung von `https://<cmcname.domain-name>` an.

Die **CMC-Anmeldeseite** wird eingeblendet und fordert Sie zum Einlegen einer Smart Card auf.

ANMERKUNG: Falls Sie die Standard-HTTPS-Schnittstellennummer (80) geändert haben, greifen Sie mit `<cmcname.domain-name>:<port number>` auf den CMC zu, wobei cmcname der CMC-Hostname für den CMC ist; *Domänenname* ist der Domänenname und *Schnittstellennummer* die HTTPS-Schnittstellennummer.

2 Legen Sie die Smart Card ein und klicken Sie auf **Anmeldung**.

Das Dialogfeld PIN wird angezeigt.

3 Geben Sie die PIN ein und klicken Sie auf **Senden**.

ANMERKUNG: Wenn der Smart Card-Benutzer in Active Directory vorhanden ist, wird kein Active Directory-Kennwort benötigt. Ansonsten müssen Sie sich mit dem entsprechenden Benutzernamen und Kennwort anmelden.

Sie sind über Ihre Active Directory-Anmeldedaten bei CMC angemeldet.

Anmelden beim CMC unter Verwendung der einfachen Anmeldung

Wenn die einfache Anmeldung (SSO) aktiviert ist, können Sie sich ohne die Eingabe Ihrer Anmeldeinformationen für die Domänen-Benutzerauthentifizierung (also Benutzername und Kennwort) bei CMC anmelden. Um diese Funktion zu nutzen, benötigen Sie eine Enterprise-Lizenz.

ANMERKUNG: Sie können bei SSO nicht die IP-Adresse verwenden. Kerberos überprüft Ihre Anmeldeinformationen gegenüber dem vollständig qualifizierten Domänennamen (FQDN).

Bevor Sie sich über SSO bei CMC anmelden, müssen Sie Folgendes sicherstellen:

- Sie haben sich über ein gültiges Active Directory-Benutzerkonto bei Ihrem System angemeldet.
- Die Option für die einmalige Anmeldung ist während der Active Directory-Konfiguration aktiviert.

So melden Sie sich am CMC unter Verwendung von SSO an:

1 Melden Sie sich unter Verwendung Ihres Netzwerkkontos beim Clientsystem an.

2 Greifen Sie auf die CMC-Webschnittstelle über `https://<cmcname.domain-name>` zu.

Beispiel: cmc-6G2WXF1.cmcad.lab, wobei cmc-6G2WXF1 der CMC-Name ist und cmcad.lab der Domänenname.

ANMERKUNG: Falls Sie die Standard-HTTPS-Schnittstellennummer (80) geändert haben, greifen Sie mit `<cmcname.domain-name>:<port number>` auf die CMC-Webschnittstelle zu, wobei *cmcname* der CMC-Hostname für den CMC ist; Domänenname ist der Domänenname und Schnittstellennummer die HTTPS-Schnittstellennummer.

Der CMC meldet Sie an und verwendet dabei die Kerberos-Anmeldeinformationen, die von Ihrem Browser zwischengespeichert wurden, als Sie sich unter Verwendung Ihres gültigen Active Directory-Kontos angemeldet haben. Falls die Anmeldung nicht erfolgreich ist, wird der Browser auf die normale CMC-Anmeldeseite geleitet.

ANMERKUNG: Falls Sie sich nicht bei der Active Directory-Domäne angemeldet haben und nicht Internet Explorer als Browser verwenden, schlägt die Anmeldung fehl und der Browser zeigt eine leere Seite an.

Anmeldung beim CMC unter Verwendung einer seriellen, Telnet- oder SSH-Konsole

Sie können sich beim CMC entweder mit einer seriellen, einer Telnet- oder einer SSH-Verbindung anmelden.

Nachdem Sie die Terminalemulationssoftware Ihrer Management Station und den verwalteten Knoten im BIOS konfiguriert haben, führen Sie die folgenden Tasks aus, um sich beim CMC anzumelden:

1 Verbinden Sie sich mit dem CMC unter Verwendung der Terminalemulationssoftware Ihrer Management Station.
2 Geben Sie Ihren CMC-Benutzernamen und das Kennwort ein und drücken dann <Eingabe>.
Sie sind am CMC angemeldet.

Verwandte Links

Verwenden der Telnet-Konsole mit CMC
Konfigurieren von Linux Minicom
Verwenden von SSH mit dem CMC

Auf den CMC über RACADM zugreifen

RACADM bietet eine Reihe von Befehlen an, mit denen Sie den CMC über eine textbasierte Oberfläche konfigurieren und verwalten können. Auf RACADM kann über eine Telnet-/SSH- oder eine serielle Verbindung zugegriffen werden, unter Verwendung der Dell CMC-Konsole auf dem KVM oder im Remote-Zugriff unter Verwendung der auf einer Management Station installierten RACADM-Befehlszeilenschnittstelle.

Die RACADM-Schnittstelle wird wie folgt klassifiziert:

- Remote-RACADM - damit können Sie RACADM-Befehle auf einer Management Station mit der Option -r und dem DNS-Namen oder der IP-Adresse des CMC ausführen.

  ANMERKUNG: Remote-RACADM ist Teil der *Dell Systems Management Tools und Dokumentation-DVD* und wird auf einer Management Station installiert.
- Firmware-RACADM - damit können Sie sich über Telnet, SSH oder eine serielle Verbindung am CMC anmelden. Mit Firmware-RACADM wird die RACADM-Implementierung ausgeführt, die Teil der CMC-Firmware ist.

Sie können RACADM-Befehle in Skripts im Remote-Zugriff zum Konfigurieren mehrerer CMCs verwenden. Sie können keine Skripts direkt auf der CMC-Web-Schnittstelle ausführen, da CMC kein Scripting unterstützt.

Weitere Informationen zu RACADM finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

Für weitere Informationen zur Konfiguration mehrerer CMCs, siehe Konfigurieren mehrerer CMCs über RACADM.

Anmeldung beim CMC mit Authentifizierung mit öffentlichem Schlüssel

Sie können sich über SSH beim CMC anmelden, ohne ein Kennwort einzugeben. Sie können auch einen einzelnen RACADM-Befehl als Befehlszeilenargument an die SSH-Anwendung senden. Die Befehlszeilenoptionen verhalten sich ähnlich wie Remote-RACADM, da die Sitzung endet, nachdem der Befehl ausgeführt wurde.

Stellen Sie vor der Anmeldung über SSH beim CMC sicher, dass die öffentlichen Schlüssel hochgeladen wurden. Um diese Funktion zu nutzen, benötigen Sie eine Enterprise-Lizenz.

Beispiel:

- **Anmelden**: `ssh service@<domain>` oder `ssh service@<IP_address>` , wobei IP_address die CMC IP-Adresse ist.

- **Senden von RACADM-Befehlen**: `ssh service@<domain> racadm getversion` und `ssh service@<domain> racadm getsel`

Wenn Sie sich mit den Dienstkonto anmelden und beim Erstellen des öffentlichen/privaten Schlüsselpaars wurde ein Kennsatz eingerichtet, werden Sie u. U. aufgefordert, diesen Kennsatz erneut einzugeben. Wenn ein Kennsatz mit den Schlüsseln verwendet wird, bieten Client-Systeme, die Windows und Linux ausführen, Methoden zur Automatisierung. Für Client-Systeme, die Windows ausführen, können Sie die Anwendung „Pageant" verwenden. Sie läuft im Hintergrund und macht die Eingabe des Kennsatzes transparent. Für Client-Systeme, die Linux ausführen, können Sie die Anwendung „sshagent" verwenden. Informationen über Einrichtung und Verwendung dieser Anwendungen finden Sie in der zur Anwendung gehörenden Dokumentation.

CMC-Mehrfachsitzungen

Hier können Sie eine Liste mit mehreren CMC-Sitzungen einsehen, die durch die Verwendung der diversen Schnittstellen möglich sind.

Tabelle 11. CMC-Mehrfachsitzungen

Schnittstelle	Anzahl der Sitzungen
CMC-Webschnittstelle	4
RACADM	4
Telnet	4
SSH	4

Ändern des standardmäßigen Anmeldungskennworts

Die Warnmeldung, die Sie auffordert das standardmäßige Anmeldungskennwort zu ändern, wird angezeigt, wenn:

- Sie sich beim CMC mit der Berechtigung **Benutzer konfigurieren** anmelden.
- Die Warnungsfunktion des standardmäßigen Kennworts aktiviert ist.
- Der standardmäßige Benutzername und das Kennwort des derzeit aktivierten Kontos `root` bzw. `calvin` sind.

Die gleiche Warnungsmeldung wird angezeigt, wenn Sie sich unter Verwendung von Active Directory oder LDAP anmelden. Konten von Active Directory oder LDAP werden nicht berücksichtigt, wenn bestimmt wird, ob ein Konto (lokal) `root` und `calvin` als Anmeldeinformationen hat. Es wird außerdem eine Warnungsmeldung angezeigt, wenn Sie sich beim CMC unter Verwendung von SSH, Telnet, Remote-RACADM oder Webschnittstelle anmelden. Für Webschnittstelle, SSH und Telnet wird eine einzelne Warnungsmeldung für jede Sitzung angezeigt. Für Remote-RACADM wird für jeden Befehl eine Warnungsmeldung angezeigt.

Um die Anmeldeinformationen zu ändern, müssen Sie über die Berechtigung **Benutzer konfigurieren** verfügen.

ANMERKUNG: Eine CMC-Protokollmeldung wird generiert, wenn auf der CMC-Anmeldeseite die Option Diese Warnung nicht mehr anzeigen ausgewählt wird.

Ändern des standardmäßigen Anmeldekennworts unter Verwendung von Web-Schnittstelle

Wenn Sie sich an der CMC-Webschnittstelle anmelden und die Seite **Standardmäßige Kennwortwarnung** angezeigt wird, können Sie das Kennwort ändern. Gehen Sie dabei folgendermaßen vor:

1 Wählen Sie die Option **Standardmäßiges Kennwort ändern**.

2 Geben Sie im Feld **Neues Kennwort** das neue Kennwort ein.

Das Kennwort darf maximal 20 Zeichen lang sein. Die Zeichen sind maskiert. Folgende Zeichen werden unterstützt:

- 0-9

- A-Z
- a-z
- Sonderzeichen: +, &, ?, >, -, }, |, ., !, (, ', ,, _,[, ", @, #,), *, ;, $,], /, §, %, =, <, :, {, |, \

3 Geben Sie in dem Feld **Kennwort bestätigen** das Kennwort erneut ein.

4 Klicken Sie auf **Fortfahren**. Das neue Kennwort ist konfiguriert und Sie sind am CMC angemeldet.

ANMERKUNG: Das Feld Fortfahren ist nur aktiviert, wenn die Felder Neues Kennwort und Kennwort bestätigen übereinstimmen.

Weitere Informationen zu den anderen Feldern finden Sie in der *Online-Hilfe*.

Ändern eines in den Standardeinstellungen festgelegten Anmeldungskennworts unter Verwendung von RACADM

So ändern Sie ein Kennwort mithilfe der Ausführung des folgenden RACADM-Befehls:

```
racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i <index> <newpassword>
```

wobei `<Index>` ein Wert zwischen 1 und 16 ist (und für das Benutzerkonto steht) und `<newpassword>` (<NeuesKennwort>) das neue benutzerdefinierte Kennwort ist.

Weitere Informationen finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX) unter **dell.com/support/manuals**.

Aktivieren oder Deaktivieren der standardmäßigen Kennwortwarnungsmeldung

Sie können die Anzeige der standardmäßigen Kennwortwarnungsmeldung aktivieren oder deaktivieren. Dafür benötigen Sie jedoch die Berechtigung **Benutzer konfigurieren**.

Aktivieren oder Deaktivieren einer standardmäßigen Kennwortwarnungsmeldung unter Verwendung der Web-Schnittstelle

So aktivieren oder deaktivieren Sie die Anzeige der standardmäßigen Kennwortwarnungsmeldung nach der Anmeldung bei iDRAC:

1 Wählen Sie **Gehäuse-Controller** > **Benutzerauthentifizierung** > **Lokale Benutzer**.

Die Seite **Benutzer** wird angezeigt.

2 Wählen Sie im Abschnitt **Standardmäßige Kennwortwarnung** die Option **Aktivieren** aus und klicken Sie anschließend auf **Anwenden**, um die Anzeige der Seite **Standardmäßige Kennwortwarnung** anzuzeigen, wenn Sie sich beim CMC anmelden. Andernfalls klicken Sie auf **Deaktivieren**.

Alternativ können Sie, wenn diese Option aktiviert ist und Sie eine Anzeige der Warnmeldung für nachfolgende Anmeldevorgänge vermeiden wollen, erst auf die Option **Diese Warnmeldung nicht noch einmal anzeigen** auf der Seite **Standardmäßigen Kennwortwarnung** und dann auf **Anwenden** klicken.

Aktivieren oder Deaktivieren der Warnungsmeldung zum Ändern des standardmäßigen Anmeldungskennworts unter Verwendung von RACADM

Um die Anzeige der Warnmeldung zur Änderung des standardmäßigen Anmeldekennworts unter Verwendung von RACADM zu aktivieren, benutzen Sie das Objekt `acadm config -g cfgRacTuning -o cfgRacTuneDefCredentialWarningEnable<0> or <1>`. Weitere Informationen hierzu finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX) unter **dell.com/support/manuals**.

Anwendungsszenarien

Dieser Abschnitt beschreibt typische Anwendungen und Aufgaben, die Sie mit der Chassis Management Controller Version 3.0 für Dell PowerEdge VRTX durchführen können.

Umwandlung externer freigegebener PERC 8-Karten vom Modus „Hohe Verfügbarkeit“ in „Nicht-hohe Verfügbarkeit“ unter Verwendung der Webschnittstelle

Das Dell PowerEdge VRTX-Gehäuse muss 2 externe freigegebene PERC 8-Karten in PCI-Steckplatz 5 und PCI-Steckplatz 6 haben und muss sich im HA-Modus befinden.

Workflow

1. Schalten Sie das Gehäuse aus. Trennen Sie alle SAS-Kabel von externen freigegebenen PERC 8-Karten ab und schließen Sie sie an MD12x0-Gehäusen an.
2. Schalten Sie das Gehäuse ein.
3. Melden Sie sich an der CMC-Webschnittstelle an, und wechseln Sie zum **Speicher→ Controller→ Fehlerbehebung** und deaktivieren Sie **Fehlertoleranz** aus dem Dropdown-Menü für die externe freigegebene PERC 8-Karte in Steckplatz 5, klicken Sie auf **Anwenden** und wählen Sie für Steckplatz 6 deaktivieren aus, und klicken Sie dann auf **Anwenden**.
4. Zurücksetzen beider PERCs wird u. U. erst nach zwei Minuten im Nicht-HA-Modus wiedergegeben.
5. Schalten Sie das Gehäuse aus und schließen Sie die Gehäuse im Nicht-HA-Modus an.
6. Schalten Sie das Gehäuse ein.
7. Externe freigegebene PERC 8-Karte ist nicht im Modus „Hohe Verfügbarkeit“; und navigieren Sie zu **Storage→ Fehlerbehebung→ Fehlerbehebung einrichten** zum Anzeigen des Nicht-HA Status.

Umwandlung externer freigegebener PERC 8-Karten vom Modus „Nicht-hohe Verfügbarkeit“ in „Hohe Verfügbarkeit“ unter Verwendung der Webschnittstelle

Das Dell PowerEdge VRTX-Gehäuse muss 2 externe freigegebene PERC 8-Karten in PCI-Steckplatz 5 und PCI-Steckplatz 6 haben.

Workflow

1. Schalten Sie das Gehäuse aus. Trennen Sie alle SAS-Kabel von externen freigegebenen PERC 8-Karten ab und schließen Sie sie an MD12x0-Gehäusen an.
2. Schalten Sie das Gehäuse ein.
3. Melden Sie sich an der CMC-Webschnittstelle an, und wechseln Sie zum **Speicher→ Controller→ Fehlerbehebung** und aktivieren Sie **Fehlertoleranz** aus dem Dropdown-Menü für die externe freigegebene PERC 8-Karte in Steckplatz 5, klicken Sie auf **Anwenden** und wählen Sie für Steckplatz 6 deaktivieren aus, und klicken Sie dann auf **Anwenden**.
4. Zurücksetzen beider PERCs wird u. U. erst nach zwei Minuten im HA-Modus wiedergegeben.
5. Schalten Sie das Gehäuse aus und schließen Sie die Gehäuse im HA-Modus an.
6. Schalten Sie das Gehäuse ein.
7. Externe freigegebene PERC 8-Karte ist im Modus „Hohe Verfügbarkeit"; und navigieren Sie zu **Storage→ Fehlerbehebung→ Fehlerbehebung einrichten** zum Anzeigen des HA-Status.

Umwandlung externer freigegebener PERC 8-Karten vom Modus „Hohe Verfügbarkeit" in „Nicht-hohe Verfügbarkeit" unter Verwendung von RACADM

Das Dell PowerEdge VRTX-Gehäuse muss 2 externe freigegebene PERC 8-Karten in PCI-Steckplatz 5 und PCI-Steckplatz 6 haben und muss sich im HA-Modus befinden.

Workflow

1. Schalten Sie das Gehäuse aus. Trennen Sie alle SAS-Kabel von externen freigegebenen PERC 8-Karten ab und schließen Sie sie an MD12x0-Gehäusen an.
2. Schalten Sie das Gehäuse ein.
3. Melden Sie sich am CMC Racadm an und führen Sie den folgenden Befehl aus, wenn die Server ausgeschaltet sind:

   ```
   racadm  raid set controllers:RAID.ChassisSlot.5-1 -p HighAvailabilityMode None
   ```
4. Führen Sie den Befehl `racadm raid set controllers:RAID.ChassisSlot.6-1 -p HighAvailabilityMode None` auf externen freigegebenen PERC 8-Karten in Steckplatz 6 aus.
5. Zurücksetzen beider PERCs wird u. U. erst nach zwei Minuten im HA-Modus wiedergegeben.
6. Schalten Sie das Gehäuse aus und schließen Sie die Gehäuse im Nicht-HA-Modus an.
7. Schalten Sie das Gehäuse ein.
8. Die externe freigegebene PERC 8-Karte ist nicht im Modus „Hohe Verfügbarkeit", und der folgende Befehl wird zur Anzeige des Status verwendet:

   ```
   racadm raid get controllers -o -p HighAvailabilityMode
   ```

Umwandlung externer freigegebener PERC 8-Karten vom Modus „Nicht-hohe Verfügbarkeit" in „Hohe Verfügbarkeit" unter Verwendung von RACADM

Das Dell PowerEdge VRTX-Gehäuse muss externe freigegebene PERC 8-Karten in PCI-Steckplatz 5 und PCI-Steckplatz 6 haben.

Workflow

1. Schalten Sie das Gehäuse aus. Trennen Sie alle SAS-Kabel von externen freigegebenen PERC 8-Karten ab und schließen Sie sie an MD12x0-Gehäusen an.
2. Schalten Sie das Gehäuse ein.

3 Melden Sie sich am CMC Racadm an und führen Sie den folgenden Befehl aus, wenn die Server ausgeschaltet sind:

```
racadm raid set controllers:RAID.ChassisSlot.5-1 –p HighAvailabilityMode ha
```

4 Führen Sie den Befehl `racadm raid set controllers:RAID.ChassisSlot.6-1 –p HighAvailabilityMode ha` auf externen freigegebenen PERC 8-Karten in Steckplatz 6 aus.

5 Zurücksetzen beider PERCs wird u. U. erst nach zwei Minuten im HA-Modus wiedergegeben.

6 Schalten Sie das Gehäuse aus und schließen Sie die Gehäuse im HA-Modus an.

7 Schalten Sie das Gehäuse ein.

8 Eine externe freigegebene PERC 8-Karte befindet sich im Modus „Hohe Verfügbarkeit“ (HA), und der HA-Status wird mithilfe des folgenden Befehls gesehen:

```
racadm raid get controllers -o -p HighAvailabilityMode
```

.

4

Aktualisieren der Firmware

Sie können die Firmware für Folgendes aktualisieren:

- CMC
- Gehäuseinfrastruktur
- VRTX Expander- oder Storage Backplane Expander-Firmware integrierter oder externer Gehäuse
- Physische Festplatten (HDD) pro Gehäuse

ANMERKUNG: Sie können die HDD-Firmware aktualisieren, nur falls erforderlich.

Sie können die Firmware für folgende E/A- und Serverkomponenten aktualisieren:

- E/A-Modul
- BIOS
- iDRAC
- Lifecycle-Controller
- 32–Bit-Diagnose
- Treiberpaket des Betriebssystems
- Netzwerkschnittstellen-Controller
- RAID-Controller auf dem Servermodul

ANMERKUNG: Die Firmware-Aktualisierung kann mehrere Minuten in Anspruch nehmen.

Themen:

Herunterladen der CMC-Firmware

Bevor Sie mit der Firmwareaktualisierung beginnen, laden Sie die aktuelle Firmwareversion von der Website **support.dell.com** herunter und speichern Sie sie auf Ihrem lokalen System.

Während der Aktualisierung der VRTX Chassis-Firmware sollten die Firmware-Versionen der Gehäusekomponenten in der folgenden Reihenfolge aktualisiert werden:

1 Blade-Komponenten-Firmware
2 CMC-Firmware
3 Gehäuseinfrastruktur-Firmware
4 Freigegebene PERC8-Firmware (integriert und extern)
5 Interne Speicherrückwandplatinen-Firmware und Erweiterungen externer Gehäuse
6 HDD-Firmware (externe und integrierte Gehäuse)

Weitere Informationen über die Aktualisierungssequenz für das VRTX-Gehäuse finden Sie in den *Anmerkungen zur Version CMC Firmware 2.0* unter **dell.com/cmcmanuals**.

Aktuelle Firmware-Versionen anzeigen

Sie können die aktuellen Firmware-Versionen über die CMC-Webschnittstelle oder über RACADM anzeigen.

Anzeige der aktuell installierten Firmwareversionen über die CMC-Webschnittstelle

Wählen Sie in der CMC-Webschnittstelle eine der folgenden Seiten aus, um die derzeit installierten Firmwareversionen anzuzeigen:

- **Gehäuseübersicht** > **Aktualisieren**
- **Gehäuseübersicht** > **Gehäuse-Controller** > **Aktualisieren**
- **Gehäuseübersicht** > **Server-Übersicht** > **Serverkomponentenaktualisierung**
- **Gehäuseübersicht** > **E/A-Modulübersicht** > **Aktualisieren**
- **Gehäuseübersicht** > **Speicher** > **Speicherkomponentenaktualisierung**

Die Seite **Firmware-Aktualisierung** zeigt die aktuelle Version der Firmware für jede aufgeführte Komponente an und ermöglicht Ihnen, die Firmware mit der neuesten Version zu aktualisieren.

Wenn sich im Gehäuse ein Server einer früheren Generation befindet, dessen iDRAC sich im Wiederherstellungsmodus befindet oder wenn der CMC beschädigte iDRAC-Firmware erkennt, wird der iDRAC einer früheren Generation ebenfalls auf der Seite **Firmware-Aktualisierung** aufgeführt.

Anzeige der aktuell installierten Firmwareversionen über RACADM

Verwenden Sie den Unterbefehl `racadm getsysinfo`, um die IP-Informationen für iDRAC und CMC, und die CMC-Service-Tag-Nummer oder Systemkennnummer unter Verwendung von RACADM anzuzeigen. Weitere Informationen über RACADM-Befehle finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

CMC-Firmware aktualisieren

Sie können die CMC-Firmware über die Webschnittstelle oder RACADM konfigurieren. Bei der Firmware-Aktualisierung werden die aktuellen CMC-Einstellungen standardmäßig beibehalten. Während des Aktualisierungsvorgangs können Sie die CMC-Konfigurationseinstellungen auf die werkseitigen Standardeinstellungen zurückzusetzen.

ANMERKUNG: Um Firmware auf dem CMC zu aktualisieren, müssen Sie die Berechtigung als Gehäusekonfigurations-Administrator besitzen.

Wenn eine Sitzung an der Internet-Benutzeroberfläche verwendet wird, um die Firmware für eine Systemkomponente zu aktualisieren, muss die Einstellung **Inaktivitätszeitüberschreitung (0, 60-10800)** zur Anpassung an die Dateiübertragungszeit auf einen höheren Wert festgelegt werden. Manchmal kann die Zeit zur Übertragung der Firmware-Datei bis zu 30 Minuten betragen. Informationen zur Einstellung des Wertes für die Inaktivitätszeitüberschreitung finden Sie unter Dienste konfigurieren.

Während der CMC-Firmware-Aktualisierungen laufen einige oder alle Lüftereinheiten im Gehäuse mit 100 % Geschwindigkeit.

Wenn im Gehäuse redundante CMCs installiert sind, wird es dringend empfohlen, dass beide auf die gleiche Firmware-Version aktualisiert werden. CMCs mit unterschiedlicher Firmware können im Falle eines Failovers zu unerwarteten Ergebnissen führen.

ANMERKUNG:

- Die CMC-Firmware kann für ein Gehäuse mit 1600W-Netzteil nicht auf eine frühere Version als 2.0 aktualisiert werden.
- Aktualisierungen oder Rollbacks der CMC-Firmware werden nur für die Firmware-Versionen 1.2, 1.25, 1.3, 1.31, 1.35, 1.36, 2.0, 2.01, 2.04 und höher unterstützt. Für alle andere Versionen aktualisieren Sie zunächst auf eine dieser Versionen und anschließend auf die erforderliche Version.

Nach dem erfolgreichen Abschluss des Firmware-Uploads wird der aktive CMC zurückgesetzt und ist vorübergehend nicht verfügbar. Wenn ein Standby-CMC vorhanden ist, tauschen Standby-CMC und aktiver CMC die Rollen. Der Standby-CMC wird zum aktiven CMC. Falls eine Aktualisierung nur auf den aktiven CMC angewendet wird nachdem der Reset abgeschlossen wurde, führt der aktive CMC das aktualisierte Image nach Abschluss des Resets nicht aus. Nur der Standby-CMC verfügt über dieses Image. Im Allgemeinen wird dringend empfohlen, für den aktiven CMC und den Standby-CMC identische Firmware-Versionen beizubehalten.

Nachdem der Standby-CMC aktualisiert wurde, tauschen Sie die CMC-Rollen, damit der neu aktualisierte CMC als aktiver CMC und der CMC mit der früheren Firmware als Standby-CMC fungiert. Lesen Sie für weitere Informationen zum Tauschen von Rollen den Abschnitt zum `cmcchangeover`-Befehl im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX). Durch Ausführen dieses Befehls können Sie überprüfen, ob die Aktualisierung erfolgreich war und die neue Firmware einwandfrei funktioniert, bevor Sie die Firmware für den zweiten CMC aktualisieren. Nachdem beide CMCs aktualisiert wurden, können Sie den `cmcchangeover`-Befehl verwenden, um die vorhergehenden Rollen der CMCs wiederherzustellen. CMC Firmwareversion 2.x aktualisiert sowohl den primären CMC als auch den redundanten CMC ohne Ausführung des `cmcchangeover`-Befehls.

Während der abschließenden Phase der Firmware-Aktualisierung im CMC werden die Browsersitzung und die Verbindung zum CMC vorübergehend unterbrochen, da der CMC nicht mit dem Netzwerk verbunden ist. Der CMC gibt den Gesamtzustand des Gehäuses aufgrund des verübergehenden Verlusts der Netzwerkverbindung als kritisch an. Wenn der CMC nach einigen Minuten neu startet, melden Sie sich am CMC an. Der CMC gibt den Gesamtzustand des Gehäuses dann als fehlerfrei an und die Netzwerkverbindung zum CMC ist hergestellt. Nach dem Reset des CMC wird die neue Firmware-Version auf der Seite **Firmware-Aktualisierung** angezeigt.

Damit andere Benutzer beim Reset nicht getrennt werden, benachrichtigen Sie autorisierte Benutzer, die sich möglicherweise am CMC anmelden, und überprüfen Sie die Seite **Sitzungen** auf aktive Sitzungen. Klicken Sie zum Öffnen der Seite **Sitzungen** im linken Fensterbereich auf **Gehäuseübersicht**, dann auf **Netzwerk** und schließlich auf **Sitzungen**.

Bei der Dateiübertragung zum und vom CMC dreht sich während der Übertragung das Dateiübertragungssymbol. Wenn das Symbol nicht animiert ist, stellen Sie sicher, dass Ihr Browser so konfiguriert ist, dass Animationen zugelassen sind. Weitere Informationen zum Zulassen von Animationen im Browser finden Sie unter Animationen im Internet Explorer zulassen.

ANMERKUNG: Wenn Sie in der aktuellen Version des CMC die Länge der Steckplatznamen auf mehr als 15 Zeichen konfiguriert haben, wird beim Zurückstufen der CMC-Firmware die Länge der Steckplatznamen auf 15 Zeichen abgeschnitten.

Signiertes CMC-Firmware-Image

Für VRTX CMC 2.0 oder höher enthält die Firmware eine Signatur. Die CMC-Firmware überprüft die Signatur, um die Authentizität der hochgeladenen Firmware sicherzustellen. Der Firmware-Update-Vorgang ist nur dann erfolgreich, wenn das Firmware-Image vom CMC als gültiges und unverändertes Image des Dienstanbieters authentifiziert wurde. Die Firmware-Aktualisierung wird beendet, wenn CMC die Signatur des hochgeladenen Firmware-Images nicht überprüfen kann. Ein Warnungsereignis wird protokolliert, und es wird eine entsprechende Fehlermeldung eingeblendet.

Die Signaturüberprüfung kann auf VRTX-Firmware-Versionen 1.2 und höher durchgeführt werden. Für Firmware-Zurückstufungen auf VRTX-Versionen vor 1.2 nehmen Sie zunächst eine Aktualisierung der Firmware auf eine VRTX CMC-Version höher als oder gleich 1.2, jedoch vor 2.0, vor. Nach dieser Aktualisierung kann eine Firmware-Zurückstufung auf frühere, nicht signierte VRTX-Versionen vorgenommen werden.

Aktualisieren der CMC-und Hauptplatinen-Firmware

Die gemeinsamen Funktionen von externen freigegebenen PERC 8-Karten stehen erst dann zur Verfügung, wenn CMC- und Hauptplatinen-Firmware aktualisiert wurden.

ANMERKUNG:

- Ziehen Sie zur Anzeige des MD12x0-Verkabelungsschemas das *Benutzerhandbuch für das Upgrade von PowerEdge VRTX zur Unterstützung gemeinsamer Speichererweiterung* oder das Handbuch für *Dell gemeinsam genutzte PowerEdge RAID-Controller (PERC) 8-Karten für Dell PowerEdge VRTX-Systeme* unter dell.com/support/manuals zu Rate.
- Der externe freigegebene Speicheradapter setzt voraus, dass Sie den CMC v2.20 oder höher und die Hauptplatine v2.21 oder höher aktualisieren, um die externe freigegebene PERC 8-Karte zu unterstützen.
- Sie können keine Herunterstufung der CMC-Firmware vor 2.2 mit externen freigegebenen Adaptern ausführen.

So aktualisieren Sie die CMC- und Hauptplatinen-Firmware:

1 Aktualisieren der CMC-Firmware
2 Aktualisieren Sie die Hauptplatinen-Firmware.
3 Schalten Sie das Gehäuse aus und installieren Sie freigegebene Speicheradapter im PCIe-Steckplatz 5 und 6.
4 Schalten Sie das Gehäuse wieder ein.
5 Nach dem Einschalten des Gehäuses aktualisieren Sie die externen freigegebenen Speicheradapter.

ANMERKUNG: Die externe freigegebene PERC 8-Karte befindet sich standardmäßig im nicht fehlertoleranten Modus. Sie muss in den Fehlertoleranz-Modus versetzt werden, nachdem sie korrekt verkabelt wurde. Weitere Informationen finden Sie im Dokument *Upgrading PowerEdge VRTX to Support Shared Storage Expansion* (Upgrade von PowerEdge VRTX zur Unterstützung gemeinsamer Speichererweiterung).

Im Fall, dass Sie ein Rollback der CMC- oder MPC/Hauptplatinen-Firmware- oder CMC- und MPC-Firmware-Version ausführen möchten, führen Sie die folgenden Aufgaben durch:

Zum Rollback der CMC- und Hauptplatinen-Firmware:

1 Schalten Sie das Gehäuse aus.
2 Entfernen Sie alle externen Speicheradapter aus den PCI-Steckplätzen.
3 Schalten Sie das Gehäuse ein.
4 Führen Sie das Rollback der CMC- und/oder Hauptplatinen-Firmware aus.

Sie können keine Herunterstufung der CMC ausführen, wenn ein externer freigegebener Speicheradapter erkannt wurde.

Wenn die Prozesse nicht der Reihe nach befolgt werden, wird das Systemverhalten zufällig und Teile des Systems können instabil werden. Der CMC protokolliert IOV- oder RAID-Controller-Meldungen. In der älteren Version des CMC sind nur freigegebene VA-

Speicherzuordnungen für PERC 1 und PERC 2 sichtbar. Alle externen freigegebenen VA-Speicherzuordnungen sind in der vorhergehenden Version des CMC nicht vorhanden. Wenn nach dem Rollback eine externe freigegebene PERC 8-Karte eingesetzt wird, wird sie vom CMC als nicht freigegebenerAdapter behandelt. Es kann vorkommen, dass der HOST-PERC-Treiber die externe freigegebene PERC 8-Karte nicht unterstützt.

CMC-Firmware über die Webschnittstelle aktualisieren

ANMERKUNG:

- Stellen Sie vor dem Anwenden der CMC-Aktualisierung sicher, dass das Gehäuse eingeschaltet ist. Wenn die Blades eingeschaltet sind, ist es zum Ausführen der CMC-Aktualisierung nicht erforderlich, sie auszuschalten.
- Das Zurückstufen der CMC-Firmware vor Version 2.1 mit externen freigegebenen Adaptern ist blockiert.

So aktualisieren Sie die CMC-Firmware unter Verwendung der CMC-Webschnittstelle:

1 Gehen Sie im linken Fensterbereich zu einer der folgenden Seiten:
   - **Gehäuseübersicht** > **Aktualisieren**
   - **Gehäuseübersicht** > **Gehäuse-Controller** > **Aktualisieren**
2 Wählen Sie auf der Seite **Firmware-Aktualisierung** im Abschnitt **CMC-Firmware** die erforderlichen Komponenten in der Spalte **Aktualisierungsziele** für den CMC oder die CMCs aus, (falls ein Standby-CMC vorhanden ist), den/die Sie aktualisieren möchten und klicken Sie dann auf **CMC-Aktualisierung anwenden**.
3 Klicken Sie im Feld **Firmware-Image** auf **Durchsuchen** (Internet Explorer oder Firefox) oder **Datei auswählen** (Google Chrome), um zum Dateispeicherort zu gelangen. Der Standardname der CMC-Firmware-Imagedatei lautet `vrtx_cmc.bin`.
4 Klicken Sie auf **Begin Firmware Update (Firmware-Update beginnen)**. Der Abschnitt **Fortschritt der Firmware-Aktualisierung** bietet Statusinformationen zur Firmwareaktualisierung. Ein Statusindikator wird auf der Seite während des Aktualisierungsvorganges angezeigt. Die Übertragungszeit kann je nach Verbindungsgeschwindigkeit variieren. Wenn der interne Aktualisierungsprozess beginnt, wird die Seite laufend aktualisiert und zeigt den Firmwareaktualisierungszeitgeber an.
5 Bei einem Standby-CMC zeigt das Feld **Aktualisierungsstatus** den Text **Fertig** an, wenn die Aktualisierung abgeschlossen ist. Bei einem aktiven CMC wird die Browsersitzung und die Verbindung zum CMC während der abschließenden Phase der Firmware-Aktualisierung vorübergehend unterbrochen, weil der aktive CMC nicht mit dem Netzwerk verbunden ist. Sie müssen sich nach einigen Minuten neu anmelden, wenn der aktive CMC neu gestartet ist. Nach dem Reset des CMC wird die neue Firmware auf der Seite **Firmware-Aktualisierung** angezeigt.

   ANMERKUNG: Nach der Firmware-Aktualisierung löschen Sie die Dateien aus dem Cache des Internet-Browsers. Anweisungen zum Löschen des Browser-Cache finden Sie in der Online-Hilfe zu Ihrem Webbrowser.

Zusätzliche Anweisungen:

- Klicken Sie während der Dateiübertragung nicht auf das Symbol **Aktualisierung** und navigieren Sie nicht zu einer anderen Seite.
- Um den Prozess abzubrechen, klicken Sie auf die Option **Dateiübertragung und Aktualisierung abbrechen**. Diese Option ist nur während der Dateiübertragung verfügbar.
- Das Feld **Aktualisierungsstatus** zeigt den Firmware-Aktualisierungsstatus an.

ANMERKUNG: Der Aktualisierungsvorgang kann für den CMC einige Minuten dauern.

Aktualisieren der CMC-Firmware unter Verwendung von RACADM

Verwenden Sie den Unterbefehl `fwupdate`, um die CMC-Firmware über RACADM zu aktualisieren. Weitere Informationen zu RACADM-Befehlen finden Sie unter *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

ANMERKUNG: Führen Sie den Firmware-Update-Befehl nur über eine Remote-RACADM-Sitzung auf einmal aus.

Gehäuseinfrastruktur-Firmware aktualisieren

Der Aktualisierungsvorgang für die Gehäuseinfrastruktur-Firmware aktualisiert die Komponenten wie Hauptplatine und PCIe-Subsystem-Management-Firmware.

ANMERKUNG: Um die Gehäuseinfrastruktur-Firmware zu aktualisieren, stellen Sie sicher, dass das Gehäuse eingeschaltet und die Server ausgeschaltet sind.

ANMERKUNG: Wenn die Hauptplatine auf eine neuere Version aktualisiert wird, werden das Gehäuse und der Chassis Management Controller möglicherweise neu gestartet.

Aktualisierung der Gehäuseinfrastruktur-Firmware unter Verwendung der CMC Web-Schnittstelle

1 Gehen Sie zu einer der folgenden Seiten:
   - **Gehäuseübersicht** > **Aktualisieren**
   - **Gehäuseübersicht** > **Gehäuse-Controller** > **Aktualisieren**
2 Wählen Sie auf der Seite **Firmware-Aktualisierung** im Abschnitt **Gehäuseinfrastruktur-Firmware** in der Spalte **Ziele aktualisieren** die Option und klicken Sie dann auf **Gehäuseinfrastruktur-Firmware anwenden** .
3 Klicken Sie auf der Seite **Firmware-Aktualisierung** auf **Durchsuchen** und wählen Sie dann die entsprechende Gehäuseinfrastruktur-Firmware.
4 Klicken Sie auf **Firmware-Aktualisierung beginnen** und dann klicken Sie auf **Ja**.
   Der Abschnitt **Fortschritt der Firmware-Aktualisierung** bietet Statusinformationen zur Firmwareaktualisierung. Während des Aktualisierungsvorganges wird auf der Seite ein Statusindikator angezeigt. Die Übertragungszeit kann je nach Verbindungsgeschwindigkeit variieren. Wenn der interne Aktualisierungsprozess beginnt, wird die Seite laufend aktualisiert und zeigt den Firmwareaktualisierungszeitgeber an.

Zusätzliche Anweisungen:

- Verwenden Sie während der Dateiübertragung nicht die Schaltfläche **Aktualisierung** und navigieren Sie nicht zu einer anderen Seite.
- Das Feld **Aktualisierungsstatus** zeigt den Firmware-Aktualisierungsstatus an.

Wenn die Aktualisierung abgeschlossen ist, gibt es einen kurzzeitigen Verlust der Konnektivität auf der Hauptplatine, da sie zurückgesetzt wird, und die neue Firmware wird auf der Seite **Firmware-Aktualisierung** angezeigt.

Aktualisierung der Gehäuseinfrastruktur-Firmware mit RACADM

Um die Gehäuseinfrastruktur-Firmware mit RACADM zu aktualisieren, verwenden Sie den `fwupdate`-Unterbefehl. Weitere Informationen zur Verwendung der RACADM-Befehle finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

Server-iDRAC-Firmware aktualisieren

Sie können die Firmware für iDRAC über die CMC-Web-Schnittstelle oder über RACADM aktualisieren. Für diese Funktion benötigen Sie eine Enterprise-Lizenz.

Die iDRAC-Firmware-Version muss 1.40.40 oder höher für Server mit iDRAC sein.

Der iDRAC (auf einem Server) wird zurückgesetzt und ist vorübergehend nach einer Firmware-Aktualisierung nicht verfügbar.

ANMERKUNG: Um die iDRAC-Firmware unter Verwendung des Chassis Management-Controllers zu aktualisieren, muss eine SD-Karte im Gehäuse verfügbar sein. Für die Aktualisierung der iDRAC-Firmware über die iDRAC-Webschnittstelle ist jedoch eine SD-Karte im CMC-Modul nicht erforderlich. Weitere Informationen zum Starten der iDRAC-Webschnittstelle über CMC finden Sie unter Starten von iDRAC von der Server-Statusseite.

Server-iDRAC Firmware über die Webschnittstelle aktualisieren

So aktualisieren Sie die iDRAC-Firmware im Server:

1 Gehen Sie zu einer der folgenden Seiten:
- **Gehäuseübersicht** > **Aktualisieren**.
- **Serverübersicht** > **Aktualisieren** > **Serverkomponentenaktualisierung**.

Die Seite **Firmware-Aktualisierung** wird angezeigt.

ANMERKUNG:
Sie können auch Server-iDRAC-Firmware unter **Gehäuseübersicht** > **Server-Übersicht** > **Aktualisierung** aktualisieren. Weitere Informationen finden Sie unter Aktualisieren der Serverkomponenten-Firmware.

2 Klicken Sie zum Aktualisieren der iDRAC7- oder iDRAC8-Firmware im Abschnitt **iDRAC7-Firmware** bzw. **iDRAC8-Firmware** auf den Link **Aktualisierung** des Servers, für den Sie die Firmware aktualisieren möchten.

Die Seite **Serverkomponentenaktualisierung** wird angezeigt. Um fortzufahren, lesen Sie Aktualisieren der Serverkomponenten-Firmware.

3 Im Feld **Firmware-Image** geben Sie den Pfad zur Firmware-Image-Datei auf Ihrer Managementstation oder dem gemeinsam genutzten Netzwerk ein oder klicken Sie auf **Durchsuchen**, um zum Dateispeicherort zu navigieren. Der Standardname für das iDRAC-Firmware-Image ist **firming.imc**.

4 Klicken Sie auf **Firmware-Aktualisierung beginnen** und dann klicken Sie auf **Ja**.

Der Abschnitt **Fortschritt der Firmware-Aktualisierung** bietet Statusinformationen zur Firmwareaktualisierung. Eine Fortschrittsleiste zeigt den Status des Hochladevorgangs an. Die Übertragungszeit kann je nach Verbindungsgeschwindigkeit variieren. Wenn der interne Aktualisierungsprozess beginnt, wird die Seite laufend aktualisiert und zeigt den Firmwareaktualisierungszeitgeber an.

ANMERKUNG: Zusätzliche Anweisungen:
- Verwenden Sie während der Dateiübertragung nicht die Schaltfläche **Aktualisierung** und navigieren Sie nicht zu einer anderen Seite.
- Um den Prozess abzubrechen, klicken Sie auf **Dateiübertragung und Aktualisierung abbrechen**. Diese Option ist nur während der Dateiübertragung verfügbar.
- Das Feld **Aktualisierungsstatus** zeigt den Firmware-Aktualisierungsstatus an.

Die Aktualisierung der iDRAC-Firmware kann bis zu zehn Minuten dauern.

Aktualisieren der Serverkomponenten-Firmware

Die Eins-zu-n-Aktualisierungsfunktion in der CMC ermöglicht Ihnen, die Serverkomponenten-Firmware über mehrere Server zu aktualisieren. Sie können die Serverkomponenten unter Verwendung der Dell Update Packages aktualisieren, die auf dem lokalen System oder auf einer Netzwerkfreigabe verfügbar sind. Dieser Vorgang wird aktiviert, indem die Lifecycle-Controller-Funktionalität auf dem Server genutzt wird.

Der Lifecycle-Controller-Dienst ist auf jedem der Server verfügbar und wird durch iDRAC unterstützt. Sie können Firmware von Komponenten und Geräten auf den Servern unter Verwendung des Lifecycle-Controller-Dienstes verwalten. Der Lifecycle-Controller verwendet für die Aktualisierung der Firmware einen Authentifizierungsalgorithmus, der die Anzahl der Neustarts auf effiziente Art und Weise reduziert.

Der Lifecycle Controller bietet eine Modulaktualisierungsunterstützung für iDRAC7 und Server mit neueren Versionen.

ANMERKUNG: Vor der Verwendung der Lifecycle-Controller-basierten Aktualisierungsfunktion müssen die Server-Firmwareversionen aktualisiert werden. Sie müssen auch die CMC-Firmware vor dem Aktualisieren der Firmware-Module für die Serverkomponente aktualisieren.

ANMERKUNG: Um die Komponenten-Firmware zu aktualisieren, muss die CSIOR-Option für Server aktiviert sein. So aktivieren Sie CSIOR auf:

- Server der 12. Generation und höher – Wählen Sie nach dem Neustart des Servers aus dem F2-Setup **iDRAC-Einstellungen** > **Lifecycle Controller** aus, aktivieren Sie **CSIOR** und speichern Sie die Änderungen.
- Server der 13. Generation – Drücken Sie nach dem Neustart des Servers, wenn Sie dazu aufgefordert werden, auf die Taste F10, um auf den Lifecycle-Controller zuzugreifen. Wechseln Sie zu der Seite **Hardware-Bestandsliste**, indem Sie **Hardware-Konfiguration** > **Hardware-Bestandsaufnahme** auswählen. Auf der Seite **Hardware-Bestandsliste,** klicken Sie auf **Systembestandsaufnahme beim Neustart sammeln**.

Die Methode **Aktualisierung über Datei** ermöglicht Ihnen die Aktualisierung der Serverkomponenten-Firmware unter Verwendung der DUP-Dateien, die auf einem lokalen System gespeichert sind. Sie können die einzelnen Serverkomponenten für die Firmwareaktualisierung unter Verwendung der erforderlichen DUP-Dateien auswählen. Sie können eine umfassende Anzahl an Komponenten gleichzeitig aktualisieren, indem Sie eine SD-Karte zum Speichern einer DUP-Datei mit mehr als 48 MB Speicherkapazität verwenden.

ANMERKUNG: Beachten Sie Folgendes:

- Stellen Sie während der Auswahl der einzelnen zu aktualisierenden Server-Komponenten sicher, dass keine Abhängigkeiten zwischen den ausgewählten Komponenten bestehen. Andernfalls kann die Auswahl bestimmter Komponenten, bei denen Abhängigkeiten zu anderen Komponenten bestehen, dazu führen, dass der Server unerwartet ausfällt.
- Stellen Sie sicher, dass die empfohlene Reihenfolge für die Aktualisierung der Serverkomponenten eingehalten wird. Andernfalls kann die Komponenten-Firmware-Aktualisierung unter Umständen nicht erfolgreich abgeschlossen werden.

  Aktualisieren Sie immer die Firmware-Module der Serverkomponente in der folgenden Reihenfolge:

  – BIOS
  – Lifecycle-Controller
  – iDRAC

Mit der Aktualisierung aller Blades mit nur einem Klick oder der Methode **Aktualisierung über Netzwerkfreigabe** können Sie die Firmware der Serverkomponenten anhand von DUP-Dateien durchführen, die auf einer Netzwerkfreigabe gespeichert sind. Mit der auf Dell Repository Manager (DRM) basierenden Aktualisierungsfunktion können Sie auf die auf der Netzwerkfreigabe gespeicherten DUP-Dateien zugreifen und die Serverkomponenten in einem einzigen Vorgang aktualisieren. Sie haben die Möglichkeit, ein benutzerdefiniertes Remote-Repository mit Firmware-DUPs und binären Images zu erstellen und dieses unter Verwendung von Dell Repository Manager auf der Netzwerkfreigabe freizugeben. Alternativ können Sie mit Dell Repository Manager (DRM) nach den neuesten Firmware-Aktualisierungen suchen. Dell Repository Manager (DRM) sorgt dafür, dass Ihre Dell Systeme stets über das neueste BIOS sowie aktuelle Treiber, Firmware und Software verfügen. Auf der Support-Website (**support.dell.com**) können Sie eine Suche nach neuesten Aktualisierungen für die unterstützten Plattformen nach Marke und Modell oder nach Service-Tag-Nummer durchführen. Sie können die Aktualisierungen herunterladen oder anhand der Suchergebnisse ein Repository anlegen. Weitere Informationen zur Verwendung von DRM zum Suchen nach den neuesten Firmware-Aktualisierungen finden Sie unter Verwenden des Dell Repository Managers zum Suchen nach den neuesten Aktualisierungen auf der Dell Support-Site im Dell Tech Center. Informationen zum Speichern der Bestandsdatei, die DRM als Eingabe für die Repository-Erstellung heranzieht, finden Sie unter Speichern des Bestandsaufnahmenreports des Gehäuses unter Verwendung der CMC Web-Schnittstelle.

ANMERKUNG: Die Methode „Aktualisieren aller Blades durch einmaliges Klicken“ bietet folgende Vorteile:

- Sie ermöglicht Ihnen mit wenigen Klicks alle Komponenten auf allen Blade-Servern zu aktualisieren.
- Alle Aktualisierungen sind in einem Verzeichnis gebündelt. Dadurch wird verhindert, dass die Firmwares der Komponenten einzeln hochgeladen werden.
- Schnellere und konsistente Methode zur Aktualisierung der Server-Komponenten
- Sie ermöglicht Ihnen ein Standard-Image mit den erforderlichen Aktualisierungsversionen der Serverkomponenten zu verwalten, dass dazu verwendet werden kann, in einem einzigen Vorgang mehrere Server zu aktualisieren.
- Sie können die Aktualisierungsverzeichnisse von der Dell Server Update Utility (SUU)-Download-DVD kopieren oder die erforderlichen Aktualisierungsversionen in Dell Repository Manager (DRM) erstellen und anpassen. Zur Erstellung dieses Verzeichnisses sind Sie nicht auf die neueste Version von Dell Repository Manager angewiesen. Allerdings bietet Dell Repository Manager in Version 1.8 eine Option zum Erstellen eines Repositorys (Verzeichnis mit Aktualisierungen) anhand der von den Servern im Gehäuse exportierten Bestandsaufnahme. Weitere Informationen zum Erstellen eines Repositorys unter Verwendung von Dell Repository Manager finden Sie in den Benutzerhandbüchern *Dell Repository Manager Data Center Version 1.8 User's Guide* und *Dell Repository Manager Business Client Version 1.8 User's Guide* unter **dell.com/support/manuals**.

Der Lifecycle-Controller bietet Modulaktualisierungssupport für iDRAC6 und iDRAC7. Es wird empfohlen, die CMC-Firmware zu aktualisieren, bevor die Firmwaremodule der Serverkomponenten aktualisiert werden. Nach der Aktualisierung der CMC-Firmware können Sie über die Webschnittstelle auf der Seite **Gehäuseübersicht** > **Serverübersicht** > **Aktualisierung** > **Serverkomponentenaktualisierung** die Firmware der Serverkomponenten aktualisieren. Es wird außerdem empfohlen, alle Komponentenmodule eines Servers auszuwählen und zusammen zu aktualisieren. Dadurch können die optimierten Algorithmen des Lifecycle-Controllers zur Aktualisierung der Firmware verwendet und die Anzahl der Neustarts verringert werden.

Um die Serverkomponenten-Firmware mithilfe der CMC Web-Schnittstelle zu aktualisieren, klicken Sie auf **Gehäuseübersicht** > **Server-Übersicht** > **Aktualisierung** > **Serverkomponenten-Aktualisierung**.

Wenn der Server den Lifecycle-Controller-Dienst nicht unterstützt, wird im Abschnitt **Komponente/Gerät-Firmware-Bestandsaufnahme** der Text **Nicht unterstützt** angezeigt. Für die neueste Generation von Servern können Sie die Lifecycle-Controller-Firmware installieren und die iDRAC-Firmware aktualisieren, um den Lifecycle-Controller-Dienst zu aktivieren. Für ältere Servergenerationen ist diese Aktualisierung möglicherweise nicht durchführbar.

Normalerweise wird die Lifecycle-Controller-Firmware über ein geeignetes Installationspaket installiert, das auf dem Server-Betriebssystem ausgeführt werden muss. Für unterstützte Server ist ein spezielles Reparatur-/Installationspaket mit der Dateinamenerweiterung **.usc** verfügbar. Diese Datei ermöglicht Ihnen, die Lifecycle-Controller-Firmware über die Firmware-Aktualisierungseinrichtung zu installieren, die auf der systemeigenen iDRAC-Web-Browser-Schnittstelle verfügbar ist.

Die Lifecycle-Controller-Firmware kann auch über ein entsprechendes Installationspaket installiert werden, das auf dem Serverbetriebssystem ausgeführt werden muss. Weitere Informationen finden Sie im *Dell Lifecycle Controller-Benutzerhandbuch*.

Wenn der Dienst Lifecycle-Controller des Servers deaktiviert ist, wird der Abschnitt **Komponente/Gerät-Firmware-Bestandsaufnahme** angezeigt.

```
Lifecycle Controller may not be enabled.
```

Sequenz der Serverkomponentenaktualisierung

Wenn Sie Komponenten einzeln aktualisieren, müssen Sie die Firmwareversionen für die Serverkomponenten in der folgenden Sequenz aktualisieren:

- iDRAC
- Lifecycle-Controller
- Diagnose (optional)
- BS-Treiberpakete
- BIOS
- NIC
- RAID

- Sonstige Komponenten

ANMERKUNG: Wenn Sie die Firmwareversionen für alle Serverkomponenten gleichzeitig aktualisieren, dann wird die Aktualisierungssequenz vom Lifecycle-Controller bestimmt.

Aktivierung des Lifecycle Controllers

Sie können den Lifecycle Controller-Dienst während des Einschaltens eines Servers aktivieren:

- Klicken Sie für den Zugriff von iDRAC-Servern auf der Startkonsole auf das **System-Setup** die Taste <F2>.
- Gehen Sie auf der Seite **System-Setup-Hauptmenü** zu **iDRAC-Einstellungen** > **Lifecycle-Controller** und klicken Sie auf **Aktiviert**. Gehen Sie auf die Seite **System-Setup Hauptmenü** und klicken Sie auf **Fertigstellen**, um die Einstellungen zu speichern.

Das Abbrechen des Systemdienstes ermöglicht Ihnen, alle zeitlich eingeplanten, anstehenden Aufträge abzubrechen und sie aus der Warteschlange zu entfernen.

Lesen Sie für weitere Informationen über den Lifecycle Controller, unterstützte Server-Komponenten und die Gerätefirmware-Verwaltung das:

- *Lifecycle Controller-Remote Services Quick Start Guide* (Lifecycle Controller Remote Services-Benutzerhandbuch).
- **delltechcenter.com/page/Lifecycle+Controller**

Auf der Seite **Serverkomponenten-Aktualisierung** können Sie verschiedene Firmware-Komponenten auf dem Server aktualisieren. Zur Verwendung der Merkmale und Funktionen dieser Seite müssen Sie über folgendes verfügen:

- Für CMC: **Server Administrator**-Berechtigung.
- Für iDRAC: **iDRAC-Konfigurations**berechtigung und **iDRAC-Anmeldungs**berechtigung.

Im Fall von unzureichenden Berechtigungen können Sie nur die Firmware-Bestandsliste von Komponenten und Geräten auf dem Server anzeigen lassen. Sie können keine Komponenten oder Geräte für irgendeinen Typ von Lifecycle Controller-Vorgang auf dem Server auswählen.

Auswählen des Aktualisierungstyp der Serverkomponenten-Firmware unter Verwendung der CMC Web-Schnittstelle

So wählen Sie den Typ der Serverkomponentenaktualisierung aus:

1 Wählen Sie in der Systemstruktur **Server-Übersicht** aus und klicken Sie auf **Aktualisierung** > **Serverkomponentenaktualisierung**. Die Seite **Serverkomponentenaktualisierung** wird angezeigt.
2 Wählen Sie im Abschnitt **Aktualisierungstyp auswählen** die erforderliche Aktualisierungsmethode:
   - **Von Datei aktualisieren**
   - **Von Netzwerkfreigabe aktualisieren**

Filtern von Komponenten für Firmware-Aktualisierungen

Informationen über alle Komponenten und Geräte werden über alle Server hinweg auf einmal abgerufen. Um diese große Menge an Informationen zu verwalten, stellt der Lifecycle-Controller verschiedene Filtermechanismen zur Verfügung.

ANMERKUNG: Um diese Funktion verwenden zu können, benötigen Sie eine Enterprise-Lizenz.

Der Abschnitt **Komponenten-/Geräte-Aktualisierungsfilter** auf der Seite **Serverkomponentenaktualisierung**, mit dem Sie Daten anhand der Komponente filtern können, ist nur für den Modus **Aktualisierung nach Datei** verfügbar.

Diese Filter ermöglichen Ihnen Folgendes:

- Eine oder mehr Kategorien von Komponenten oder Geräten für das bequeme Anzeigen auswählen.
- Firmwareversionen von Komponenten und Geräten über den Server hinweg vergleichen.
- Um die Kategorie einer bestimmten Komponente bzw. eines Gerätes basierend auf Typen oder Modellen einzuengen, filtern Sie automatisch die ausgewählten Komponenten und Geräte.

> **ANMERKUNG: Die automatische Filterfunktion ist während der Verwendung des Dell Update Package (DUP) von Bedeutung. Die Aktualisierungsprogrammierung eines DUP kann auf dem Typ oder Modell einer Komponente oder eines Gerätes basieren. Die Funktionsweise der automatischen Filterung ist so ausgelegt, dass die auf eine Erstauswahl folgenden Auswahlentscheidungen minimiert werden.**

Es folgen einige Beispiele für die Anwendung der Filtermechanismen:

- Bei Auswahl des BIOS-Filters wird nur die BIOS-Bestandsliste aller Server angezeigt. Wenn der Serversatz aus mehreren Servermodellen besteht und ein Server für eine BIOS-Aktualisierung ausgewählt wird, entfernt die automatische Filterlogik automatisch alle anderen Server, die nicht mit dem Modell des ausgewählten Servers übereinstimmen. Dadurch wird sichergestellt, dass die Auswahl des BIOS-Firmware-Aktualisierungs-Image (DUP) mit dem richtigen Servermodell kompatibel ist.

  In manchen Fällen kann ein BIOS-Firmware-Aktualisierungs-Image über mehrere Servermodelle hinweg kompatibel sein. Derartige Optimierungen werden für den Fall ignoriert, dass diese Kompatibilität zukünftig nicht länger gegeben ist.
- Automatisches Filtern ist für Firmware-Aktualisierungen von NICs (Network Interface Controllers) und RAID-Controllern von Bedeutung. Diese Gerätekategorien haben verschiedene Typen und Modelle. Analog dazu können die Firmware-Aktualisierungs-Images (DUPs) in optimierter Form zur Verfügung stehen, wobei ein einziges DUP zur Aktualisierung mehrerer Typen oder Modelle von Geräten einer gegebenen Kategorie programmiert werden kann.

Filtern von Komponenten für Firmware-Aktualisierungen mit der CMC-Webschnittstelle

So filtern Sie die Geräte

1 Gehen Sie im linken Fensterbereich zu **Server-Übersicht** und klicken Sie dann auf **Aktualisierung**.

2 Wählen Sie auf der Seite **Serverkomponentenaktualisierung** im Abschnitt **Komponente/Geräteaktualisierungsfilter** eines oder mehrere der Folgenden aus:
   - **BIOS**
   - **iDRAC**
   - **Lifecycle-Controller**
   - **32-Bit Diagnose**
   - **BS-Treiberpaket**
   - **Netzwerkschnittstellencontroller (I/F)**
   - **RAID-Controller**

   Der Abschnitt **Komponenten-/Geräte-Aktualisierungsfilter** wird nur für den Firmware-Aktualisierungsmodus **Aktualisierung nach Datei** angezeigt.

   Der Abschnitt **Firmware-Bestandsaufnahme** zeigt nur die zugeordneten Komponenten oder Geräte auf allen Servern im Gehäuse an. Nachdem Sie ein Element aus dem Drop-Down-Menü ausgewählt haben, werden nur die Komponenten oder Geräte, die denen in der Liste zugeordnet sind, angezeigt.

   Nachdem der gefilterte Satz an Komponenten und Geräten im Bestandsaufnahmeabschnitt angezeigt wird, kann eine weitere Filterung auftreten, wenn eine Komponente oder ein Gerät für die Aktualisierung ausgewählt wird. Wenn z.B. der BIOS-Filter ausgewählt wird, zeigt der Bestandsaufnahmeabschnitt alle Server nur mit ihrer BIOS-Komponente an. Wenn eine BIOS-Komponente auf einem der Server ausgewählt wird, wird die Bestandsaufnahme weiter gefiltert, um die Server anzuzeigen, die mit der Modellbezeichnung des ausgewählten Servers übereinstimmen.

   Wenn ein Filter nicht ausgewählt wird und im Bestandsaufnahmeabschnitt eine Auswahl zur Aktualisierung einer Komponente oder eines Gerätes vorgenommen wird, dann wird der mit dieser Auswahl verbundene Filter automatisch aktiviert. Es kann eine weitere Filterung auftreten, bei der der Bestandsaufnahmeabschnitt alle Server anzeigt, die eine Übereinstimmung mit der gewählten

Komponente hinsichtlich des Modells, Typs oder irgendeiner anderen Identitätsform aufweisen. Wenn z.B. eine BIOS-Komponente auf einem der Server für die Aktualisierung ausgewählt wird, wird der Filter automatisch auf BIOS eingestellt und der Bestandsaufnahmeabschnitt zeigt die Server an, die mit der Modellbezeichnung des ausgewählten Servers übereinstimmen.

Komponenten für die Firmware-Aktualisierung über RACADM filtern

Um Komponenten für die Firmware-Aktualisierung über RACADM zu filtern, benutzen Sie den Befehl **getversion**:

```
racadm getversion -l [-m <Modul>] [-f <Filter>]
```

Weitere Informationen finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX), verfügbar unter **dell.com/support/manuals**.

Anzeigen der Firmware-Bestandsliste

Sie können die Zusammenfassung der Firmware-Versionen für alle Komponenten und Geräte für alle aktuell im Gehäuse vorhandenen Server und deren Status anzeigen.

ANMERKUNG: Um diese Funktion verwenden zu können, benötigen Sie eine Enterprise-Lizenz.

Firmwarebestandsaufnahme über die CMC-Webschnittstelle anzeigen

So zeigen Sie die Firmware-Bestandsaufnahme an:

1 Klicken Sie im linken Fensterbereich auf **Server-Übersicht** und klicken Sie dann auf **Aktualisierung**.

2 Zeigen Sie auf der Seite **Serverkomponenten-Aktualisierung** die Firmware-Bestandsaufnahmedetails im Abschnitt **Komponente/Gerät-Firmware-Bestandsaufnahme** an. Sie können auf dieser Seite folgende Informationen anzeigen:

- Server, die derzeit den Lifecycle-Controller-Dienst nicht unterstützen, werden als **Nicht unterstützt** aufgeführt. Es steht ein Hyperlink zur Verfügung, der zu einer alternativen Seite führt, auf der es möglich ist, nur die iDRAC-Firmware zu aktualisieren. Diese Seite unterstützt nur iDRAC-Firmware-Aktualisierung und keine Aktualisierung irgendwelcher anderer Komponenten oder Geräte des Servers. iDRAC-Firmware-Aktualisierung ist nicht von dem Lifecycle-Controller-Dienst abhängig.
- Wird der Server als **Nicht bereit** aufgeführt, weist dies darauf hin, dass sich der iDRAC auf dem Server zum Zeitpunkt des Abrufens der Firmware-Bestandsaufnahme noch in der Initialisierungsphase befand. Warten Sie, bis der iDRAC komplett betriebsbereit ist und aktualisieren Sie dann die Seite, damit die Firmware-Bestandsaufnahme erneut abgerufen werden kann.
- Wenn die Bestandsaufnahme der Komponenten und Geräte nicht dem entspricht, was physisch auf dem Server installiert ist, rufen Sie den Lifecycle-Controller während des Server-Startvorgangs auf. Diese Aktion ist beim Aktualisieren der integierten Komponenten- und Geräteinformationen hilfreich und ermöglicht Ihnen die Prüfung der derzeit installierten Komponenten und Geräte. Der Bestand zeigt die Komponenten- und Geräteinformationen ungenau an, wenn:
  - Die Server-iDRAC-Firmware aktualisiert wird, um die Lifecycle Controller-Funktionalität neu bei der Serververwaltung einzuführen.
  - Die neuen Geräte in den Server eingesetzt werden.

  Um diese Maßnahme zu automatisieren, stellt das iDRAC-Konfigurationshilfsprogramm eine Option bereit, auf die über die Startkonsole zugegriffen werden kann.

  1 Damit iDRAC-Server auf **System-Setup** zugreifen können, drücken Sie auf der Startkonsole <F2>.

  2 Klicken Sie auf der Seite **System-Setup-Hauptmenü** auf **iDRAC-Einstellungen** > **Systeminventar beim Neustart erfassen**, wählen Sie **Aktiviert** und gehen Sie zurück zur Seite **System-Setup-Hauptmenü**. Klicken Sie dann auf **Fertigstellen**, um die Einstellungen zu speichern.
- Es stehen Optionen zum Durchführen der verschiedenen Lifecycle Controller-Vorgänge, wie z.B. Aktualisierung, Rollback, Neuinstallation und Joblöschung zur Verfügung. Es kann immer nur ein Vorgangstyp durchgeführt werden. Nicht unterstützte

Komponenten und Server werden möglicherweise als Teil der Bestandsaufnahme aufgeführt, Lifecycle Controller-Vorgänge sind jedoch zulässig.

Die folgende Tabelle zeigt Informationen zu Komponenten und Geräten auf dem Server an:

Tabelle 12. Komponenten- und Geräteinformationen

Feld	Beschreibung
Steckplatz	Zeigt den vom Server im Gehäuse besetzten Steckplatz an. Steckplatznummern sind sequenzielle IDs von 1 bis 4 (für die vier im Gehäuse verfügbaren Steckplätze), mit denen die Position des Servers im Gehäuse identifiziert werden kann. Wenn weniger als vier Steckplätze mit Servern belegt sind, werden nur die mit Servern bestückten Steckplätze angezeigt.
Name	Zeigt den Namen des Servers in den einzelnen Steckplätzen an.
Modell	Zeigt das Modell des Servers an.
Komponente/Gerät	Zeigt eine Beschreibung der Komponente oder des Geräts auf dem Server an. Wenn die Spaltenbreite zu schmal ist, stellt das Mouse-Over-Hilfswerkzeug eine Ansicht mit der Beschreibung bereit.
Aktuelle Version	Zeigt die aktuelle Version der Komponente oder des Geräts auf dem Server an.
Rollback-Version	Zeigt die Rollback-Version der Komponente oder des Geräts auf dem Server an.
Jobstatus	Zeigt den Jobstatus von jeglichen Vorgängen an, die auf dem Server geplant sind. Der Jobstatus wird kontinuierlich dynamisch aktualisiert. Wenn ein Jobabschluss über den Status als abgeschlossen erkannt wird, werden für den Fall, dass sich bei einer der Komponenten oder Geräte die Firmwareversion geändert hat, die Firmwareversionen der Komponenten und Geräte auf dem Server automatisch aktualisiert. Neben dem aktuellen Status ist auch ein Info-Symbol vorhanden, das zusätzliche Informationen über den aktuellen Jobstatus bereitstellt. Diese Informationen können angezeigt werden, indem auf das Symbol geklickt wird oder der Mauszeiger über dem Symbol angehalten wird.
Aktualisierung	Klicken Sie, um die Komponenten oder das Gerät für die Firmware-Aktualisierung auf dem Server auszuwählen.

Anzeigen der Firmware-Bestandsliste über RACADM

Um die Firmware-Bestandsliste über RACADM anzuzeigen, verwenden Sie den `getversion`-Befehl:

```
racadm getversion -l [-m <Modul>] [-f <Filter>]
```

Weitere Informationen finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX), verfügbar unter **dell.com/support/manuals**.

Speichern des Bestandsaufnahmenreports des Gehäuses mit der CMC-Web-Schnittstelle

So speichern Sie den Bestandsaufnahmenreport des Gehäuses:

1. Wählen Sie in der Systemstruktur **Server-Übersicht** aus und klicken Sie auf **Aktualisierung** > **Serverkomponentenaktualisierung**.
   Die Seite **Serverkomponentenaktualisierung** wird angezeigt.
2. Klicken Sie auf **Bestandsbericht speichern**.
   Die Datei *Inventory.xml* ist in einem externen System gespeichert.

ANMERKUNG: Die Dell Repository Manager-Anwendung verwendet die Datei *Inventory.xml* als Eingabe zur Erstellung eines Repository der Updates für alle im Gehäuse verfügbaren Blades. Dieses Repository kann später auf eine Netzwerkfreigabe exportiert werden. Der Firmware-Aktualisierungsmodus Von Netzwerkfreigabe aktualisieren verwendet diese Netzwerkfreigabe für die Aktualisierung der Komponenten aller Server. Auf den einzelnen Servern muss die CSIOR-Funktion aktiviert sein, und Sie müssen den Bestandsaufnahmenreport des Gehäuses bei jeder Änderung der Hardware- oder Softwarekonfiguration des Gehäuses speichern.

Konfigurieren der Netzwerkfreigabe mit der CMC Web-Schnittstelle

So konfigurieren oder bearbeiten Sie den Standort oder die Anmeldeinformationen der Netzwerkfreigabe:

1 Gehen Sie in der CMC Web-Schnittstelle, in der Systemstruktur, zu **Serverübersicht**, und klicken Sie anschließend auf **Netzwerkfreigabe**.

Die Seite **Netzwerkfreigabe bearbeiten** wird angezeigt.

ANMERKUNG: Wenn Sie über den gleichen Ordner für Gehäuse, Server und das Startidentitätsprofil verfügen, wird die Leistung bei mehr als 100 Profilen möglicherweise beeinträchtigt.

2 Konfigurieren Sie im Abschnitt **Einstellungen der Netzwerkfreigabe** die folgenden Einstellungen nach Bedarf:

- Protokoll
- IP-Adresse oder Host-Name
- Freigabenname
- Aktualisierungsordner
- Dateiname (optional)

ANMERKUNG: Das Eingeben eines Dateinamens ist nur dann optional, wenn der standardmäßige Katalogdateiname catalog.xml lautet. Wenn der Katalogdateiname geändert wird, dann muss der neue Name in dieses Feld eingegeben werden.

- Profil-Ordner
- Domain Name
- Benutzername
- Kennwort
- SMB-Version

ANMERKUNG: Die Option SMB-Version ist nur dann verfügbar, wenn der Protokoll-Typ CIFS ist.

ANMERKUNG: Wenn Sie ein mit einer Domäne registriertes CIFS verwenden und mithilfe der IP mit den lokalen Benutzeranmeldeinformationen für CIFS auf das CIFS zugreifen, muss der Hostname oder die Host-IP in das Feld Domänenname eingegeben werden.

Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.

3 Klicken Sie auf **Verzeichnis testen**, um sicherzustellen, dass die Verzeichnisse les- und beschreibbar sind.

4 Klicken Sie auf **Netzwerkverbindung testen**, um sicherzustellen, dass der Standort der Netzwerkfreigabe zugreifbar ist.

Falls Sie eine SMB-Version anwenden, wird die Bereitstellung der vorhandenen Netzwerkfreigabe aufgehoben und die Netzwerkfreigabe wieder bereitgestellt, sobald Sie auf **Netzwerkverbindung testen** klicken oder zu anderen GUI-Seiten navigieren.

5 Klicken Sie auf **Anwenden**, um die Änderungen für die Eigenschaften der Netzwerkfreigabe zu übernehmen.

ANMERKUNG:

Klicken Sie auf **Zurück**, um zur Seite **Serverkomponentenaktualisierung** zurückzukehren.

Lifecycle-Controller-Jobvorgänge

ANMERKUNG: Um diese Funktion zu verwenden, benötigen Sie eine Enterprise-Lizenz.

Sie können Lifecycle-Controller-Vorgänge wie diese durchführen:

- Neuinstallation
- Zurücksetzen
- Aktualisierung
- Jobs löschen

Es kann immer nur ein Vorgangstyp durchgeführt werden. Nicht unterstützte Komponenten und Server werden möglicherweise als Teil der Bestandsliste aufgeführt, Lifecycle Controller-Vorgänge sind jedoch zulässig.

Zum Durchführen der verschiedenen Lifecycle Controller-Vorgänge brauchen Sie:

- Für CMC: Server Administrator-Berechtigung.
- Für iDRAC: iDRAC-Konfigurationsberechtigung und iDRAC-Anmeldungsberechtigung.

Ein Lifecycle Controller-Vorgang, der auf einem Server geplant wurde, kann 10 bis 15 Minuten dauern, bis er abgeschlossen wird. Der Vorgang beinhaltet mehrere Neustarts des Servers, wobei die Firmwareinstallation ausgeführt wird, die außerdem eine Firmwareprüfstufe beinhaltet. Sie können den Fortschritt dieses Prozesses auf der Serverkonsole einsehen. Wenn auf einem Server mehrere Komponenten oder Geräte vorhanden sind, die aktualisiert werden müssen, können Sie alle Aktualisierungen in einem geplanten Vorgang konsolidieren, wodurch die Anzahl der erforderlichen Neustarts minimiert wird.

In manchen Fällen wird ein weiterer Vorgang gestartet, wenn ein Vorgang gerade über eine andere Sitzung oder einen anderen Kontext für die Planung eingereicht wird. In diesem Fall wird eine Bestätigungsmeldung angezeigt, die auf die Situation hinweist und der Vorgang darf nicht eingereicht werden. Warten Sie, bis der Vorgang abgeschlossen wurde und reichen Sie den Vorgang anschließend erneut ein.

Verlassen Sie die Seite nicht, wenn ein Vorgang für die Planung eingereicht wurde. Wird ein Versuch unternommen, wird eine Bestätigungsmeldung angezeigt, die ein Abbrechen der beabsichtigten Navigation ermöglicht. Anderenfalls wird der Vorgang unterbrochen. Eine Unterbrechung, insbesondere während eines Aktualisierungsvorgangs, kann einen Abbruch des Hochladens der Firmware-Image-Datei vor der ordnungsgemäßen Fertigstellung verursachen. Stellen Sie nach dem Einreichen eines Vorgangs zur Planung sicher, dass die Bestätigungsmeldung zur Anzeige der erfolgreichen Planung des Vorgangs bestätigt wird.

Serverkomponenten-Firmware neu installieren

Sie können das Firmware-Image der aktuell installierten Frimware für die ausgewählten Komponenten oder Geräte über einen oder mehrere Server hinweg erneut installieren. Das Firmware-Image steht innerhalb des Lifecycle Controllers zur Verfügung.

Neuinstallation der Serverkomponenten-Firmware über die Webschnittstelle

So führen Sie eine Neuinstallation der Serverkomponenten-Firmware aus:

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Aktualisierung**.
2. Wählen Sie auf der Seite **Serverkomponentenaktualisierung** im Abschnitt **Aktualisierungstyp auswählen** die Option **Aktualisierung von Datei** aus.
3. Wählen Sie in der Spalte **Aktuelle Version** die Option für die Komponente oder das Gerät aus, für die oder das Sie die Firmware neu istallieren möchten.
4. Wählen Sie eine der folgenden Optionen:
   - **Jetzt neu starten** - Server sofort neu starten.

- **Bei nächstem Neustart** – Manuell zu einem späteren Zeitpunkt neu starten.

5 Klicken Sie auf **Neu installieren**. Die Firmware-Version für die ausgewählten Komponenten oder Geräte wird neu installiert.

Zurücksetzen der Serverkomponenten-Firmware

Sie können das Firmware-Image der zuvor installierten Frimware für ausgewählte Komponenten oder Geräte über einen oder mehrere Server hinweg installieren. Das Firmware-Image steht innerhalb des Lifecycle Controllers für einen Rollback-Vorgang zur Verfügung. Die Verfügbarkeit unterliegt der Versionskompatibilitätslogik des Lifecycle Controllers. Es wird auch angenommen, dass die vorherige Aktualisierung mittels des Lifecycle Controllers stattgefunden hat.

ANMERKUNG: Um diese Funktion verwenden zu können, benötigen Sie eine Enterprise-Lizenz.

Zurücksetzen der Serverkomponenten-Firmware über die CMC-Webschnittstelle

So setzen Sie die Serverkomponenten-Firmware auf eine vorherige Version zurück:

1 Klicken Sie im linken Fensterbereich auf **Server-Übersicht→ Aktualisieren**.

2 Wählen Sie auf der Seite **Serverkomponentenaktualisierung** im Abschnitt **Aktualisierungstyp auswählen** die Option **Aktualisierung von Datei** aus.

3 Wählen Sie in der Spalte **Version zurücksetzen** die Option für die Komponente oder das Gerät, für die oder das Sie die Firmware zurücksetzen möchten.

4 Wählen Sie eine der folgenden Optionen:

- **Jetzt neu starten** - Server sofort neu starten.
- **Bei nächstem Neustart** – Manuell zu einem späteren Zeitpunkt neu starten.

5 Klicken Sie auf **Zurücksetzen**. Die vorher installierte Firmware-Version für die ausgewählten Komponenten oder Geräte wird neuinstalliert.

Aktualisieren der Serverkomponenten-Firmware

Sie können die nächste Version des Firmware-Image für die ausgewählten Komponenten oder Geräte über einen oder mehrere Server hinweg installieren. Das Firmware-Image steht innerhalb des Lifecycle Controllers für einen Rollback-Vorgang zur Verfügung. Um diese Funktion zu nutzen, benötigen Sie eine Enterprise-Lizenz.

ANMERKUNG: Stellen Sie für iDRAC- und Betriebssystem-Treiber-Pakete sicher, dass die Erweiterte Speicherfunktion aktiviert ist.

Es wird empfohlen, die Jobswarteschlange zu löschen, bevor Sie die Aktualisierung einer Serverkomponentenfirmware initialisieren. Auf der Seite **Lifecycle Controller-Jobs** ist eine Liste mit allen Jobs auf den Servern vorhanden. Diese Seite ermöglicht die Löschung einzelner/mehrerer Jobs oder die Bereinigung aller Jobs auf dem Server.

BIOS-Aktualisierungen sind Servermodell-spezifisch. Manchmal wird die Aktualisierung möglicherweise auf alle NIC-Geräte auf dem Server angewendet, obwohl ein einzelnes NIC-Gerät (Network Interface Controller) für eine Firmwareaktualisierung ausgewählt wurde. Dieses Verhalten gehört zur Lifecycle Controller-Funktionalität und insbesondere zur im DUP (Dell Update Package) enthaltenen Programmierung. Derzeit werden DUPs (Dell Update Packages) mit einer Größe von weniger als 48 MB unterstützt.

Wenn die Größe des Aktualisierungsdatei-Images größer ist, zeigt der Jobsstatus an, dass das Herunterladen fehlgeschlagen ist. Werden auf einem Server mehrere Serverkomponenten-Aktualisierungen versucht, überschreitet die kombinierte Größe aller Firmware-Aktualisierungen möglicherweise 48 MB. In einem solchen Fall schlägt eine der Komponenten-Aktualisierungen fehl, da deren Aktualisierungsdatei abgeschnitten wird. Zum Aktualisieren mehrerer Komponenten auf einem Server wird empfohlen, zuerst die Lifecycle-Controller- und 32-Bit-Diagnose-Komponenten zusammen zu aktualisieren. Diese benötigen keinen Neustart des Servers und können relativ schnell abgeschlossen werden. Die anderen Komponenten können anschließend zusammen aktualisiert werden.

Alle Lifecycle Controller-Aktualisierungen werden für die unverzügliche Ausführung geplant. Die Systemdienste können diese Ausführung jedoch manchmal verzögern. In solchen Situationen schlägt die Aktualisierung infolgedessen fehl, da die durch den CMC gehostete Remote-Freigabe nicht länger zur Verfügung steht.

Aktualisieren der Serverkomponenten-Firmware von Datei über die CMC Web-Schnittstelle

So aktualisieren Sie die Version der Serverkomponenten-Firmware auf die nächste Version mithilfe der Methode **Aktualisierung von Datei**:

1 Gehen Sie in der CMC-Web-Schnittstelle in der Systemstruktur zu **Server-Übersicht** und klicken Sie anschließend auf **Aktualisieren** > **Server-Komponentenaktualisierung**.

Die Seite **Serverkomponentenaktualisierung** wird angezeigt.

2 Wählen Sie im Abschnitt **Aktualisierungstyp auswählen** die Option **Aktualisierung von Datei** aus. Weitere Informationen finden Sie unter Auswählen des Aktualisierungstyps der Serverkomponenten-Firmware unter Verwendung der CMC Web-Schnittstelle

3 Filtern Sie im Abschnitt **Komponenten-/Geräte-Aktualisierungsfilter** die Komponente oder das Gerät (wahlweise). Weitere Informationen finden Sie unter Filtern von Komponenten für Firmware-Aktualisierungen über die CMC-Web-Schnittstelle.

4 Wählen Sie in der Spalte **Aktualisieren** das/die Kontrollkästchen für die Komponente oder das Gerät, für die oder das Sie die Firmware auf die nächste Version aktualisieren möchten. Verwenden Sie das STRG-Tastenkürzel, um einen Komponenten- oder Gerätetyp für die Aktualisierung über alle zutreffenden Server hinweg auszuwählen. Das Drücken und Halten der STRG-Taste markiert alle Komponenten in gelb. Wählen Sie bei gedrückter STRG-Taste die erforderliche Komponente oder das Gerät aus, indem Sie das zugehörige Kontrollkästchen in der Spalte **Aktualisieren** aktivieren.

Eine sekundäre Tabelle wird angezeigt, die den ausgewählten Typ der Komponente oder des Geräts sowie einen Wähler für die Firmware-Imagedatei aufführt. Für jeden Komponententyp wird ein Wähler für die Firmware-Image-Datei angezeigt.

Einige Geräte wie Netzwerkschnittstellen-Controller (NICs) und RAID-Controller können viele Typen und Modelle enthalten. Die Aktualisierungsauswahllogik filtert den entsprechenden Gerätetyp bzw. das Modell basierend auf den ursprünglich ausgewählten Geräten. Der primäre Grund für dieses automatische Filterverhalten ist es, das für die Kategorie nur eine Firmware-Imagedatei angegeben werden kann.

ANMERKUNG: Die Größenbeschränkung für die Aktualisierung von entweder einzelnen DUPs oder kombinierten DUPs kann ignoriert werden, wenn die Funktion "Erweiterter Speicher" installiert und aktiviert wurde. Weitere Informationen zum Aktivieren des erweiterten Speichers finden Sie unter CMC Erweiterte Speicherkarte konfigurieren.

5 Geben Sie die Firmware-Image-Datei für die ausgewählte(n) Komponente(n) bzw. das/die ausgewählte(n) Gerät(e) an. Das ist eine Microsoft Windows Dell Update Package (DUP)-Datei.

6 Wählen Sie eine der folgenden Optionen:

- **Jetzt neu starten** – Sofort neu starten. Die Firmware-Aktualisierung wird sofort angewandt.
- **Bei nächstem Neustart** – Manuell zu einem späteren Zeitpunkt neu starten. Die Firmware-Aktualisierung wird nach dem nächsten Neustart angewandt.

ANMERKUNG: Dieser Schritt ist für Lifecycle-Controller- und 32-Bit-Diagnose-Firmwareaktualisierung nicht gültig. Ein Server-Neustart ist für diese Geräte nicht erforderlich.

7 Klicken Sie auf **Aktualisieren**. Die Firmware-Version für die ausgewählten Komponenten oder Geräte wird aktualisiert.

Einzelklick-Aktualisierung der Serverkomponenten unter Verwendung der Netzwerkfreigabe

Die Server oder Serverkomponenten-Aktualisierung erfolgt über eine Netzwerk-Freigabe mithilfe von Dell Repository Manager. Die Dell PowerEdge VRTX-Gehäuse-Integration vereinfacht dabei die Aktualisierung, indem benutzerdefinierte Firmware-Pakete verwendet werden, so dass die Bereitstellung schneller und einfacher durchgeführt werden kann. Die Aktualisierung von einer Netzwerkfreigabe bietet die Flexibilität zur gleichzeitigen Aktualisierung aller 12G-Server mit einem einzelnen Katalog von einer CIFS- oder von einer NFS.

Diese Methode bietet eine schnelle und einfache Möglichkeit zur Erstellung eines benutzerdefinierten Repository für verbundene Systeme unter Verwendung des Dell Repository Manager und der Gehäuse-Bestandsaufnahme-Datei, die mit der CMC-Webschnittstelle exportiert wird. Mit DRM können Sie ein vollständig benutzerdefiniertes Repository erstellen, das nur die Aktualisierungspakete für die jeweilige Systemkonfiguration enthält. Ferner können Sie Repositories erstellen, die nur Aktualisierungen für veraltete Geräte enthalten, oder ein Baseline-Repository, das Aktualisierungen für alle Geräte enthält. Sie können auch Update-Pakete für Linux oder Windows anhand des gewünschten Aktualisierungsmodus erstellen. Mit DRM können Sie das Repository auf eine CIFS- oder NFS-Freigabe speichern. Mit der CMC-Webschnittstelle können Sie Anmeldeinformationen und Standortinformationen der Freigabe konfigurieren. Anschließend können Sie mit der CMC-Web-Schnittstelle die Serverkomponenten-Aktualisierung für einen einzelnen Server oder für mehrere Server ausführen.

Voraussetzungen für die Verwendung des Aktualisierungsmodus mit Netzwerkfreigabe

Folgende Voraussetzungen sind erforderlich, um Serverkomponenten-Firmware im Netzwerkfreigabe-Modus zu aktualisieren:

- Die Server müssen der 12. Generation oder höher angehören und müssen über eine iDRAC-Enterprise-Lizenz verfügen.
- Die CMC-Version muss Version 2.0 oder höher sein.
- Lifecycle Controller muss auf den Servern aktiviert sein.
- iDRAC Version 1.50.50 oder höher muss auf den Servern der 12. Generation verfügbar sein.
- Dell Repository Manager 1.8 oder höher muss auf dem System installiert sein.
- Sie müssen über CMC-Administratorrechte verfügen.

Aktualisieren der Serverkomponenten-Firmware über die Netzwerkfreigabe unter Verwendung der CMC-Web-Schnittstelle

So aktualisieren Sie die Version der Serverkomponenten-Firmware zur nächsten Version mit dem **Aktualisierung über Netzwerkfreigabe**-Modus:

1. Gehen Sie in der CMC-Webschnittstelle in der Systemstruktur zu **Server-Übersicht** und klicken Sie anschließend auf **Aktualisieren** > **Server-Komponentenaktualisierung**.

   Die Seite **Serverkomponentenaktualisierung** wird angezeigt.
2. Wählen Sie im Abschnitt **Aktualisierungstyp auswählen** die Option **Aktualisierung über Netzwerkfreigabe**. Weitere Informationen finden Sie unter Auswählen des Typs der Serverkomponenten-Firmwareaktualisierung.
3. Wenn die Netzwerkfreigabe nicht angeschlossen ist, konfigurieren Sie die Netzwerkfreigabe für das Gehäuse. Klicken Sie zum Konfigurieren oder Bearbeiten der Einzelheiten der Netzwerkfreigabe in der Tabelle der Netzwerkfreigabe-Eigenschaften auf **Bearbeiten**. Weitere Informationen finden Sie unter Konfigurieren der Netzwerkfreigabe mit der CMC Web-Schnittstelle.
4. Klicken Sie auf **Bestandsaufnahmebericht speichern**, um die Datei der Gehäusebestandsaufnahme zu exportieren, die die Komponenten- und Firmwaredetails enthält.

   Die Datei *Inventory.xml* wird auf ein externes System gespeichert. Der Dell Repository Manager verwendet die Datei *inventory.xml* zur Erstellung benutzerdefinierter Bündel von Updates. Das Repository wird in der von CMC konfigurierten CIFS- oder NFS-Freigabe gespeichert. Weitere Informationen zum Erstellen eines Repository mithilfe von Dell Repository Manager finden Sie im *Dell Repository Manager Data Center Version 1.8-Benutzerhandbuch* und im *Dell Repository Manager-Business-Client-Version 1.8-Benutzerhandbuch* unter **dell.com/support/manuals**.
5. Klicken Sie auf **Auf Aktualisierung prüfen**, um die in der Netzwerkfreigabe verfügbaren Aktualisierungen anzuzeigen.

   Der Abschnitt **Firmware-Bestandsaufnahme der Komponenten/Geräte** zeigt für alle Server, die im Gehäuse vorhanden sind, die aktuellen Firmwareversionen der Komponenten und Geräte an, sowie Firmwareversionen der DUPs, die in der Netzwerkfreigabe verfügbar sind.

ANMERKUNG: **Klicken Sie neben einem Steckplatz auf Ausblenden, um die Komponente und die Gerätefirmware-Details für den bestimmten Steckplatz auszublenden. Um alle Details anzuzeigen, klicken Sie auf Erweitern.**

6 Wählen Sie im Abschnitt **Firmware-Bestandsaufnahme der Komponenten/Geräte** das gegenüberliegende Kontrollkästchen **Alle auswählen/abwählen** aus, um alle unterstützten Server auszuwählen. Wählen Sie alternativ das Kontrollkästchen gegenüber dem Server aus, für den Sie die Serverkomponenten-Firmware aktualisieren möchten. Sie können für den Server keine individuellen Komponenten auswählen.

7 Wählen Sie eine der folgenden Optionen aus, um anzugeben, ob ein Systemneustart erforderlich ist, nachdem die Aktualisierungen geplant sind:

- Jetzt neu starten – Aktualisierungen werden geplant, und der Server wird neu gestartet, wobei die Aktualisierungen sofort an den Serverkomponenten angewandt werden.
- Beim nächsten Neustart – Aktualisierungen werden geplant, aber erst nach dem nächsten Neustart des Servers angewandt.

8 Klicken Sie auf **Aktualisieren**, um die Firmwareaktualisierungen für die verfügbaren Komponenten der ausgewählten Server zu planen.

Eine Meldung erscheint, deren Inhalt von der Art der enthaltenen Aktualisierungen abhängt, und in der Sie aufgefordert werden, zu bestätigen, wenn Sie fortfahren möchten.

9 Klicken Sie auf **OK**, um fortzufahren und die Planung der Firmwareaktualisierung für die ausgewählten Server abzuschließen. Hinweis:

ANMERKUNG: **Die Auftragsstatus-Spalte zeigt den Auftragsstatus der geplanten Vorgänge auf dem Server an. Der Auftragsstatus wird dynamisch aktualisiert.**

Unterstützte Firmwareversionen für die Serverkomponentenaktualisierung

Der folgende Abschnitt enthält die Serverkomponentenaktualisierung für CMC.

Die folgende Tabelle listet die unterstützten Firmwareversionen für Serverkomponenten in einem Szenario auf, bei dem die vorhandene Version der CMC-Firmware 3.1 ist und die Serverkomponenten von der N-1-Version auf die N-Version aktualisiert werden.

ANMERKUNG: **Die Aktualisierung der Serverkomponenten-Firmware von der N-1-Version auf die N-Version ist erfolgreich, wenn die CMC-Firmwareversion 2.0 oder höher bei allen Servern der 12., 13. und 14. Generation ist, die in der folgenden Tabelle beschrieben werden.**

Tabelle 13. Unterstützte Version der Serverkomponente für die Serverkomponentenaktualisierung auf die N-Version

Plattform	Serverkomponente	Vorhergehende Komponentenversion (N-1-Version)	Aktualisierte Komponentenversion (N-Version)
M520	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle-Controller	2.52.52.52	2.60.60.60
	Diagnose	4231A0	4247A1
	BIOS	2.4.2	2.6.1
	NIC	19.2.0	20.00.00.13
M620	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle-Controller	2.52.52.52	2.60.60.60
	Diagnose	4231A0	4247A1
	BIOS	2.5.4	2.6.1

Plattform	Serverkomponente	Vorhergehende Komponentenversion (N-1-Version)	Aktualisierte Komponentenversion (N-Version)
M820	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle-Controller	2.52.52.52	2.60.60.60
	Diagnose	4231A0	4247A1
	BIOS	2.6.1	2.6.1
M630	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle-Controller	2.52.52.52	2.60.60.60
	Diagnose	4239.44	4239A36
	BIOS	2.6.0	2.7.1
M830	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle-Controller	2.52.52.52	2.60.60.60
	Diagnose	4239.44	4239A36
	BIOS	2.5.4	2.7.1
M640	iDRAC	3.15.15.15	3.21.21.21
	Lifecycle-Controller	3.15.15.15	3.21.21.21
	Diagnose	4301A13	4301A13
	BIOS	1.3.7	1.4.8

Geplante Serverkomponenten-Firmware-Jobs löschen

ANMERKUNG: Um diese Funktion verwenden zu können, benötigen Sie eine Enterprise-Lizenz.

Sie können Jobs löschen, die für die ausgewählten Komponenten und/oder Geräte über einen oder mehrere Server hinweg geplant sind.

Geplante Serverkomponenten-Firmware-Jobs über die Webschnittstelle löschen

So löschen Sie geplante Serverkomponenten-Firmware-Jobs:

1. Klicken Sie im linken Fensterbereich auf **Server-Übersicht** und klicken Sie anschließend auf **Aktualisieren**.
2. Filtern Sie auf der Seite **Serverkomponenten-Aktualisierung** die Komponente oder das Gerät (optional).
3. Falls in der Spalte **Jobstatus** ein Kontrollkästchen neben dem Jobstatus angezeigt ist, gibt dies an, dass ein Lifecycle-Controller-Job aktiv ist und sich derzeit im angegebenen Zustand befindet. Dieser Job kann für einen Jobslöschungsvorgang ausgewählt werden.
4. Klicken Sie auf **Job löschen**. Die Jobs werden für die/das ausgewählte(n) Komponente(n) oder Gerät(e) gelöscht.

Speicherkomponenten über die CMC-Webschnittstelle aktualisieren

Achten Sie darauf, dass die DUPs für die erforderlichen Speicherkomponenten heruntergeladen sind.
So aktualisieren Sie die Speicherkomponenten:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Speicher** > **Aktualisierung**.

2 Klicken Sie auf der Seite **Speicherkomponenteaktualisierung** auf **Durchsuchen**.

Daraufhin wird das Dialogfeld **Datei zum Hochladen auswählen** angezeigt.

3 Navigieren Sie zum Speicherort, an dem die erforderliche DUP-Datei heruntergeladen und von der Dell Support-Site gespeichert wurde. Wählen Sie dann die DUP-Datei aus, und klicken Sie auf **Öffnen**.

Der DUP-Dateiname und der Pfad werden im Feld **Durchsuchen** angezeigt.

4 Klicken Sie auf **Hochladen**.

Das DUP wird auf den CMC hochgeladen. Der Abschnitt **Speicherkomponentenaktualisierung** zeigt nur die Komponenten, die durch die heruntergeladene DUP unterstützt werden. Die aktuelle Version, die neueste verfügbare Version und das Kontrollkästchen **Aktualisieren** werden für die Komponenten angezeigt.

5 Aktivieren Sie die entsprechenden Kontrollkästchen zum **Aktualisieren** für die erforderlichen Komponenten.

6 Klicken Sie auf **Aktualisieren**.

Die Firmware-Aktualisierung wird für die ausgewählten Komponenten gestartet. Der Fortschritt wird in der Spalte **Aktualisieren** angezeigt.

Nachdem der Vorgang abgeschlossen ist, wird eine entsprechende Meldung angezeigt wird, die den Abschluss oder das Scheitern der Firmware-Aktualisierung anzeigt.

ANMERKUNG:

- Die Server müssen ausgeschaltet sein, bevor Sie die Firmware aktualisieren.
- Die Komponente aktualisiert andere entsprechende Komponenten im System auf die gleiche Weise. Die SPERCs werden beispielsweise auf die gleiche Weise aktualisiert wie die vorhandenen SPERCs, und die EMMs werden auf die gleiche Weise wie die integrierten EMMs aktualisiert.
- Klicken Sie auf  zur Anzeige der HDD verschiedener Gehäuse.

iDRAC-Firmware mittels CMC wiederherstellen

iDRAC-Firmware wird normalerweise mit dem iDRAC, z. B. über die iDRAC-Webschnittstelle, mit der CM-CLP-Befehlszeilenschnittstelle oder mit betriebssystemspezifischen Aktualisierungspaketen, die von der Website **support.dell.com** heruntergeladen wurden, aktualisiert. Weitere Informationen finden Sie im *iDRAC-Benutzerhandbuch*.

Für frühere Generationen von Servern ist es möglich, beschädigte Firmware wiederherzustellen, indem der neue Vorgang zum Aktualisieren von iDRAC-Firmware verwendet wird. Wenn der CMC beschädigte iDRAC-Firmware erkennt, wird der Server auf der Seite **Firmware-Aktualisierung** aufgeführt. Beenden Sie die Tasks, die in Server-iDRAC-Firmware aktualisieren erwähnt sind.

5

Gehäuseinformationen anzeigen und Funktionszustandsüberwachung von Gehäuse und individuellen Komponenten

Sie können Informationen anzeigen und den Funktionszustand für Folgendes überwachen:

- Aktive und Standby-CMC
- Alle Server und einzelne Server
- E/A-Modul
- Lüfter
- Netzteile
- Temperatursensoren
- Festplattenlaufwerke
- LCD-Baugruppe
- Speicher-Controller
- PCIe-Geräte

ANMERKUNG: Der Funktionszustand externer Komponenten beeinträchtigt den gesamten Funktionszustand der Speicherkomponente mit vorhandenem Funktionszustand des Speichers und integrierte Speicherkomponenten in VRTX. Es gibt an, dass die externen Komponenten den Funktionszustand der Komponenten im Gehäuse nicht beeinträchtigen.

Themen:

Gehäuse- und Komponenten-Zusammenfassungen anzeigen

Wenn Sie sich an der CMC-Webschnittstelle anmelden, zeigt die Seite **Gehäusefunktionszustand** den Funktionszustand des Gehäuses und seiner Komponenten an. Sie zeigt eine Grafikansicht des Gehäuses und seiner Komponenten an. Die Seite wird dynamisch aktualisiert und die Farben der Komponenten-Untergrafiken und Texthinweise werden automatisch geändert, um den derzeitigen Zustand widerzuspiegeln.

Um den Gehäusefunktionszustand anzuzeigen, klicken Sie auf **Gehäuseübersicht**. Das System zeigt den Gesamtfunktionszustand des Gehäuses, der aktiven und Standby-CMCs, der Servermodule, der E/A-Module (EAMs), der Lüfter, der Netzteileinheiten (PSUs), der LCD-Einheit, des Speicher-Controllers und der PCIe-Geräte an. Detaillierte Informationen über die einzelnen Komponenten erhalten Sie, wenn Sie auf die jeweilige Komponente klicken. Außerdem werden die neuesten Ereignisse im CMC-Hardwareprotokoll angezeigt. Weitere Informationen finden Sie in der *Online-Hilfe*.

ANMERKUNG: Nach einem Aus- und Wiedereinschalten oder einem „racreset“ eines Gehäuses werden die Warnungen eines physischen Laufwerks, das sich im Zustand „Offline“ befindet, entfernt.

Wenn Ihr Gehäuse als Gruppenführung konfiguriert wurde, wird nach der Anmeldung die Seite **Gruppenfunktionszustand** angezeigt. Sie zeigt die Informationen und Warnungen auf Gehäuseebene an. Es werden alle aktiven kritischen und nicht-kritischen Warnungen angezeigt.

Gehäuse-Grafiken

Das Gehäuse wird in Vorder- und Rückansicht dargestellt (jeweils die oberen und unteren Bilder). Server, DVDs, HDDs, KVMs, und LCD-Display werden in der Vorderansicht gezeigt und die restlichen Komponenten werden in der Rückansicht gezeigt. Die Komponentenauswahl wird durch eine blaue Einfärbung angezeigt und durch Anklicken des Bildes der erforderlichen Komponente gesteuert. Wenn eine Komponente im Gehäuse enthalten ist, wird ein Symbol dieses Komponententyps in der Grafik auf der Position (Steckplatz) angezeigt, in der die Komponente installiert ist. Leere Positionen werden mit einem anthrazitfarbenen Hintergrund angezeigt. Das Komponentensymbol zeigt visuell den Zustand der Komponente an. Andere Komponenten zeigen Symbole an, die die physische Komponente visuell darstellen. Wenn der Cursor auf einer Komponente positioniert wird, wird eine Quickinfo mit zusätzlichen Informationen über diese Komponente angezeigt.

Tabelle 14. Serversymbolzustände in Systemen der 13. Generation

Symbol	Beschreibung
	Ein Server ist vorhanden und eingeschaltet und arbeitet normal.
	Ein Server ist vorhanden, ist aber ausgeschaltet.
	Ein Server ist vorhanden, meldet aber einen nicht-kritischen Fehler.
	Ein Server ist vorhanden, meldet aber einen kritischen Fehler.
	Es ist kein Server vorhanden.

Tabelle 15. Serversymbolzustände in Systemen der 14. Generation

Symbol	Beschreibung
	Ein Server ist vorhanden und eingeschaltet und arbeitet normal.
	Ein Server ist vorhanden, ist aber ausgeschaltet.

Symbol	Beschreibung
	Ein Server ist vorhanden, meldet aber einen nicht-kritischen Fehler.
	Ein Server ist vorhanden, meldet aber einen kritischen Fehler.
	Es ist kein Server vorhanden.

ANMERKUNG: Standardmäßig werden die Serversymbolzustände für Dell PowerEdge-Systeme der 13. Generation angezeigt, wenn Sie bei ausgeschaltetem Gehäuse einen PowerEdge-Server der 14. Generation einlegen.

Ausgewählte Komponenteninformationen

Die Informationen für die ausgewählte Komponente werden in drei getrennten Bereichen angezeigt:

- Funktionszustand, Leistung und Eigenschaften – Zeigt die aktiven, kritischen und nicht-kritischen Ereignisse gemäß der Anzeige im Hardwareprotokoll und die mit der Zeit variierenden Leistungsdaten an.
- Eigenschaften – Zeigt die Komponenteneigenschaften an, die sich nicht mit der Zeit ändern oder sich nur selten ändern.
- Direktlinks – Bietet Links zum Wechsel zu den am häufigsten besuchten Seiten und auch Links zu den am häufigsten durchgeführten Aktionen. Nur Links, die für die ausgewählte Komponente gelten, werden in diesem Bereich angezeigt.

In der folgenden Tabelle sind die Komponenteneigenschaften und Informationen aufgelistet, die auf der Seite **Gehäuse-Funktionszustand** der Web-Schnittstelle angezeigt werden.

ANMERKUNG: Beim Multi-Chassis-Management (MCM, gehäuseübergreifende Verwaltung) werden sämtliche Direktlinks im Zusammenhang mit dem Server nicht angezeigt.

Tabelle 16. Komponenteneigenschaften

Komponente	Funktionszustand und Leistung, Eigenschaften	Eigenschaften	Quicklinks
LCD-Baugruppe	• LCD-Funktionszustand • Gehäuse-Funktionszustand	• Netzschalter des Gehäuse • LCD-Bedienfeld sperren • LCD-Sprache • LCD-Ausrichtung	Frontblendenkonfiguration

Aktive und Standby-CMCs	• Redundanzmodus • MAC-Adresse • IPv4 • IPv6	• Firmware • Standby-Firmware • Letzte Aktualisierung • Hardware	• CMC-Status • Netzwerkbetrieb • Firmware-Aktualisierung
Alle Server und einzelne Server	• Stromzustand • Stromverbrauch • Funktionszustand • Zugeordneter Strom • Temperatur	• Name • Modell • Service Tag • Host-Name • iDRAC • CPLD • BIOS • Betriebssystem • CPU-Informationen • Gesamtsystemspeicher	• Serverstatus • Remote-Konsole starten • iDRAC-GUI starten • Server ausschalten • Ordentliches Herunterfahren • Remote-Dateifreigabe • iDRAC-Netzwerk bereitstellen • Serverkomponentenaktualisierung **ANMERKUNG: Quick-Links zum Ausschalten des Servers und zum Ordentlichen Herunterfahren werden nur dann angezeigt, wenn der Stromzustand des Servers auf EIN lautet. Wenn der Stromzustand des Servers AUS ist, wird der Direktlink Server einschalten angezeigt.**
KVM-Steckplatz	Funktionszustand	• KVM zugeordnet • Steckplatz 1: Frontblende USB/Video aktiviert • Steckplatz 2: Frontblende USB/Video aktiviert • Steckplatz 3: Frontblende USB/Video aktiviert • Steckplatz 4: Frontblende USB/Video aktiviert	Frontblendenkonfiguration
DVD-Steckplatz	• Funktionszustand • Stromzustand	• DVD zugeordnet • Steckplatz 1: DVD aktiviert • Steckplatz 2: DVD aktiviert • Steckplatz 3: DVD aktiviert • Steckplatz 4: DVD aktiviert	Frontblendenkonfiguration
Laufwerks-Steckplatz	• Funktionszustand • Zustand	• Modell • Seriennummer • Stromstatus • Firmware-Version • Größe • Typ	• Zustand der physischen Festplatte • Setup der physischen Festplatte • Controller für diese physische Festplatte anzeigen • Ansicht der virtuellen Festplatten für diese physische Festplatte.

Netzteileinheiten	Stromstatus	Kapazität	• Netzteilstatus • Stromverbrauch • Systembudget
PCIe-Geräte	• Installiert • Zugewiesen	• Modell • Server-Steckplatzzuordung • Hersteller-ID • Geräte-ID • Steckplatztyp • Zugewiesener Strom • Struktur • Stromstatus	• PCIe-Status • PCIe Einrichtung
Lüfter	• Geschwindigkeit • PWM (% von Max.) • Lüfter-Offset	• Warnungsschwelle • Kritischer Schwellenwert	• Lüfterstatus • Lüfterkonfiguration
Gebläse	• Geschwindigkeit • PWM (% von Max.) • Erweiterter Kühlmodus	• Warnungsschwelle • Kritischer Schwellenwert	• Lüfterstatus • Lüfterkonfiguration
SPERC-Steckplatz	• Installiert • Zugewiesen	• Modell • Server-Steckplatzzuordung • Hersteller-ID • Geräte-ID • Steckplatztyp • Zugewiesener Strom • Struktur • Stromstatus	• Controller-Status • Controller-Setup
Externer freigegebener PERC 8-Kartensteckplatz	• Installiert • Zugewiesen	• Modell • Server-Steckplatzzuordung • Hersteller-ID • Geräte-ID • Steckplatztyp • Zugewiesener Strom • Struktur • Stromstatus	• PCIe Steckplatzstatus • PCIe Einrichtung
EAM-Steckplatz	• Stromzustand • Rolle	• Modell • Service Tag	EAM-Status EAM-GUI starten

Servermodellnamen und Service-Tag-Nummer anzeigen

Sie können den Modellname und die Service-Tag-Nummer der einzelnen Server momentan durch Ausführung der folgenden Schritte ermitteln:

1 Im linken Fenster des Strukturknotens **Server-Übersicht** werden alle Server (STECKPLATZ-01 bis STECKPLATZ-04) in der Liste der Server angezeigt. Wenn ein Server nicht am Steckplatz vorhanden ist, wird das entsprechende Bild in der Grafik grau unterlegt angezeigt. Wenn ein Server mit voller Höhe Steckplatz 1 und Steckplatz 3 belegt, zeigt Steckplatz 3 den Steckplatznamen als **Erweiterung von 1** an.

2 Positionieren Sie den Cursor auf dem Steckplatznamen oder der Steckplatznummer eines Servers. Falls verfügbar, wird eine Quickinfo mit dem Modellnamen und der Service-Tag-Nummer des Servers angezeigt.

Gehäusezusammenfassung anzeigen

Um die Gehäusezusammenfassungsinformationen im linken Fensterbereich anzuzeigen, klicken Sie auf **Gehäuseübersicht** > **Eigenschaften** > **Zusammenfassung**.

Die Seite **Gehäusezusammenfassung** wird angezeigt. Weitere Informationen zu dieser Seite finden Sie in der *Online-Hilfe*.

Gehäuse-Controllerinformationen und Status anzeigen

Um Gehäuse-Controllerinformationen und Status anzuzeigen, klicken Sie in der CMC-Web-Schnittstelle auf **Gehäuseübersicht** > **Gehäuse-Controller**.

Die Seite **Gehäuse-Controller-Status** wird angezeigt. Weitere Informationen finden Sie in der *Online-Hilfe*.

Informationen und Funktionszustand von allen Servern anzeigen

Um den Funktionszustand von allen Servern anzuzeigen, haben Sie die folgenden Möglichkeiten:

- Klicken Sie auf **Gehäuseübersicht.** Die Seite **Gehäusefunktionszustand** bietet einen grafischen Überblick über alle Server, die im Gehäuse installiert sind. Der Serverfunktionszustand wird durch die Farbe der Server-Untergrafik angegeben. Weitere Informationen über den Gehäuse-Funktionszustand finden Sie in der *Online-Hilfe*.
- Klicken Sie auf **Gehäuseübersicht** > **Serverübersicht**. Die Seite **Serverstatus** enthält eine Übersicht zu den Servern im Gehäuse. Weitere Informationen finden Sie in der *Online-Hilfe*.

Anzeigen des Funktionszustands eines einzelnen Servers

So zeigen Sie den Funktionszustand von einzelnen Servern an:

1 Klicken Sie auf **Gehäuse-Übersicht** > **Eigenschaften** > **Funktionszustand**.

Die Seite **Gehäusefunktionszustand** bietet einen grafischen Überblick über alle Server, die im Gehäuse installiert sind. Der Serverfunktionszustand wird durch die Farbe der Server-Untergrafik angegeben. Positionieren Sie den Cursor auf einer einzelnen Server-Untergrafik. Ein entsprechender Texthinweis oder Bildschirmtipp wird angezeigt. Der Texthinweis liefert zusätzliche Informationen zum Server. Klicken Sie auf die Server-Untergrafik, um die E/A-Modul-Zusammenfassung rechts auf der Seite anzuzeigen. Weitere Informationen finden Sie in der *Online-Hilfe*.

2 Klicken Sie im linken Fenterbereich auf **Gehäuseübersicht** und erweitern Sie **Server-Übersicht**. Es werden alle Server (1 - 4) in der erweiterten Liste angezeigt. Klicken Sie auf den Steckplatz, in dem sich das Speicher-Array befindet.

Die Seite **Serverstatus** (nicht zu verwechseln mit der Seite **Status der Server** bietet den Funktionszustand des Servers im Gehäuse und eine Start-URL zur iDRAC-Webschnittstelle, die die Firmware darstellt, die zur Verwaltung des Servers verwendet wird. Weitere Informationen finden Sie in der *Online-Hilfe*.

ANMERKUNG: Um die iDRAC-Weboberfläche zu verwenden, müssen Sie für iDRAC einen Benutzernamen und ein Kennwort aufweisen. Weitere Informationen zum iDRAC und zur Verwendung der iDRAC-Webschnittstelle finden Sie im *Integrated Dell Remote Access Controller User's Guide* (Benutzerhandbuch zur integrierten Firmware des Dell Remote Access Controllers).

Anzeigen der Informationen und des Funktionszustands des EAM

Um den Funktionszustand der EAMs über die CMC-Webschnittstelle anzuzeigen, führen Sie einen der folgenden Schritte aus:

1 Klicken Sie auf **Gehäuseübersicht**.

Die Seite **Gehäusefunktionszustand** wird angezeigt. Die Grafik im linken Fensterbereich zeigt die Rück-, Vorder- und Seitenansicht des Gehäuses an und enthält den Funktionszustand für das EAM. Der EAM-Funktionszustand wird durch die Farbe der EAM-Untergrafik angegeben. Positionieren Sie den Cursor auf der einzelnen EAM-Untergrafik. Der Texthinweis liefert zusätzliche Informationen zu diesem EAM. Klicken Sie auf die EAM-Untergrafik, um die EAM-Informationen im rechten Fensterbereich anzuzeigen.

2 Wechseln Sie zu **Gehäuseübersicht** > **E/A-Modul-Übersicht**.

Die Seite **E/A-Modul-Status** enthält eine Übersicht zu einem mit dem Gehäuse verbundenen E/A-Modul. Weitere Informationen finden Sie in der *Online-Hilfe*.

ANMERKUNG: Stellen Sie nach Aktualisierung oder Aus-/Einschalten des EAM/IOA sicher, dass das Betriebssystem des EAM/IOA auch korrekt gestartet wird. Andernfalls wird der EAM-Status als „Offline“ angezeigt.

Informationen und Funktionszustand der Lüfter anzeigen

CMC steuert die Geschwindigkeit des Gehäuselüfters indem es die Lüftergeschwindigkeit, basierend auf Systemereignisse erhöht oder vermindert. Sie können den Lüfter in drei Modi, wie Niedrig, Mittel und Hoch. Weitere Informationen über die Konfiguration eines Lüfters finden Sie in der *Online-Hilfe*.

Um die Eigenschaften der Lüfter unter Verwendung von RACADM-Befehlen einzurichten, geben Sie in der CLI-Schnitstelle den folgenden Befehl ein.

```
racadm fanoffset [-s <off|low|medium|high>]
```

Weitere Informationen über die RACADM-Befehle finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX), das unter **dell.com/cmcmanuals** verfügbar ist.

ANMERKUNG: CMC überwacht die Temperatursensoren im Gehäuse und reguliert die Lüftergeschwindigkeit automatisch nach Bedarf. Sie können dies jedoch außer Kraft setzen, um eine minimale Lüftergeschwindigkeit durch den Befehl racadm fanoffset aufrechtzuerhalten. Wenn das automatische Überwachen unter Verwendung dieses Befehls außer Kraft gesetzt wird, wird CMC den Lüfter immer bis zur ausgewählten Geschwindigkeit laufen lassen, selbst wenn das Gehäuse es nicht erfordert, dass die Lüfter bei dieser Geschwindigkeit laufen.

Der CMC erstellt eine Warnung und erhöht die Lüftergeschwindigkeiten, wenn die folgenden Ereignisse auftreten:

- Der Schwellenwert der CMC-Umgebungstemperatur wird überschritten.
- Ein Lüfter funktioniert nicht mehr.
- Ein Lüfter wird aus dem Gehäuse entfernt.

ANMERKUNG: Während der Aktualisierung der CMC- oder iDRAC-Firmware auf einem Server drehen sich einige oder alle Lüfter im Gehäuse mit 100 % Leistung. Dies ist normal.

So zeigen Sie den Funktionszustand der Lüfter über die CMC-Webschnittstelle an:

1 Gehen Sie zu **Chassis Overview**.

Die Seite **Gehäusefunktionszustand** wird angezeigt. Der untere Abschnitt der Gehäuse-Grafiken zeigt die linke Ansicht des Gehäuses und enthält den Funktionszustand der Lüfter. Der Lüfter-Funktionszustand wird durch die Farbe der Lüfter-Untergrafik angegeben. Positionieren Sie den Cursor auf die Lüfter-Untergrafik. Der Texthinweis liefert zusätzliche Informationen zum Lüfter. Klicken Sie auf die Lüfter-Untergrafik, um die Lüfter-Informationen im rechten Fensterbereich anzuzeigen.

2 Gehen Sie zu **Gehäuseübersicht** > **Lüfter**.

Die Seite **Lüfterstatus** zeigt die Messwerte für den Status, die Geschwindigkeit (in Umdrehungen pro Minute oder U/Min.) und die Schwellenwerte der Lüfter im Gehäuse an. Es können ein oder mehrere Lüfter vorhanden sein.

ANMERKUNG: Im Falle eines Fehlers bei der Datenübertragung zwischen dem CMC und der Lüftereinheit kann der CMC den Funktionsstatus der Lüftereinheit weder abrufen noch anzeigen.

ANMERKUNG: Die folgende Meldung wird angezeigt, wenn beide Lüfter nicht in den Steckplätzen vorhanden sind oder wenn ein Lüfter sich bei einer niedrigen Geschwindigkeit dreht:

```
Fan <number> is less than the lower critical threshold.
```

Weitere Informationen finden Sie in der *Online-Hilfe*.

Konfigurieren von Lüftern

Lüfter-Offset – Eine Funktion, die erhöhte Kühlung für die Speicher- und PCIe-Bereiche des Gehäuses angibt. Diese Funktion ermöglicht es Ihnen, den Luftstrom für die HDDs, freigegebenen PERC-Controller und PCIe-Erweiterungssteckplätze zu erhöhen. Ein Beispiel der Nutzung der Option „Lüfter-Offset“ ist die Verwendung von hochleistungs- oder benutzerdefinierten PCIe-Karten, die eine höhere Kühlung als normal benötigen. Die Funktion „Lüfter-Offset“ bietet die Optionen „Aus, Niedrig, Mittel und Hoch“. Diese Einstellungen entsprechen einer Lüftergeschwindigkeit (Zunahme) von jeweils 20%, 50% und 100% der maximalen Geschwindigkeit. Es gibt auch Optionen für eine minimale Geschwindigkeit, die 35% für Niedrig, 65% für Mittel und 100% für Hoch sind.

Wenn Sie zum Beispiel die Lüfter-Offset-Einstellung „Mittel“ verwenden, erhöht sich die Drehzahl der Lüfter 1–6 um 50% der maximalen Geschwindigkeit. Diese Zunahme ist über der Geschwindigkeit, die das System schon für die Kühlung auf Basis der installieren Hardware-Konfiguration eingestellt hat.

Wenn eine beliebige der Lüfter-Offset-Optionen aktiviert ist, erhöht sich der Stromverbrauch. Mit Offset auf Niedrig eingestellt, wird das System lauter; es wird merklich lauter mit Offset auf Mittel eingestellt und deutlich lauter mit Offset auf Hoch eingestellt. Wenn die Option „Lüfter-Offset“ nicht aktiviert ist, werden die Lüftergeschwindigkeiten auf die Standardgeschwindigkeiten heruntergesetzt, die für die Systemkühlung für die installierten Hardwarekonfigurationen notwendig sind.

Zum Festlegen der Offset-Funktion gehen Sie auf **Gehäuseübersicht** > **Lüfter** > **Setup**. Wählen Sie auf der Seite **Erweiterte Lüfterkonfigurationen** in der Tabelle **Lüfterkonfiguration** im Drop-Down-Menü **Wert** eine Option aus, die dem **Lüfter-Offset** entspricht.

Weitere Informationen über die Funktion „Lüfter-Offset“ finden sie in der *Online-Hilfe*.

Um diese Funktionen unter Verwendung von RACADM-Befehlen einzurichten, verwenden Sie den folgenden Befehl:

```
racadm fanoffset [-s <off|low|medium|high>]
```

Weitere Informationen über die RACADM-Befehle, die mit „Lüfter-Offset“ in Verbindung stehen finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX), verfügbar unter dell.com/support/manuals.

Erweiterter Kühlmodus (ECM) – ist eine CMC-Funktion, die Ihnen eine erhöhte Kühlungskapazität für im PowerEdge VRTX-Gehäuse installierten Servern ermöglicht. Beispielsverwendungen für ECM sind der Betrieb in einer hohen Außenumgebung oder die Verwendung von Servern mit installierten hohen Strom-CPUs (≥120W). Die erhöhte Kühlungskapazität wird durch das Ausführen der vier Lüfter mit höherer Geschwindigkeit erreicht. Als Ergebnis erhöht sich, wenn ECM aktiviert ist, der Stromverbrauch und der Lärmpegel.

Bei Aktivierung erhöht ECM nur die Kühlungskapazität auf den Servertsteckplätzen innerhalb des Gehäuses. Es ist ebenfalls wichtig anzumerken, dass ECM nicht dazu entworfen wurde, eine ständige erhöhte Kühlung der Server zu bieten. Selbst wenn ECM aktiviert ist,

werden die erhöhten Lüftergeschwindigkeiten nur ausgeführt, wenn eine erhöhte Kühlung notwendig ist. Beispiele für eine solche Situation können hoher Servernutzungslevel oder -stress oder hohe Umgebungstemperaturen sein.

Standardmäßig ist ECM aus. Wenn ECM aktiviert ist, können die Lüfter ca. 20% mehr Zuluft pro Blade liefern.

Zum Festlegen der Offset-Funktion gehen Sie auf **Gehäuseübersicht** > **Lüfter** > **Setup**. Wählen Sie auf der Seite **Erweiterte Lüfterkonfigurationen** in der Tabelle **Lüfterkonfiguration** im Drop-Down-Menü **Wert** eine Option aus, die dem **Erweiterten Kühlmodus** entspricht.

Weitere Informationen über die EMC-Funktion finden sie in der *Online-Hilfe*.

Anzeigen von Frontblenden-Eigenschaften

So zeigen Sie die Frontblenden-Eigenschaften an:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Frontblende**.

2 Auf der Seite **Eigenschaften** können Sie Folgendes anzeigen:

- **Netzschaltereigenschaften**
- **LCD-Eigenschaften**
- **KVM – Eigenschaften**
- **DVD-Laufwerk – Eigenschaften**

KVM-Informationen und Funktionszustand anzeigen

Um den Funktionszustand der mit dem Gehäuse verbundenen KVMs anzuzeigen, führen Sie eine der folgenden Optionen aus:

1 Klicken Sie auf **Gehäuseübersicht**.

Die Seite **Gehäusefunktionszustand** wird angezeigt. Der linke Bereich zeigt die Vorderansicht des Gehäuses an und enthält den Funktionszustand eines KVM. Der KVM-Funktionszustand wird durch die Farbe der KVM-Untergrafik angegeben. Bewegen Sie den Zeiger über die KVM-Untergrafik und ein entsprechender Texthinweis oder Bildschirmtipp wird angezeigt. Der Texthinweis liefert zusätzliche Informationen über das KVM. Klicken Sie auf die KVM-Untergrafik, um die Informationen zum KVM im rechten Bereich anzuzeigen.

2 Klicken Sie alternativ dazu auf **Gehäuseübersicht** > **Frontblende**.

Sie könne auf der Seite **Status**, im Abschnitt **KVM-Eigenschaften,** den Status und die Eigenschaften eines KVM, das dem Gehäuse zugeordnet ist, anzeigen. Weitere Informationen finden Sie in der *Online-Hilfe*.

Anzeigen von Informationen und Funktionszustand für die LCD

So zeigen Sie den Funktionszustand eines LCD an:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht**.

Die Seite **Gehäusefunktionszustand** wird angezeigt. Der linke Bereich zeigt die Vorderansicht des Gehäuses an. Der LCD-Funktionszustand wird durch die Farbe der LCD-Untergrafik angegeben.

2 Positionieren Sie den Cursor auf die LCD-Untergrafik. Der entsprechende Texthinweis oder Bildschirmtipp, der zusätzliche Informationen zur LCD bietet, wird angezeigt.

3 Klicken Sie auf die LCD-Untergrafik, um die Informationen zur LCD im rechten Bereich anzuzeigen. Weitere Informationen finden Sie in der *Online Help*.

Gehen Sie alternativ auf **Gehäuseübersicht** > **Frontblende** > **Eigenschaften** > **Status**. Sie können auf der Seite **Status** unter **LCD-Eigenschaften** den Status der LCD, die auf dem Gehäuse verfügbar ist, anzeigen. Weitere Informationen finden Sie in der *Online-Hilfe*.

Informationen und Funktionszustand der Temperatursensoren anzeigen

So zeigen Sie den Funktionszustand der Temperatursensoren an:

Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Temperatursensoren**.

Die Seite **Temperatursensorstatus** zeigt den Status und die Messergebnisse der Temperatursonden des gesamten Gehäuses an (Gehäuse und Server). Weitere Informationen finden Sie in der *Online-Hilfe*.

ANMERKUNG: Der Temperatursondenwert kann nicht bearbeitet werden. Jede Änderung, die den Schwellenwert überschreitet erzeugt eine Warnung, die eine Änderung der Lüftergeschwindigkeit verursacht. Wenn z. B. die Temperatursonde der CMC-Umgebung den Schwellenwert überschreitet, wird sich die Geschwindigkeit der Gehäuselüfter erhöhen.

Anzeigen der Speicherkapazität und des Status der Storage-Komponenten

Um die Kapazität und den Fehlertoleranzstatus der Speicherkomponenten anzuzeigen, führen Sie einen der folgenden Schritte aus:

1 Gehen Sie zu **Chassis Overview**.

Die Seite **Gehäuse-Funktionszustand** wird angezeigt. Informationen zu Speicherkapazitätsdetails, zum Fehlertoleranzmodus (Aktiv/Passiv) und zum Fehlertoleranzstatus (Aktiviert) werden im rechten Fenster angezeigt. Diese Fehlertoleranzinformationen werden nur angezeigt, wenn die Fehlertoleranzfunktion für die Speicherkomponenten aktiviert ist.

Der untere Abschnitt der Gehäusegrafiken stellt die linke Anzeige des Gehäuses dar. Schieben Sie den Mauszeiger über die Untergrafik der Speicherkomponente. Der Texthinweis liefert zusätzliche Informationen zu den Speicherkomponenten. Klicken Sie auf die Untergrafik für die Speicherkomponente, um die Informationen im rechten Fensterbereich anzuzeigen.

2 Klicken Sie alternativ im linken Fensterbereich auf **Gehäuseübersicht** > **Speicher** > **Eigenschaften** > **Status**.

Die **Speicherübersicht** wird mit den folgenden Informationen angezeigt:

- Die graphische Übersicht der physischen Festplattenlaufwerke, die im Gehäuse installiert sind und deren Status anzeigen.
- Die Zusammenfassung aller Speicherkomponenten mit Links zu deren entsprechenden Seiten anzeigen.
- Die verwendete Kapazität und die Gesamtkapazitätof der Speicher anzeigen.
- Controller-Informationen anzeigen.

ANMERKUNG: Im Falle eines Fehlertoleranz-Controllers wird das folgende Format verwendet: *<Gemeinsam genutzte PERC-Nummer>* (Integrierte <Nummer>). Beispiel: Der aktive Controller ist „Gemeinsam genutzter PERC8“ (Integrierter 1), und der Peer-Controller ist „Gemeinsam genutzter PERC8“ (Integrierter 2).

- Vor kurzem protokolliere Speicherereignisse anzeigen.

ANMERKUNG: Weitere Informationen finden Sie in der *Online-Hilfe*.

6

Den CMC konfigurieren

Mit Chassis Management Controller können Sie Eigenschaften konfigurieren, Benutzer einrichten und Warnungen für die Ausführung von Remote-Verwaltungstasks einrichten.

Bevor Sie mit der Konfiguration des CMC beginnen, müssen Sie zuerst die CMC-Netzwerkeinstellungen konfigurieren, sodass Sie den CMC im Fernzugriff verwalten können. Diese ursprüngliche Konfiguration weist die TCP/IP-Netzwerkbetriebsparameter zu, die den Zugriff auf den CMC aktivieren. Weitere Informationen finden Sie unter Einrichtung des Erstzugriffs auf den CMC.

Sie können CMC über die Webschnittstelle or RACADM konfigurieren.

ANMERKUNG: Für die Erstkonfiguration des CMCs müssen Sie als Benutzer root angemeldet sein, um RACADM-Befehle auf einem Remote-System ausführen zu können. Es kann ein weiterer Benutzer mit Konfigurationsrechten für den CMC erstellt werden.

Nachdem das CMC eingerichtet wurde und die grundlegenden Konfigurationen durchgeführt wurden, können Sie das Folgende ausführen:

- Ändern der Netzwerkeinstellungen falls erforderlich.
- Schnittstellen für den Zugriff auf CMC Konfigurieren.
- LCD-Anzeige konfigurieren.
- Gehäusegruppe einrichten, falls erforderlich.
- Server, E/A-Modul oder Frontblende konfigurieren.
- VLAN-Einstellungen konfigurieren.
- Erforderliche Zertifikate abrufen.
- Hinzufügen und Konfiguration von CMC-Benutzern mit Berechtigungen.
- Konfiguration und Aktivierung von E-Mail-Warnmeldungen and SNMP-Traps.
- Einrichten der Stromobergrenzungsrichtlinie, falls erforderlich.

ANMERKUNG: Die folgenden Zeichen könne in der Eigenschaftszeichenkette beider CMC-Schnittstellen (GUI und CLI) nicht verwendet werden:

- &#
- < und > zusammen
- ; (Semikolon)

Themen:

Anzeigen und Ändern von CMC-Netzwerk-LAN-Einstellungen

Die LAN-Einstellungen, z. B. Community-Zeichenkette und SMTP-Server-IP-Adresse, betreffen die CMC-Einstellungen sowie die externen Einstellungen des Gehäuses.

Wenn Sie zwei CMCs (Aktiv und Standby) im Gehäuse haben und sie mit dem Netzwerk verbunden sind, dann übernimmt der Standby-CMC automatisch die Netzwerkeinstellungen des aktiven CMC im Falle eines Failovers.

Wenn IPv6 beim Start aktiviert ist, dann werden alle vier Sekunden drei Router-Anfragen ausgesendet. Wenn externe Netzwerk-Switches das Spanning Tree Protocol (STP) ausführen, können die externen Switch-Schnittstellen mehr als 12 Sekunden blockiert sein, während die IPv6-Router-Anfragen ausgesendet werden. In diesen Fällen kann die IPv6-Konnektivität zeitweise eingeschränkt sein, bis die Router-Ankündigungen unverlangt von den IPv6-Routern ausgesendet sind.

ANMERKUNG: Durch Ändern der CMC-Netzwerkeinstellungen wird möglicherweise die aktuelle Netzwerkverbindung getrennt.

ANMERKUNG: Um CMC-Netzwerkeinstellungen einzurichten, müssen Sie die Berechtigung als Gehäusekonfiguration-Administrator besitzen.

Anzeigen und Bearbeiten von CMC-Netzwerk-LAN-Einstellungen über die CMC-Webschnittstelle

So werden die CMC-LAN-Netzwerkeinstellungen unter Verwendung der CMC-Webschnittstelle angezeigt und geändert:

1. Klicken Sie in der Systemstruktur auf **Gehäuseübersicht** und klicken Sie dann auf **Netzwerk**. Die Seite **Netzwerkkonfiguration** zeigt die aktuelle Netzwerkeinstellungen an.
2. Ändern Sie bei Bedarf die allgemeinen, IPv4- oder IPv6-Einstellungen. Weitere Informationen finden Sie in der *Online-Hilfe*.
3. Klicken Sie auf **Änderungen anwenden** für jeden Abschnitt, um die Einstellungen anzuwenden.

Anzeigen und Ändern der CMC-Netzwerk-LAN-Einstellungen mittels RACADM

Um IPv4-Einstellungen anzuzeigen, verwenden Sie die Objekte aus der Gruppe **cfgCurrentLanNetworking** mit den Unterbefehlen `getniccfg` und `getconfig`.

Um IPv6-Einstellungen anzuzeigen, verwenden Sie die Objekte aus der Gruppe **cfgIpv6LanNetworking** mit dem Unterbefehl `getconfig`.

Um IPv4- und IPv6-Adressierungsinformationen für das Gehäuse anzuzeigen, benutzen Sie den Unterbefehl `getsysinfo`.

Weitere Informationen über die Unterbefehle und Objekte finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

Enabling the CMC Network Interface

Um die CMC-Netzwerkschnittstelle für IPv4 bzw. IPv6 zu aktivieren oder zu deaktivieren, geben Sie Folgendes ein:

```
racadm config -g cfgLanNetworking -o cfgNicEnable 1
racadm config -g cfgLanNetworking -o cfgNicEnable 0
```

ANMERKUNG: Der CMC NIC ist standardmäßig aktiviert.

Um die CMC-IPv4-Adressierung zu aktivieren oder zu deaktivieren, geben Sie Folgendes ein:

```
racadm config -g cfgLanNetworking -o cfgNicIPv4Enable
1
racadm config -g cfgLanNetworking -o cfgNicIPv4Enable
0
```

ANMERKUNG: Die CMC-IPv4-Adressierung ist standardmäßig aktiviert.

Um die CMC-IPv6-Adressierung zu aktivieren oder zu deaktivieren, geben Sie Folgendes ein:

```
racadm config -g cfgIpv6LanNetworking -o cfgIPv6Enable
1
racadm config -g cfgIpv6LanNetworking -o cfgIPv6Enable
0
```

ANMERKUNG: Beachten Sie Folgendes:

- Zwischen dem Ändern der Netzwerkeinstellungen und der tatsächlichen Anwendung besteht eine Verzögerung von 30 Sekunden.
- Die CMC-IPv6-Adressierung ist standardmäßig deaktiviert.

Standardmäßig fordert der CMC für IPv4 automatisch eine CMC-IP-Adresse vom DHCP-Server (Dynamisches Host-Konfigurationsprotokoll) an und empfängt diese. Sie können die DHCP-Funktion deaktivieren und eine statische CMC-IP-Adresse, ein statisches Gateway und eine statische Subnetzmaske bestimmen.

Um DHCP für ein IPv4-Netzwerk zu deaktivieren und eine statische CMC-IP-Adresse, Gateway und Subnetzmaske festzulegen, geben Sie Folgendes ein:

```
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0
racadm config -g cfgLanNetworking -o cfgNicIpAddress <static IP address>
racadm config -g cfgLanNetworking -o cfgNicGateway <static gateway>
racadm config -g cfgLanNetworking -o cfgNicNetmask <static subnet mask>
```

Standardmäßig fordert der CMC für IPv6 automatisch eine CMC-IP-Adresse vom IPv6-Autokonfigurationsverfahren an und empfängt diese.

Um die AutoConfiguration-Funktion für ein IPv6-Netzwerk zu deaktivieren und eine statische CMC-IPv6-Adresse, ein Gateway und eine Präfixlänge festzulegen, geben Sie Folgendes ein:

```
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6AutoConfig 0
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6Address <IPv6 address>
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6PrefixLength 64
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6Gateway <IPv6 address>
```

Aktivieren oder Deaktivieren von DHCP für die CMC-Netzwerkschnittstellenadresse

Wenn aktiviert, wird über die CMC-Funktion DHCP für NIC-Adresse automatisch eine IP-Adresse vom DHCP-Server (Dynamisches Host-Konfigurationsprotokoll) angefordert und abgerufen. Diese Funktion ist standardmäßig aktiviert.

Sie können die Funktion „DHCP für NIC-Adresse“ deaktivieren und eine statische IP-Adresse, eine statische Subnetzmaske und ein statisches Gateway angeben. Weitere Informationen finden Sie unter Einrichtung des Erstzugriffs auf den CMC.

DHCP für DNS-Server-IP-Adressen aktivieren oder deaktivieren

Die CMC-Funktion DHCP für DNS-Server-Adresse ist standardmäßig deaktiviert. Wenn aktiviert, werden mit dieser Funktion die primären und sekundären DNS-Server-Adressen vom DHCP-Server abgerufen. Um diese Funktion zu verwenden, müssen Sie keine statischen DNS-Server-IP-Adressen konfigurieren.

Um die Funktion „DHCP für DNS-Adresse“ zu deaktivieren und die statischen und alternativen DNS-Server-Adressen festzulegen, geben Sie Folgendes ein:

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
```

Um die Funktion „DHCP für DNS-Adresse“ für IPv6 zu deaktivieren und bevorzugte statische und alternative DNS-Server-Adressen anzugeben, geben Sie Folgendes ein:

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6DNSServersFromDHCP6 0
```

Statische DNS-Server-IP-Adressen einrichten

ANMERKUNG: Die Einstellungen der statischen DNS-IP-Adressen sind nur gültig, wenn die Funktion „DCHP für DNS-Server-Adresse“ deaktiviert ist.

Um die bevorzugten primären und sekundären DNS-IP-Server-Adressen für IPv4 festzulegen, geben Sie Folgendes ein:

```
racadm config -g cfgLanNetworking -o cfgDNSServer1 <IP-Adresse> racadm config -g
cfgLanNetworking -o cfgDNSServer2 <IPv4-Adresse>
```

Um die bevorzugten und sekundären DNS-IP-Server-Adressen für IPv4 festzulegen, geben Sie Folgendes ein:

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6DNSServer1 <IPv6-Adresse> racadm config -g
cfgIPv6LanNetworking -o cfgIPv6DNSServer2 <IPv6-Adresse>
```

Konfigurieren von IPv4- und IPv6-DNS-Einstellungen

- **CMC-Registrierung** – Zum Registrieren des CMC am DNS-Server geben Sie Folgendes ein:

  ```
  racadm config -g cfgLanNetworking -o
  cfgDNSRegisterRac 1
  ```

  ANMERKUNG: Manche DNS-Server registrieren nur Namen, die höchstens 31 Zeichen enthalten. Achten Sie darauf, dass der bestimmte Name innerhalb der DNS-erforderlichen Einschränkung liegt.

  ANMERKUNG: Die folgenden Einstellungen sind nur gültig, wenn Sie den CMC am DNS-Server registriert haben, indem Sie cfgDNSRegisterRac auf 1 gesetzt haben.

- **CMC-Name** – Der Standardname des CMC-Moduls auf dem DNS-Server lautet cmc-<*Service-Tag-Nummer*>. Um den CMC-Namen auf dem DNS-Server zu ändern, geben Sie Folgendes ein:

  ```
  racadm config -g cfgLanNetworking -o cfgDNSRacName <name>
  ```

  wobei <*name*> eine Zeichenkette von bis zu 63 alphanumerischen Zeichen und Bindestrichen ist. Beispiel: cmc-1, d-345.

  ANMERKUNG: Wenn kein DNS-Domänenname angegeben ist, beträgt die Maximalzahl von Zeichen 63. Wenn ein Domänenname festgelegt wurde, muss die Anzahl der Zeichen im CMC-Namen plus die Anzahl von Zeichen im DNS-Domänennamen kleiner als oder gleich 63 Zeichen sein.

- **DNS-Domänenname** – Der Standard-DNS-Domänenname ist ein einzelnes Leerzeichen. Um einen DNS-Domänenname festzulegen, geben Sie Folgendes ein:

  ```
  racadm config -g cfgLanNetworking -o
  cfgDNSDomainName <name>
  ```

wobei <*name*> eine Zeichenkette von bis zu 254 alphanumerischen Zeichen und Bindestrichen ist. Beispiel: p45, a-tz-1, r-id-001.

Konfigurieren von „Automatische Verhandlung“, „Duplexmodus“ und „Netzwerkgeschwindigkeit“ für IPv4 und IPv6

Wenn die automatische Verhandlungsfunktion aktiviert ist, bestimmt sie, ob der CMC automatisch den Duplexmodus und die Netzwerkgeschwindigkeit mittels Kommunikation mit dem nächsten Router oder Switch festlegt. Die automatische Verhandlungsfunktion ist standardmäßig aktiviert.

Sie können die automatische Verhandlung deaktivieren und den Duplexmodus sowie die Netzwerkgeschwindigkeit festlegen, indem Sie Folgendes eingeben:

```
racadm config -g cfgNetTuning -o cfgNetTuningNicAutoneg 0
racadm config -g cfgNetTuning -o cfgNetTuningNicFullDuplex <duplex mode>
```

wobei:

<*duplex mode*> ist 0 (Halbduplex) oder 1 (Vollduplex, Standardeinstellung)

```
racadm config -g cfgNetTuning -o cfgNetTuningNicSpeed <speed>
```

wobei:

<*speed*> ist 10 oder 100 (Standardeinstellung)

Einstellen der maximalen Übertragungseinheit für IPv4 und IPv6

Mithilfe der Eigenschaft „Maximale Übertragungseinheit“ (Maximum Transmission Unit, MTU) können Sie die maximale Größe von Paketen festlegen, die über die Schnittstelle übertragen werden können. Zum Einstellen der MTU geben Sie Folgendes ein:

```
racadm config -g cfgNetTuning -o cfgNetTuningMtu <mtu>
```

wobei <*mtu*> ein Wert zwischen 576 und1500 inklusive ist (Standardeinstellung: 1500).

ANMERKUNG: IPv6 erfordert einen MTU-Wert von mindestens 1280. Wenn IPv6 aktiviert und `cfgNetTuningMtu` auf einen geringeren Wert eingestellt ist, verwendet der CMC einen MTU-Wert von 1280.

Konfiguration von CMC-Netzwerk und Anmeldesicherheitseinstellungen

Mit den Funktionen des CMC zum Blockieren von IP-Adressen und Benutzern können Sie Sicherheitsprobleme durch das Ausprobieren von Kennwörtern verhindern. Diese Funktionen ermöglichen es Ihnen, bestimmte IP-Adressen und Benutzer zu blockieren, die Zugriff auf den CMC haben. Die Funktion zum Blockieren von IP-Adressen ist standardmäßig im CMC aktiviert. Sie können die IP-Bereichsattribute über die CMC-Webschnittstelle oder RACADM festlegen. Um die Funktionen zum Blockieren von IP-Adressen und Benutzern zu verwenden, aktivieren Sie die Optionen über die CMC-Webschnittstelle oder RACADM. Konfigurieren Sie die Richtlinieneinstellungen für die Anmeldesperrung so, dass Sie die Anzahl der erfolglosen Anmeldeversuche für einen bestimmten Benutzer oder eine bestimmte IP-Adresse festlegen können. Nach Überschreitung dieses Wertes wird der Benutzer blockiert und kann sich erst nach Ablauf der Sperrungsdauer wieder anmelden.

ANMERKUNG: Das Blockieren über IP-Adressen ist nur auf IPV4-Adressen anwendbar.

Konfiguration von IP-Bereichsattributen über die CMC-Webschnittstelle

ANMERKUNG: Um die folgenden Schritte auszuführen, müssen Sie die Berechtigung als Gehäusekonfigurations-Administrator besitzen.

So konfigurieren Sie IP-Bereichsattribute über die CMC-Webschnittstelle:

1. Wählen Sie im linken Fensterbereich **Gehäuseübersicht** aus und klicken Sie auf **Netzwerk** > **Netzwerk**. Die Seite **Netzwerkkonfiguration** wird angezeigt.
2. Klicken Sie im Abschnitt IPv4-Einstellungen auf **Erweiterte Einstellungen**.

   Die Seite **Anmeldesicherheit** wird angezeigt.

   Alternativ können Sie auf die Seite Anmeldesicherheit zugreifen, indem Sie im linken Fensterbereich **Gehäuseübersicht** wählen und auf **Sicherheit** > **Anmeldung** klicken.
3. Um die Funktion zum Prüfen des IP-Bereichs zu aktivieren, wählen Sie im Abschnitt **IP-Bereich** die Option **IP-Bereich aktiviert**.

   Die Felder **IP-Bereichsadresse** und **IP-Bereichsmaske** werden aktiviert.
4. Geben Sie in die Felder **IP-Bereichsadresse** und **IP-Bereichsmaske** den Bereich der IP-Adressen und die IP-Bereichsmasken ein, die Sie für den Zugriff auf den CMC sperren möchten.

   Weitere Informationen finden Sie in der *Online-Hilfe*.
5. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

Konfiguration von IP-Bereichsattributen mit RACADM

Sie können die folgenden IP-Bereichsattribute für den CMC mit RACADM konfigurieren:

- Die Funktion zum Prüfen des IP-Bereichs
- Den Bereich der IP-Adressen, die Sie für den Zugriff auf den CMC blockieren möchten
- Die IP-Bereichsmaske, die Sie für den Zugriff auf den CMC blockieren möchten

Die IP-Filterung vergleicht die IP-Adresse eines eingehenden Anmeldeversuchs mit dem festgelegten IP-Adressenbereich. Die Anmeldung der eingehenden IP-Adresse wird nur dann zugelassen, wenn Folgendes identisch ist:

- **cfgRacTuneIpRangeMask** Bit-weise mit eingehender IP-Adresse
- **cfgRacTuneIpRangeMask** Bit-weise mit **cfgRacTuneIpRangeAddr**

- Um die Funktion zum Prüfen des IP-Bereichs zu aktivieren, verwenden Sie die folgende Eigenschaft unter der Gruppe `cfgRacTuning`:

  ```
  cfgRacTuneIpRangeEnable <0/1>
  ```
- Um den Bereich der IP-Adressen festzulegen, die Sie für den Zugriff auf den CMC blockieren möchten, verwenden Sie die folgende Eigenschaft unter der Gruppe `cfgRacTuning`:

  ```
  cfgRacTuneIpRangeAddr
  ```
- Um die IP-Bereichsmaske festzulegen, die Sie für den Zugriff auf den CMC blockieren möchten, verwenden Sie die folgende Eigenschaft unter der Gruppe `cfgRacTuning`:

  ```
  cfgRacTuneIpRangeMask
  ```

Konfigurieren der virtuellen LAN-Tag-Einstellungen für CMC

Mit der VLAN-Funktion können mehrere VLANs auf dem gleichen physischen Netzwerkkabel koexistieren, außerdem kann der Netzwerkverkehr für Sicherheits- und Lastverteilungszwecke abgesondert werden. Wenn Sie die VLAN-Funktionalität aktivieren, wird jedem Netzwerkpaket ein VLAN-Tag zugewiesen.

Konfiguration der virtuellen LAN-Tag-Eigenschaften für CMC mittels RACADM

1 Aktivieren Sie die Funktionen für das virtuelle LAN (VLAN) des externen Gehäuseverwaltungsnetzwerks:

```
racadm config -g cfgLanNetworking -o cfgNicVLanEnable 1
```

2 Geben Sie die VLAN-Kennung für das externe Gehäuseverwaltungsnetzwerk an:

```
racadm config -g cfgLanNetworking -o cfgNicVlanID <VLAN id>
```

Gültige Werte für <*VLAN id*> sind 1– 4000 und 4021– 4094. Der Standardwert ist 1.

Beispiel:

```
racadm config -g cfgLanNetworking -o cfgNicVlanID 1
```

3 Dann geben Sie die VLAN-Priorität für das externe Gehäuseverwaltungsnetzwerk an:

```
racadm config -g cfgLanNetworking -o cfgNicVLanPriority <VLAN priority>
```

Gültige Werte für <*VLAN priority*> sind 0–7. Der Standardwert ist 0.

Beispiel:

```
racadm config -g cfgLanNetworking -o cfgNicVLanPriority 7
```

Sie können auch sowohl VLAN-Kennung als auch VLAN-Priorität in einem einzigen Befehl eingeben:

```
racadm setniccfg -v <VLAN id> <VLAN priority>
```

Beispiel:

```
racadm setniccfg -v 1 7
```

4 Zum Entfernen des CMC-VLAN deaktivieren Sie die VLAN-Funktionen des externen Gehäuseverwaltungsnetzwerks:

```
racadm config -g cfgLanNetworking -o cfgNicVLanEnable 0
```

Sie können das CMC-VLAN auch mithilfe des folgenden Befehls entfernen:

```
racadm setniccfg -v
```

Konfiguration der virtuellen LAN-Tag-Eigenschaften für CMC mithilfe der Webschnittstelle

So konfigurieren Sie virtuelles LAN (VLAN) für CMC mithilfe der CMC-Webschnittstelle:

1 Gehen Sie zu einer der folgenden Seiten:

- Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** und dann auf **Netzwerk** > **VLAN**.
- Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Server-Übersicht** und dann auf**Netzwerk** > **VLAN**.

Die Seite **VLAN-Tag-Einstellungen** wird angezeigt. VLAN-Tags sind Gehäuseeigenschaften. Sie bleiben mit dem Gehäuse verbunden, selbst wenn eine Komponente entfernt wird.

2 Aktivieren Sie im Abschnitt **CMC** VLAN für CMC, legen Sie die Priorität fest und weisen Sie die ID zu. Weitere Informationen über die Felder finden Sie in der *Online-Hilfe*.

3 Klicken Sie auf **Anwenden**. Die VLAN-Tag-Einstellungen werden gespeichert.

Sie können auch über **Gehäuseübersicht** > **Server** > **Setup** > **VLAN** auf diese Seite zugreifen.

Federal Information Processing Standards

Die Agenturen und Vertragspartner der Bundesregierung der Vereinigten Staaten verwenden Federal Information Processing Standards (FIPS), ein Computersicherheitsstandard, der alle Anwendungen mit kommunikativen Schnittstellen betrifft. Die Bestimmungen 140–2 bestehen aus vier Ebenen – Ebene 1, Ebene 2, Ebene 3 und Ebene 4. Die FIPS-Bestimmungen unter 140–2 legen fest, dass alle kommunikativen Schnittstellen über die folgenden Sicherheitseigenschaften verfügen müssen:

- Authentifizierung
- Vertraulichkeit
- Meldungsintegrität
- Unleugbarkeit
- Verfügbarkeit
- Zugriffskontrolle

Wenn eines der Merkmale von kryptografischen Algorithmen abhängig ist, muss FIPS diese Algorithmen genehmigen.

Standardmäßig ist der FIPS-Modus deaktiviert. Wenn FIPS aktiviert ist, ist die minimale Schlüsselgröße für OpenSSL FIPS SSH-2 RSA 2048 Bit.

ANMERKUNG: PSU-Firmware-Update wird nicht unterstützt, wenn der FIPS-Modus im Gehäuse aktiviert ist.

Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.

Die folgenden Funktionen/Anwendungen unterstützen FIPS:

- Web-GUI
- RACADM
- WSMan
- SSH v2
- SMTP
- Kerberos
- NTP-Client
- NFS

ANMERKUNG: SNMP ist nicht FIPS-konform. Im FIPS-Modus funktionieren alle SNMP-Funktionen, mit Ausnahme der Authentifizierung nach Message-Digest Algorithm, Version 5 (MD5).

Aktivieren des FIPS-Modus unter Verwendung der CMC Web-Schnittstelle

So aktivieren Sie FIPS:

1 Klicken Sie im linken Fenster auf **Gehäuseübersicht**.

Die Seite **Gehäusefunktionszustand** wird angezeigt.

2 Klicken Sie in der Menüleiste auf **Netzwerk**.

Die Seite **Netzwerkkonfiguration** wird angezeigt.

3 Wählen Sie im Abschnitt **Federal Information Processing Standards (FIPS)** aus dem Drop-Down-Menü **FIPS-Modus** die Option **Aktiviert** aus.

Eine Meldung wird angezeigt, die besagt, dass der CMC durch das Aktivieren von FIPS auf die Standardeinstellungen zurückgesetzt wird.

4 Klicken Sie auf **OK**, um fortzufahren.

Aktivieren des FIPS-Modus unter Verwendung von RACADM

Um den FIPS-Modus zu aktivieren, führen Sie den folgenden Befehl aus:

```
racadm config -g cfgRacTuning -o cfgRacTuneFipsModeEnable 1
```

.

Deaktivieren des FIPS-Modus

Um den FIPS-Modus zu deaktivieren, setzen Sie den CMC auf die Werkseinstellungen zurück.

Dienste konfigurieren

Sie können die folgenden Dienste auf CMC konfigurieren und aktivieren:

- CMC Serielle Konsole – Aktivieren Sie den Zugriff auf CMC unter Verwendung der seriellen Konsole.
- Web Server – Aktivieren Sie den Zugriff auf CMC Web-Schnittstelle. Die Deaktivierung des Web Servers deaktiviert auch den Remote-RACADM.
- SSH – Aktivieren Sie den Zugriff auf CMC über Firmware RACADM.
- Telnet – Aktivieren Sie den Zugriff auf CMC über Firmware RACADM
- RACADM – Aktivieren Sie den Zugriff auf CMC mittels RACADM.
- SNMP – Aktivieren Sie CMC zum Versenden von SNMP-Traps für Ereignisse.
- Remote-Syslog – Aktivieren Sie CMC, um Ereignisse auf einem Remote-Server zu protokollieren. Um diese Funktion zu nutzen, benötigen Sie eine Enterprise-Lizenz.

Der CMC enthält einen Web Server, der dazu konfiguriert ist, das SSL-Sicherheitsprotokoll des Industriestandards zu verwenden, um verschlüsselte Daten über das Internet von Clients zu empfangen bzw. sie an sie zu übermitteln. Der Web Server enthält ein von Dell™ selbstsigniertes, digitales SSL- Zertifikat (Server-ID) und ist dafür verantwortlich, sichere HTTP-Aufforderung von Clienten zu empfangen bzw. auf diese zu antworten. Dieser Dienst ist für die webbasierte Schnittstelle und das Remote-RACADM-CLI-Hilfsprogramm erforderlich, damit mit den CMC kommuniziert werden kann.

Im Falle eines Web Server-Resets warten Sie mindestens eine Minute, bis die Dienste wieder verfügbar werden. Ein Web Server-Reset tritt meist als Resultat eines der folgenden Ereignisse auf:

- Die Netzwerkkonfiguration oder Netzwerksicherheitseigenschaften wurden über die CMC-Webbenutzerschnittstelle oder RACADM geändert.
- Die Web Server-Schnittstellenkonfiguration wird über die Webbenutzerschnittstelle oder RACADM geändert.
- CMC wird zurückgesetzt.
- Ein neues SSL-Serverzertifikat wird hochgeladen.

ANMERKUNG: Zum Modifizieren von Diensteeinstellungen müssen Sie Berechtigungen als Gehäusekonfiguration-Administrator aufweisen.

Remote-Syslog ist ein zusätzliches Protokollziel für den CMC. Nach der Konfiguration von Remote-Syslog wird jeder neue vom CMC erzeugte Protokolleintrag an die Ziele weitergeleitet.

ANMERKUNG: Weil das Netzwerkübertragungsprotokoll für die weitergeleiteten Protokolleinträge UDP ist, gibt es weder eine Garantie, dass Protokolleinträge zugestellt werden, noch gibt es Feedback an CMC darüber, ob die Protokolleinträge erfolgreich empfangen wurden.

Dienste unter Verwendung der CMC-Webschnittstelle konfigurieren

So konfigurieren Sie CMC-Dienste über die CMC-Webschnittstellle:

1 Klicken Sie im linken Fensterbereich auf **Gehäuse-Übersicht**, und klicken Sie dann auf **Netzwerk** > **Dienste**. Die Seite **Diensteverwaltung** wird angezeigt.

2 Konfigurieren Sie die folgenden Dienste nach Bedarf:
   - CMC seriell
   - Webserver
   - SSH
   - Telnet
   - Remote-RACADM
   - SNMP
   - Remote-Syslog

   Weitere Informationen zu den Feldern finden Sie in der *Online-Hilfe*.

3 Klicken Sie auf **Anwenden**; dies aktualisiert alle Standard-Zeitüberschreitungen und alle maximalen Zeitüberschreitungsgrenzwerte.

Dienste über RACADM konfigurieren

Verwenden Sie für die Aktivierung und Konfiguration der verschiedenen Dienste die folgenden RACADM-Objekte:

- `cfgRacTuning`
- `cfgRacTuneRemoteRacadmEnable`

Weitere Informationen über diese Objekte finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX) unter dell.com/support/manuals.

Wenn die Firmware auf dem Server eine Funktion nicht unterstützt, bewirkt das Konfigurieren einer Eigenschaft zu dieser Funktion, dass ein Fehler angezeigt wird. Wenn zum Beispiel RACADM verwendet wird, um Remote-Syslog auf einem nicht unterstützten iDRAC zu aktivieren, wird eine Fehlermeldung angezeigt.

Wenn, in gleicher Weise, mit dem RACADM-`getconfig`-Befehl die iDRAC-Eigenschaften angezeigt werden, werden die Eigenschaftswerte einer Funktion, die auf dem Server nicht unterstützt wird, als N/A angezeigt.

Beispiel:

```
$ racadm getconfig -g cfgSessionManagement -m server-1 # cfgSsnMgtWebServerMaxSessions=N/A #
cfgSsnMgtWebServerActiveSessions=N/A # cfgSsnMgtWebServerTimeout=N/A #
cfgSsnMgtSSHMaxSessions=N/A # cfgSsnMgtSSHActiveSessions=N/A # cfgSsnMgtSSHTimeout=N/A #
cfgSsnMgtTelnetMaxSessions=N/A # cfgSsnMgtTelnetActiveSessions=N/A # cfgSsnMgtTelnetTimeout=N/A
```

Erweiterte CMC-Speicherkarte konfigurieren

Sie können die optionalen wechselbaren Flash-Datenträger für die Verwendung als erweiterten nicht-flüchtigen Speicher aktivieren oder reparieren. Der Betrieb einiger CMC-Funktionen ist von erweitertem nicht-flüchtigem Speicher abhängig.

So aktivieren oder reparieren Sie den wechselbaren Flash-Datenträger mithilfe der CMC-Webschnittstelle:

1 Gehen Sie im linken Fensterbereich auf **Gehäuseübersicht** und klicken Sie dann auf **Gehäuse-Controller** > **Flash-Datenträger**.

2 Wählen Sie aus der Seite **Wechselbarer Flash-Datenträger** aus dem Drop-Down-Menü je nach Bedarf eine der folgenden Optionen aus:

- **Datenträger des aktiven Controllers reparieren**
- **Verwendung des Flash-Datenträgers zum Speichern von Gehäusedaten abbrechen**

Weitere Informationen zu diesen Optionen finden Sie in der *Online-Hilfe*.

3 Klicken Sie auf **Anwenden**, um die ausgewählten Optionen anzuwenden.

Wenn im Gehäuse zwei CMCs vorhanden sind, müssen beide CMCs (Aktiv und Standby) Flash-Datenträger enthalten, Wenn nicht beide, der aktive und der Standby-CMC Flash-Datenträger enthalten, wird die Erweiterte Speicherfunktion herabgesetzt.

Einrichten einer Gehäusegruppe

CMC ermöglicht Ihnen die Überwachung mehrerer Gehäuse von einem einzigen Führungsgehäuse aus. Bei aktivierter Gehäusegruppe erzeugt der CMC des Führungsgehäuses eine grafische Darstellung des Status des Führungsgehäuses und von allen in der Gehäusegruppe enthaltenen Gehäusen. Um diese Funktion zu nutzen, benötigen Sie eine Enterprise-Lizenz.

Im Folgenden werden die Gehäusegruppenfunktionen dargestellt:

- Zeigt Abbildungen der Vorder- und Rückseite jedes Gehäuses an, wobei ein Satz für die Führung und ein Satz für jedes Mitglied angezeigt wird.
- Mögliche Beeinträchtigungen des Funktionszustands der Gruppenführung und der Gruppenmitglieder sind jeweils an der Komponente, die entsprechende Symptome aufweist an roten bzw. gelben Overlays und einem X bzw. ! zu erkennen. Details sind unterhalb der Gehäuseabbildung abzulesen, wenn Sie auf die Gehäuseabbildung oder **Details** klicken.
- Es sind Schnellstart-Links zum Öffnen der Webseiten von Mitgliedsgehäusen oder Servern vorhanden.
- Für eine Gruppe sind ein Server und eine Eingabe-/Ausgabebestandsliste verfügbar.
- Es ist eine Option verfügbar, um die Eigenschaften eines neuen Mitglieds mit den Eigenschaften des Führungsgehäuses zu synchronisieren, wenn das neue Mitglied zur Gruppe hinzugefügt wird.

Eine Gehäuseguppe kann maximal acht Mitglieder enthalten. Des Weiteren kann ein Führungs- bzw. ein Mitgliedgehäuse nur Teil einer Gruppe sein. Wenn diese bereits Teil einer Gruppe sind, können weder Führungs- noch Mitgliedsgehäuse einer weiteren Gruppe beitreten. Gehäuse können aus einer Gruppe gelöscht werden und später zu einer anderen Gruppe hinzugefügt werden.

So legen Sie eine Gehäusgruppe unter Verwendung der CMC-Webschnittstelle fest:

1 Melden Sie sich mit Gehäuseadministratorrechten am Führungsgehäuse an.

2 Klicken Sie auf **Setup** > **Gruppenverwaltung**.

3 Wählen Sie auf der **Gehäusegruppen**seite unter **Rolle Führung**. Es wird ein Feld zum Hinzufügen des Gruppennamens angezeigt.

4 Geben Sie den Gruppennamen im Feld **Gruppenname** ein und klicken Sie anschließend auf **Anwenden.**

ANMERKUNG: Für einen Domänennamen gelten die gleichen Regeln wie für den Gruppennamen.

Die Gehäusegruppe wechselt beim Erstellen der Gehäusegruppe automatisch zur **Gehäusegruppen**-Seite. Der linke Fensterbereich zeigt die Gruppe über den Gruppennamen an und das Führungsgehäuse sowie die nicht bestückten Mitgliedergehäuse werden im linken Fensterbereich angezeigt.

Hinzufügen von Mitgliedern zu einer Gehäusegruppe

Gehen Sie nach dem Einrichten der Gehäusegruppe wie folgt vor, um Mitglieder zur Gruppe hinzuzufügen:

1 Melden Sie sich mit Gehäuseadministratorrechten am Führungsgehäuse an.

2 Wählen Sie in der Struktur das Führungsgehäuse aus.

3 Klicken Sie auf **Setup** > **Gruppenverwaltung**.

4 Geben Sie unter **Gruppenverwaltung** die IP-Adresse des Mitglieds, oder seinen DNS-Namen im Feld **Hostname/IP-Adresse** an.
5 Geben Sie im Feld **Benutzername** einen Benutzernamen mit Gehäuseadministratorrechten für das Mitgliedsgehäuse an.
6 Geben Sie im Feld **Kennwort** das zugehörige Kennwort an.
7 Wählen Sie optional die Option **Neues Mitglied mit den Eigenschaften des Führungsgehäuses synchronisieren** aus, um die Eigenschaften des Führungsgehäuses auf das Mitglied zu übertragen.
8 Klicken Sie auf **Anwenden**.
9 Um maximal acht Mitglieder hinzuzufügen, schließen Sie die Tasks in Schritt 4 bis Schritt 8 ab. Die Gehäusenamen der neuen Mitglieder werden im Dialogfeld **Mitglieder** angezeigt.

ANMERKUNG: Die für ein Mitglied eingegebenen Anmeldeinformationen werden sicher an das Mitgliedsgehäuse weitergegeben, um zwischen dem Mitglieds- und dem Führungsgehäuse eine Vertrauensstellung einzurichten. Die Anmeldeinformationen werden auf keinem der Gehäuse dauerhaft gespeichert und nach dem anfänglichen Einrichten der Vertrauensstellung nie wieder ausgetauscht.

Entfernen eines Mitglieds aus der Führung

Sie können ein Mitglied aus der Gruppe des Führungsgehäuses entfernen. Entfernen eines Mitglieds:

1 Melden Sie sich mit Gehäuseadministratorrechten am Führungsgehäuse an.
2 Wählen Sie im linken Fensterbereich das Gehäuse aus.
3 Klicken Sie auf **Setup** > **Gruppenverwaltung**.
4 Wählen Sie aus der Liste **Mitglieder entfernen** den zu löschenden Mitgliedernamen aus, und klicken Sie anschließend auf **Anwenden**.
Das Führungsgehäuse benachrichtigt anschließend das Mitglied, bzw. die Mitglieder, sollten mehr als eines ausgewählt worden sein, dass es bzw. sie aus der Gruppe entfernt wurde(n). Der Mitgliedsname wird aus dem Dialogfeld entfernt. Das Mitgliedsgehäuse erhält die Nachricht möglicherweise nicht, wenn der Kontakt zwischen dem Führung und dem Mitglied aufgrund eines Netzwerkproblems verhindert wird. Deaktivieren Sie in diesem Falle das Mitglied des Mitgliedsgehäuses, um das Entfernen abzuschließen.

Auflösen einer Gehäusgruppe

So lösen Sie eine Gehäusegruppe vom Führungsgehäuse aus auf:

1 Melden Sie sich mit Administratorrechten am Führungsgehäuse an.
2 Wählen Sie im linken Fensterbereich das Führungsgehäuse aus.
3 Klicken Sie auf **Setup** > **Gruppenverwaltung**.
4 Wählen Sie auf der Seite **Gehäusegruppen** unter **Rolle**, **Keine** aus und klicken Sie anschließend auf **Anwenden**.
Das Führungsgehäuse benachrichtigt anschließend alle Mitglieder, dass sie aus der Gruppe entfernt wurden. Das Führungsgehäuse kann einer anderen Gruppe als Führung oder Mitglied zugewiesen werden.

Wenn der Kontakt zwischen der Führung und dem Mitglied aufgrund eines Netzwerkproblems verhindert wird, erhält das Mitgliedsgehäuse die Nachricht möglicherweise nicht. Deaktivieren Sie in diesem Falle das Mitglied des Mitgliedsgehäuses, um das Entfernen abzuschließen.

Deaktivieren eines einzelnen Mitglieds am Mitgliedsgehäuse

Gelegentlich kann ein Mitglied durch das Führungsgehäuse nicht aus einer Gruppe entfernt werden. Dies kann bei einem Verlust der Netzwerkverbindung zum Mitglied vorkommen. So entfernen Sie ein Mitglied aus einer Gruppe im Mitgliedsgehäuse:

1 Melden Sie sich mit Gehäuseadministratorrechten am Mitgliedsgehäuse an.
2 Klicken Sie im linken Fensterbereich au **Gehäuseübersicht** > **Setup** > **Gruppenverwaltung**.
3 Wählen Sie **Keine** und klicken Sie anschließend auf **Anwenden**.

Zugreifen auf die Webseite eines Mitgliedsgehäuses oder Servers

Über die Gruppenseite des Führungsgehäuses können Sie auf die Webseite des Mitgliedsgehäuses, die Remote-Konsole des Servers oder die Webseite des iDRAC-Servers zugreifen. Wenn das Mitgliedsgerät dieselben Anmeldeinformationen wie das Führungsgehäuse besitzt, können Sie diese Anmeldeinformationen für den Zugriff auf das Mitgliedsgerät verwenden.

ANMERKUNG: Bei der Verwaltung mehrerer Gehäuse werden einmalige Anmeldung (Single Sign-On, SSO) und Smart Card-Anmeldung nicht unterstützt. Um über das Führungsgehäuse mit einmaliger Anmeldung auf Mitglieder zugreifen zu können, ist bei Führungsgehäuse und Mitgliedern ein gemeinsamer Benutzername bzw. Kennwort erforderlich. Die Verwendung eines gemeinsamen Benutzernamens bzw. Kennworts funktioniert nur in Verbindung mit Active Directory-, lokalen und LDAP-Benutzern.

So navigieren Sie zu Mitgliedsgeräten:

1 Melden Sie sich am Führungsgehäuse an.
2 Wählen Sie in der Struktur **Gruppe: Name** aus.
3 Wenn ein Mitglieds-CMC das benötigte Ziel ist, dann wählen Sie für das gewünschte Gehäuse **CMC starten** aus.

   Wenn ein Server in einem Gehäuse das benötigte Ziel ist, verfahren Sie folgendermaßen:

   a Wählen Sie das Bild des Zielgehäuses aus.
   b Wählen Sie im Gehäusebild, das im Bereich **Zustand** angezeigt wird, den Server aus.
   c Wählen Sie im Feld **Direktlinks** das Zielgerät aus. Es wird ein neues Fenster mit der Zielseite oder dem Anmeldebildschirm angezeigt.

      ANMERKUNG: In MCM werden sämtliche Direktlinks im Zusammenhang mit dem Server nicht angezeigt.

Propagieren der Führungsgehäuseeigenschaften auf ein Mitgliedsgehäuse

Sie können die Eigenschaften eines Führungsgehäuses auf ein Mitgliedsgehäuse einer Gruppe anwenden. Um ein Mitglied mit den Führungseigenschaften zu synchronisieren:

1 Melden Sie sich mit Administratorrechten am Führungsgehäuse an.
2 Wählen Sie in der Struktur das Führungsgehäuse aus.
3 Klicken Sie auf **Setup** > **Gruppenverwaltung**.
4 Wählen Sie im Abschnitt **Gehäuseeigenschaften propagieren** eine der Propagierungstypen aus:
   - Propagierung bei Änderung - Wählen Sie diese Option zur automatischen Propagierung der ausgewählten Gehäuseeigenschaften-Einstellungen aus. Die Änderungen der Eigenschaften werden bei jeder Änderung der Führungseigenschaften an alle aktuellen Gruppenmitglieder propagiert.
   - Manuelle Propagierung - Wählen Sie diese Option zur manuellen Propagierung der Führungseigenschaften der Gehäusegruppe zu seinen Mitgliedern. Die Einstellungen für die Führungsgehäuseeigenschaften werden nur zu den Gruppenmitgliedern propagiert, wenn der Führungsgehäuse-Administrator auf **Propagieren** klickt.
5 Wählen Sie im Abschnitt **Propagierungseigenschaften** die Kategorien der Führungskonfigurationseigenschaften aus, die an die Gehäusemitglieder propagiert werden sollen.

   Wählen Sie ausschließlich die Einstellungskategorien aus, die Sie übergreifend auf allen Mitgliedern der Gehäusegruppe identisch konfigurieren möchten. Wählen Sie zum Beispiel die Kategorie **Protokollierungs- und Warnmeldungseigenschaften** aus, um zu aktivieren, dass alle Gehäuse in der Gruppe die Protokollierungs- und Warnmeldungskonfigurationseinstellungen des Führungsgehäuses teilen.
6 Klicken Sie auf **Save** (Speichern).

Wurde **Propagierung bei Änderung** ausgewählt, übernehmen die Gehäusemitglieder die Eigenschaften des Führungsgehäuses. Wenn **Manuelle Propagierung** ausgewählt wurde, klicken Sie auf **Propagieren**, wann immer Sie die ausgewählten Einstellungen zu den Mitgliedsgehäusen propagieren möchten. Weitere Informationen zur Propagierung von Führungsgehäuseeigenschaften auf ein Mitgliedsgehäuse finden Sie in der *Online-Hilfe*.

Blade-Bestandsaufnahme für MCM-Gruppe

Eine Gruppe ist ein Führungsgehäuse, das zwischen 0 und 8 Gehäusegruppenmitglieder hat. Auf der Seite **Funktionszustand der Gehäusegruppe** werden alle Mitgliedsgehäuse angezeigt. Hier können Sie den Bericht zur Server-Bestandsaufnahme über die Download-Funktion eines Standard-Internet-Browsers in eine Datei speichern. Der Bericht enthält Daten zu:

- allen Servern, die sich derzeit in der Gehäusegruppe befinden (einschließlich Führungsgehäuse).
- leeren Einschüben und Erweiterungseinschüben (einschließlich Servermodule mit voller Höhe und doppelter Breite).

Speichern des Berichts zur Serverbestandsaufnahme

So speichern Sie den Bericht zur Serverbestandsaufnahme über die CMC-Webschnittstelle:

1 Wählen Sie im linken Fensterbereich die **Gruppe** aus.
2 Klicken Sie auf der Seite **Funktionszustand der Gehäusegruppe** auf **Bericht zur Bestandsliste speichern**. Das Dialogfeld **Datei-Download** wird angezeigt und Sie werden dazu aufgefordert, die Datei zu öffnen oder zu speichern.
3 Klicken Sie auf **Speichern**, und geben Sie den Pfad- und Dateinamen für den Bericht zur Serverbestandsaufnahme ein.

ANMERKUNG: Das Führungsgehäuse der Gehäusegruppe, sowie die Mitgliedsgehäuse der Gehäusegruppe und die Servermodule im zugeordneten Gehäuse müssen eingeschaltet sein, um einen präzisen Bericht zur Server-Bestandsaufnahme anzuzeigen.

Exportierte Daten

Der Bericht zur Server-Bestandsaufnahme enthält Daten, die kürzlich im Rahmen der normalen Abfrage durch das Führungsgehäuse der Gehäusegruppe (alle 30 Sekunden) von jedem Mitglied in der Gehäusegruppe gemeldet wurden.

So erstellen Sie einen präzisen Bericht zur Server-Bestandsaufnahme:

- Das Führungsgehäuse der Gehäusegruppe sowie alle Mitgliedsgehäuse der Gehäusegruppe müssen **eingeschaltet** sein.
- Alle Server im verknüpften Gehäuse müssen eingeschaltet sein.

Die Bestandsaufnahmedaten für das verknüpfte Gehäuse und die verknüpften Server sind möglicherweise nicht im Bericht enthalten, falls sich ein Teilbereich der Mitgliedsgehäuse der Gehäusegruppe im folgenden Zustand befinden:

- Im Zustand **Gehäusegruppe ist ausgeschaltet**
- Ausgeschaltet

ANMERKUNG: Wenn ein Server eingesetzt wird, während das Gehäuse ausgeschaltet ist, wird die Modellnummer in der Webschnittstelle erst angezeigt, wenn das Gehäuse wieder eingeschaltet wird.

Die folgende Tabelle listet die spezifischen Datenfelder und Anforderungen für Felder auf, die für jeden Server gemeldet werden müssen:

Tabelle 17. Beschreibungen der Felder der Servermodul-Bestandsaufnahme

Datenfeld	Beispiel
Gehäusename	Rechenzentrum für Führungsgehäuse
Gehäuse-IP-Adresse	192.168.0.1
Einschubposition	1
Steckplatzname	SLOT-01
Host-Name	Unternehmens-Webserver **ANMERKUNG: Es wird ein Server-Administrator-Agent benötigt, der auf dem Server ausgeführt wird. Ansonsten wird er leer angezeigt.**
Betriebssystem	Windows Server 2008 **ANMERKUNG: Es wird ein Server-Administrator-Agent benötigt, der auf dem Server ausgeführt wird. Ansonsten wird er leer angezeigt.**
Modell	PowerEdgeM610
Service Tag	1PB8VF1
Gesamtsystemspeicher	4 GB **ANMERKUNG: Erfordert VRTX CMC 1.0 (oder neuer) auf dem Mitglied. Ansonsten wird es leer angezeigt.**
Anzahl der CPUs	2 **ANMERKUNG: Erfordert VRTX CMC 1.0 (oder neuer) auf dem Mitglied. Ansonsten wird es leer angezeigt.**
CPU-Info	Intel (R) Xeon (R) CPU E5502 mit 1,87 GHzn **ANMERKUNG: Erfordert VRTX CMC 1.0 (oder neuer) auf dem Mitglied. Ansonsten wird es leer angezeigt.**

Datenformat

Der Bestandsaufnahmebericht wird in einem .CSV -Dateiformat generiert, damit er in verschiedene Tools importiert werden kann, wie z. B. Microsoft Excel. Die .CSV -Datei für den Bestandsaufnahmebericht kann in die Vorlage importiert werden, indem Sie in MS Excel **Date** > **Aus Text** auswählen. Nachdem der Bestandsaufnahmebericht nach MS Excel importiert wurde und falls eine Nachricht angezeigt wird, in der zusätzliche Informationen angefordert werden, wählen Sie „Trennzeichen-getrennt“ aus, um die Datei nach MS Excel zu importieren.

Bestandsaufnahme und Firmwareversionen der Gehäusegruppe

Die Seite **Gehäusegruppen-Firmwareversion** zeigt Bestandsaufnahme und Firmwareversionen der Gruppen der Server und der Serverkomponenten im Gehäuse an. Mit dieser Seite können Sie außerdem Bestandsinformationen organisieren und die Ansicht der Firmwareversionen filtern. Die Ansicht bezieht sich auf die Server oder eine der folgenden Gehäuseserverkomponenten:

- BIOS
- iDRAC
- CPLD
- USC

- Diagnose
- BS-Treiber
- RAID
- NIC

ANMERKUNG: Die Bestandsinformationen zu Gehäusegruppe, Mitgliedsgehäuse, Servern und Serverkomponenten werden jedes Mal aktualisiert, wenn ein Gehäuse zur Gruppe hinzugefügt oder daraus entfernt wird.

Anzeigen der Bestandslisten von Gehäusegruppen

Um mithilfe der CMC-Webschnittstelle eine Gehäusegruppe anzeigen zu lassen, wählen Sie im linken Fensterbereich **Gruppe** aus. Klicken Sie auf **Eigenschaften** > **Firmware-Version**. Die Seite **Gehäusegruppen-Firmware-Version** zeigt alle Gehäuse in der Gruppe an.

Anzeigen ausgewählter Bestandslisten von Gehäusegruppen über die Webschnittstelle

So lassen Sie sich eine ausgewählte Bestandsaufnahme von Gehäusen mithilfe der CM-Webschnittstelle anzeigen:

1 Wählen Sie in der Systemstruktur **Gruppe** aus. Klicken Sie auf **Eigenschaften** > **Firmware-Version**.
Die Seite **Gehäusegruppen-Firmware-Version** zeigt alle Gehäuse der Gruppe an.

2 Wählen Sie im Abschnitt **Gehäuse auswählen** das Mitgliedsgehäuse, für das Sie sich die Bestandsaufnahme anzeigen lassen möchten.
Der Abschnitt **Firmware-Anzeigefilter** zeigt die Serverbestandsaufnahme für das ausgewählte Gehäuse und die Firmware-Versionen aller Server-Komponenten an.

Anzeigen ausgewählter Firmwareversionen von Serverkomponenten über die Webschnittstelle

So können Sie ausgewählte Firmwareversionen von Serverkomponenten über die Webschnittstelle anzeigen:

1 Wählen Sie im linken Fensterbereich **Gruppe** aus. Klicken Sie auf **Eigenschaften** > **Firmware-Version**.
Die Seite **Gehäusegruppen-Firmware-Version** zeigt alle Gehäuse der Gruppe an.

2 Wählen Sie im Abschnitt **Gehäuse auswählen** das Mitgliedsgehäuse, für das Sie sich die Bestandsaufnahme anzeigen lassen möchten.

3 Wählen Sie im Abschnitt **Firmware-Anzeigefilter** die Option **Komponenten**.

4 Wählen Sie in der Liste **Komponenten** die erforderliche Komponente – BIOS, iDRAC, CPLD, USC, Diagnose, Betriebssystemtreiber, RAID-Geräte (bis zu 2) und NIC-Geräte (bis zu 6) – aus, deren Firmwareversion angezeigt werden soll.
Die Firmwareversionen der ausgewählten Komponenten aller Server im ausgewählten Mitgliedsgehäuse werden angezeigt.

Gehäusekonfigurationsprofile

Die Funktion „Gehäusekonfigurationsprofile“ ermöglicht Ihnen die Konfiguration des Gehäuses anhand eines Gehäusekonfigurationsprofils, das auf der Netzwerkfreigabe oder der lokalen Management Station gespeichert ist, sowie die Wiederherstellung der Gehäusekonfiguration.

Um auf die Seite **Gehäusekonfigurationsprofile** der CMC Web-Schnittstelle zuzugreifen, wechseln Sie in der Systemstruktur zu **Gehäuseübersicht**, und klicken Sie auf **Setup** > **Profile**. Die Seite **Gehäusekonfigurationsprofile** wird angezeigt.

Mithilfe der Funktion „Gehäusekonfigurationsprofile“ können Sie die folgenden Aufgaben ausführen:

- Konfigurieren eines Gehäuses unter Verwendung von Gehäusekonfigurationsprofilen auf der lokalen Management Station für die Erstkonfiguration

- Speichern der derzeitigen Einstellungen der Gehäusekonfiguration in einer XML-Datei auf der Netzwerkfreigabe oder der lokalen Management Station
- Wiederherstellen der Gehäusekonfiguration
- Importieren von Gehäuseprofilen (XML-Dateien) von einer lokalen Management Station in die Netzwerkfreigabe
- Exportieren von Gehäuseprofilen (XML-Dateien) von der Netzwerkfreigabe in eine lokale Management Station
- Bearbeiten, Löschen, Exportieren oder Anwendung einer Kopie der auf der Netzwerkfreigabe gespeicherten Profile.

Speichern der Gehäusekonfiguration

Sie können die derzeitige Gehäusekonfiguration in einer XML-Datei auf einer Netzwerkfreigabe oder auf der lokalen Management Station speichern. Die Konfigurationen umfassen alle Eigenschaften des Gehäuses, die unter Verwendung der CMC Web-Schnittstelle und der RACADM-Befehle geändert werden können. Sie können die gespeicherte XML-Datei auch zum Wiederherstellen der Konfiguration auf dem gleichen Gehäuse oder zum Konfigurieren anderer Gehäuse verwenden.

ANMERKUNG: Die Server- und iDRAC-Einstellungen werden nicht zusammen mit der Gehäusekonfiguration gespeichert oder wiederhergestellt.

Führen Sie zum Speichern der derzeitigen Gehäusekonfiguration die folgenden Schritte aus:

1 Rufen Sie die Seite **Gehäusekonfigurationsprofile** auf. Geben Sie im Abschnitt **Speichern und sichern** > **Derzeitige Konfiguration speichern** einen Namen für das Profil in das Feld **Profilname** ein.

   ANMERKUNG: Beim Speichern der derzeitigen Gehäusekonfiguration wird der erweiterte Standard-ASCII-Zeichensatz unterstützt. Die folgenden Sonderzeichen werden jedoch nicht unterstützt:

   “, ., *, >, <, \, /, : und |

2 Wählen Sie einen der folgenden Profiltypen unter **Profiltyp** aus:
   - **Ersetzen** – Dies umfasst Attribute der gesamten CMC-Konfiguration, mit Ausnahme von reinen Schreibattributen wie Benutzerkennwörter und Service-Tag-Nummern. Dieser Profiltyp wird als Backup-Konfigurationsdatei für die Wiederherstellung der gesamten Gehäusekonfiguration verwendet, einschließlich der Identitätsinformationen, wie beispielsweise IP-Adressen.
   - **Klonen** – Dies umfasst alle Profilattribute vom Typ **Ersetzen**. Identitätsattribute wie MAC-Adresse und IP-Adresse werden aus Sicherheitsgründen auskommentiert. Dieser Profiltyp wird zum Klonen eines neuen Gehäuses verwendet.

3 Wählen Sie einen der folgenden Speicherorte aus dem Drop-down-Menü **Profil-Speicherort** aus, an dem das Profil gespeichert werden soll:
   - **Lokal** – Speichert das Profil auf der lokalen Management Station.
   - **Netzwerkfreigabe** – Speichert das Profil an einem freigegebenen Speicherort.

4 Klicken Sie auf **Speichern**, um das Profil am ausgewählten Speicherort zu speichern.

   Nachdem der Vorgang abgeschlossen wurde, wird die Meldung `Operation Successful` angezeigt.

   ANMERKUNG: Um die Einstellungen anzuzeigen, die in der XML-Datei gespeichert werden, wählen Sie das gespeicherte Profil im Abschnitt Gespeicherte Profile aus, und klicken Sie in der Spalte Profile anzeigen auf Anzeigen.

Wiederherstellen eines Gehäusekonfigurationsprofils

Sie können die Konfiguration eines Gehäuses wiederherstellen, indem Sie die Backup-Datei (**.xml** oder **.bak**) auf der lokalen Management Station oder auf der Netzwerkfreigabe, auf der die Gehäusekonfiguration gespeichert ist, importieren. Die Konfigurationen umfassen alle Eigenschaften des Gehäuses, die unter Verwendung der CMC Web-Schnittstelle, der RACADM-Befehle und der Einstellungen verfügbar sind.

Führen Sie zum Wiederherstellen der Gehäusekonfiguration die folgenden Schritte aus:

1 Rufen Sie die Seite **Gehäusekonfigurationsprofile** auf. Klicken Sie im Abschnitt **Konfiguration wiederherstellen** > **Gehäusekonfiguration wiederherstellen** auf **Durchsuchen**, und wählen Sie die Backup-Datei aus, um die gespeicherte Gehäusekonfiguration zu importieren.

2 Klicken Sie auf **Konfiguration wiederherstellen**, um eine verschlüsselte Backup-Datei (**.bak**) oder eine **.xml**-Datei mit einem gespeicherten Profil auf den CMC hochzuladen.

Nach erfolgreichem Abschluss des Wiederherstellungsvorgangs kehrt die CMC Web-Schnittstelle zur Anmeldeseite zurück.

ANMERKUNG: Wenn die Backup-Dateien (.bak) von früheren Versionen des CMC auf die neueste Version des CMC hochgeladen werden, auf dem FIPS aktiviert ist, müssen Sie alle 16 lokalen CMC-Benutzerkennwörter neu konfigurieren. Das Kennwort des ersten Benutzers wird hingegen auf „calvin“ zurückgesetzt.

ANMERKUNG: Wenn ein Gehäusekonfigurationsprofil von einem CMC, der die FIPS-Funktion nicht unterstützt, auf einen CMC mit aktiviertem FIPS importiert wird, bleibt FIPS im CMC aktiviert.

ANMERKUNG: Wenn Sie den FIPS-Modus im Gehäusekonfigurationsprofil ändern, wird `DefaultCredentialMitigation` aktiviert.

Anzeigen gespeicherter Gehäusekonfigurationsprofile

Rufen Sie zum Anzeigen der auf der Netzwerkfreigabe gespeicherten Gehäusekonfigurationsprofile die Seite **Gehäusekonfigurationsprofile** auf. Wählen Sie im Abschnitt **Gehäusekonfigurationsprofile** > **Gespeicherte Profile** das Profil aus, und klicken Sie in der Spalte **Profil anzeigen** auf **Anzeigen**. Die Seite **Einstellungen anzeigen** wird angezeigt. Weitere Informationen über die angezeigten Einstellungen finden Sie in der *CMC-Online-Hilfe*.

Anwenden von Gehäusekonfigurationsprofilen

Sie können eine Gehäusekonfiguration auf ein Gehäuse anwenden, sofern das Gehäusekonfigurationsprofil als gespeichertes Profil auf der Netzwerkfreigabe verfügbar ist. Zum Initiieren einer Gehäusekonfiguration können Sie ein gespeichertes Profil auf ein Gehäuse anwenden.

So wenden Sie ein Profil auf ein Gehäuse an:

1 Rufen Sie die Seite **Gehäusekonfigurationsprofile** auf. Wählen Sie im Abschnitt **Gespeicherte Profile** das gespeicherte Profil aus, das Sie anwenden möchten.

2 Klicken Sie auf **Profil anwenden**.

Es wird eine Warnmeldung mit dem Hinweis angezeigt, dass durch Anwenden eines neuen Profils die aktuellen Einstellungen überschrieben und das ausgewählte Gehäuse neu gestartet wird. Sie werden aufgefordert, die Meldung zu bestätigen, falls Sie mit dem Vorgang fortfahren möchten.

3 Klicken Sie auf **OK**, um das Profil auf das Gehäuse anzuwenden.

Exportieren von Gehäusekonfigurationsprofilen

Sie können auf einer Netzwerkfreigabe gespeicherte Gehäusekonfigurationsprofile an einem festgelegten Pfad auf einer Management Station exportieren.

So exportieren Sie ein gespeichertes Profil:

1 Rufen Sie die Seite **Gehäusekonfigurationsprofile** auf. Wählen Sie im Abschnitt **Gehäusekonfigurationsprofile** > **Gespeicherte Profile** das gewünschte Profil aus, und klicken Sie auf **Kopie des Profils exportieren**.

Eine Meldung zum **Datei-Download** wird angezeigt und Sie werden dazu aufgefordert, die Datei zu öffnen oder zu speichern.

2 Klicken Sie auf **Speichern** oder **Öffnen**, um das Profil auf den erforderlichen Standort zu exportieren.

Bearbeiten von Gehäusekonfigurationsprofilen

Sie können den Namen eines Gehäusekonfigurationsprofils für ein Gehäuse bearbeiten.

So bearbeiten Sie den Namen eines Gehäusekonfigurationsprofils:

1 Rufen Sie die Seite **Gehäusekonfigurationsprofile** auf. Wählen Sie im Abschnitt **Gehäusekonfigurationsprofile** > **Gespeicherte Profile** das gewünschte Profil aus, und klicken Sie auf **Profil bearbeiten**.

Das Fenster **Profil bearbeiten** wird angezeigt.

2 Geben Sie den gewünschten Profilnamen in das Feld **Profilname** ein, und klicken Sie auf **Profil bearbeiten**.

Die Meldung `Operation Successful` wird angezeigt.

3 Klicken Sie auf **OK**.

Löschen von Gehäusekonfigurationsprofilen

Sie können ein Gehäusekonfigurationsprofil löschen, das auf der Netzwerkfreigabe gespeichert ist.

So löschen Sie ein gespeichertes Gehäusekonfigurationsprofil:

1 Rufen Sie die Seite **Gehäusekonfigurationsprofile** auf. Wählen Sie im Abschnitt **Gehäusekonfigurationsprofile** > **Gespeicherte Profile** das gewünschte Profil aus, und klicken Sie auf **Profil löschen**.

Es wird eine Warnmeldung mit dem Inhalt angezeigt, dass das ausgewählte Profil durch den Profillöschvorgang dauerhaft gelöscht wird.

2 Klicken Sie auf **OK**, um das ausgewählte Profil zu löschen.

Mehrere CMCs über RACADM konfigurieren

Mit RACADM können Sie einen oder mehrere CMCs mit identischen Eigenschaften konfigurieren.

Wenn Sie eine spezifische CMC-Karte mit deren Gruppen-ID und Objekt-ID abfragen, erstellt RACADM die `racadm.cfg`-Konfigurationsdatei aus den abgerufenen Informationen. Wenn Sie die Datei zu einem oder mehreren CMCs exportieren, können Sie in kürzester Zeit Ihre Controller mit identischen Eigenschaften konfigurieren.

ANMERKUNG: Einige Konfigurationsdateien enthalten eindeutige CMC-Informationen (wie die statische IP-Adresse), die vor dem Exportieren der Datei zu anderen CMCs geändert werden müssen.

1 Verwenden Sie RACADM, um den Ziel-CMC abzufragen, der die gewünschte Konfiguration enthält.

ANMERKUNG: Die erstellte Konfigurationsdatei ist myfile.cfg. Sie können die Datei umbenennen. Die erstellte .cfg-Datei enthält keine Benutzerkennwörter. Wenn die .cfg-Datei auf den neuen CMC hochgeladen wurde, müssen Sie alle Kennwörter erneut hinzufügen.

2 Geben Sie Folgendes in die Befehlszeile ein:

```
racadm getconfig -f myfile.cfg
```

ANMERKUNG: Das Umleiten der CMC-Konfiguration zu einer Datei mit `getconfig-f` wird nur mit der Remote-RACADM-Schnittstelle unterstützt.

3 Modifizieren Sie die Konfigurationsdatei mit einem Klartext-Editor (optional). Formatierungen in der Konfigurationsdatei können die RACADM-Datenbank beschädigen.

4 Verwenden Sie die neu erstellte Konfigurationsdatei, um einen Ziel-CMC zu modifizieren. Geben Sie in der Befehlszeile Folgendes ein:

```
racadm config -f myfile.cfg
```

5 Setzen Sie den konfigurierten Ziel-CMC zurück. Geben Sie in der Befehlszeile Folgendes ein:

```
racadm reset
```

Der Unterbefehl `getconfig -f myfile.cfg` fordert die CMC-Konfiguration für den aktiven CMC an und erstellt die Datei **myfile.cfg**. Falls erforderlich, können Sie die Datei umbenennen oder an einem anderen Ort speichern.

Sie können den Befehl `getconfig` dazu ausführen, die folgenden Maßnahmen auszuführen:

- Alle Konfigurationseigenschaften in einer Gruppe anzeigen (nach Gruppenname und -index).
- Alle Konfigurationseigenschaften für einen Benutzer nach Benutzernamen anzeigen.

Der Unterbefehl `config` lädt die Informationen auf andere CMCs. Der Server Administrator verwendet den Befehl `config` zur Synchronisierung der Benutzer- und Kennwort-Datenbank.

CMC-Konfigurationsdatei erstellen

Die CMC-Konfigurationsdatei, **<Dateiname>.cfg**, wird zusammen mit dem Befehl `racadm config -f <filename>.cfg` verwendet, um eine einfache Textdatei zu erstellen. Mithilfe dieses Befehls können Sie eine Konfigurationsdatei (ähnlich einer **.ini**-Datei) erstellen und den CMC über diese Datei konfigurieren.

Es kann ein beliebiger Dateiname verwendet werden. Die Datei erfordert keine **.cfg**-Erweiterung (obwohl dieser Unterabschnitt auf diese Endung verweist).

ANMERKUNG: Lesen Sie für weitere Informationen zum Unterbefehl `getconfig` das *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

RACADM parst die **.cfg**-Datei, wenn sie zum ersten Mal auf den CMC geladen wird, um zu prüfen, ob eine gültige Gruppe und Objektnamen vorhanden sind und ob einige einfache Syntaxregeln befolgt werden. Fehler werden mit der Zeilennummer markiert, in der der Fehler ermittelt wurde. Eine Meldung beschreibt das Problem. Die vollständige Datei wird auf Richtigkeit geparst und alle Fehler werden angezeigt. Wenn in der **.cfg** Datei ein Fehler festgestellt wird, werden Schreibbefehle nicht an den CMC übertragen. Sie müssen alle Fehler korrigieren, bevor eine Konfiguration erfolgen kann.

Um vor dem Erstellen der Konfigurationsdatei eine Prüfung auf Fehler vorzunehmen, verwenden Sie die Option `-c` zusammen mit dem Unterbefehl `config`. Mit der Option `-c` überprüft `config` nur die Syntax und schreibt nicht auf den CMC.

Beachten Sie beim Erstellen einer **.cfg**-Datei folgende Richtlinien:

- Wenn der Parser auf eine indizierte Gruppe trifft, ist der Wert des verankerten Objekts für die Unterscheidung der einzelnen Indizes ausschlaggebend.

  Die Parser liest alle Indizes aus dem CMC für diese Gruppe ein. Alle Objekte in dieser Gruppe sind Modifikationen, wenn der CMC konfiguriert wird. Wenn ein modifiziertes Objekt einen neuen Index repräsentiert, wird der Index während der Konfiguration auf dem CMC erstellt.
- Sie können in einer **.cfg**-Datei keinen gewünschten Index angeben.

  Indizes können erstellt und gelöscht werden. Im Laufe der Zeit kann die Gruppe durch genutzte und ungenutzte Indizes fragmentiert werden. Wenn ein Index vorhanden ist, wird er modifiziert. Wenn kein Index vorhanden ist, wird der erste verfügbare Index verwendet.

  Diese Methode sorgt für Flexibilität, wenn indizierte Einträge hinzugefügt werden, wobei Sie keine genauen Index-Übereinstimmungen zwischen allen verwalteten CMCs herstellen müssen. Neue Benutzer werden zum ersten verfügbaren Index hinzugefügt. Eine **.cfg**-Datei, die auf einem CMC richtig geparst und ausgeführt wird, wird auf einem anderen möglicherweise nicht richtig ausgeführt, falls alle Indizes belegt sind und ein neuer Benutzer hinzugefügt werden muss.
- Verwenden Sie den Unterbefehl `racresetcfg`, um beide CMCs mit identischen Eigenschaften zu konfigurieren.

  Verwenden Sie den Unterbefehl `racresetcfg` zum Zurücksetzen des CMC auf die ursprünglichen Standardeinstellungen, und führen Sie anschließend den Befehl `racadm config -f <filename>.cfg` aus. Stellen Sie sicher, dass die **.cfg**-Datei enthält alle gewünschten Objekte, Benutzer, Indizes und anderen Parameter enthält. Eine vollständige Liste von Objekten und Gruppen finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

VORSICHT: Verwenden Sie den Unterbefehl `racresetcfg`, um die Datenbank und die CMC- Netzwerkschnittstellen-Einstellungen auf die ursprünglichen Standardeinstellungen zurückzusetzen und alle Benutzer und Benutzerkonfigurationen zu entfernen. Solange der Root-Benutzer verfügbar ist, werden die Einstellungen anderer Benutzer ebenfalls auf die Standardeinstellungen zurückgesetzt.

- Wenn Sie `racadm getconfig -f <filename> .cfg` eingeben, erstellt der Befehl eine **.cfg**-Datei für die aktuelle CMC-Konfiguration. Diese Konfigurationsdatei kann als Beispiel und Ausgangspunkt für Ihre spezifische **cfg**-Datei verwendet werden.

Parsing-Regeln

- Zeilen, die mit dem Raute-Zeichen (#) beginnen, werden als Anmerkungen behandelt.

  Eine Kommentarzeile muss in Spalte eins beginnen. Ein „#"-Zeichen in einer anderen Spalte wird als das Zeichen „#" behandelt.

  Einige Modemparameter können „#"-Zeichen in den Zeichenketten enthalten. Ein Escape-Zeichen ist nicht erforderlich. Sie möchten vielleicht eine **.cfg**-Datei mithilfe des Befehls `racadm getconfig -f <filename> .cfg` erstellen und dann den Befehl `racadm config -f <filename> .cfg` für einen anderen CMC ausführen, ohne Escape-Zeichen hinzuzufügen.

  Beispiel:

```
#
# This is a comment
[cfgUserAdmin]
cfgUserAdminPageModemInitString= <Modem init # not
a comment>
```

- Alle Gruppeneinträge müssen in Klammern stehen ([und]).

  Das Anfangszeichen „[", das einen Gruppennamen anzeigt, muss sich in Spalte eins befinden. Der Gruppenname muss vor allen anderen Objekten in dieser Gruppe angegeben werden. Objekte, die keinen zugewiesenen Gruppennamen enthalten, erzeugen Fehler. Die Konfigurationsdaten sind in Gruppen organisiert, wie es im Kapitel über Datenbankeigenschaften im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX) definiert ist. Das folgende Beispiel zeigt einen Gruppennamen, ein Objekt und den Eigenschaftswert des Objekts an.

```
[cfgLanNetworking] -{group name}
cfgNicIpAddress=143.154.133.121 {object name}
{object value}
```

- Alle Parameter werden als „Objekt=Wert"-Paare ohne Leerzeichen zwischen „Objekt", „=" und „Wert" angegeben. Leerzeichen nach dem Wert werden ignoriert. Ein Leerzeichen innerhalb einer Wertezeichenkette bleibt unverändert. Jedes Zeichen rechts neben dem „=" (z. B. ein zweites „=", ein „#", „[", „]" usw.) wird wie eingegeben übernommen. Bei diesen Zeichen handelt es sich um gültige Zeichen für Modem-Chat-Skripts.

```
[cfgLanNetworking] -{group name}
cfgNicIpAddress=143.154.133.121 {object value}
```

- Der **.cfg**-Parser ignoriert einen Index-Objekt-Eintrag.

  Benutzer können nicht angeben, welcher Index verwendet werden soll. Wenn der Index bereits vorhanden ist, wird dieser entweder verwendet oder ein neuer Eintrag wird im ersten verfügbaren Index für diese Gruppe erstellt.

  Der Befehl `racadm getconfig -f <filename>.cfg` setzt eine Anmerkung vor die Index-Objekte, sodass Sie die enthaltenen Anmerkungen sehen können.

ANMERKUNG: Sie können eine indizierte Gruppe manuell mit folgendem Befehl erstellen:
`racadm config -g <groupname>  -o <anchored object> -i <index 1-4> <unique anchor name>`

- Die Zeile für eine indizierte Gruppe kann nicht aus einer **.cfg**-Datei gelöscht werden. Wenn Sie die Zeile mit einem Texteditor löschen, hält RACADM beim Parsen der Konfigurationsdatei an und gibt eine Warnung zum Fehler aus.

  Benutzer müssen ein indiziertes Objekt manuell mit folgendem Befehl entfernen:

```
racadm config -g <groupname>  -o <objectname> -i <index 1-4> ""
```

ANMERKUNG: Eine NULL-Zeichenkette (durch zwei "-Zeichen gekennzeichnet) weist iDRAC an, den Index für die angegebene Gruppe zu löschen.

Um den Inhalt einer indizierten Gruppe anzuzeigen, verwenden Sie den folgenden Befehl:

```
racadm getconfig -g <groupname> -i <index 1-4>
```

- Für indizierte Gruppen muss das erste Objekt nach dem [ ]-Paar als Objektanker fungieren. Im Folgenden finden Sie Beispiele für aktuelle indizierte Gruppen:

  ```
  [cfgUserAdmin]
  cfgUserAdminUserName= <USER_NAME>
  ```

- Wenn bei Verwendung von Remote-RACADM zur Erfassung der Konfigurationsgruppen in einer Datei eine Schlüsseleigenschaft innerhalb einer Gruppe nicht festgelegt ist, wird die Konfigurationsgruppe nicht als Teil der Konfigurationsdatei gespeichert. Falls diese Konfigurationsgruppen auf andere CMCs geklont werden müssen, muss die Schlüsseleigenschaft festgelegt werden, bevor der Befehl `getconfig -f` ausgeführt wird. Alternativ können Sie die fehlenden Eigenschaften manuell in die Konfigurationsdatei eingeben, nachdem Sie den Befehl `getconfig -f` ausgeführt haben. Dies gilt für alle RACADM-indizierten Gruppen.

  Dies ist die Liste der indizierten Gruppen, die dieses Verhalten und die entsprechenden Schlüsseleigenschaften aufweisen:

  - cfgUserAdmin – cfgUserAdminUserName
  - cfgEmailAlert – cfgEmailAlertAddress
  - cfgTraps – cfgTrapsAlertDestIPAddr
  - cfgStandardSchema – cfgSSADRoleGroupName
  - cfgServerInfo – cfgServerBmcMacAddress

CMC-IP-Adresse modifizieren

Wenn Sie die CMC-IP-Adresse in der Konfigurationsdatei ändern, entfernen Sie alle unnötigen `<variable> = <value>`-Einträge. Es verbleibt lediglich die tatsächliche Bezeichnung der variablen Gruppe mit "[" und "]" zusammen mit den beiden `<variable> = <value>`-Einträgen, die sich auf die IP-Adressenänderung beziehen.

Beispiel:

```
#
# Object Group "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.10.110
cfgNicGateway=10.35.10.1
```

Die Datei wird aktualisiert wie folgt:

```
#
# Object Group "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.9.143
# comment, the rest of this line is ignored
cfgNicGateway=10.35.9.1
```

Mit dem Befehl `racadm config -f <myfile>.cfg` wird die Datei geparst, und Fehler werden nach Zeilennummer identifiziert. Eine korrekte Datei aktualisiert die richtigen Einträge. Außerdem kann derselbe `getconfig`-Befehl (siehe vorheriges Beispiel) zur Bestätigung der Aktualisierung verwendet werden.

Verwenden Sie diese Datei, um unternehmensweite Änderungen herunterzuladen, oder um neue Systeme mit dem Befehl `racadm getconfig -f <myfile>.cfg` über das Netzwerk zu konfigurieren.

ANMERKUNG: *Anchor* ist ein reserviertes Wort und sollte nicht in der .cfg-Datei verwendet werden.

Konfigurieren mehrerer CMCs über RACADM unter Verwendung von Gehäusekonfigurationsprofilen

Unter Verwendung von Gehäusekonfigurationsprofilen können Sie eine Gehäusekonfiguration als XML-Datei exportieren und in ein anderes Gehäuse importieren.

Verwenden Sie den RACADM-Befehl **get** zum Exportieren und den Befehl **set** zum Importieren. Sie können Gehäuseprofile (XML-Dateien) vom CMC auf eine Netzwerkfreigabe oder eine lokale Management Station exportieren und Gehäuseprofile (XML-Dateien) von einer Netzwerkfreigabe oder einer lokalen Management Station importieren.

ANMERKUNG: Standardmäßig erfolgt der Exportvorgang als Klontyp. Mit `--clone` können Sie das Klontypprofil in der XML-Datei abrufen.

Der Import- und Exportvorgang auf bzw. von der Netzwerkfreigabe kann über lokales RACADM sowie über Remote-RACADM erfolgen. Der Import- und Export Vorgang auf bzw. von der lokalen Management Station kann hingegen nur über die Remote-RACADM-Schnittstelle durchgeführt werden.

Exportieren von Gehäusekonfigurationsprofilen

Sie können Gehäusekonfigurationsprofile mithilfe des Befehls **get** auf die Netzwerkfreigabe exportieren.

1 Geben Sie Folgendes ein, um die Gehäusekonfigurationsprofile als **clone.xml**-Datei unter Verwendung des Befehls **get** auf eine CIFS-Netzwerkfreigabe zu exportieren:

```
racadm get -f clone.xml -t xml -l //xx.xx.xx.xx/PATH -u USERNAME -p PASSWORDCMC
```

2 Geben Sie Folgendes ein, um die Gehäusekonfigurationsprofile als **clone.xml**-Datei unter Verwendung des Befehls **get** auf eine NFS-Netzwerkfreigabe zu exportieren:

```
racadm get -f clone.xml -t xml -l xx.xx.xx.xx:/PATH
```

Sie können Gehäusekonfigurationsprofile über eine Remote-RACADM-Schnittstelle auf eine Netzwerkfreigabe exportieren.

1 Geben Sie Folgendes ein, um die Gehäusekonfigurationsprofile als clone.xml-Datei auf eine CIFS-Netzwerkfreigabe zu exportieren:

```
racadm -r xx.xx.xx.xx -u USERNAMECMC -p PASSWORDCMC get -f clone.xml -t xml -l //xx.xx.xx.xx/
PATH -u USERNAME -p PASSWORD
```

2 Geben Sie Folgendes ein, um die Gehäusekonfigurationsprofile als clone.xml-Datei auf eine NFS-Netzwerkfreigabe zu exportieren:

```
racadm -r xx.xx.xx.xx -u USERNAMECMC -p PASSWORDCMC get -f clone.xml -t xml -l xx.xx.xx.xx:/
PATH
```

Sie können Gehäusekonfigurationsprofile über eine Remote-RACADM-Schnittstelle auf eine lokale Management Station exportieren.

1 Geben Sie Folgendes ein, um die Gehäusekonfigurationsprofile als clone.xml-Datei zu exportieren:

```
racadm -r xx.xx.xx.xx -u USERNAMECMC -p PASSWORDCMC get -f clone.xml -t xml
```

Importieren von Gehäusekonfigurationsprofilen

Sie können Gehäusekonfigurationsprofile mithilfe des Befehls **set** von einer Netzwerkfreigabe in ein anderes Gehäuse importieren.

1 Geben Sie Folgendes ein, um die Gehäusekonfigurationsprofile von einer CIFS-Netzwerkfreigabe zu importieren:

```
racadm set -f clone.xml -t xml -l //xx.xx.xx.xx/PATH -u USERNAME -p PASSWORDCMC
```

2 Geben Sie Folgendes ein, um die Gehäusekonfigurationsprofile von einer NFS-Netzwerkfreigabe zu importieren:

```
racadm set -f clone.xml -t xml -l xx.xx.xx.xx:/PATH
```

Sie können Gehäusekonfigurationsprofile über eine Remote-RACADM-Schnittstelle von einer Netzwerkfreigabe importieren.

1 Geben Sie Folgendes ein, um die Gehäusekonfigurationsprofile von einer CIFS-Netzwerkfreigabe zu importieren:

```
racadm -r xx.xx.xx.xx -u USERNAMECMC -p PASSWORDCMC  set -f clone.xml -t xml -l //
xx.xx.xx.xx/PATH -u USERNAME -p PASSWORD
```

2 Geben Sie Folgendes ein, um die Gehäusekonfigurationsprofile von einer NFS-Netzwerkfreigabe zu importieren:

```
racadm -r xx.xx.xx.xx -u USERNAMECMC -p PASSWORDCMC set -f clone.xml -t xml -l xx.xx.xx.xx:/
PATH
```

Sie können Gehäusekonfigurationsprofile über eine Remote-RACADM-Schnittstelle von einer lokalen Management Station importieren.

1 Geben Sie Folgendes ein, um die Gehäusekonfigurationsprofile als clone.xml-Datei zu exportieren:

```
racadm -r xx.xx.xx.xx -u USERNAMECMC -p PASSWORDCMC set -f clone.xml -t xml
```

Parsing-Regeln

Sie können die Eigenschaften einer exportierten XML-Datei mit Gehäusekonfigurationsprofilen manuell bearbeiten.

Eine XML-Datei enthält die folgenden Eigenschaften:

- **Systemkonfiguration** – Dies ist der übergeordnete Knoten.
- **Komponente** – Dies ist der primäre untergeordnete Knoten.
- **Attributes** (Attribute) – Enthält Name und Wert. Sie können diese Felder bearbeiten. Beispielsweise können Sie den Wert `Asset Tag` wie folgt bearbeiten:

  ```
  <Attribute Name="ChassisInfo.1#AssetTag">xxxxxx</Attribute>
  ```

Beispiel für eine XML-Datei:

```
<SystemConfiguration Model="PowerEdge M1000e
"ServiceTag="NOBLE13"
TimeStamp="Tue Apr  7 14:17:48 2015" ExportMode="2">
<!--Export type is Replace-->
<!--Exported configuration may contain commented attributes. Attributes may be commented due to
dependency,
destructive nature, preserving server identity or for security reasons.-->
<Component FQDD="CMC.Integrated.1">
<Attribute Name="ChassisInfo.1#AssetTag">00000</Attribute>
<Attribute Name="ChassisLocation.1#DataCenterName"></Attribute>
<Attribute Name="ChassisLocation.1#AisleName"></Attribute>
<Attribute Name="ChassisLocation.1#RackName"></Attribute>
….
</Component>
</SystemConfiguration>
```

Anzeigen und Beenden der CMC-Sitzungen

Sie können die Anzahl der Benutzer anzeigen, die derzeit bei iDRAC7 angemeldet sind und die Benutzersitzungen beenden.

ANMERKUNG: Um eine Sitzung zu beenden, müssen Sie die Berechtigung als Gehäusekonfiguration-Administrator besitzen.

Anzeigen und Beenden der CMC-Sitzungen über die Webschnittstelle

So verwalten oder beenden Sie eine Sitzung über die Webschnittstelle:

1 Wählen Sie in der Systemstruktur **Gehäuseübersicht** aus und klicken Sie auf **Netzwerk** > **Sitzungen**.
Daraufhin werden auf der Seite **Sitzungen** die Sitzungs-ID, der Benutzername, die IP-Adresse und der Sitzungstyp angezeigt. Weitere Informationen zu diesen Eigenschaften finden Sie in der *Online-Hilfe*.

2 Um die Sitzung zu beenden, klicken Sie für die Sitzung auf **Beenden**.

Anzeigen und Beenden der CMC-Sitzungen über RACADM

Sie benötigen Administratorberechtigungen, um CMC-Sitzungen über RACADM beenden zu können.

Verwenden Sie zum Anzeigen der aktuellen Benutzersitzungen den Befehl `getssninfo`.

Verwenden Sie zum Beenden einer Benutzersitzung den Befehl `closessn`.

Weitere Informationen über diese Befehle finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX) unter **dell.com/support/manuals**.

7

Server konfigurieren

Sie können die folgenden Einstellungen eines Servers konfigurieren:

- Steckplatznamen
- iDRAC-Netzwerkeinstellungen
- DRAC-VLAN-Tag-Einstellungen
- Erstes Startgerät
- Server-FlexAddress
- Remote-Dateifreigabe
- BIOS-Einstellungen unter Verwendung der Funktion zum Klonen von Servern

Themen:

Steckplatznamen konfigurieren

Steckplatznamen werden zur Identifizierung einzelner Server verwendet. Beim Wählen von Steckplatznamen gelten die folgenden Regeln:

- Namen dürfen maximal 24 nicht erweiterte ASCII-Zeichen (ASCII-Codes 32 bis 126) enthalten. Standard- und Sonderzeichen sind in den Namen zugelassen.
- Steckplatznamen müssen innerhalb des Gehäuses eindeutig sein. Steckplätze dürfen nicht denselben Namen wie ein anderer Steckplatz haben.
- Bei den Zeichenketten wird nicht zwischen Groß- und Kleinschreibung unterschieden. `Server-1, server-1, and SERVER-1` sind identische Namen.
- Steckplatznamen dürfen nicht mit einer der folgenden Zeichenketten beginnen:
  - Switch-
  - Fan-
  - PS-
  - DRAC-
  - MC-
  - Gehäuse
  - Housing-Left
  - Housing-Right
  - Housing-Center
- Die Zeichenketten `Server-1` bis `Server-4` können verwendet werden, aber nur für den entsprechenden Steckplatz. Zum Beispiel ist `Server-3` ein gültiger Name für Steckplatz 3, aber nicht für Steckplatz 4. `Server-03` dagegen ist ein gültiger Name für einen beliebigen Steckplatz.

ANMERKUNG: Um einen Steckplatznamen zu ändern, müssen Sie Berechtigungen als Gehäusekonfiguration-Administrator besitzen.

Die Einstellung des Steckplatznamens in der Webschnittstelle befindet sich nur auf dem CMC. Wird der Server vom Gehäuse entfernt, verbleibt die Einstellung des Steckplatznamens nicht beim Server.

Die Einstellung des Steckplatznamens in der CMC-Webschnittstelle setzt immer die Änderungen außer Kraft, die auf der iDRAC-Schnittstelle am Anzeigenamen vorgenommen wurden.

So bearbeiten Sie einen Steckplatznamen über die CMC-Webschnittstelle:

1 Klicken Sie im linken Fenster auf **Gehäuseübersicht** > **Serverübersicht** > **Setup** > **Steckplatznamen**.
2 Bearbeiten Sie auf der Seite **Steckplatznamen** im Feld **Steckplatznamen** den Steckplatzname.
3 Um den Hostnamen eines Servers als Steckplatznamen zu verwenden, wählen Sie die Option **Hostnamen für Steckplatznamen verwenden** aus. Dadurch werden die statischen Steckplatznamen durch den Hostnamen des Servers (oder den Systemnamen) überschrieben, falls verfügbar. Dazu muss der OMSA-Agent auf dem Server installiert sein. Ausführlichere Informationen zum OMSA-Agenten finden Sie im *Dell OpenManage Server Administrator User's Guide* (Dell OpenManage Server Administrator-Benutzerhandbuch) unter dell.com/support/manuals.
4 Um den iDRAC-DNS-Namen als Steckplatznamen zu verwenden, wählen Sie die Option **iDRAC-DNS-Namen als Steckplatznamen verwenden** aus. Diese Option ersetzt die statischen Steckplatznamen durch die entsprechenden iDRAC-DNS-Namen, falls verfügbar. Wenn keine iDRAC-DNS-Namen verfügbar sind, werden die standardmäßigen oder bearbeiteten Steckplatznamen angezeigt.

   ANMERKUNG: Um die Option iDRAC-DNS-Namen als Steckplatznamen verwenden verwenden zu können, müssen Sie die Option Gehäusekonfiguration-Administrator-Berechtigung besitzen.
5 Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

Um den Standardsteckplatznamen (STECKPLATZ-01 bis STECKPLATZ-04) basierend auf der Position des Serversteckplatzes) zum Server wiederherzustellen, klicken Sie auf **Standardwert wiederherstellen**.

iDRAC Netzwerkeinstellungen konfigurieren

Um diese Funktion zu verwenden, müssen Sie eine Enterprise-Lizenz aufweisen. Sie können die iDRAC-Netzwerkkonfigurationseinstellungen für einen Server konfigurieren. Sie können die QuickDeploy-Einstellungen verwenden, um die Standard- iDRAC-Netzwerkkonfigurationseinstellungen und das Stammkennwort für Server, die zu einem späteren Zeitpunkt installiert werden, zu konfigurieren. Diese Standardeinstellungen sind die Einstellungen der schnellen iDRAC Bereitstellung.

Weitere Informationen zu iDRAC finden Sie im *iDRAC-Benutzerhandbuch* unter **dell.com/support/manuals**.

iDRAC QuickDeploy-Netzwerkeinstellungen (iDRAC Netzwerkeinstellungen zur schnellen Bereitstellung) konfigurieren

Verwenden Sie die QuickDeploy-Einstellungen, um die Netzwerkeinstellungen für neu eingefügte Server zu konfigurieren.

So aktivieren Sie die iDRAC-Einstellungen für die schnelle Bereitschaft und stellen sie ein:

1 Klicken Sie im linken Fenster auf **Serverübersicht** > **Setup** > **iDRAC**.
2 Legen sie auf der Seite **iDRAC bereitstellen**, im Abschnitt **QuickDeploy-Einstellungen**, die Einstellungen fest, die in der folgenden Tabelle erwähnt wurden. Weitere Informationen über die Felder finden Sie in der *Online-Hilfe*.

Tabelle 18. QuickDeploy-Einstellungen

Einstellung	Beschreibung
Maßnahme, wenn der Server eingefügt wird	Wählen Sie eine der folgenden Optionen aus der Liste: • Keine Maßnahme – Die Maßnahme wird nicht ausgeführt, wenn der Server eingefügt wird. • Nur QuickDeploy — Wählen Sie diese Option, um iDRAC-Neztwerkeinstellungen zu aktivieren, wenn ein neuer Server in das Gehäuse eingesetzt wird. Die angegebenen Einstellungen zur automatischen Bereitstellung werden zum Konfigurieren des neuen iDRAC verwendet. Hierzu zählt das root-Benutzerkennwort, wenn root-Kennwort ändern ausgewählt wird. • Nur Serverprofil – Wählen Sie diese Option aus, um das zugewiesene Serverprofil anzuwenden, wenn ein neuer Server in das Gehäuse eingesetzt wird. • Quick Deploy und Serverprofil – Wählen Sie diese Option, um zuerst die iDRAC-Netzwerkeinstellungen und dann das zugewiesene Serverprofil anzuwenden, wenn ein neuer Server in das Gehäuse eingesetzt wird. .
iDRAC-root-Kennwort nach Einsetzen des Servers einstellen	Wählen Sie die Option zur Änderung des iDRAC-Stammkennworts, um den Wert, der im Feld **iDRAC-Stammkennwort** bereitgestellt ist, anzupassen.
iDRAC-root-Kennwort	Wenn **iDRAC-Stammkennwort bei Servereinfügung einstellen** und **QuickDeploy aktiviert** gewählt wird, wird der Kennwortwert einem Server-iDRAC-Stammbenutzerkennwort zugewiesen, wenn der Server in ein Gehäuse eingefügt wird. Das Kennwort kann 1 bis 20 druckbare Zeichen (einschließlich Leerzeichen) aufweisen.
iDRAC-root-Kennwort bestätigen	Mit dieser Option können Sie das Kennwort noch einmal in das Feld **Kennwort** eingeben.
iDRAC-LAN aktivieren	Aktiviert oder deaktiviert den iDRAC-LAN-Kanal. Diese Option ist standardmäßig gelöscht.
iDRAC IPv4 aktivieren	Aktiviert oder deaktiviert IPv4 auf dem iDRAC. Diese Option ist standardmäßig ausgewählt.
iDRAC-IPMI-über-LAN aktivieren	Aktiviert oder deaktiviert den IPMI-über-LAN-Kanal für jeden iDRAC, der sich in dem Gehäuse befindet. Standardmäßig ist diese Option ausgewählt.
iDRAC IPv4 DHCP aktivieren	Aktiviert oder deaktiviert DHCP für jeden iDRAC, der sich in dem Gehäuse befindet. Wenn diese Option aktiviert ist, sind die Felder **QuickDeploy-IP**, **QuickDeploy-Subnetzmaske** und **QuickDeploy-Gateway** deaktiviert und können nicht geändert werden, da DHCP verwendet wird, um diese Einstellungen automatisch für jeden iDRAC zuzuweisen. Um diese Option auszuwählen, müssen Sie die Option **iDRAC IPv4 aktivieren** auswählen. Quick Deploy-IP bietet zwei Optionen: 2 und 4.
iDRAC-IPv4-Adresse starten (Steckplatz 1)	Gibt die statische IP-Adresse des iDRAC des Servers in Steckplatz 1 des Gehäuses an. Die IP-Adresse jedes nachfolgenden iDRAC wird für jeden Steckplatz jeweils um 1 erhöht, angefangen mit der statischen IP-Adresse von Steckplatz 1. Falls die IP-Adresse plus die Steckplatznummer größer als die Subnetzmaske ist, wird eine Fehlermeldung angezeigt. **ANMERKUNG: Die Subnetzmaske und das Gateway werden nicht wie die IP-Adresse erhöht.** Wenn zum Beispiel die ursprüngliche IP-Adresse `192.168.0.250` und die Subnetzmaske `255.255.0.0` ist, dann ist die IP-Adresse für QuickDeploy für Steckplatz 15: `192.168.0.265`. Wenn die Subnetzmaske `255.255.255.0` wäre,

Einstellung	Beschreibung
	würde die Fehlermeldung `QuickDeploy IP address range is not fully within QuickDeploy Subnet` angezeigt, wenn Sie entweder auf **QuickDeploy-Einstellungen speichern** oder **Automatische Bestückung mit QuickDeploy-Einstellungen** klicken.
iDRAC IPv4-Netzmaske	Gibt die QuickDeploy-Subnetzmaske an, die allen neu eingefügten Servern zugewiesen ist.
iDRAC IPv4-Gateway	Gibt den schnellen Bereitstellungs-Standard-Gateway an, der allen DRACs, die sich im Gehäuse befinden, zugewiesen ist.
iDRAC IPv6 aktivieren	Aktiviert die IPv6-Adressierung für jedes im Gehäuse vorhandenen iDRAC, das IPv6 fähig ist.
iDRAC IPv6-Autokonfiguration aktivieren	Aktiviert den iDRAC zur Beschaffung von IPv6-Einstellungen (Adresse und Präfixlänge) von einem DHCPv6-Server und aktiviert auch statuslose automatische Adresskonfiguration. Diese Option ist standardmäßig aktiviert.
iDRAC IPv6-Gateway	Gibt das Standard-IPv6-Gateway an, das den iDRACs zugewiesen wird. Der Standardwert ist "::".
iDRAC IPv6-Präfixlänge	Gibt die Präfixlänge an, die den IPv6-Adressen auf dem iDRAC zugewiesen wird. Der Standardwert ist 64.
CMC-DNS-Einstellungen verwenden	Kommuniziert die CMC-DNS-Server-Einstellungen (IPv4 und IPv6) zum iDRAC, wenn ein Blade-Server in das Gehäuse eingesetzt wird.

3 Klicken Sie auf **QuickDeploy-Einstellungen speichern**, um die Auswahl zu speichern. Wenn Sie die Änderungen an den Einstellungen des iDRAC-Netzwerkes vorgenommen haben, klicken Sie auf **iDRAC-Netzwerkeinstellungen anwenden**, um die Einstellungen zur iDRAC bereitzustellen.

Die QuickDeploy-Funktion wird nur ausgeführt, wenn sie aktiviert ist und ein Server im Gehäuse eingefügt ist. Wenn **iDRAC-Stammkennwort bei Servereinfügung einstellen** und **QuickDeploy aktiviert** aktiviert sind, wird der Benutzer aufgefordert, die LCD-Schnittstelle zu verwenden, um die Kennwortänderung zu erlauben oder nicht zu erlauben. Wenn Netzwerkeinstellungen vorhanden sind, die sich von den aktuellen iDRAC-Einstellungen unterscheiden, wird der Benutzer aufgefordert, die Änderungen entweder anzunehmen oder abzulehnen.

ANMERKUNG: Wenn eine LAN- oder IPMI-über-LAN-Abweichung vorhanden ist, wird der Benutzer aufgefordert, die IP-Adresseinstellungen für QuickDeploy anzunehmen. Wenn der Unterschied in der DHCP-Einstellung liegt, wird der Benutzer aufgefordert, die DHPC-QuickDeploy-Einstellung anzunehmen.

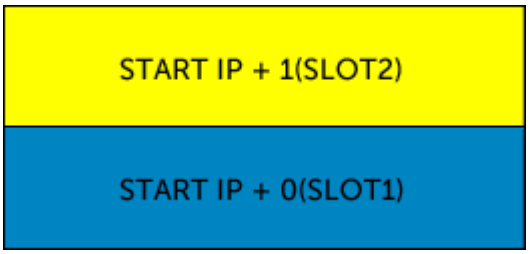
Um die QuickDeploy-Einstellungen in den Abschnitt **iDRAC-Netzwerkeinstellungen** zu kopieren, klicken Sie auf **Mit QuickDeploy-Einstellungen automatisch bestücken**. Die Netzwerkkonfigurationseinstellungen zur schnellen Bereitstellung werden in die entsprechenden Felder der Tabelle **iDRAC-Netzwerkkonfigurationseinstellungen** kopiert.

ANMERKUNG: An den QuickDeploy-Feldern vorgenommene Änderungen sind sofort wirksam, aber Änderungen, die an einer oder mehreren der iDRAC-Servernetzwerkkonfigurationseinstellungen vorgenommen wurden, nehmen unter Umständen ein paar Minuten in Anspruch, um von der CMC zu einem iDRAC zu propagieren. Wenn Aktualisieren zu früh betätigt wird, werden eventuell nur teilweise richtige Daten für einen oder mehrere iDRAC-Server angezeigt.

Zuweisen von QuickDeploy-IP-Adresse zu Servern

Die Abbildung zeigt die QuickDeploy-IP-Adressenzuweisung zu den Servern an, wenn vier Server mit halber Bauhöhe im VRTX-Gehäuse vorliegen:

Die folgende Abbildung zeigt QuickDeploy-IP-Adressenzuweisung zu den Servern an, wenn zwei Blades mit voller Bauhöhe im VRTX-Gehäuse vorliegen:



iDRAC-Netzwerkeinstellungen für individuelle Server-iDRAC ändern

Mithilfe dieser Funktion können Sie die iDRAC-Netzwerkkonfigurationseinstellungen für jeden installierten Server konfigurieren. Die anfänglichen Werte, die für jedes Feld angezeigt werden, sind die aktuellen vom iDRAC gelesenen Werte. Um diese Funktion zu verwenden, müssen Sie eine Enterprise-Lizenz aufweisen.

So ändern Sie die iDRAC-Netzwerkeinstellungen:

1 Klicken Sie im linken Fensterbereich auf **Server-Übersicht**, und klicken Sie dann auf **Setup**. Auf der Seite **iDRAC bereitstellen** führt der Abschnitt **iDRAC-Netzwerkeinstellungen** die iDRAC IPv4- und IPv6-Netzwerkkonfigurationseinstellungen aller installierten Server auf.

2 Ändern Sie entsprechend den Serveranforderungen die iDRAC-Netzwerkeinstellungen.

> **ANMERKUNG: Sie müssen die Option LAN aktivieren auswählen, um die IPv4- oder IPv6-Einstellungen festzulegen. Weitere Informationen über die Felder finden Sie in der *Online-Hilfe*.**

3 Um die Einstellung auf dem iDRAC bereitzustellen, klicken Sie auf **iDRAC-Netzwerkeinstellungen anwenden**. Alle Änderungen an den **Einstellungen zur schnellen Bereitstellung** werden ebenfalls gespeichert.

Die Tabelle **iDRAC-Netzwerkeinstellungen** zeigt zukünftige Netzwerkkonfigurationseinstellungen; die für installierte Server angezeigten Werte können die gleichen sein wie die Werte der zurzeit installierten iDRAC-Netzwerkkonfigurationseinstellungen (müssen es aber nicht). Klicken Sie auf **Aktualisierung**, um die Seite **iDRAC-Bereitstellung** mit jeder installierten iDRAC-Netzwerkkonfigurationseinstellung zu aktualisieren, nachdem Äderungen vorgenommen wurden.

> **ANMERKUNG: An den Feldern der schnellen Bereitstellung vorgenommene Änderungen sind sofort wirksam, aber Änderungen, die an einer oder mehreren der iDRAC-Servernetzwerkkonfigurationseinstellungen vorgenommen wurden, nehmen unter Umständen ein paar Minuten in Anspruch, um von der CMC zu einem iDRAC zu propagieren. Wenn Aktualisierung zu früh gedrückt wird, werden eventuell nur teilweise richtige Daten für einen oder mehrere iDRAC-Server angezeigt.**

iDRAC-Netzwerkeinstellungen über RACADM ändern

RACADM `config` oder `getconfig`Befehle unterstützen die Option `-m <module>` für die folgenden Konfigurationsgruppen:

- `cfgLanNetworking`
- `cfgIPv6LanNetworking`
- `cfgRacTuning`
- `cfgRemoteHosts`
- `cfgSerial`
- `cfgSessionManagement`

Weitere Informationen über die Standardwerte und -Bereiche finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX), verfügbar unter **dell.com/support/manuals**.

Konfigurieren von iDRAC-VLAN-Tag-Einstellungen

Virtuelle LAN-Tags (VLAN-Tags) ermöglichen, dass mehrere VLANs auf demselben physischen Netzwerkkabel existieren können und Netzwerkverkehr für Sicherheits- und Lastverteilungszwecke abgesondert werden kann. Wenn Sie die VLAN-Funktionalität aktivieren, wird jedem Netzwerkpaket ein VLAN-Tag zugewiesen. VLAN-Tags sind Gehäuseeigenschaften. Sie bleiben an das Gehäuse gebunden, selbst wenn eine Komponente entfernt wird.

ANMERKUNG: Die mit dem CMC konfigurierte VLAN-ID wird nur dann auf iDRAC angewendet, wenn iDRAC sich im dedizierten Modus befindet. Wenn iDRAC sich im freigegebenen LOM-Modus befindet, werden die in iDRAC vorgenommenen Änderungen der VLAN-ID nicht in der CMC-GUI angezeigt.

Konfigurieren von virtuellen iDRAC-LAN-Tag-Einstellungen unter Verwendung von RACADM

- Geben Sie die VLAN-Kennung und die Priorität eines bestimmten Servers mit dem folgenden Befehl ein:

  ```
  racadm setniccfg -m server-<n> -v <VLAN-ID> <VLAN priority>
  ```

  Gültige Werte für <*n*> sind 1–4.

  Gültige Werte für <*VLAN*> sind 1– 4000 und 4021– 4094. Die Standardeinstellung ist 1.

  Gültige Werte für <*VLAN priority*> sind 0 – 7. Die Standardeinstellung ist 0.

  Beispiel:

  ```
  racadm setniccfg -m server-1 -v 1 7
  ```

  Beispiel:

- Um ein Server-VLAN zu entfernen, deaktivieren Sie die VLAN-Funktionen des angegebenen Servernetzwerks:

  ```
  racadm setniccfg -m server-<n> -v
  ```

  Gültige Werte für <*n*> sind 1–4.

  Beispiel:

  ```
  racadm setniccfg -m server- 1 -v
  ```

Konfigurieren der iDRAC-VLAN-Tag-Einstellungen mittels der Webschnittstelle

So konfigurieren Sie die VLAN für den Server:

1 Gehen Sie zu einer der folgenden Seiten:
   - Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Netzwerk** > **VLAN**.
   - Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Server-Übersicht** und dann auf **Setup** > **VLAN**.

2 Aktivieren Sie auf der Seite **VLAN Tag Settings** im Abschnitt **iDRAC** VLAN für die Server(s), legen Sie die Priorität fest und geben Sie die ID ein. Weitere Informationen über die Felder finden Sie in der *Online-Hilfe*.

3 Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

Erstes Startlaufwerk einstellen

Sie können das CMC-Startlaufwerk für jeden Server festlegen. Dieses muss nicht unbedingt das erste Startlaufwerk für den Server sein und könnte nicht unbedingt ein Gerät in diesem Server repräsentieren; stattdessen stellt es ein Gerät dar, das vom CMC als erstes Startlaufwerk für diesem Server verwendet wird. Dieses Gerät kann als erstes Startgerät oder als Gerät für einen einmaligen Start festgelegt werden. So können Sie ein spezielles Image starten, um beispielsweise Diagnoseaufgaben durchzuführen oder ein Betriebssystem neu zu installieren.

Sie können das erste Startgerät nur für den nächsten Start oder für alle nachfolgenden Neustarts einstellen. Sie können auch das erste Startgerät für den Server einstellen. Beim nächsten und allen nachfolgenden Neustarts startet das System von dem ausgewählten Gerät, das in der BIOS-Startreihenfolge an erster Stelle bleibt, bis eine erneute Änderung entweder von der CMC-Webschnittstelle (**Gehäuseübersicht** > **Serverübersicht** > **Setup** > **Erstes Startgerät**) oder von der BIOS-Startreihenfolge aus erfolgt.

ANMERKUNG: Die Einstellungen für das erste Startgerät in der CMC-Web-Schnittstelle überschreiben die Starteinstellungen im System-BIOS.

Das von Ihnen angegebene Startlaufwerk muss vorhanden sein und einen startfähigen Datenträger enthalten.

Sie können die folgenden Geräte für ersten Start einstellen.

Tabelle 19. Startlaufwerke

Startlaufwerk	Beschreibung
PXE	Start von einem PXE (Preboot Execution Environment)-Protokoll über die Netzwerkschnittstellenkarte.
Festplattenlaufwerk	Start von der Festplatte auf dem Server.
Lokale CD/DVD	Start von einem CD- oder DVD-Laufwerk auf dem Server.
Virtuelle Diskette	Start vom virtuellen Diskettenlaufwerk. Das Diskettenlaufwerk (oder ein Disketten-Image) befindet sich auf einem anderen Computer im Verwaltungsnetzwerk und ist mit dem Konsolen-Viewer der iDRAC-GUI verbunden.
Virtuelle CD/DVD	Start von einem virtuellen CD- oder DVD-Laufwerk oder CD- oder DVD-ISO-Image. Das optische Laufwerk oder die ISO-Image-Datei befindet sich auf einem anderen Computer oder auf einem anderen Startlaufwerk im Verwaltungsnetzwerk und ist mit dem Konsolen-Viewer der iDRAC-GUI verbunden.
Lokale SD-Karte	Start von der lokalen SD (Secure Digital)-Karte – nur für Server, die iDRAC 6- und iDRAC 7-Systeme unterstützen.
Lokale Diskette	Start von einer Diskette im lokalen Diskettenlaufwerk.
Remote-Dateifreigabe	Start von einem RFS (Remote File Share)-Abbild. Die Abbilddatei wird über den iDRAC-GUI-Konsolen-Viewer angehängt.

Festlegen des ersten Startlaufwerks für mehrere Server über die CMC-Webschnittstelle

ANMERKUNG: Um das erste Startgerät für Server festzulegen, müssen Sie Server Administrator-Berechtigungen oder Gehäusekonfiguration-Administrator-Berechtigungen und iDRAC-Anmeldeberechtigungen haben.

So stellen Sie das erste Startlaufwerk für mehrere Server ein:

1. Klicken Sie im linken Fensterbereich auf **Serverübersicht** > **Setup** > **Erstes Startgerät**. Eine Serverliste wird angezeigt.
2. In der Spalte **Erstes Startgerät** im Drop-Down-Menü des entsprechenden Servers, wählen Sie das zu verwendende Startlaufwerk für einen Server aus.
3. Wenn der Server bei jedem Hochfahren von dem ausgewählten Gerät starten soll, deaktivieren Sie die Option **Einmalig starten** für den betreffenden Server. Wenn der Server beim nächsten Hochfahren einmalig von dem ausgewählten Laufwerk starten soll, aktivieren Sie die Option **Einmalig starten** für den betreffenden Server.
4. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

Festlegen des ersten Startgeräts für individuellen Server mit der CMC-Webschnittstelle

ANMERKUNG: Um das erste Startgerät für Server festzulegen, müssen Sie Server Administrator-Berechtigungen oder Gehäusekonfiguration-Administrator-Berechtigungen und iDRAC-Anmeldeberechtigungen haben.

So stellen Sie das erste Startlaufwerk für einzelne Server ein:

1. Wählen Sie im linken Fensterbereich **Server-Übersicht** aus und klicken Sie dann auf den Server, für den Sie das erste Startgerät einstellen wollen.
2. Wählen Sie **Setup** > **Erstes Startgerät**. Die Seite **Erstes Startgerät** wird angezeigt.
3. Wählen Sie im Dropdown-Menü **Erstes Startgerät** für jeden Server das zu verwendende Startgerät.
4. Wenn der Server bei jedem Hochfahren von dem ausgewählten Gerät starten soll, löschen Sie die Option **Einmaliger Start** für den betreffenden Server. Wenn der Server beim nächsten Hochfahren einmalig von dem ausgewählten Laufwerk starten soll, wählen Sie die Option **Einmalig starten** für den Server.
5. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

Erstes Startgerät über RACADM festlegen

Um das erste Startgerät festzulegen, verwenden Sie das Objekt `cfgServerFirstBootDevice`.

Um den einmaligen Start für ein Gerät einzurichten, verwenden Sie das Objekt `cfgServerBootOnce`.

Weitere Informationen über diese Objekte finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX) unter dell.com/support/manuals.

Server-FlexAddress konfigurieren

Weitere Informationen über die Konfiguration von FlexAddress für Server finden Sie unter Konfigurieren von FlexAddress für Chassis-Level Fabric und Steckplätze unter Verwendung der CMC Web Interface. Um diese Funktion zu verwenden, müssen Sie eine Enterprise-Lizenz aufweisen.

Remote-Dateifreigabe konfigurieren

Die Funktion für die Remote-Dateifreigabe für virtuelle Datenträger ordnet ein Freigabelaufwerk im Netzwerk über den CMC einem oder mehreren Servern zu, um ein Betriebssystem bereitzustellen oder zu aktualisieren. Wenn eine Verbindung besteht, kann auf die Remote-Datei wie auf eine Datei auf dem lokalen Server zugegriffen werden. Zwei Datenträgertypen werden unterstützt: Diskettenlaufwerke und CD/DVD-Laufwerke.

Zur Ausführung eines Remote-Dateifreigabevorgangs (Verbinden, Trennen oder Bereitstellen) müssen Sie über die Berechtigung als **Gehäusekonfiguration-Administrator** oder **Server Administrator** verfügen. Um diese Funktion verwenden zu können, benötigen Sie eine Enterprise-Lizenz.

ANMERKUNG: Wenn Sie CIFS verwenden und Teil einer Active Directory-Domäne sind, dann geben Sie den Domänennamen mit der IP-Adresse im Imagedatei-Pfad ein.

So konfigurieren Sie die Remote-Dateifreigabe:

1. Klicken Sie im linken Fensterbereich auf **Server-Übersicht** > **Setup** > **Remote-Dateifreigabe**.
2. Geben Sie auf der Seite **Remote-Dateifreigabe bereitstellen** die entsprechenden Daten in die Felder ein. Weitere Informationen über die Feldbeschreibungen finden Sie in der *Online-Hilfe*.
3. Klicken Sie auf **Verbinden**, um eine Verbindung zu einer Remote-Dateifreigabe herzustellen. Um eine Verbindung zu einer Remote-Dateifreigabe herzustellen, müssen Sie den Pfad, den Benutzernamen und das Kennwort angeben. Ein erfolgreicher Vorgang erlaubt den Zugriff auf den Datenträger.

   Klicken Sie auf **Trennen**, um eine zuvor verbundene Remote-Dateifreigabe zu trennen.

   Klicken Sie auf **Bereitstellen**, um das Datenträgergerät bereitzustellen.

   ANMERKUNG: Bevor Sie auf die Schalfläche Bereitstellen klicken, stellen Sie sicher, dass alle Arbeitsdateien gespeichert wurden, da diese Maßnahme den Server neu startet.

   Wenn Sie auf **Bereitstellen** klicken, werden die folgendenTasks ausgeführt:
   - Die Remote-Dateifreigabe ist verbunden.
   - Die Datei ist als erstes Startgerät für die Server ausgewählt.
   - Der Server wird neu gestartet.
   - Strom wird an den Server geliefert, falls der Server ausgeschaltet ist.

Konfiguration von Profileinstellungen durch das Replizieren von Serverkonfigurationen

Die Funktion zur Replikation von Serverkonfigurationen ermöglicht es Ihnen, alle Profileinstellungen von einem bestimmten Server auf einen oder mehrere andere Server anzuwenden. Profileinstellungen, die repliziert werden können, sind diejenigen Einstellungen, die geändert werden können und zur Replikation auf andere Server gedacht sind. Die folgenden drei Profilgruppen für Server werden angezeigt und können repliziert werden:

- BIOS – Diese Gruppe enthält nur die BIOS-Einstellungen eines Servers. Diese Profile werden vom CMC für PowerEdge VRTX Version 1.00 und höher erzeugt.
- BIOS und Start – Diese Gruppe enthält die BIOS- und Start-Einstellungen eines Servers. Diese Profile werden vom CMC für PowerEdge VRTX Version 1.00 und höher erzeugt.
- Alle Einstellungen – Diese Version umfasst alle Einstellungen eines Servers und der Komponenten auf diesem Server. Diese Profile werden generiert von
  - CMC für PowerEdge VRTX Version 1.00 und höher
  - Server der 12. Generation mit iDRAC7 1.00.00 oder höher und Lifecycle Controller 2 Version 1.1 oder höher
  - Server der 13. Generation mit iDRAC8 und Lifecycle Controller 2.00.00.00 oder höher

Die Funktion zum Replizieren von Serverkonfigurationen unterstützt iDRAC7-Server und höher. Es werden auch frühere Generationen von RAC-Servern aufgelistet; sie sind auf der Hauptseite jedoch ausgegraut und für die Verwendung mit dieser Funktion nicht aktiviert.

So verwenden Sie die Funktion zum Replizieren von Serverkonfigurationen:

- iDRAC muss in der erforderlichen Mindestversion vorliegen.
- Der Server muss eingeschaltet sein.

Sie können Folgendes durchführen:

- Anzeigen der Profil-Einstellungen eines Servers oder eines gespeicherten Profils.
- Speichern eines Profils eines Servers.
- Anwenden eines Profils auf andere Server.
- Importieren von gespeicherten Profilen von einer Management Station oder Remote-Dateifreigabe.
- Bearbeiten des Profilnamens und der Beschreibung.
- Exportieren von gespeicherten Profilen in eine Management Station oder Remote-Dateifreigabe.
- Löschen von gespeicherten Profilen.
- Ausgewählte Profile mittels der Funktion **Quick Deploy** für Zielgeräte bereitstellen.
- Anzeigen der Protokollaktivität für letzte Server-Profil-Tasks.

Zugriff auf die Seite Serverprofile

Mit der Seite **Serverprofile**, können Sie Serverprofile zu einem oder mehreren Servern hinzufügen, sie verwalten und auf einen oder mehrere Server anwenden.

Um über die CMC-Webschnittstelle auf die Seite **Serverprofile** zuzugreifen, navigieren Sie in dem linken Fensterbereich zu **Gehäuseübersicht** > **Serverübersicht.**Klicken Sie auf**Setup** > **Profile**. Die Seite **Serverprofile** wird angezeigt.

Hinzufügen oder Speichern eines Profils

Bevor Sie die Eigenschaften eines Servers kopieren, übernehmen Sie die Eigenschaften zunächst in ein gespeichertes Profil. Erstellen Sie ein gespeichertes Profil, und versehen Sie dieses mit einem Namen und (optional) mit einer Beschreibung. Sie können auf dem nicht flüchtigen, erweiterten CMC-Speichermedium bis zu 16 gespeicherte Profile abspeichern.

ANMERKUNG: Wenn eine Remote-Freigabe verfügbar ist, können Sie maximal 100 Profile unter Verwendung des erweiterten CMC-Speicher und der Remote-Freigabe speichern. Weitere Informationen über die Remote-Freigabe finden Sie unter Konfigurieren der Netzwerkfreigabe mit der CMC Web-Schnittstelle.

Das Entfernen oder Deaktivieren des nicht flüchtigen, erweiterten Speichermediums verhindert den Zugriff auf das gespeicherte Profil und deaktiviert die Funktion „Server-Konfigurationsreplikation“.

So fügen Sie ein Profil hinzu oder speichern Sie es:

1 Öffnen Sie die Seite **Serverprofile**. Klicken Sie im Abschnitt **Serverprofile** auf **Profile anwenden und speichern**.

2 Wählen Sie den Server aus, dessen Einstellungen Sie zur Generierung des Profils nutzen möchten, und klicken Sie dann auf **Profil speichern**.

Der Abschnitt **Profil speichern** wird angezeigt.

3 Wählen Sie **Extended Storage** oder **Netzwerkfreigabe** als Speicherort für das Profil aus.

ANMERKUNG: Die Option Netzwerkfreigabe ist nur dann aktiviert, und die Einzelheiten werden nur dann im Abschnitt Gespeicherte Profile angezeigt, wenn die Netzwerkfreigabe bereitgestellt und zugreifbar ist. Wenn die Netzwerkfreigabe nicht angeschlossen ist, konfigurieren Sie die Netzwerkfreigabe für das Gehäuse. Klicken Sie zum Konfigurieren der Netzwerkfreigabe im Abschnitt Gespeicherte Profile auf Bearbeiten. Weitere Informationen zum Konfigurieren der Netzwerkfreigabe finden Sie unter Konfigurieren der Netzwerkfreigabe mit der CMC Web-Schnittstelle.

4 Geben Sie in den Feldern **Profilname** und **Beschreibung** den Profilnamen und eine Beschreibung (optional) ein, und klicken Sie auf **Profil speichern**.

ANMERKUNG: Beim Speichern eines Serverprofils wird der erweiterte ASCII-Standardzeichensatz unterstützt, wobei die folgenden Sonderzeichen jedoch nicht unterstützt werden:

), ‘, ., *, >, <, \, /, :, |, #, ?, und ,

Der CMC kommuniziert mit dem LC, um die verfügbaren Serverprofileinstellungen abzurufen und diese als ein Profil mit Namen zu speichern.

Eine Fortschrittsanzeige zeigt an, dass der Speichervorgang durchgeführt wird. Nachdem der Vorgang abgeschlossen wurde, wird die Meldung „Vorgang erfolgreich“ angezeigt.

ANMERKUNG: Der Prozess zur Übernahme der Einstellungen läuft im Hintergrund. Es kann eine gewisse Zeit dauern, bis das neue Profil angezeigt wird. Wird das neue Profil nicht angezeigt, überprüfen Sie das Profilprotokoll auf Fehler.

Profil anwenden

Serverkonfigurationen können nur dann repliziert werden, wenn Serverprofile als gespeicherte Profile im nichtflüchtigen CMC-Speichermedium verfügbar oder auf der Remote-Freigabe gespeichert sind. Um eine Replikation von Serverkonfigurationen zu initiieren, können Sie ein gespeichertes Profil auf einen oder mehrere Server anwenden.

ANMERKUNG: Wenn ein Server Dell Lifecycle Controller nicht unterstützt oder das Gehäuse ausgeschaltet ist, können Sie kein Profil auf den Server anwenden.

So wenden Sie ein Profil auf einen oder mehrere Server an:

1 Rufen Sie die Seite **Serverprofile** auf. Wählen Sie im Abschnitt **Profile speichern und anwenden** den oder die Server aus, auf die Sie das ausgewählte Profil anwenden möchten.

Das Drop-Down-Menü **Profil auswählen** wird aktiviert.

ANMERKUNG: Im Drop-Down-Menü Profil auswählen werden alle verfügbaren Profile nach Typ zu sortiert angezeigt, einschließlich der Profile, die auf der Remote-Freigabe bzw. auf der SD-Karte gespeichert sind.

2 Wählen Sie aus dem Drop-down-Menü **Profil auswählen** das Profil aus, das Sie anwenden möchten.

Die Option **Profil anwenden** wird aktiviert.

3 Klicken Sie auf **Apply Profile** (Profil anwenden).

Eine Meldung wird angezeigt und weist darauf hin, dass die aktuellen Einstellungen durch das Anwenden eines neuen Serverprofils überschrieben und die ausgewählten Server neu gestartet werden. Sie werden dazu aufgefordert, dies zu bestätigen, falls Sie mit dem Vorgang fortfahren möchten.

ANMERKUNG: Um den Klonvorgang für Server durchführen zu können, muss die CSIOR-Option (Collect System Inventory on Restart) für die Server aktiviert sein. Ist die CSIOR-Option deaktiviert, wird eine Warnmeldung mit dem Hinweis angezeigt, dass CSIOR für die Server nicht aktiviert ist. Um den Blade-Klonvorgang abschließen zu können, stellen Sie sicher, dass die CSIOR-Option auf den Servern aktiviert ist.

4 Klicken Sie auf **OK**, um das Profil auf den ausgewählten Server anzuwenden.

Das ausgewählte Profil wird auf den/die Server angewendet, und der/die Server kann/können bei Bedarf sofort neu gestartet werden. Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.

Importieren eines Profils

Sie können ein Serverprofil, das auf einer Management Station gespeichert wurde auf CMC importieren.

So importieren Sie ein gespeichertes Profil von CMC:

1 Klicken Sie auf der Seite **Serverprofile**, im Abschnitt **Gespeicherte Profile** auf **Profil importieren**.

Der Abschnitt **Serverprofil importieren** wird angezeigt.

2 Klicken Sie auf **Durchsuchen**, um auf das Profil an dem erforderlichen Standort zuzugreifen und klicken Sie dann auf **Profil importieren**.

Weitere Informationen zu den Feldern finden Sie in der *Online-Hilfe*.

Exportieren eines Profils

Sie können ein gespeichertes Serverprofil in einen bestimmten Dateiordnerpfad oder auf eine Management Station exportieren.

Zum Exportieren eines gespeicherten Profils:

1 Rufen Sie die Seite **Serverprofile** auf. Wählen Sie im Abschnitt **Gespeicherte Profile** das gewünschte Profil aus, und klicken Sie auf **Kopie des Profils exportieren**.

Eine Meldung zum **Datei-Download** wird angezeigt und Sie werden dazu aufgefordert, die Datei zu öffnen oder zu speichern.

2 Klicken Sie auf **Speichern** oder **Öffnen**, um das Profil auf den erforderlichen Standort zu exportieren.

ANMERKUNG: Wenn das Quellprofil auf der SD-Karte gespeichert ist, wird eine Meldung angezeigt, die darauf hinweist, dass die Beschreibung verloren geht, wenn das Profil exportiert wird. Klicken Sie auf OK, um das Profil zu exportieren.

Sie werden dazu aufgefordert, den Zielspeicherort für die Datei auszuwählen:

- Lokal oder Netzwerkfreigabe, wenn sich die Quelldatei auf einer SD-Karte befindet.

ANMERKUNG: Die Option Netzwerkfreigabe ist nur dann aktiviert, und die Einzelheiten werden nur dann im Abschnitt Gespeicherte Profile angezeigt, wenn die Netzwerkfreigabe bereitgestellt und zugreifbar ist. Wenn die Netzwerkfreigabe nicht angeschlossen ist, konfigurieren Sie die Netzwerkfreigabe für das Gehäuse. Klicken Sie zum Konfigurieren der Netzwerkfreigabe im Abschnitt Gespeicherte Profile auf Bearbeiten. Weitere Informationen finden Sie unter Konfigurieren der Netzwerkfreigabe mit der CMC Web-Schnittstelle.

- Lokal oder SD-Karte, wenn sich die Quelldatei in der Netzwerkfreigabe befindet.

Weitere Informationen zu den Feldern finden Sie in der *Online-Hilfe*.

3 Wählen Sie, basierend auf den angezeigten Optionen, **Lokal**, **Erweiterter Speicher** oder **Netzwerkfreigabe** als Zielspeicherort.

- Wenn Sie **Lokal** auswählen, erscheint ein Dialogfeld und Sie können das Profil in einem lokalen Verzeichnis speichern.
- Wenn Sie **Erweiterter Speicher** oder **Netzwerkfreigabe** auswählen, wird das Dialogfeld **Profil speichern** angezeigt.

4 Klicken Sie auf **Profil speichern**, um das Profil am gewünschten Speicherort zu speichern.

ANMERKUNG: Die CMC Web-Schnittstelle erfasst das normale Server-Konfigurationsprofil (Snapshot des Servers), das für die Replikation auf einem Zielsystem verwendet werden kann. Allerdings werden einige Konfigurationen, wie z. B. RAID- und Identitätsattribute, nicht auf den neuen Server übertragen. Weitere Informationen zu alternativen Exportmodi für RAID-Konfigurationen und Identitätsattributen finden Sie im Whitepaper *Server Cloning with Server Configuration Profiles* (Erstellen von Serverklonen mit Serverkonfigurationsprofilen) unter DellTechCenter.com.

Bearbeiten des Profils

Sie können den Namen und die Beschreibung eines Serverprofils, das auf dem nicht flüchtigen CMC-Datenträger (SD-Karte) gespeichert ist, oder die Namen eines Serverprofils auf der Remote-Freigabe bearbeiten.

So bearbeiten Sie ein gespeichertes Profil:

1 Wählen Sie auf der Seite **Serverprofile** im Abschnitt **Gespeicherte Profile** das gewünschte Profil aus, und klicken Sie dann auf **Profil bearbeiten**.

Der Abschnitt **Serverprofil bearbeiten – <Profilname>** wird angezeigt.

2 Bearbeiten Sie den Profilnamen und die Beschreibung des Serverprofils wie erforderlich, und klicken Sie dann auf **Profil bearbeiten**.

ANMERKUNG: Sie können die Beschreibung des Profils nur für Profile auf SD-Karten bearbeiten.

Weitere Informationen finden Sie in der *Online-Hilfe*.

Löschen eines Profils

Sie können ein Serverprofil löschen, das auf dem nicht flüchtigen CMC-Datenträger (SD-Karte) oder auf der Netzwerkfreigabe gespeichert ist.

So löschen Sie ein gespeichertes Profil:

1 Wählen Sie auf der Seite **Serverprofile** im Abschnitt **Gespeicherte Profile** das gewünschte Profil, und klicken Sie dann auf **Profil löschen**.

Es wird eine Warnmeldung angezeigt, dass der Profillöschvorgang das ausgewählte Profil dauerhaft löschen wird.

2 Klicken Sie auf **OK**, um das ausgewählte Profil zu löschen.

Weitere Informationen finden Sie in der *Online-Hilfe*.

Anzeigen der Profileinstellungen

Um die Profileinstellungen eines ausgewählten Servers anzuzeigen, rufen Sie die Seite **Serverprofile** auf. Klicken Sie im Abschnitt **Serverprofile**, in der Spalte **Serverprofil** des erforderlichen Servers, auf **Anzeigen**. Die Seite **Einstellungen anzeigen** wird angezeigt.

Weitere Informationen zu den angezeigten Einstellungen finden Sie in der *Online-Hilfe*.

ANMERKUNG: Mit der CMC Serverkonfigurations-Replikation werden die korrekten Einstellungen für einen bestimmten Server nur dann abgerufen und angezeigt, wenn die Option Collect System Inventory on Restart (CSIOR) aktiviert ist.

So aktivieren Sie CSIOR auf:

- Server der 12. Generation – Drücken Sie nach dem Neustart des Servers, wenn das Firmenlogo angezeigt wird, die Taste F2. Klicken Sie auf der Seite **iDRAC-Einstellungen** im linken Fensterbereich auf **Lifecycle Controller** und anschließend auf **CSIOR**, um die Änderungen zu übernehmen.
- Server der 13. Generation – Drücken Sie nach dem Neustart des Servers, wenn Sie dazu aufgefordert werden, auf die Taste F10, um auf den Dell Lifecycle-Controller zuzugreifen. Wechseln Sie zur Seite **Hardware-Bestandsliste** , indem Sie auf **Hardware-Konfiguration > Hardware-Bestandsaufnahme** klicken. Auf der Seite **Hardware-Bestandsliste** klicken Sie auf **Systembestandsaufnahme beim Neustart sammeln**.

Gespeicherte Profileinstellungen anzeigen

Zum Anzeigen der Profileinstellungen der gespeicherten Server-Profile gehen Sie zur Seite **Serverprofile**. Klicken Sie im Abschnitt **Gespeicherte Profile** auf **Anzeigen** in der Spalte **Profil anzeigen** des jeweiligen Servers. Die Seite **Einstellungen anzeigen** wird angezeigt. Weitere Informationen über die angezeigten Einstellungen finden Sie in der *Online-Hilfe*.

Profilprotokoll anzeigen

Um sich das Profilprotokoll anzeigen zu lassen, navigieren Sie auf der Seite **Serverprofile** zum Abschnitt **Neu erstelltes Profilprotokoll**. Dieser Abschnitt listet die 10 letzten Profilprotokolleinträge direkt von Serverkonfigurationvorgängen auf. In jedem Profileintrag sind der Schweregrad, Zeit und Datum der Übermittlung des Serverreplikationsvorgangs der Konfiguration und die Beschreibung der Replikationsprotokollmeldung aufgeführt. Die Protokolleinträge sind auch im RAC-Protokoll verfügbar. Um sich weitere verfügbare Einträge anzeigen zu lassen, klicken Sie auf **Zum Profilprotokoll gehen**. Die Seite **Profilprotokoll** wird angezeigt. Weitere Informationen finden Sie in der *Online-Hilfe*.

Fertigstellungsstatus und Fehlerbehebung

So überprüfen Sie den Fertigstellungsstatus für ein angewendetes BIOS-Profil:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Serverübersicht** > **Setup** > **Profile**.

2 Notieren Sie sich auf der Seite **Serverprofile** die Job-ID (JID) des übermittelten Jobs aus dem Abschnitt **Neu erstelltes Profilprotokoll**.

3 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Fehlerbehebung** > **Lifecycle Controller-Jobs**. Suchen Sie die gleiche JID in der Tabelle **Jobs.** Weitere Informationen über die Ausführung von Lifecycle Controller-Jobs finden Sie in Lifecycle Controller-Jobvorgänge.

4 Klicken Sie auf den Link **Protokoll anzeigen**, um die Ergebnisse von *Lclogview* vom iDRAC-Lifecycle Controller für den spezifischen Server anzuzeigen.

   Die für den Abschluss oder den Fehler angezeigten Ergebnisse sind vergleichbar mit den im iDRAC-Lifecycle Controller-Protokoll für den spezifischen Server angezeigten Informationen.

Quick Deploy von Profilen

Mit der Quick Deploy-Funktion können Sie gespeicherte Profile einem Serversteckplatz zuweisen. Jeder Server, der die Replikation der Serverkonfiguration unterstützt und in einen Steckplatz eingesetzt wird, wird mit dem zugewiesenen Profil dieses Steckplatzes konfiguriert. Sie können die Quick Deploy-Aktion nur ausführen, wenn die Option **Aktion, wenn der Server eingesetzt wird** auf der Seite **iDRAC bereitstellen** auf **Serverprofil** oder **Quick Deploy und Serverprofil** eingestellt ist. Wenn Sie diese Option auswählen, kann das zugewiesene Serverprofil angewandt werden, wenn ein neuer Server in das Gehäuse eingesetzt wird. Um zur Seite **iDRAC bereitstellen** zu gelangen, wählen Sie **Server-Übersicht** > **Setup** > **iDRAC** aus. Profile, die bereitgestellt werden können, sind auf der SD-Karte oder einer Remote-Freigabe gespeichert. Um die Profile für Quick Deploy einstellen zu können, müssen Sie über die Rechte eines **Gehäuse-Administrators** verfügen.

ANMERKUNG:

Zuweisen von Serverprofilen zu Steckplätzen

Über die Seite **Serverprofile** können Sie Serverprofile Steckplätzen zuweisen. So weisen Sie ein Profil einem Gehäusesteckplatz zu:

1 Klicken Sie auf der Seite **Serverprofile** auf **Profile für QuickDeploy.**

   Die aktuellen Zuweisungen der Profile zu den Steckplätzen, die in der Auswahlliste in der Spalte **Profile zuweisen** aufgeführt sind, werden angezeigt.

   ANMERKUNG: Sie können die Quick Deploy-Maßnahme nur dann ausführen, wenn die Option Maßnahme beim Einfügen des Servers auf der Seite iDRAC bereitstellen auf Server-Profil oder Quick Deploy, dann Server-Profil eingestellt ist. Durch die Auswahl dieser Option kann das zugewiesene Server-Profil angewendet werden, sobald ein neuer Server in das Gehäuse eingefügt wird.

2 Wählen Sie aus dem Drop-Down-Menü das Profil aus, das dem erforderlichen Steckplatz zugewiesen werden soll. Sie können ein ausgewähltes Profil auf mehrere Steckplätze anwenden.

3 Klicken Sie auf **Profil zuweisen**.

   Das Profil wird den ausgewählten Steckplätzen zugewiesen.

ANMERKUNG:

- Ein Steckplatz, dem kein Serverprofil zugewiesen wurde, wird durch den Zusatz „Kein Profil ausgewählt“ gekennzeichnet, der in der Auswahlliste erscheint.
- Wählen Sie zum Entfernen der Profilzuweisung von einem oder mehreren Steckplätzen die entsprechenden Steckplätze aus, und klicken Sie dann auf **Zuweisung entfernen**. Es wird eine Meldung mit dem Hinweis angezeigt, dass durch das Entfernen eines Profils von einem oder mehreren Steckplätzen die Konfigurationseinstellungen des Profils von allen in den Steckplätzen eingefügten Servern entfernt werden, wenn die Funktion **Quick Deploy-Profile** aktiviert ist. Klicken Sie auf **OK**, um die Profilzuweisungen zu löschen.
- Um alle Profilzuweisungen eines Steckplatzes zu entfernen, wählen Sie im Drop-Down-Menü **Kein Profil ausgewählt.**

ANMERKUNG: Wenn ein Profil mit der Funktion Quick Deploy-Profile für einen Server bereitgestellt wird, werden die Fortschritte und Ergebnisse der Anwendung im Profilprotokoll festgehalten.

ANMERKUNG:

- Wenn sich ein zugewiesenes Profil auf der Netzwerkfreigabe befindet und diese nicht zugreifbar ist, wenn ein Server in den Steckplatz eingefügt wird, wird auf der LCD-Anzeige eine Meldung angezeigt, dass das zugewiesene Profil für Steckplatz <X> nicht verfügbar ist.
- Die Option **Netzwerkfreigabe** ist nur dann aktiviert, und die Einzelheiten werden nur dann im Abschnitt **Gespeicherte Profile** angezeigt, wenn die Netzwerkfreigabe bereitgestellt und zugreifbar ist. Wenn die Netzwerkfreigabe nicht angeschlossen ist, konfigurieren Sie die Netzwerkfreigabe für das Gehäuse. Klicken Sie zum Konfigurieren der Netzwerkfreigabe im Abschnitt **Gespeicherte Profile** auf **Bearbeiten**. Weitere Informationen finden Sie unter Konfigurieren der Netzwerkfreigabe mit der CMC Web-Schnittstelle.

Startidentitätsprofile

Um auf die Seite **Startkonfigurationsprofile** der CMC Web-Schnittstelle zuzugreifen, wechseln Sie in der Systemstruktur zu **Gehäuseübersicht** > **Serverübersicht**. Klicken Sie auf **Setup** > **Profile**. Die Seite **Serverprofile** wird angezeigt. Klicken Sie auf der Seite **Serverprofile** auf **Startidentitätsprofile**.

Die Startidentitätsprofile enthalten die NIC- oder FC-Einstellungen, die zum Starten eines Servers über ein SAN-Zielgerät sowie für die eindeutige virtuelle MAC-Adresse und den WWN erforderlich sind. Da diese Einstellungen über eine CIFS- oder NFS-Freigabe für mehrere Gehäuse zur Verfügung stehen, können Sie die Identität eines nicht funktionsfähigen Servers eines Gehäuses ohne großen Aufwand per Remote-Zugriff auf einen Ersatzserver im selben oder in einem anderen Gehäuse verschieben. Dieser kann dann mit dem Betriebssystem und den Anwendungen des ausgefallenen Servers gestartet werden. Der Hauptvorteil dieser Funktion ist die Verwendung eines eindeutigen virtuellen MAC-Adresspools, auf den alle Gehäuse gemeinsam zugreifen können.

Diese Funktion ermöglicht Ihnen die Online-Verwaltung von Servervorgängen ohne physischen Eingriff, falls der Server ausfallen sollte. Mithilfe der Funktion „Startidentitätsprofile“ können Sie die folgenden Aufgaben durchführen:

- Erstmaliges Setup
  - Erstellen Sie einen Bereich virtueller MAC-Adressen. Zum Erstellen einer MAC-Adresse benötigen Sie Berechtigungen vom Typ Gehäusekonfiguration-Administrator und Server-Administrator.
  - Speichern Sie Vorlagen für Startidentitätsprofile, und passen Sie die Startidentitätsprofile auf der Netzwerkfreigabe durch Bearbeiten und Einfügen der SAN-Startparameter an, die von den einzelnen Servern verwendet werden.
  - Bereiten Sie die Server, die die Erstkonfiguration verwenden vor, bevor Sie die zugehörigen Startidentitätsprofile anwenden.
  - Anwenden der Startidentitäten auf die einzelnen Server und Starten der Server über SAN
- Konfigurieren eines oder mehrerer Ersatz-Standby-Server für die schnelle Wiederherstellung
  - Vorbereiten der Standby-Server, die die Erstkonfiguration verwenden, bevor die zugehörigen Startidentitätsprofile angewendet werden

- Transferieren Sie die Arbeitslast eines ausgefallenen Servers auf einen neuen Server, indem Sie die folgenden Aufgaben ausführen:
  - Löschen Sie die Startidentität des nicht funktionierenden Servers, um eine potenzielle Duplizierung der MAC-Adressen zu vermeiden, für den Fall, dass der Server wiederhergestellt werden kann.
  - Wenden Sie die Startidentität des ausgefallenen Servers auf einen Ersatz-Standby-Server an.
  - Starten Sie den Server mit den neuen Einstellungen für die Startidentität, um die Arbeitslast schnell wiederherzustellen.

Speichern von Startidentitätsprofilen

Sie können Startidentitätsprofile auf der CMC-Netzwerkfreigabe speichern. Die Anzahl der speicherbaren Profile hängt von der Verfügbarkeit der MAC-Adressen ab. Weitere Informationen finden Sie unter *Konfigurieren der Netzwerkfreigabe unter Verwendung der CMC Web-Schnittstelle*.

Bei Emulex Fibre Channel (FC)-Karten ist das Attribut **Über SAN starten aktivieren/deaktivieren** in der Option ROM standardmäßig deaktiviert. Aktivieren Sie das Attribut in der Option ROM, und wenden Sie das Startidentitätsprofil auf den Server an, der über SAN startet.

So speichern Sie ein Profil:

1 Rufen Sie die Seite **Serverprofile** auf. Wählen Sie im Abschnitt **Startidentitätsprofile** den Server aus, der über die erforderlichen Einstellungen verfügt, die Sie zum Generieren des Profils verwenden möchten, und wählen Sie die FQDD aus dem Drop-down-Menü **FQDD** aus.

2 Klicken Sie auf **Identität speichern**. Der Abschnitt **Identität speichern** wird angezeigt.

> **ANMERKUNG: Die Startidentität wird nur gespeichert, wenn die Option Netzwerkfreigabe aktiviert und zugreifbar ist. Die Details werden im Abschnitt Gespeicherte Profile angezeigt. Wenn die Netzwerkfreigabe nicht verbunden ist, konfigurieren Sie die Netzwerkfreigabe für das Gehäuse. Klicken Sie dazu im Abschnitt Gespeicherte Profile auf Bearbeiten. Weitere Informationen finden unter *Konfigurieren der Netzwerkfreigabe unter Verwendung der CMC Web-Schnittstelle*.**

3 Geben Sie in die Felder **Basisprofilname** und **Anzahl der Profile** den Profilnamen und die Anzahl der zu speichernden Profile ein.

> **ANMERKUNG: Beim Speichern eines Startidentitätsprofils wird der erweiterte Standard-ASCII-Zeichensatz unterstützt. Die folgenden Sonderzeichen werden jedoch nicht unterstützt:**
>
>), “, ., *, >, <, \, /, :, |, #, ?, und ,

4 Wählen Sie eine MAC-Adresse für das Basisprofil aus dem Drop-down-Menü **Virtuelle MAC-Adresse** aus, und klicken Sie auf **Profil speichern**.

Die Anzahl der erstellten Vorlagen basiert auf der Anzahl der Profile, die Sie angegeben haben. Der CMC kommuniziert mit dem Lifecycle Controller, um die verfügbaren Serverprofileinstellungen abzurufen und diese als namentliches Profil zu speichern. Das Format für die Namensdatei lautet <base profile name>_<profile number>_<MAC address>. Beispiel: FC630_01_0E0000000000.

Eine Fortschrittsanzeige zeigt an, dass der Speichervorgang durchgeführt wird. Nachdem der Vorgang abgeschlossen wurde, wird die Meldung **Vorgang erfolgreich** angezeigt.

> **ANMERKUNG: Der Prozess zur Übernahme der Einstellungen findet im Hintergrund statt. Es kann eine gewisse Zeit dauern, bis das neue Profil angezeigt wird. Wird das neue Profil nicht angezeigt, überprüfen Sie das Profilprotokoll auf etwaige Fehler.**

Anwenden von Startidentitätsprofilen

Sie können Startidentitätsprofil-Einstellungen anwenden, wenn die Startidentitätsprofile als gespeicherte Profile auf der Netzwerkfreigabe verfügbar sind. Um die Konfiguration der Startidentitäten zu initiieren, können Sie ein gespeichertes Profil auf einen einzelnen Server anwenden.

ANMERKUNG: Wenn ein Server Lifecycle Controller nicht unterstützt oder das Gehäuse ausgeschaltet ist, können Sie kein Profil auf den Server anwenden.

So wenden Sie ein Profil auf einen Server an:

1 Gehen Sie zur Seite **Server Profiles** (Serverprofile). Wählen Sie im Abschnitt **Boot Identity profiles** (Startidentitätsprofile) den Server aus, auf den Sie das ausgewählte Profil anwenden möchten.

Das Drop-down-Menü **Profil auswählen** wird aktiviert.

ANMERKUNG: Im Drop-down-Menü Profil auswählen werden alle auf der Netzwerkfreigabe verfügbaren Profile nach Typ sortiert angezeigt.

2 Wählen Sie aus dem Drop-down-Menü **Profil auswählen** das Profil aus, das Sie anwenden möchten.

Die Option **Identität anwenden** wird aktiviert.

3 Klicken Sie auf **Identität anwenden**.

Es wird eine Warnmeldung angezeigt, dass das Anwenden einer neuen Identität die aktuellen Einstellungen überschreibt und darüber hinaus den ausgewählten Server neu startet. Sie werden dazu aufgefordert, dies zu bestätigen, falls Sie mit dem Vorgang fortfahren möchten.

ANMERKUNG: Um Vorgänge zur Replikation der Serverkonfiguration auf dem Server durchzuführen, muss die CSIOR-Option für die Server aktiviert sein. Wenn die CSIOR-Option deaktiviert ist, wird eine Warnmeldung angezeigt, dass CSIOR für den Server nicht aktiviert ist. Um den Vorgang zur Replikation der Serverkonfiguration abzuschließen, aktivieren Sie die CSIOR-Option auf dem Server.

4 Klicken Sie auf **OK**, um das Startidentitätsprofil auf den ausgewählten Server anzuwenden.

Das ausgewählte Profil wird auf den Server angewendet und der Server wird sofort neu gestartet. Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.

ANMERKUNG: Sie können ein Startidentitätsprofil jeweils nur auf eine NIC-FQDD-Partition auf einem Server anwenden. Um das gleiche Startidentitätsprofil auf eine NIC-FQDD-Partition auf einem anderen Server anzuwenden, müssen Sie es von dem Server löschen, auf den es zuerst angewendet wurde.

Löschen von Startidentitätsprofilen

Bevor Sie ein neues Startidentitätsprofil auf einen Standby-Server anwenden, können Sie die vorhandenen Startidentitätskonfigurationen eines ausgewählten Servers löschen, indem Sie die Option **Identität löschen** verwenden, die in der CMC Web-Schnittstelle verfügbar ist.

So löschen Sie Startidentitätsprofile:

1 Rufen Sie die Seite **Serverprofile** auf. Wählen Sie im Abschnitt **Startidentitätsprofile** den Server aus, auf dem Sie das Startidentitätsprofil löschen möchten.

ANMERKUNG: Diese Option ist nur dann aktiviert, wenn ein Server ausgewählt wurde und Startidentitätsprofile auf dem ausgewählten Server angewendet wurden.

2 Klicken Sie auf **Identität löschen**.

3 Klicken Sie auf **OK**, um das Startidentitätsprofil auf dem ausgewählten Server zu löschen.

Der Löschvorgang deaktiviert die E/A-Identität und die Persistenzrichtlinie des Servers. Nach Abschluss des Löschvorgangs wird der Server ausgeschaltet.

Anzeigen gespeicherter Startidentitätsprofile

Rufen Sie zum Anzeigen der auf der Netzwerkfreigabe gespeicherten Startidentitätsprofile die Seite **Serverprofile** auf. Wählen Sie im Abschnitt **Startidentitätsprofile** > **Gespeicherte Profile** das Profil aus, und klicken Sie in der Spalte **Profil anzeigen** auf **Anzeigen**. Die Seite **Einstellungen anzeigen** wird angezeigt. Weitere Informationen über die angezeigten Einstellungen finden Sie in der *CMC-Online-Hilfe*.

Importieren von Startidentitätsprofilen

Sie können Startidentitätsprofile, die auf der Management Station gespeichert sind, in die Netzwerkfreigabe importieren.

Gehen Sie folgendermaßen vor, um ein gespeichertes Profil von der Management Station in die Netzwerkfreigabe zu importieren:

1 Rufen Sie die Seite **Serverprofile** auf. Klicken Sie im Abschnitt **Startidentitätsprofile** > **Gespeicherte Profile** auf **Profil importieren**.

Der Abschnitt **Profil importieren** wird angezeigt.

2 Klicken Sie auf **Durchsuchen**, um auf das Profil an dem erforderlichen Standort zuzugreifen und klicken Sie dann auf **Profil importieren**.

Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.

Exportieren von Startidentitätsprofilen

Sie können auf einer Netzwerkfreigabe gespeicherte Startidentitätsprofile an einem festgelegten Pfad auf einer Management Station exportieren.

So exportieren Sie ein gespeichertes Profil:

1 Rufen Sie die Seite **Serverprofile** auf. Wählen Sie im Abschnitt **Startidentitätsprofile** > **Gespeicherte Profile** das gewünschte Profil aus, und klicken Sie auf **Profil exportieren**.

Eine Meldung zum **Datei-Download** wird angezeigt und Sie werden dazu aufgefordert, die Datei zu öffnen oder zu speichern.

2 Klicken Sie auf **Speichern** oder **Öffnen**, um das Profil auf den erforderlichen Standort zu exportieren.

Löschen von Startidentitätsprofilen

Sie können ein Startidentitätsprofil löschen, das auf der Netzwerkfreigabe gespeichert ist.

So löschen Sie ein gespeichertes Profil:

1 Rufen Sie die Seite **Serverprofile** auf. Wählen Sie im Abschnitt **Startidentitätsprofile** > **Gespeicherte Profile** das gewünschte Profil aus, und klicken Sie auf **Profil löschen**.

Es wird eine Warnmeldung mit dem Inhalt angezeigt, dass das ausgewählte Profil durch den Profillöschvorgang dauerhaft gelöscht wird.

2 Klicken Sie auf **OK**, um das ausgewählte Profil zu löschen.

Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.

Verwalten des virtuellen MAC-Adresspools

Mithilfe der Option **Virtuellen MAC-Adresspool verwalten** können Sie MAC-Adressen erstellen, hinzufügen, entfernen und deaktivieren. Sie können Unicast-MAC-Adressen im virtuellen MAC-Adresspool verwenden. Die folgenden MAC-Adressbereiche sind im CMC zulässig:

- 02:00:00:00:00:00 - F2:FF:FF:FF:FF:FF
- 06:00:00:00:00:00 - F6:FF:FF:FF:FF:FF
- 0A:00:00:00:00:00 - FA:FF:FF:FF:FF:FF
- 0E:00:00:00:00:00 - FE:FF:FF:FF:FF:FF

Um die Option **Virtuelle MAC-Adresse verwalten** über die CMC Web-Schnittstelle anzuzeigen, wechseln Sie in der Strukturansicht zu **Gehäuseübersicht** > **Serverübersicht**. Klicken Sie auf **Setup** > **Profile** > **Startidentitätsprofile**. Der Abschnitt **Virtuellen MAC-Adresspool verwalten** wird angezeigt.

ANMERKUNG: Die virtuellen MAC-Adressen werden in der Datei vmacdb.xml auf der Netzwerkfreigabe verwaltet. Eine ausgeblendete Sperrdatei (.vmacdb.lock) wird zur Netzwerkfreigabe hinzugefügt und entfernt, um Startidentitätsvorgänge von mehreren Gehäusen zu serialisieren.

Erstellen eines MAC-Pools

Sie können einen MAC-Pool im Netzwerk erstellen, indem Sie die Option **Virtuellen MAC-Adresspool verwalten** verwenden, die in der CMC Web-Schnittstelle verfügbar ist.

ANMERKUNG: Der Abschnitt MAC-Pool erstellen wird nur angezeigt, wenn die MAC-Adressdatenbank (vmacdb.xml) nicht auf der Netzwerkfreigabe verfügbar ist. In dem Fall sind die Optionen MAC-Adresse hinzufügen und MAC-Adresse entfernen deaktiviert.

So erstellen Sie einen MAC-Pool:

1 Rufen Sie die Seite **Serverprofile** auf. Geben Sie im Abschnitt **Startidentitätsprofile** > **Virtuellen MAC-Adresspool verwalten** die
2 erste MAC-Adresse des MAC-Adresspools in das Feld **Erste MAC-Adresse** ein.
3 Geben Sie die Anzahl der MAC-Adressen in das Feld **Anzahl der MAC-Adressen** ein.
4 Klicken Sie auf **MAC-Pool erstellen**, um den MAC-Adresspool zu erstellen.

Nachdem die Datenbank auf der Netzwerkfreigabe erstellt wurde, werden bei **Virtuellen MAC-Adresspool verwalten** die Liste und der Status der MAC-Adressen angezeigt, die auf der Netzwerkfreigabe gespeichert sind. In diesem Abschnitt können Sie jetzt MAC-Adressen hinzufügen oder aus dem MAC-Adresspool entfernen.

Hinzufügen von MAC-Adressen

Sie können einen MAC-Adressbereich zur Netzwerkfreigabe hinzufügen, indem Sie die Option **MAC-Adressen hinzufügen** verwenden, die in der CMC Web-Schnittstelle verfügbar ist.

ANMERKUNG: Sie können keine MAC-Adresse hinzufügen, die bereits im MAC-Adresspool vorhanden ist. Es wird eine Fehlermeldung angezeigt, die darauf hinweist, dass die MAC-Adresse, deren Hinzufügung versucht wurde, bereits im Pool vorhanden ist.

So fügen Sie MAC-Adressen zur Netzwerkfreigabe hinzu:

1 Rufen Sie die Seite **Serverprofile** auf. Klicken Sie im Abschnitt **Startidentitätsprofile** > **Virtuellen MAC-Adresspool verwalten** auf **MAC-Adressen hinzufügen**.
2 erste MAC-Adresse des MAC-Adresspools in das Feld **Erste MAC-Adresse** ein.
3 Geben Sie die Anzahl der hinzuzufügenden MAC-Adressen in das Feld **Anzahl der MAC-Adressen** ein.

Die gültigen Werte liegen zwischen 1 und 3000.

4 Klicken Sie auf **OK**, um die MAC-Adressen hinzuzufügen.

Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.

Weitere Informationen finden Sie in der Online-Hilfe zu *CMC für Dell PowerEdge FX2/FX2s*.

Entfernen von MAC-Adressen

Sie können einen MAC-Adressbereich aus der Netzwerkfreigabe entfernen, indem Sie die Option **MAC-Adressen entfernen** verwenden, die in der CMC Web-Schnittstelle verfügbar ist.

ANMERKUNG: MAC-Adressen können nicht entfernt werden, wenn sie auf dem Knoten aktiv sind oder einem Profil zugeordnet sind.

So entfernen Sie MAC-Adressen von der Netzwerkfreigabe:

1 Rufen Sie die Seite **Serverprofile** auf. Klicken Sie im Abschnitt **Startidentitätsprofile** > **Virtuellen MAC-Adresspool verwalten** auf **MAC-Adressen entfernen**.
2 Geben Sie die erste MAC-Adresse des MAC-Adresspools in das Feld **Erste MAC-Adresse** ein.
3 Geben Sie die Anzahl der zu entfernenden MAC-Adressen in das Feld **Anzahl der MAC-Adressen** ein.
4 Klicken Sie auf **OK**, um die MAC-Adressen zu entfernen.

Deaktivieren von MAC-Adressen

Sie können aktive MAC-Adressen deaktivieren, indem Sie die Option **MAC-Adresse(n) deaktivieren** verwenden, die in der CMC Web-Schnittstelle verfügbar ist.

ANMERKUNG: Verwenden Sie die Option MAC-Adresse(n) deaktivieren nur dann, wenn der Server nicht auf den Befehl Identität löschen reagiert, oder wenn die MAC-Adresse von keinem der Server verwendet wird.

So entfernen Sie MAC-Adressen von der Netzwerkfreigabe:

1 Rufen Sie die Seite **Serverprofile** auf. Wählen Sie im Abschnitt **Startidentitätsprofile** > **Virtuellen MAC-Adresspool verwalten** die MAC-Adresse(n) aus, die Sie deaktivieren möchten.
2 Klicken Sie auf **MAC-Adresse(n) deaktivieren**.

iDRAC mit einfacher Anmeldung starten

Der CMC ermöglicht nur eine begrenzte Verwaltung von individuellen Gehäusekomponenten, wie etwa von Servern. Zur kompletten Verwaltung dieser individuellen Komponenten liefert der CMC einen Ausgangspunkt für die webbasierte Schnittstelle des Management-Controllers (iDRAC) eines Servers.

Ein Benutzer kann die iDRAC-Webschnittstelle eventuell starten, ohne sich ein zweites Mal anmelden zu müssen, da diese Funktion die einfache Anmeldung verwendet. Richtlinien zur einfachen Anmeldung werden im Folgenden beschrieben:

- Ein CMC-Benutzer mit Serveradministratorberechtigung wird über die einfache Anmeldung automatisch bei iDRAC angemeldet. Sobald dieser Benutzer sich auf der iDRAC-Website befindet, erhält er automatisch Administratorrechte. Dies gilt sogar dann, wenn dieser Benutzer kein Konto auf iDRAC besitzt oder wenn das Konto nicht über Administratorrechte verfügt.
- Ein CMC-Benutzer, der **NICHT** über die Serveradministratorberechtigung verfügt, aber dasselbe Konto auf iDRAC besitzt, wird über die einfache Anmeldung automatisch bei iDRAC angemeldet. Sobald dieser Benutzer sich auf der iDRAC-Website befindet, erhält er automatisch die Berechtigungen, die für das iDRAC-Konto erstellt wurden.
- Ein CMC-Benutzer, der nicht über die Serveradministratorberechtigung verfügt oder nicht dasselbe Konto auf dem iDRAC besitzt, wird über die einfache Anmeldung nicht automatisch bei iDRAC angemeldet. Dieser Benutzer wird bei einem Klick auf **iDRAC-GUI starten** zur iDRAC-Anmeldungsseite geleitet.

ANMERKUNG: Der Begriff „dasselbe Konto“ bedeutet in diesem Zusammenhang, dass der Benutzer für CMC und für iDRAC denselben Anmeldenamen mit einem übereinstimmenden Kennwort besitzt. Der Benutzer, der denselben Anmeldenamen ohne ein übereinstimmendes Kennwort hat, wird als Benutzer mit demselben Konto betrachtet.

ANMERKUNG: Benutzer werden eventuell aufgefordert, sich bei iDRAC anzumelden (siehe den dritten Aufzählungspunkt unter den Richtlinien zur einfachen Anmeldung).

ANMERKUNG: Wenn iDRAC-Netzwerk-LAN deaktiviert ist (LAN aktiviert = Nein), ist einfache Anmeldung nicht verfügbar.

Wenn Sie auf **iDRAC-GUI starten** klicken, wird möglicherweise eine Fehlerseite angezeigt, wenn Folgendes zutrifft:

- Der Server wurde aus dem Gehäuse entfernt.
- Die iDRAC-IP-Adresse wurde geändert.
- Es tritt ein Problem mit der iDRAC-Netzwerkverbindung auf.

Wenn die iDRAC-Webschnittstelle beim MCM auf einem Mitgliedsgehäuse aufgerufen wird, müssen die Benutzeranmeldeinformationen von Führungs- und Mitgliedsgehäuse identisch sein. Andernfalls wird die aktuelle Sitzung des Mitgliedsgehäuses abgebrochen, und die Anmeldeseite des Mitgliedsgehäuses wird angezeigt.

iDRAC von der Seite Serverstatus starten

So starten Sie die iDRAC-Verwaltungskonsole für einen individuellen Server:

1 Erweitern Sie im linken Fensterbereich **Server-Übersicht**. Es werden alle vier Server in der erweiterten Liste **Server-Übersicht** angezeigt.
2 Klicken Sie auf den Server, für den Sie die iDRAC-Webschnittstelle starten möchten.
3 Klicken Sie auf der Seite **Serverstatus** auf **iDRAC starten**.
Die iDRAC-Webschnittstelle wird angezeigt. Informationen über die Feldbeschreibungen finden Sie in der *Online-Hilfe*.

iDRAC über die Seite Serverstatus starten

Start der iDRAC-Verwaltungskonsole von der Seite **Server-Status** aus:

1 Klicken Sie im linken Fensterbereich auf **Server-Übersicht**.
2 Klicken Sie auf der Seite **Servers-Status** auf **iDRAC starten** für den Server, für den Sie die iDRAC-Webschnittstelle starten wollen.

Starten der Remote-Konsole

Sie können eine Keyboard-Video-Mouse (KVM)-Sitzung direkt auf dem Server starten. Die Remote-Konsolen-Funktion wird nur unterstützt, wenn alle folgenden Bedingungen erfüllt sind:

- Der Gehäusestrom ist eingeschaltet.
- Server, die iDRAC7 und iDRAC8 unterstützen.
- Die LAN-Schnittstelle auf dem Server ist aktiviert.
- Auf dem Host-System ist JRE 6 Aktualisierung 16 (Java Runtime Environment) oder höher installiert.
- Der Browser auf dem Host-System lässt Popup-Fenster zu (Popup-Blocker ist deaktiviert).

Die Remote-Konsole kann auch von der iDRAC-Webschnittstelle gestartet werden. Weitere Informationen finden Sie im *iDRAC User's Guide* (iDRAC-Benutzerhandbuch) unter dell.com/support/manuals.

Remote-Konsole von der Seite Gehäusefunktionszustand starten

So starten Sie eine Remote-Konsole von der CMC-Webschnittstelle:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** und dann auf **Eigenschaften**.
2 Klicken Sie auf der Seite **Gehäusefunktionszustand** auf den angegebenen Server in der Gehäuse-Grafik.
3 Klicken Sie im Abschnitt **Quicklinks** auf den Link **Remote-Konsole**, um die Remote-Konsole zu starten.

Remote-Konsole von der Seite „Status der Server“ starten

So starten Sie eine Remote-Konsole für einen individuellen Server:

1 Erweitern Sie im linken Fensterbereich **Serverübersicht**. Alle vier Server werden in der erweiterten Liste der Server angezeigt.
2 Klicken Sie auf den Server, für den Sie die Remote-Konsole starten wollen.
3 Klicken sie auf der Seite **Serverstatus** auf **Remote-Konsole starten**.

Remote-Konsole von der Seite Status der Server starten

So starten Sie eine Remote-Konsole von der Seite **Status der Server**:

1 Wählen Sie im linken Fensterbereich **Server-Übersicht** aus und klicken Sie auf **Eigenschaften** > **Status**. Die Seite **Serverstatus** wird angezeigt.

2 Klicken Sie für den erforderlichen Server auf **Remote-Konsole starten**.

8

CMC für das Versenden von Warnungen konfigurieren

Sie können Warnungen und Aktionen für bestimmte Ereignisse festlegen, die auf dem Gehäuse eintreten. Ein Ereignis wird erzeugt, wenn ein Gerät oder der Status eines Dienstes geändert wurde oder ein Fehlerzustand festgestellt wird. Wenn ein Ereignis mit einem Ereignis-Filter übereinstimmt und Sie diesen Filter für die Generierung einer Warnnachricht (E-Mail-Warnung oder SNMP-Trap) konfiguriert haben, wird eine Warnung an mindestens ein konfiguriertes Ziel gesendet, z. B. an eine E-Mail-Adresse, eine IP-Adresse oder einen externen Server.

So konfigurieren Sie CMC zum Versenden von Warnungen:

1 Aktivieren Sie die Option **Gehäuseereigniswarnungen**.
2 Optional können Sie die Warnungen auf der Basis der Kategorie oder des Schweregrads filtern.
3 Konfigurieren Sie die Einstellungen für die E-Mail-Warnung oder die SNMP-Trap-Einstellungen.
4 Aktivieren Sie die Gehäuseereigniswarnungen, um eine E-Mail-Warnung oder SNMP-Traps an konfigurierte Ziele zu senden.

Themen:

Warnungen aktivieren und deaktivieren

Um Warnungen an konfigurierte Ziele zu senden, müssen Sie die globale Warnungsoption aktivieren. Diese Eigenschaft überschreibt die individuellen Warnungseinstellungen.

Stellen Sie sicher, dass die SNMP- oder E-Mail-Warnungsziele konfiguriert werden, um Warnungen empfangen zu können.

Warnungen über die CMC-Web-Schnittstelle aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie die Generierung von Warnungen:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Warnungen**.
2 Wählen Sie auf der Seite **Gehäuseereignisse**, im Abschnitt **Aktivierung der Gehäusewarnung,** die Option **Gehäuseereigniswarnungen aktivieren** aus, um die Aktivierung der Warnung zu aktivieren oder das Löschen der Warnung zu aktivieren.
3 Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

Warnungen filtern

Sie können Warnungen auf der Basis der Kategorie und des Schweregrads filtern.

Warnungen über die CMC-Web-Schnittstelle filtern

So filtern Sie Warnungen auf der Basis der Kategorie und des Schweregrads:

ANMERKUNG: Um Konfigurationsänderungen der Gehäuseereignisse anzuwenden, müssen Sie die Berechtigung zur Warnungskonfiguration besitzen.

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Warnungen**.

2 Wählen Sie auf der Seite **Gehäuseereignisse**, im Abschnitt **Warnungsfilter,** eine oder mehrere der folgenden Kategorien aus:

- **Systemzustand**
- **Bei Lagerung**
- **Konfiguration**
- **Audit**
- **Updates**

3 Wählen Sie eine oder mehrere der folgenden Schweregrade aus:

- **Kritisch**
- **Warnung**
- **Informativ**

Der Abschnitt **Überwachte Warnungen** zeigt die Ergebnisse auf der Basis der ausgewählten Kategorie und des Schweregrads an. Weitere Informationen über die Feldbeschreibungen auf dieser Seite finden Sie in der *Online-Hilfe*.

4 Klicken Sie auf **Anwenden**.

Ereigniswarnungen über RACADM einrichten

Zur Einrichtung einer Ereigniswarnung verwenden Sie den Befehl `eventfilters`. Weitere Informationen finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX) unter **dell.com/support//manuals**.

Konfiguration von Warnungszielen

Die Management Station verwendet Simple Network Management Protocol (SNMP), um Daten vom CMC zu erhalten.

Sie können die IPv4- und IPv6-Warnungsziele, die E-Mail-Einstellungen und die SMTP-Server-Einstellungen konfigurieren und diese Einstellungen testen.

Stellen Sie vor der Konfiguration der Einstellungen für E-Mail-Warnungen oder SNMP-Trap sicher, dass Sie über die Berechtigung Gehäusekonfigurations-Administrator verfügen.

SNMP-Trap-Warnungsziele konfigurieren

Sie können die IPv6- oder IPv4-Adressen für den Empfang von SNMP-Traps konfigurieren.

SNMP-Trap-Warnungsziele über die CMC-Webschnittstelle konfigurieren

So konfigurieren Sie IPv4- oder IPv6-Warnzieleinstellungen über die CMC-Webschnittstelle:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Warnungen** > **Trap-Einstellungen**.

2 Geben Sie auf der Seite **Warnungsziele bei Gehäuseereignissen** Folgendes ein:

- Geben Sie im Feld **Ziel** eine gültige IP-Adresse ein. Verwenden Sie das 4-Punkt-IPv4-Format, die Standard-IPv6-Adressnotation oder FQDN. Beispiel: **123.123.123.123** oder **2001:db8:85a3::8a2e:370:7334** oder **dell.com**.

  Wählen Sie ein Format, das mit der Netzwerk-Technologie/Infrastruktur in Einklang steht. Die Testtrap-Funktionalität kann keine inkorrekten Einstellungen aufgrund der aktuellen Netzwerkkonfiguration erkennen (z. B. die Verwendung eines IPv6-Ziels in einer reinen IPv4-Umgebung).
- Geben Sie im Feld **Community-Zeichenkette** einen gültigen Community-Namen ein, zu der die Ziel-Management Station gehört.

  Diese Community-Zeichenkette unterscheidet sich von der Community-Zeichenkette auf der Seite **Gehäuseübersicht** > **Netzwerk** > **Dienste**. Die Community-Zeichenkette der SNMP-Traps ist die Community, die der CMC für ausgehende Traps zu Management Stationen verwendet. Die Community-Zeichenkette auf der Seite **Gehäuseübersicht** > **Netzwerk** > **Dienste** ist die Community-Zeichenkette, die von Management Stationen zur Abfrage des SNMP-Daemon auf dem CMC verwendet wird.
- Wählen Sie unter **Aktiviert** die Option der entsprechenden Ziel-IP aus, um die IP-Adresse zum Empfangen der Traps zu aktivieren. Sie können bis zu vier IP-Adressen festlegen.

3 Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

4 Um zu überprüfen, ob die IP-Adressen die SNMP-Traps empfangen, klicken Sie auf **Senden** in der Spalte **SNMP Trap testen**.

Die IP-Warnziele sind damit konfiguriert.

SNMP-Trap-Warnungsziele über RACADM konfigurieren

So konfigurieren Sie IP-Warnungsziel über RACADM:

1 Öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC und melden Sie sich an.

ANMERKUNG: Es kann nur eine Filtermaske für SNMP- und E-Mail-Warnungen festgelegt werden. Wenn Sie bereits eine Filtermaske ausgewählt haben, überspringen Sie Task 2 und gehen Sie zu Schritt 3.

2 Aktivieren Sie die Erstellung von Warnungen:

```
racadm config -g cfgAlerting -o cfgAlertingEnable 1
```

3 Geben Sie die Ereignisfilter durch Ausführung des Befehls `racadm eventfilters set` an.

a Um alle verfügbaren Einstellungen zu löschen, führen Sie den folgenden Befehl aus: `racadm eventfilters set -c cmc.alert.all -n none`

b Konfigurieren Sie die Verwendung des Schweregrads als Parameter. Wenn zum Beispiel allen informativen Ereignisse in der Speicherkategorie das Ausschalten als Maßnahme und E-Mail und SNMP als Benachrichtigungen zugewiesen sind: `racadm eventfilters set -c cmc.alert.storage.info -n email,snmp`

c Konfigurieren Sie die Verwendung der Unterkategorie als Parameter. Wenn zum Beispiel allen Konfigurationen in der Unterkategorie Lizenzierung in der Kategorie Audit das Ausschalten als Maßnahme zugewiesen ist, und alle Benachrichtigungen aktiviert sind: `racadm eventfilters set -c cmc.alert.audit.lic -n all`

d Konfigurieren Sie die Verwendung der Unterkategorie und des Schweregrads als Parameter.Wenn zum Beispiel allen Informationsereignissen in der Unterkategorie Lizenzierung in der Kategorie Audit das Ausschalten als Maßnahme zugewiesen ist, und alle Benachrichtigungen deaktiviert sind: `racadm eventfilters set -c cmc.alert.audit.lic.info -n none`

4 Trap-Warnungen aktivieren:

```
racadm config -g cfgTraps -o cfgTrapsEnable 1 -i <Index>
```

wobei `<index>` ein Wert von 1 - 4 ist. Die Indexnummer wird vom CMC verwendet, um bis zu vier konfigurierbare Ziele für Trap-Warnungen zu unterscheiden. Geben Sie Trap-Ziele als korrekt formatierte numerische Adressen (IPv6 oder IPv4) oder vollqualifizierte Domänennamen (FQDNs) an.

5 Bestimmen Sie eine Ziel-IP-Adresse, um Trap-Warnungen zu erhalten:

```
racadm config -g cfgTraps -o cfgTrapsAlertDestIPAddr <IP-Adresse> -i <Index>
```

wobei `<IP address>` ein gültiges Ziel ist und `<index>` der Indexwert, der in Schritt 4 angegeben wurde.

6 Geben Sie den Community-Namen an:

```
racadm config -g cfgTraps -o cfgTrapsCommunityName <Community-Name> -i <Index>
```

wobei `<community name>` die SNMP-Community ist, zu der das Gehäuse gehört, und `<index>` der Indexwert, der Sie in Schritt 4 und 5 angegeben wurde.

Sie können bis zu vier Ziele für den Empfang von Trap-Warnungen konfigurieren. Um weitere Ziele hinzuzufügen, wiederholen Sie die Tasks in den Schritten 2 bis 6.

ANMERKUNG: Die Befehle in Schritten 2 bis 6 überschreiben alle vorhandenen Einstellungen, die für den angegebenen Index konfiguriert wurden (1-4). Um festzustellen, ob ein Index über zuvor konfigurierte Werte verfügt, geben Sie Folgendes ein: `racadm get config -g cfgTraps -i <index>`. Wenn der Index konfiguriert ist, werden für die Objekte cfgTrapsAlertDestIPAddr und cfgTrapsCommunityName Werte angezeigt.

7 So testen Sie ein Ereignis-Trap für ein Warnungsziel. Geben Sie Folgendes ein:

```
racadm testtrap -i <Index>
```

wobei `<index>` ein Wert von 1-4 ist und das Warnungsziel darstellt, das Sie testen möchten.

Wenn Sie sich über die Indexnummer nicht sicher sind, führen Sie den folgenden Befehl aus:

```
racadm getconfig -g cfgTraps -i <Index>
```

Konfigurieren von E-Mail-Benachrichtigungen

Wenn der CMC ein Gehäuseereignis ermittelt, wie z. B. eine Umgebungswarnung oder einen Komponentenfehler, kann er so konfiguriert werden, dass eine E-Mail-Warnung an eine oder mehrere E-Mail-Adressen gesendet wird.

Konfigurieren Sie den SMTP-E-Mail-Server so, dass von der CMC-IP-Adresse weitergeleitete E-Mails angenommen werden können; eine Funktion, die bei den meisten Mail-Servern aus Sicherheitsgründen normalerweise deaktiviert ist. Anleitungen für eine sichere Konfiguration finden Sie in der mit dem SMTP-Server mitgelieferten Dokumentation.

ANMERKUNG: Wenn Ihr Mail-Server Microsoft Exchange Server 2007 ist, ist sicherzustellen, dass der iDRAC-Domänenname so konfiguriert ist, dass der Mail-Server die E-Mail-Warnungen des iDRAC empfängt.

ANMERKUNG: E-Mail-Warnungen unterstützen sowohl IPv4- als auch IPv6-Adressen. Der DRAC DNS-Domänenname muss beim Nutzen von IPv6 festgelegt werden.

Wenn Ihr Netzwerk über einen SMTP-Server verfügt, der periodisch IP-Adressen ausgibt und erneuert, und die Adressen unterschiedlich sind, ergibt sich eine Zeitspanne, während der diese Einstellung der Eigenschaften aufgrund einer Änderung in der festgelegten SMTP-Server-IP-Adresse nicht funktioniert. Verwenden Sie in solchen Fällen den DNS-Namen.

E-Mail-Warnungseinstellungen über CMC-Webschnittstelle konfigurieren

So konfigurieren Sie die E-Mail-Warnungseinstellungen über die Web-Schnittstelle:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Warnungen** > **E-Mail-Warnungseinstellungen**.

2 Geben Sie die SMTP-E-Mail-Servereinstellungen und die E-Mail-Adressen an, um die Warnungen zu erhalten. Weitere Informationen über die Feldbeschreibungen finden Sie in der *Online Hilfe*.

3 Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

4 Klicken Sie auf **Senden** unter **Test-E-Mail**, um eine Test-E-Mail an ein angegebenes E-Mail-Warnungsziel zu senden.

E-Mail-Warnungseinstellungen mit RACADM konfigurieren

Um eine Test-E-Mail an ein E-Mail-Warnungsziel unter Verwendung von RACADM zu senden, gehen Sie wie folgt vor:

1 Öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC und melden Sie sich an.

2 Aktivieren Sie die Erstellung von Warnungen:

```
racadm config -g cfgAlerting -o cfgAlertingEnable 1
```

ANMERKUNG: Es kann nur eine Filtermaske für SNMP- und E-Mail-Warnungen festgelegt werden. Überspringen Sie Schritt 3, wenn Sie bereits eine Filtermaske festgelegt haben.

3 Geben Sie die Ereignisse an, für die Warnungen erstellt werden müssen:

```
racadm config -g cfgAlerting -o cfgAlertingFilterMask <mask value>
```

wobei `<mask value>` ein hexadezimaler Wert zwischen 0x0 and 0xffffffff ist und mit den vorangestellten Zeichen 0x ausgedrückt werden muss. Die Tabelle Filtermasken für Ereignis-Traps liefert die Filtermasken für jeden Ereignistyp. Eine Anleitung zum Berechnen des Hexadezimalwerts für die Filtermaske, die Sie aktivieren möchten, finden Sie in Schritt 3 in Konfigurieren von SNMP-Trap-Zielen über RACADM.

4 So aktivieren Sie die Erstellung von E-Mail-Warnungen:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable 1 -i <Index>
```

wobei `<index>` ein Wert von 1 - 4 ist. Die Indexnummer wird vom CMC verwendet, um bis zu vier konfigurierbare Ziel-E-Mail-Adressen zu unterscheiden.

5 So geben Sie die Ziel-E-Mail-Adresse zum Erhalt von E-Mail-Warnungen an:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertAddress <email address> -i <index>
```

wobei `<email address>` eine gültige E-Mail-Adresse ist und `<index>` der Indexwert, den Sie in Schritt 4 angegeben haben.

6 Geben Sie den Namen des Teilnehmers an, der E-Mail-Warnungen empfangen soll:

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEmailName <email name> -i <index>
```

wobei `<email name>` (<E-Mail-Name>) der Name der Person oder Gruppe ist, die E-Mail-Warnungen empfängt, und `<Index>` der Indexwert ist, den Sie in Schritt 4 und 5 angegeben haben. Der E-Mail-Name darf bis zu 32 alphanumerische Zeichen, Bindestriche, Unterstriche und Punkte enthalten. Leerstellen sind nicht gültig.

7 Einrichten des SMTP-Hosts:

```
racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr host.domain
```

Dabei ist `host.domain` die FQDN.

Sie können bis zu vier Ziel-E-Mail-Adressen für den Empfang von E-Mail-Warnungen konfigurieren. Um weitere E-Mail-Adressen hinzuzufügen, führen Sie die Tasks in Schritt 2 bis 6 aus.

ANMERKUNG: Die Befehle in den Schritten 2 bis 6 überschreiben alle vorhandenen Einstellungen, die Sie für den angegebenen Index konfiguriert haben (1-4). Um festzustellen, ob ein Index über zuvor konfigurierte Werte verfügt, geben Sie Folgendes ein: `racadm get config -g cfgEmailAlert -i <index>`. Wenn der Index konfiguriert ist, werden für die Objekte cfgEmailAlertAddress und cfgEmailAlertEmailName Werte angezeigt.

Weitere Informationen finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX) unter **dell.com/support/manuals**.

9

Benutzerkonten und Berechtigungen konfigurieren

Sie können Benutzerkonten mit spezifischen (rollenbasierten) Berechtigungen einrichten, um Ihr System über CMC zu verwalten und um die Systemsicherheit zu gewährleisten. Standardmäßig ist CMC mit einem lokalen Administratorkonto konfiguriert. Der Standardbenutzername lautet `root`, und das Kennwort lautet `calvin`. Als Administrator können Sie Benutzerkonten einrichten, damit andere Benutzer auf CMC zugreifen können.

Sie können maximal 16 lokale Benutzer einrichten oder Verzeichnisdienste benutzen, wie z. B. Microsoft Active Directory oder LDAP, um weitere Benutzerkonten einzurichten. Durch die Verwendung eines Verzeichnisdienstes verfügen Sie über einen zentralen Standort für die Verwaltung berechtigter Benutzerkonten.

CMC unterstützt den rollenbasierten Zugriff auf Benutzer mit einem Satz aus zugewiesenen Berechtigungen. Die folgenden Rollen sind verfügbar: Administrator, Operator, Schreibgeschützt oder Kein/e/r. Die Rolle definiert den Umfang der zugewiesenen Berechtigungen.

Themen:

Typen von Benutzern

Es gibt zwei Typen von Benutzern:

- CMC-Benutzer oder Gehäuse-Benutzer
- iDRAC-Benutzer oder Server-Benutzer (da iDRAC auf einem Server resident ist)

CMC- und iDrac-Benutzer können lokale Benutzer oder Verzeichnisdienstbenutzer sein.

Mit Ausnahme des Falls, dass der CMC-Benutzer über die Berechtigung **Serveradministrator** verfügt, werden die einem CMC-Benutzer gewährten Berechtigungen nicht automatisch auf denselben Benutzer auf einem Server übertragen, da Serverbenutzer unabhängig von CMC-Benutzern erstellt werden. Anders gesagt befinden sich Active Directory-CMC-Benutzer und Active Directory-iDRAC-Benutzer in zwei unterschiedlichen Zweigen der Active Directory-Struktur. Um einen lokalen Serverbenutzer zu erstellen, muss sich der Administrator für Benutzerkonfiguration direkt am Server anmelden. Der Administrator für Benutzerkonfiguration kann auf dem CMC keinen Serverbenutzer und auf einem Server keinen CMC-Benutzer erstellen. Diese Regel schützt die Sicherheit und Integrität der Server.

Tabelle 20. Benutzertypen

Berechtigung	Beschreibung
CMC-Anmeldung, Benutzer	Der Benutzer kann sich am CMC anmelden und alle CMC-Daten anzeigen. Er kann aber keine Daten hinzufügen oder ändern oder Befehle ausführen.

Berechtigung	Beschreibung
	Ein Benutzer kann andere Berechtigungen ohne CMC-Anmeldebenutzerberechtigung besitzt. Diese Funktion ist sinnvoll, wenn sich ein Benutzer vorübergehend nicht anmelden darf. Wenn die CMC-Anmeldebenutzerberechtigung dieses Benutzers wiederhergestellt ist, erhält der Benutzer alle zuvor gewährten Berechtigungen zurück.
Gehäusekonfiguration-Administrator	Benutzer können Daten hinzufügen oder ändern, die: • das Gehäuse identifizieren, z. B. den Gehäusenamen und die Gehäuseposition. • dem Gehäuse speziell zugewiesen sind, z. B. der IP-Modus (statisch oder DHCP), statische IP-Adresse, statischer Gateway und statische Subnetzmaske. • Dienste für das Gehäuse bereitstellen, z. B. Datum und Uhrzeit, Firmware-Aktualisierung und CMC-Reset. • dem Gehäuse zugeordnet sind, z. B. der Name des Steckplatzes und die Steckplatzpriorität. Obwohl diese Eigenschaften für die Server gelten, handelt es sich bei ihnen ausschließlich um Gehäuseeigenschaften, die sich auf die Steckplätze und nicht auf die Server selbst beziehen. Aus diesem Grund können Steckplatznamen und Steckplatzprioritäten hinzugefügt oder geändert werden, unabhängig davon, ob sich Server in den Steckplätzen befinden oder nicht. Wenn ein Server in ein anderes Gehäuse eingesetzt wird, übernimmt der den Namen und die Priorität, welche dem jeweiligen Steckplatz in dem neuen Gehäuse zugewiesen wurden. Der vorherige Steckplatzname sowie die vorherige Steckplatzpriorität verbleiben bei dem vorhergehenden Gehäuse. **ANMERKUNG: CMC-Benutzer mit der Berechtigung Gehäusekonfigurations-Administrator können die Energieeinstellungen konfigurieren. Es ist jedoch die Berechtigung Gehäusesteuerungs-Administrator erforderlich, um Gehäusestromvorgänge einschließlich Einschalten, Ausschalten sowie Aus- und Einschalten durchzuführen.**
Benutzerkonfigurations-Administrator	Ein Benutzer kann: • Einen neuen Benutzer hinzufügen. • Das Kennwort eines Benutzers ändern. • Die Berechtigungen eines Benutzers ändern. • Die Anmeldungsberechtigung eines Benutzers unter Beibehaltung des Namens des Benutzers und anderer Berechtigungen in der Datenbank aktivieren oder deaktivieren.
Administrator zum Löschen von Protokollen	Ein Benutzer kann das Hardwareprotokoll und das CMC-Protokoll löschen.
Gehäusesteuerungs-Administrator (Strombefehle)	CMC-Benutzer mit der Berechtigung **Gehäusestrom-Administrator** können alle Vorgänge im Zusammenhang mit der Energieversorgung durchführen. Sie können Gehäusestromvorgänge einschließlich Einschalten, Ausschalten sowie Aus- und Einschalten steuern. **ANMERKUNG: Für die Konfiguration von Stromversorgungseinstellungen ist eine Berechtigung als Administrator für die Gehäusekonfiguration erforderlich.**
Server Administrator	Die Server-Administrator-Berechtigung ist eine Pauschalberechtigung, die einem CMC-Benutzer alle Rechte zum Ausführen beliebiger Vorgänge auf beliebigen, im Gehäuse vorhandenen Servern gewährt. Wenn ein Benutzer mit der Berechtigung **Serveradministrator** eine Aktion ausgibt, die auf einem Server ausgeführt werden soll, sendet die CMC-Firmware den Befehl zum Zielserver, ohne die Berechtigungen des Benutzers auf dem Server zu überprüfen. Mit anderen Worten: Die Berechtigung **Serveradministrator** überschreibt alle fehlenden Administratorrechte auf dem Server. Ohne die **Server Administrator**-Berechtigung kann ein auf dem Gehäuse erstellter Benutzer nur dann einen Befehl auf einem Server ausführen, wenn alle folgenden Bedingungen erfüllt werden: • Derselbe Benutzername ist auf dem Server vorhanden. • Derselbe Benutzername muss auf dem Server das identische Kennwort besitzen. • Der Benutzer muss die Berechtigung zum Ausführen des Befehls aufweisen. Wenn ein CMC-Benutzer, der nicht über die Berechtigung **Serveradministrator** verfügt, eine Aktion ausgibt, die auf einem Server ausgeführt werden soll, sendet der CMC einen Befehl mit dem Anmeldenamen und

Berechtigung	Beschreibung
	Kennwort des Benutzers an den Zielserver. Wenn der Benutzer auf dem Server nicht vorhanden ist oder das Kennwort nicht übereinstimmt, wird dem Benutzer das Ausführen der Aktion verweigert. Wenn der Benutzer auf dem Zielserver vorhanden ist und das Kennwort übereinstimmt, antwortet der Server mit den Berechtigungen, die dem Benutzer auf dem Server gewährt wurden. Basierend auf den Berechtigungen, mit denen der Server antwortet, entscheidet die CMC-Firmware, ob der Benutzer zum Ausführen der Maßnahme berechtigt ist. Im Folgenden werden die Berechtigungen und Aktionen auf dem Server aufgeführt, auf die der Serveradministrator Anspruch hat. Diese Rechte werden nur angewendet, wenn der Benutzer keine Serveradministrationsberechtigung in dem Gehäuse hat. Serverkonfiguration-Administrator: · IP-Adresse einstellen · Gateway einstellen · Subnetzmaske einstellen · Erstes Startgerät einstellen Benutzer konfigurieren: · iDRAC-Stammkennwort einstellen · iDRAC-Reset Serversteuerung-Administrator: · Einschalten · Ausschalten · Aus- und einschalten · Ordentliches Herunterfahren · Serverneustart
Warnungstests für Benutzer	Benutzer kann Testwarnungsmeldungen senden.
Administrator für Debug-Befehle	Benutzer kann Systemdiagnosebefehle ausführen.
Struktur A-Administrator	Benutzer kann die Struktur A-EAM festlegen und konfigurieren.
Struktur B-Administrator	Benutzer kann die Struktur B festlegen und konfigurieren, die der ersten Zusatzkarte in den Servern entspricht und mit dem Schaltkreis der Struktur B im gemeinsamen PCIe-Untersystem in der Hauptplatine verbunden ist.
Struktur C-Administrator	Benutzer kann die Struktur C festlegen und konfigurieren, die der zweiten Zusatzkarte in den Servern entspricht und mit dem Schaltkreis der Struktur C im gemeinsamen PCIe-Untersystem in der Hauptplatine verbunden ist.

Die CMC-Benutzergruppen bieten eine Reihe von Benutzergruppen, die voreingestellte Benutzerrechte haben.

ANMERKUNG: Wenn Sie Administrator, Hauptbenutzer oder Gastbenutzer auswählen und dann eine Berechtigung aus dem vordefinierten Satz hinzufügen oder daraus entfernen, wird die CMC-Gruppe automatisch zu Benutzerdefiniert geändert.

Tabelle 21. CMC-Gruppenberechtigungen

Benutzergruppe	Gewährte Berechtigungen
Administrator	· CMC-Anmeldung, Benutzer · Gehäusekonfiguration-Administrator · Benutzerkonfigurations-Administrator · Administrator zum Löschen von Protokollen

Benutzergruppe	Gewährte Berechtigungen
	• Server Administrator • Warnungstests für Benutzer • Administrator für Debug-Befehle • Struktur A-Administrator
Hauptbenutzer	• Anmelden • Administrator zum Löschen von Protokollen • Gehäusesteuerungs-Administrator (Strombefehle) • Server Administrator • Warnungstests für Benutzer • Struktur A-Administrator
Gastbenutzer	Anmelden
Custom (Benutzerdefiniert)	Wählen Sie eine beliebige Kombination der folgenden Berechtigungen aus: • CMC-Anmeldung, Benutzer • Gehäusekonfiguration-Administrator • Benutzerkonfigurations-Administrator • Administrator zum Löschen von Protokollen • Gehäusesteuerungs-Administrator (Strombefehle) • Server Administrator • Warnungstests für Benutzer • Administrator für Debug-Befehle • Struktur A-Administrator
Keine	Keine zugewiesenen Berechtigungen

Tabelle 22. Vergleich der Berechtigungen zwischen CMC-Administrator, Hauptbenutzer und Gastbenutzer

Berechtigungssatz	Administratorrechte	Hauptbenutzer-Berechtigungen	Gastbenutzer-Berechtigungen
CMC-Anmeldung, Benutzer	Ja	Ja	Ja
Gehäusekonfiguration-Administrator	Ja	Nein	Nein
Benutzerkonfigurations-Administrator	Ja	Nein	Nein
Administrator zum Löschen von Protokollen	Ja	Ja	Nein
Gehäusesteuerungs-Administrator (Strombefehle)	Ja	Ja	Nein
Server Administrator	Ja	Ja	Nein
Warnungstests für Benutzer	Ja	Ja	Nein
Administrator für Debug-Befehle	Ja	Nein	Nein
Struktur A-Administrator	Ja	Ja	Nein

Ändern der Einstellungen für Stammbenutzer-Administratorkonto

Zum Zweck der zusätzlichen Sicherheit wird dringend empfohlen, das Standardkennwort des Stammkontos (Benutzer 1) zu ändern. Das Stammkonto ist das Standard-Administrationskonto, das mit einem CMC geliefert wird.

So ändern Sie das Standardkennwort für das Stammkonto:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** und dann auf **Benutzerauthentifizierung**.
2 Klicken Sie auf der Seite **Benutzer,** in der Spalte **Benutzer-ID** auf **1**.

ANMERKUNG: Die Benutzer-ID 1 ist das Stammbenutzerkonto, das standardmäßig mit CMC geliefert wird. Dies kann nicht geändert werden.

3 Wählen Sie auf der Seite **Benutzerkonfiguration** die Option **Kennwort ändern** aus.
4 Geben Sie das neue Kennwort in das Feld **Kennwort** ein und geben Sie dann dasselbe Kennwort in **Kennwort bestätigen** ein.
5 Klicken Sie auf **Anwenden**. Das Kennwort für Benutzer-ID**1** wurde geändert.

Lokale Benutzer konfigurieren

Sie können in CMC bis zu 16 lokale Benutzer mit spezifischen Zugriffsberechtigungen konfigurieren. Bevor Sie einen CMC-Benutzer erstellen, müssen Sie überprüfen, ob etwaige aktuelle Benutzer vorhanden sind. Sie können Benutzernamen, Kennwörter und Rollen mit den Berechtigungen für diese Benutzer definieren. Die Benutzernamen und Kennwörter können über sichere CMC-Schnittstellen geändert werden (z. B. über die Web-Schnittstelle, RACADM oder WS-MAN).

Lokale Benutzer unter Verwendung der CMC-Webschnittstelle konfigurieren

ANMERKUNG: Sie müssen die Berechtigung Benutzer konfigurieren besitzen, um einen CMC-Benutzer zu erstellen.

So fügen Sie lokale CMC-Benutzer hinzu und konfigurieren sie:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht**, und dann auf **Benutzerauthentifizierung**.
2 Klicken Sie auf der Seite **Lokale Benutzer** in der Spalte **Benutzer-ID** auf eine Benutzer-ID-Nummer. Die Seite **Benutzerkonfiguration** wird angezeigt.

ANMERKUNG: Benutzer-ID 1 ist das Stammbenutzerkonto, das standardmäßig mit einem CMC geliefert wird. Das lässt sich nicht ändern.

3 Aktivieren Sie die Benutzer-ID, legen Sie den Benutzernamen und das Kennwort fest, und greifen Sie dann auf die Berechtigungen für den Benutzer zu. Weitere Informationen zu diesen Optionen finden Sie in der *Online-Hilfe*.
4 Klicken Sie auf **Anwenden**. Der Benutzer wird mit den erforderlichen Berechtigungen erstellt.

Lokale Benutzer über RACADM konfigurieren

ANMERKUNG: Sie müssen als Benutzer `root` angemeldet sein, um RACADM-Befehle auf einem Remote-Linux-System ausführen zu können.

Sie können bis zu 16 Benutzer in der CMC-Eigenschaftsdatenbank konfigurieren. Bevor Sie einen CMC-Benutzer manuell aktivieren, prüfen Sie, ob aktuelle Benutzer vorhanden sind.

Wenn Sie einen neuen CMC konfigurieren oder den Befehl racadm `racresetcfg` verwendet haben, ist der einzige aktuelle Benutzer `root` mit dem Kennwort `calvin`. Der `racresetcfg` Unterbefehl setzt alle Konfigurationsparameter auf die Standardeinstellungen zurück. Alle vorherigen Änderungen gehen verloren.

ANMERKUNG: Benutzer können zu einem beliebigen Zeitpunkt aktiviert und deaktiviert werden, wobei die Deaktivierung eines Benutzers diesen nicht aus der Datenbank löscht.

Um zu überprüfen, ob ein Benutzer existiert, öffnen Sie eine Telnet/SSH-Textkonsole auf dem CMC, melden Sie sich an und geben Sie dann den folgenden Befehl einmal für jeden Index von 1–16 ein:

```
racadm getconfig -g cfgUserAdmin -i <index>
```

ANMERKUNG: Sie können auch `racadm getconfig -f <myfile.cfg>` eingeben, und die Datei myfile.cfg, in der alle CMC-Konfigurationsparameter enthalten sind, anzeigen oder bearbeiten.

Mehrere Parameter und Objekt-IDs werden mit ihren aktuellen Werten angezeigt. Zwei Objekte von Bedeutung sind:

```
# cfgUserAdminIndex=XX
cfgUserAdminUserName=
```

Wenn das Objekt `cfgUserAdminUserName` keinen Wert besitzt, steht diese Indexnummer, die durch das Objekt `cfgUserAdminIndex` angezeigt wird, zur Verfügung. Wenn hinter dem "=" ein Name steht, wird dieser Index von diesem Benutzernamen verwendet.

Wenn Sie einen Benutzer mit dem Unterbefehl racadm `config` manuell aktivieren oder deaktivieren, muss der Index mit der Option `-i` angegeben werden.

Das Zeichen „#“ in den Befehlsobjekten gibt an, dass es ein Nur-Lesen-Objekt ist. Ebenso: Wenn der Befehl `racadm config -f racadm.cfg` zur Angabe einer beliebigen Anzahl von zu schreibenden Gruppen/Objekten verwendet wird, kann der Index nicht angegeben werden. Ein neuer Benutzer wird zum ersten verfügbaren Index hinzugefügt. Dieses Verhalten bietet größere Flexibilität bei der Konfiguration eines zweiten CMC mit denselben Einstellungen wie der Haupt-CMC.

CMC-Benutzer über RACADM hinzufügen

So fügen Sie der CMC-Konfiguration einen neuen Benutzer zu:

1 Legen Sie den Benutzernamen fest.
2 Legen Sie das Kennwort fest.
3 Legen Sie die Benutzerberechtigungen fest. Weitere Information über Benutzerberechtigungen finden Sie unter Typen von Benutzern.
4 Aktivieren Sie den Benutzer.

Beispiel:

Im folgenden Beispiel wird beschrieben, wie man einen neuen Benutzer namens "John" mit dem Kennwort "123456" und Anmeldeberechtigungen zum CMC hinzufügt.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName
-i 2
john
racadm config -g cfgUserAdmin -o cfgUserAdminPassword
-i 2
123456
racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminPrivilege
0x00000001
racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminEnable 1
```

ANMERKUNG: Eine Liste gültiger Bit-Maskenwerte für spezifische Benutzerberechtigungen ist im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX) enthalten. Der Standard-Berechtigungswert ist 0, was darauf hinweist, dass der Benutzer über keine aktivierten Berechtigungen verfügt.

Um zu überprüfen, ob der Benutzer mit den richtigen Berechtigungen erfolgreich hinzugefügt wurde, führen Sie einen der folgenden Befehle aus:

```
racadm getconfig -g cfgUserAdmin -i 2
```

Weitere Informationen zu RACADM-Befehlen finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX), verfügbar unter **dell.com/support/manuals**.

Einen CMC-Benutzer deaktivieren

Bei der Verwendung von RACADM müssen Benutzer manuell und individuell deaktiviert werden. Benutzer können nicht über eine Konfigurationsdatei gelöscht werden.

Für das Löschen eines CMC-Benutzers lautet die Syntax wie folgt:

```
racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i <index>"" racadm config -g
cfgUserAdmin -i 2 -o cfgUserAdminPrivilege 0x0
```

Eine Null-Kette doppelter Anführungszeichen ("") weist den CMC an, die Benutzerkonfiguration am angegebenen Index zu entfernen und dann auf die Werkseinstellungswerte zurückzusetzen.

CMC-Benutzer mit Berechtigungen aktivieren

Um einen Benutzer mit spezifischen administrativen Berechtigungen (rollenbasierte Autorität) zu aktivieren:

1 Machen Sie zuerst einen verfügbaren Benutzer-Index mithilfe der Befehlssyntax ausfindig:

```
racadm getconfig -g cfgUserAdmin -i <Index>
```

2 Geben Sie die folgenden Befehle mit dem neuen Benutzernamen und dem neuen Kennwort ein.

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <Index> <Benutzerberechtigungs-
Bitmaskenwert>
```

ANMERKUNG: Eine Liste gültiger Bit-Maskenwerte für spezifische Benutzerberechtigungen ist im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX) enthalten, das unter dell.com/support/manuals. verfügbar ist. Der Standard-Berechtigungswert ist 0, was darauf hinweist, dass der Benutzer über keine aktivierten Berechtigungen verfügt.

Konfigurieren von Active Directory-Benutzern

Wenn Ihre Firma die Microsoft Active Directory-Software verwendet, kann die Software so konfiguriert werden, dass sie Zugriff auf CMC bietet. Sie können dann bestehenden Benutzern im Verzeichnisdienst CMC-Benutzerberechtigungen erteilen und diese steuern. Das ist eine lizenzierte Funktion.

ANMERKUNG: Auf den folgenden Betriebssystemen können Sie die Benutzer der CMC-Benutzer unter Verwendung des Active Directory erkennen.

- Microsoft Windows 2000
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008

Sie können die Benutzerauthentifizierung über Active Directory konfigurieren, um sich am CMC anzumelden. Rollenbasierte Autorität kann bereitgestellt werden, die es einem Administrator ermöglicht, spezifische Berechtigungen für jeden Benutzer zu konfigurieren.

Unterstützte Active Directory-Authentifizierungsmechanismen

Sie können mit Active Directory den Benutzerzugriff auf CMC mittels zweier Methoden definieren:

- Die *Standardschemalösung*, die nur Microsoft-Standard-Active Directory-Gruppenobjekte verwendet.

- Lösung *Erweitertes Schema*, die über benutzerdefinierte Active Directory-Objekte verfügt. Alle Zugriffssteuerungsobjekte werden im Active Directory verwahrt. Bei der Konfiguration des Benutzerzugangs auf verschiedenen CMCs mit unterschiedlichen Ebenen der Benutzerberechtigung besteht maximale Flexibilität.

Übersicht des Standardschema-Active Directory

Wie in der folgenden Abbildung dargestellt, erfordert die Verwendung des Standardschemas für die Active Directory-Integration die Konfiguration unter Active Directory und unter CMC.

In Active Directory wird ein Standardgruppenobjekt als Rollengruppe verwendet. Ein Benutzer, der Zugang zum CMC hat, ist ein Mitglied der Rollengruppe. Um diesem Benutzer Zugriff auf einen bestimmten CMC zu gewähren, muss der Rollengruppenname und dessen Domänenname auf der jeweiligen CMC Karte konfiguriert werden. Die Rolle und die Berechtigungsebene wird auf jeder CMC Karte und nicht im Active Directory definiert. Sie können bis zu fünf Rollengruppen für jeden CMC konfigurieren. Tabellen-Referenznummer zeigt die Standard-Rollengruppen-Berechtigungen.

Tabelle 23. Standardeinstellungsberechtigungen der Rollengruppe

Rollengruppe	Standard-Berechtigungsebene	Gewährte Berechtigungen	Bitmaske
1	Keine	• CMC-Anmeldung, Benutzer • Gehäusekonfiguration-Administrator • Benutzerkonfigurations-Administrator • Administrator zum Löschen von Protokollen • Gehäusesteuerungs-Administrator (Strombefehle) • Server Administrator • Warnungstests für Benutzer • Administrator für Debug-Befehle • Struktur A-Administrator	0x00000fff
2	Keine	• CMC-Anmeldung, Benutzer • Administrator zum Löschen von Protokollen • Gehäusesteuerungs-Administrator (Strombefehle) • Server Administrator • Warnungstests für Benutzer • Struktur A-Administrator	0x00000ed9
3	Keine	CMC-Anmeldung, Benutzer	0x00000001
4	Keine	Keine zugewiesenen Berechtigungen	0x00000000
5	Keine	Keine zugewiesenen Berechtigungen	0x00000000

ANMERKUNG: Die Bitmasken-Werte werden nur verwendet, wenn das Standardschema mit RACADM eingerichtet wird.

ANMERKUNG: Weitere Informationen über Benutzerberechtigungen finden Sie unter Typen von Benutzern.

Active Directory-Standardschema konfigurieren

So konfigurieren Sie CMC für den Zugriff auf eine Active Directory-Anmeldung:

1 Öffnen Sie auf einem Active Directory-Server (Domänen-Controller) das **Active Directory-Benutzer- und -Computer-Snap-In**.
2 CMC-Webschnittstelle oder RACADM verwenden:

a Erstellen Sie eine Gruppe oder wählen Sie eine bestehende Gruppe aus.
b Konfigurieren Sie die Rollenberechtigung.

3 Fügen Sie den Active Directory-Benutzer als ein Mitglied der Active Directory-Gruppe hinzu, um auf den CMC zuzugreifen.

Active Directory mit Standardschema unter Verwendung der CMC-Webschnittstelle konfigurieren

ANMERKUNG: Weitere Informationen zu den verschiedenen Feldern finden Sie in der *CMC-Online-Hilfe*.

1 Wählen Sie in der Systemstruktur **Gehäuse-Übersicht** aus und klicken Sie auf **Benutzer-Authentifizierung** > **Verzeichnisdienste**. Die Seite **Verzeichnisdienste** wird angezeigt.

2 Wählen Sie **Microsoft Active Directory (Standardschema)** aus. Die für Standardschema zu konfigurierenden Einstellungen werden auf der gleichen Seite angezeigt.

3 Legen Sie im Abschnitt **Allgemeine Einstellungen** Folgendes fest:

- Wählen Sie **Active Directory aktivieren** aus, und geben Sie den Zeitüberschreitungswert für Active Directory in das Feld **AD-Zeitüberschreitung** ein.
- Um den Active Directory-Domänen-Controller über eine DNS-Suche abzurufen, wählen Sie **Domänen-Controller mit DNS suchen**, und wählen Sie dann eine der folgenden Optionen aus:
  - **Benutzerdomäne der Anmeldung** – Wählen Sie diese Option aus, um die DNS-Suche mit dem Domänennamen des Anmeldungsbenutzers auszuführen.
  - Wählen Sie ansonsten **Eine Domäne angeben** aus, und geben Sie den Domänennamen für die DNS-Suche ein.
- Um CMC zur Verwendung der festgelegten Active Directory-Domänen-Controller-Serveradressen zu aktivieren, wählen Sie die Option **Domänen-Controller-Adressen angeben** aus. Diese Server-Adressen sind die Adressen der Domänen-Controller, auf denen sich die Benutzerkonten und Rollengruppen befinden.

4 Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

ANMERKUNG: Sie müssen die Einstellungen anwenden, bevor Sie fortfahren. Wenn Sie die Einstellungen nicht anwenden, verlieren Sie die eingegebenen Einstellungen, wenn Sie zur nächsten Seite wechseln.

5 Klicken Sie im Bereich **Standardschema-Rollengruppen** auf eine **Rollengruppe**. Die Seite **Rollengruppe konfigurieren** wird angezeigt.

6 Geben Sie den Gruppenname, die Domäne und Berechtigungen für eine Rollengruppe ein.

7 Klicken Sie auf **Anwenden**, um die Einstellungen der Rollengruppe zu speichern und dann auf die Seite **Zurück zur Konfiguration**.

8 Falls Sie die Zertifikatsvalidierung aktiviert haben, müssen Sie das von der Zertifizierungsstelle signierte Root-Zertifikat der Domänengesamtstruktur auf den CMC hochladen. Geben Sie im Abschnitt **Zertifikate verwalten** den Dateipfad des Zertifikats ein oder suchen Sie nach der Zertifikatsdatei. Klicken Sie auf **Hochladen**, um die Datei auf den CMC hochzuladen.

ANMERKUNG: Der Wert Dateipfad zeigt den relativen Dateipfad des Zertifikats an, das Sie hochladen. Sie müssen den vollständigen Dateipfad eintippen, der den vollständigen Pfad und den kompletten Dateinamen und die Dateierweiterung umfasst.

Die SSL-Zertifikate für die Domänen-Controller müssen von dem von der Root-Zertifizierungsstelle signierten Zertifikat signiert werden. Das von der Root-Zertifizierungsstelle signierte Zertifikat muss auf der Management Station verfügbar sein, die auf den CMC zugreift.

9 Falls Sie die Option „Einmalige Anmeldung“ (Single Sign-On, SSO) aktiviert haben, klicken Sie im Abschnitt „**Kerberos-Keytab**“ auf **Durchsuchen**, geben Sie die Keytab-Datei an, und klicken Sie auf **Hochladen**. Wenn der Vorgang beendet ist, wird ein Meldungsfenster eingeblendet, das anzeigt, ob der Upload erfolgreich oder fehlerhaft war.

10 Klicken Sie auf **Anwenden**. Der CMC-Webserver startet automatisch neu, wenn Sie auf **Anwenden** klicken.

11 Melden Sie sich ab und dann beim CMC an, um die CMC Active Directory-Konfiguration abzuschließen.

12 Wählen Sie in der Systemstruktur **Gehäuse** aus, und navigieren Sie zur Registerkarte **Netzwerk**. Die Seite **Netzwerkkonfiguration** wird angezeigt.

13 Unter **Netzwerkeinstellungen** , wenn **DHCP verwenden (für Netzwerkschnittstellen-IP-Adresse)** ausgewählt ist, wählen Sie **DHCP zum Abrufen der DNS-Serveradresse verwenden** aus.

Um die IP-Adresse eines DNS-Servers manuell einzugeben, wählen Sie **DHCP zum Abrufen der DNS-Serveradressen verwenden** aus, und geben Sie die primäre und die alternative IP-Adresse des DNS-Servers ein.

14 Klicken Sie auf **Änderungen anwenden**.

Die Funktionskonfiguration CMC-Standardschema von Active Directory ist abgeschlossen.

Konfiguration des Active Directory mit Standardschema unter Verwendung von RACADM

Führen Sie an der RACADM-Eingabeaufforderung die folgenden Befehle aus:

- Verwenden des Befehls **config**:

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1
racadm config -g cfgActiveDirectory -o cfgADType 2
racadm config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupName <common name of the
role group>
racadm config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupDomain <fully qualified
domain name>
racadm config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupPrivilege <Bit Mask
Value for specific RoleGroup permissions>
```

```
racadm config -g cfgActiveDirectory -o cfgADDomainController1 <fully qualified domain
name or IP address of the domain controller>
racadm config -g cfgActiveDirectory -o cfgADDomainController2 <fully qualified domain
name or IP address of the domain controller>
racadm config -g cfgActiveDirectory -o cfgADDomainController3 <fully qualified domain
name or IP address of the domain controller>
```

ANMERKUNG: Geben Sie unbedingt den FQDN des Domänen-Controllers ein, nicht den FQDN der Domäne selbst. Geben Sie z.B. `servername.dell.com` ein und nicht `dell.com`.

ANMERKUNG:

Es muss mindestens eine der Adresse konfiguriert werden. CMC versucht so lange, nacheinander mit allen konfigurierten Adressen eine Verbindung herzustellen, bis eine Verbindung erfolgreich hergestellt wurde. Im Standardschema handelt es sich um die Adressen der Domänen-Controller, auf denen sich die Benutzerkonten und die Rollengruppen befinden.

```
racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog1 <fully qualified domain name
or IP address of the domain controller>
racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog2 <fully qualified domain name
or IP address of the domain controller>
racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog3 <fully qualified domain name
or IP address of the domain controller>
```

ANMERKUNG: Im Standardschema ist der Global Catalog Server nur erforderlich, wenn die Benutzerkonten und Rollengruppen in verschiedenen Domänen liegen. Im Falle mehrerer Domänen wie hier kann nur die Universalgruppe verwendet werden.

ANMERKUNG: Der FQDN oder die IP-Adresse, den/die Sie in diesem Feld angeben, sollte mit dem Feld "Servername" oder "Alternativer Servername" des Zertifikats Ihres Domänen-Controllers übereinstimmen, wenn Sie die Überprüfung des Zertifikats aktiviert haben.

Wenn Sie für den SSL-Handshake die Zertifikatsvalidierung deaktivieren möchten, führen Sie den folgenden RACADM-Befehl aus:

- Verwenden des Befehls **config**: `racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0`

In diesem Fall brauchen Sie kein (Certificate Authority (CA))-Zertifikat zu laden.

So erzwingen Sie die Zertifikatvalidierung während eines SSL-Handshake (optional):

- Verwenden des Befehls **config**: `racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1`

In diesem Fall müssen Sie mit dem folgenden RACADM-Befehl das CA-Zertifikat hochladen:

```
racadm sslcertupload -t 0x2 -f <ADS root CA certificate>
```

ANMERKUNG: Wenn die Zertifikatüberprüfung aktiviert ist, geben Sie die Adressen des Domain Controller Server und die FQDN des globalen Katalogs an. Stellen Sie sicher, dass DNS ordnungsgemäß konfiguriert ist.

Übersicht über Active Directory mit erweitertem Schema

Für die Verwendung der Lösung mit dem erweiterten Schema benötigen Sie die Active Directory-Schema-Erweiterung.

Active Directory-Schemaerweiterungen

Bei den Active Directory-Daten handelt es sich um eine verteilte Datenbank von *Attributen* und *Klassen.* Das Active Directory-Schema enthält die Regeln, die den Typ der Daten bestimmen, die der Datenbank hinzugefügt werden können bzw. darin gespeichert werden. Ein Beispiel einer Klasse, die in der Datenbank gespeichert wird, ist die Benutzerklasse. Beispielhafte Attribute der Benutzerklasse sind der Vorname, der Nachname bzw. die Telefonnummer des Benutzers.

Sie können die Active Directory-Datenbank erweitern, indem Sie Ihre eigenen einzigartigen *Attribute* und *Klassen* für besondere Anforderungen hinzufügen. Dell hat das Schema um die erforderlichen Änderungen zur Unterstützung von Remote-Management-Authentifizierung und -Autorisierung erweitert.

Jedes *Attribut* bzw. jede *Klasse*, das/die zu einem vorhandenen Active Directory-Schema hinzugefügt wird, muss mit einer eindeutigen ID definiert werden. Um branchenweit eindeutige IDs zu gewährleisten, unterhält Microsoft eine Datenbank von Active Directory-Objektbezeichnern (OIDs). Wenn also Unternehmen das Schema erweitern, sind diese Erweiterungen eindeutig und ergeben keine Konflikte. Um das Schema im Active Directory von Microsoft zu erweitern, hat Dell eindeutige OIDs (Namenserweiterungen) und eindeutig verlinkte Attribut-IDs für die Attribute und Klassen erhalten, die dem Verzeichnisdienst hinzugefügt werden.

- Dell-Erweiterung: `dell`
- Grund-OID von Dell: `1.2.840.113556.1.8000.1280`
- RACLinkID-Bereich:`12070` to `12079`

Übersicht über die Schemaerweiterungen

Dell hat das Schema um *Zuordnungs-*, *Geräte-* und *Berechtigungs*eigenschaften erweitert. Die *Zuordnungs*eigenschaft wird zur Verknüpfung der Benutzer oder Gruppen mit einem spezifischen Satz an Berechtigungen für ein oder mehrere RAC-Geräte verwendet. Dieses Modell ist unkompliziert und gibt dem Administrator höchste Flexibilität bei der Verwaltung verschiedener Benutzergruppen, RAC-Berechtigungen und RAC-Geräten im Netzwerk.

Wenn zwei CMCs im Netzwerk vorhanden sind, die Sie mit Active Directory für die Authentifizierung und Autorisierung integrieren wollen, müssen Sie mindestens ein Zuordnungsobjekt und ein RAC-Geräteobjekt für jeden CMC erstellen. Sie können verschiedene Zuordnungsobjekte erstellen, wobei jedes Zuordnungsobjekt nach Bedarf mit beliebig vielen Benutzern, Benutzergruppen oder RAC-Geräteobjekten verbunden werden kann. Die Benutzer und RAC-Geräteobjekte können Mitglieder beliebiger Domänen im Unternehmen sein.

Jedes Zuordnungsobjekt darf jedoch nur mit einem Berechtigungsobjekt verbunden werden (bzw. jedes Zuordnungsobjekt kann Benutzer, Benutzergruppen oder RAC-Geräteobjekte verbinden). Dieses Beispiel ermöglicht es dem Administrator, die Berechtigungen jedes Benutzers über spezielle CMCs zu steuern.

Das RAC-Geräteobjekt ist die Verknüpfung zur RAC-Firmware für die Active Directory-Abfrage zur Authentifizierung und Autorisierung. Wenn ein RAC dem Netzwerk hinzugefügt wird, muss der Administrator den RAC und sein Geräteobjekt mit seinem Active Directory-Namen so konfigurieren, dass Benutzer Authentifizierung und Genehmigung bei Active Directory ausführen können. Der Administrator muss außerdem auch mindestens einen RAC zum Zuordnungsobjekt hinzufügen, damit Benutzer Authentifizierungen vornehmen können.

ANMERKUNG: Das RAC-Berechtigungsobjekt gilt für CMC.

Sie können eine beliebige Anzahl an Zuordnungsobjekten erstellen. Es ist jedoch erforderlich, dass Sie mindestens ein Zuordnungsobjekt erstellen, und Sie müssen ein RAC-Geräteobjekt für jedes RAC (CMC) auf dem Netzwerk haben, das mit dem Active Directory integriert werden soll.

Das Zuordnungsobjekt lässt ebenso viele oder wenige Benutzer bzw. Gruppen und auch RAC-Geräteobjekte zu. Das Zuordnungsobjekt enthält jedoch nur ein Berechtigungsobjekt pro Zuordnungsobjekt. Das Zuordnungsobjekt verbindet die *Benutzer,* die *Berechtigungen* auf RAC- (CMC) Geräten haben.

Außerdem können Sie Active Directory-Objekte für eine einzelne Domäne oder in mehreren Domänen konfigurieren. Sie haben zum Beispiel zwei CMCs (RAC1 und RAC2) und drei vorhandene Active Directory-Benutzer (Benutzer1, Benutzer2 und Benutzer3). Sie wollen Benutzer1 und Benutzer2 eine Administratorberechtigung für beide CMCs geben und Benutzer3 eine Anmeldungsberechtigung für die RAC2-Karte.

Wenn Sie Universalgruppen von unterschiedlichen Domänen hinzufügen, erstellen Sie ein Zuordnungsobjekt mit Universalreichweite. Die durch das Dell Schema Extender-Dienstprogramm erstellten Standardzuordnungsobjekte sind lokale Domänengruppen und funktionieren nicht mit Universalgruppen anderer Domänen.

So konfigurieren Sie die Objekte für das Einzeldomänen-Szenario:

1 Erstellen Sie zwei Zuordnungsobjekte.
2 Erstellen Sie zwei RAC-Geräteobjekte, RAC1 und RAC2, die die zwei CMCs repräsentieren.
3 Erstellen Sie zwei Berechtigungsobjekte, Ber1 und Ber2, wobei Ber1 alle Berechtigungen (Administrator) und Ber2 Anmeldungsberechtigung hat.
4 Gruppieren Sie Benutzer1 und Benutzer2 in Gruppe1.
5 Fügen Sie Gruppe1 als Mitglieder im Zuordnungsobjekt 1 (A01), Ber1 als Berechtigungsobjekte in A01 und RAC1, RAC2 als RAC-Geräte in A01 hinzu.
6 Fügen Sie Benutzer3 als Mitglied im Zuordnungsobjekt 2 (A02), Ber2 als Berechtigungsobjekte in A02 und RAC2 als RAC-Geräte in A02 hinzu.

So konfigurieren Sie die Objekte für das Mehrdomänen-Szenario:

1 Stellen Sie sicher, dass sich die Gesamtstrukturfunktion der Domäne im systemeigenen oder im Windows 2003-Modus befindet.
2 Erstellen Sie zwei Zuordnungsobjekte, A01 (mit universellem Bereich) und A02 in jeder Domäne. Die Abbildung „Active Directory-Objekte in mehreren Domänen einrichten“ zeigt die Objekte in Domäne2.
3 Erstellen Sie zwei RAC-Geräteobjekte, RAC1 und RAC2, die die zwei CMCs repräsentieren.
4 Erstellen Sie zwei Berechtigungsobjekte, Ber1 und Ber2, wobei Ber1 alle Berechtigungen (Administrator) und Ber2 Anmeldungsberechtigung hat.
5 Ordnen Sie Benutzer1 und Benutzer2 in Gruppe1 ein. Die Gruppenreichweite von Gruppe 1 muss universell sein.
6 Fügen Sie Gruppe1 als Mitglieder im Zuordnungsobjekt 1 (A01), Ber1 als Berechtigungsobjekte in A01 und RAC1, RAC2 als RAC-Geräte in A01 hinzu.
7 Fügen Sie Benutzer3 als Mitglied im Zuordnungsobjekt 2 (A02), Ber2 als Berechtigungsobjekte in A02 und RAC2 als RAC-Geräte in A02 hinzu.

Active Directory mit erweitertem Schema konfigurieren

So konfigurieren Sie Active Directory für den Zugriff auf CMC:

1 Erweitern des Active Directory-Schemas.
2 Active Directory-Benutzer und Computer-Snap-In erweitern.
3 CMC-Benutzer mit Berechtigungen zum Active Directory hinzufügen.
4 Aktivieren Sie SSL auf allen Domänen-Controllern.
5 Konfigurieren Sie die CMC Active Directory-Eigenschaften über die CMC-Web-Schnittstelle oder RACADM.

Erweitern des Active Directory-Schemas

Mit der Erweiterung des Active Directory-Schemas werden eine Dell-Organisationseinheit, Schemaklassen und -attribute sowie Beispielberechtigungen und Zuordnungsobjekte zum Active Directory-Schema hinzugefügt. Bevor Sie das Schema erweitern, müssen Sie sicherstellen, dass Sie Schema-Admin-Berechtigungen auf dem Schema Master-FSMO-Rollenbesitzer (Flexible Single Master Operation) der Domänenstruktur besitzen.

Sie können das Schema mit einer der folgenden Methoden erweitern:

- Dell Schema Extender-Dienstprogramm
- LDIF-Script-Datei

Die Dell-Organisationseinheit wird dem Schema nicht hinzugefügt, wenn Sie die LDIF-Skriptdatei verwenden.

Die LDIF-Dateien und Dell Schema Extender befinden sich auf der DVD *Dell Systems Management Tools and Documentation* in den folgenden jeweiligen Verzeichnissen:

- DVD-Laufwerk:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files
- <DVDdrive>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema Extender

Lesen Sie zur Verwendung der LDIF-Dateien die Anleitungen in den Versionshinweisen im Verzeichnis LDIF_Files.

Sie können Schema Extender oder die LDIF-Dateien an einem beliebigen Standort kopieren und ausführen.

Dell Schema Extender verwenden

VORSICHT: Das Dienstprogramm Dell Schema Extender verwendet die Datei SchemaExtenderOem.ini. Um sicherzustellen, dass das Dell Schema Extender-Dienstprogramm richtig funktioniert, modifizieren Sie den Namen dieser Datei nicht.

1. Klicken Sie im **Begrüßungsbildschirm** auf **Weiter**.
2. Lesen Sie die Warnung und vergewissern Sie sich, dass Sie sie verstehen und klicken Sie dann auf **Weiter**.
3. Wählen Sie **Aktuelle Anmeldeinformationen verwenden** aus, oder geben Sie einen Benutzernamen und ein Kennwort mit Schema-Administratorrechten ein.
4. Klicken Sie auf **Weiter,** um Dell Schema Extender auszuführen.
5. Klicken Sie auf **Fertig stellen**.

   Das Schema wird erweitert. Um die Schema-Erweiterung zu überprüfen, verwenden Sie die Microsoft-Verwaltungskonsole (MMC) und das Active Directory-Schema-Snap-In, um zu prüfen, ob Klassen und Attribute vorhanden sind. Weitere Informationen zu Klassen und Attribute finden Sie in Klassen und Attribute. Näheres zur Benutzung der Verwaltungskonsole (MMC) und des Active Directory-Schema-Snap-In finden Sie in der Microsoft-Dokumentation.

Klassen und Attribute

Tabelle 24. Klassendefinitionen für Klassen, die zum Active Directory-Schema hinzugefügt wurden

Klassenname	Zugewiesene Objekt-Identifikationsnummer (OID)
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Tabelle 25. dellRacDevice Class

OID	1.2.840.113556.1.8000.1280.1.7.1.1
Beschreibung	Repräsentiert das Dell RAC-Gerät. Das RAC muss im Active Directory als delliDRACDevice konfiguriert sein. Mit dieser Konfiguration kann der CMC Lightweight Directory Access Protocol (LDAP)-Abfragen an das Active Directory senden.
Klassentyp	Strukturklasse
SuperClasses	dellProduct
Attribute	dellSchemaVersion dellRacType

Tabelle 26. delliDRACAssociationObject Class

OID	1.2.840.113556.1.8000.1280.1.7.1.2
Beschreibung	Repräsentiert das Dell-Zuordnungsobjekt. Das Zuordnungsobjekt ist die Verbindung zwischen Benutzern und Geräten.
Klassentyp	Strukturklasse
SuperClasses	Gruppe
Attribute	dellProductMembers dellPrivilegeMember

Tabelle 27. dellRAC4Privileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Beschreibung	Definiert die Berechtigungen (Autorisierungsrechte) für das CMC-Gerät.
Klassentyp	Erweiterungsklasse
SuperClasses	Keine
Attribute	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsTestAlertUser dellIsDebugCommandAdmin dellPermissionMask1 dellPermissionMask2

Tabelle 28. dellPrivileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Beschreibung	Wird als Container-Klasse für die Dell-Berechtigungen (Autorisierungsrechte) verwendet.
Klassentyp	Strukturklasse

OID	1.2.840.113556.1.8000.1280.1.1.1.4
SuperClasses	Benutzer
Attribute	dellRAC4Privileges

Tabelle 29. dellProduct Class

OID	1.2.840.113556.1.8000.1280.1.1.1.5
Beschreibung	Die Hauptklasse, von der alle Dell-Produkte abgeleitet werden.
Klassentyp	Strukturklasse
SuperClasses	Computer
Attribute	dellAssociationMembers

Tabelle 30. Liste von Attributen, die dem Active Directory-Schema hinzugefügt wurden

Zugewiesener OID/Syntax-Objektkennzeichner	Einzelbewertung
Attribut: `dellPrivilegeMember` **Beschreibung:** Liste mit `dellPrivilege`-Objekten, die zu diesem Attribut gehören. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.1 **Eindeutiger Name**: (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
Attribut: `dellProductMembers` **Beschreibung**: Die Liste von `dellRacDevices`-Objekten, die zu dieser Funktion gehören. Dieses Attribut ist die Vorwärtsverbindung zur `dellAssociationMembers`-Rückwärtsverbindung. **Link-ID**: 12070 **OID:** 1.2.840.113556.1.8000.1280.1.1.2.2 **Eindeutiger Name**: (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
Attribut: `dellIsCardConfigAdmin` **Beschreibung**: TRUE, wenn der Benutzer Kartenkonfigurationsrechte auf dem Gerät hat. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.4 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut: `dellIsLoginUser` **Beschreibung**: TRUE, wenn der Benutzer Anmeldungsrechte auf dem Gerät hat. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.3 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut: `dellIsUserConfigAdmin` **Beschreibung**: TRUE, wenn der Benutzer Benutzerkonfigurationsrechte auf dem Gerät hat. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.5 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE

Zugewiesener OID/Syntax-Objektkennzeichner	Einzelbewertung
Attribut: `dellIsLogClearAdmin` **Beschreibung**: TRUE, wenn der Benutzer Administratorrechte zum Löschen von Protokollen auf dem Gerät hat. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.6 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut: `dellIsServerResetUser` **Beschreibung**: TRUE, wenn der Benutzer Server-Reset-Rechte auf dem Gerät hat. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.7 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut: `dellIsTestAlertUser` **Beschreibung**: TRUE, wenn der Benutzerrechte für Warnungstests für Benutzer auf dem Gerät hat. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.10 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut: `dellIsDebugCommandAdmin` **Beschreibung**: TRUE, wenn der Benutzer Debug-Befehlsadministratorenrechte auf dem Gerät hat. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.11 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut: `dellSchemaVersion` **Beschreibung**: Die aktuelle Schemaversion wird verwendet, um das Schema zu aktualisieren. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.12 Zeichenfolge zum Ignorieren von Groß-/Kleinschreibung (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
Attribut: `dellRacType` **Beschreibung**: Dieses Attribut ist der aktuelle RAC-Typ für das DellRacDevice-Objekt und die Rückwärtsverknüpfung zur Vorwärtsverknüpfung von dellAssociationObjectMembers. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.13 Zeichenfolge zum Ignorieren von Groß-/Kleinschreibung (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
Attribut: `dellAssociationMembers` **Beschreibung**: Liste der dellAssociationObjectMembers, die zu diesem Produkt gehören. Dieses Attribut ist die Rückwärtsverbindung zum Attribut dellProductMembers. **Link-ID**: 12071 **OID**: 1.2.840.113556.1.8000.1280.1.1.2.14 Eindeutiger Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
Attribut: `dellPermissionsMask1` **OID**: 1.2.840.113556.1.8000.1280.1.6.2.1 Integer (LDAPTYPE_INTEGER)	

Zugewiesener OID/Syntax-Objektkennzeichner	Einzelbewertung

Attribut: `dellPermissionsMask2`

OID: 1.2.840.113556.1.8000.1280.1.6.2.2 Integer (LDAPTYPE_INTEGER)

Dell-Erweiterung zu Active Directory Benutzer- und Computer-Snap-In installieren

Wenn Sie das Schema im Active Directory erweitern, müssen Sie auch die Active Directory-Benutzer und das Computer-Snap-In erweitern, sodass der Administrator RAC-Geräte (CMC), Benutzer und Benutzergruppen, RAC-Zuordnungen und RAC-Berechtigungen verwalten kann.

Wenn Sie die Systems Management Software mit der DVD *Dell Systems Management Tools and Documentation* installieren, können Sie das Snap-In erweitern, indem Sie während des Installationsverfahrens die Option **Snap-In von Active Directory-Benutzern und -Computern** auswählen. Das *Schnellinstallationshandbuch zu Dell OpenManage-Software* enthält zusätzliche Anleitungen zur Installation von Systemverwaltungssoftware. Die Snap-In-Installation für 64-Bit-Versionen von Windows-Betriebssystemen finden Sie unter: **<DVDdrive>:\SYSMGMT\ManagementStation\support\OMActiveDirect ory_SnapIn64**

Weitere Informationen über Active Directory-Benutzer- und -Computer-Snap-In finden Sie in der Microsoft-Dokumentation.

CMC-Benutzer und -Berechtigungen zum Active Directory hinzufügen

Mit dem von Dell erweiterten Active Directory-Benutzer- und -Computer-Snap-In können Sie CMC-Benutzer und -Berechtigungen hinzuzufügen, indem Sie RAC-Gerät-, Zuordnungs- und Berechtigungsobjekte erstellen. Um die einzelnen Objekte hinzuzufügen, führen Sie folgende Verfahren durch:

- RAC-Geräteobjekt erstellen
- Erstellen eines Berechtigungsobjekts
- Erstellen eines Zuordnungsobjekts
- Einem Zuordnungsobjekt Objekte hinzufügen

RAC-Geräteobjekt erstellen

So erstellen Sie ein RAC-Geräteobjekt:

1. Klicken Sie im Fenster **Console Root (MCC)** mit der rechten Maustaste auf einen Container.
2. Wählen Sie **Neu** > **Dell Remote Management Object Advanced** aus.
3. Geben Sie auf der Seite **Neues Objekt** einen Namen für das neue Objekt ein. Der Name muss mit dem CMC-Namen übereinstimmen, den Sie in Active Directory mit Standardschema unter Verwendung der Webschnittstelle eingeben.
4. Wählen Sie **RAC-Geräteobjekt** und klicken Sie auf **OK**.

Berechtigungsobjekt erstellen

So erstellen Sie ein Berechtigungsobjekt:

ANMERKUNG: Sie müssen ein Berechtigungsobjekt in der gleichen Domäne erstellen, in der auch das verknüpfte Zuordnungsobjekt vorhanden ist.

1. Klicken Sie im Fenster **Console Root (MCC)** mit der rechten Maustaste auf einen Container.
2. Wählen Sie **Neu** > **Dell Remote Management Object Advanced** aus.
3. Geben Sie auf der Seite **Neues Objekt** einen Namen für das neue Objekt ein.
4. Wählen Sie **Berechtigungsobjekt** und klicken Sie auf **OK**.

5 Klicken Sie mit der rechten Maustaste auf das Berechtigungsobjekt, das Sie erstellt haben, und wählen Sie dann **Eigenschaften** aus.

6 Klicken Sie auf die Registerkarte **RAC-Berechtigungen** um einem Benutzer oder einer Gruppe Berechtigungen zuzuweisen. Weitere Informationen über CMC-Benutzerberechtigungen finden Sie unter Typen von Benutzern.

Zuordnungsobjekt erstellen

Das Zuordnungsobjekt wird von einer Gruppe abgeleitet und muss einen Gruppentyp enthalten. Die Zuordnungsreichweite legt den Sicherheitsgruppentyp für das Zuordnungsobjekt fest. Wenn Sie ein Zuordnungsobjekt erstellen, müssen Sie die Zuordnungsreichweite wählen, die auf den Typ von Objekten zutrifft, die Sie hinzufügen wollen. Wird z. B. Universal ausgewählt, bedeutet dies, dass Zuordnungsobjekte nur verfügbar sind, wenn die Active Directory-Domäne im systemspezifischen Modus oder einem höheren Modus funktioniert.

So erstellen Sie ein Zuordnungsobjekt:

1 Klicken Sie im Fenster **Console Root (MMC)** mit der rechten Maustaste auf einen Container.

2 Wählen Sie **Neu** > **Dell Remote Management Object Advanced** aus.

3 Geben Sie auf der Seite **Neues Objekt** einen Namen für das neue Objekt ein und wählen Sie **Zuordnungsobjekt** aus.

4 Wählen Sie den Bereich für das **Zuordnungsobjekt** und klicken Sie auf **OK**.

Objekte zu einem Zuordnungsobjekt hinzufügen

Durch die Verwendung des Fensters **Zuordnungsobjekt-Eigenschaften** können Sie Benutzer oder Benutzergruppen, Berechtigungsobjekte und RAC-Geräte oder RAC-Gerätegruppen zuordnen. Wenn Ihr System Microsoft Windows 2000 oder höher ausführt, müssen Sie Universal-Gruppen verwenden, damit sich Benutzer- oder RAC-Objekte über Domänen erstrecken.

Sie können Gruppen von Benutzern und RAC-Geräte hinzufügen.

Benutzer oder Benutzergruppen hinzufügen

So fügen Sie Benutzer oder Benutzergruppen hinzu:

1 Klicken Sie mit der rechten Maustaste auf das **Zuordnungsobjekt** und wählen Sie **Eigenschaften** aus.

2 Wählen Sie das Register **Benutzer** und klicken Sie auf **Hinzufügen.**

3 Geben Sie den Namen des Benutzers oder der Benutzergruppe ein und klicken Sie auf **OK**.

Berechtigungen hinzufügen

So fügen Sie Berechtigungen hinzu:

1 Wählen Sie das Register **Berechtigungsobjekt** und klicken Sie auf **Hinzufügen.**

2 Geben Sie den Namen des Berechtigungsobjekts ein und klicken Sie auf **OK**.

Klicken Sie auf das Register **Berechtigungsobjekt**, um das Berechtigungsobjekt der Zuordnung hinzuzufügen, welche die Berechtigungen des Benutzers bzw. der Benutzergruppe bei Authentifizierung eines RAC-Geräts definiert. Einem Zuordnungsobjekt kann nur ein Berechtigungsobjekt hinzugefügt werden.

RAC-Geräte oder RAC-Gerätegruppen hinzufügen

Um RAC-Geräte oder RAC-Gerätegruppen hinzufügen:

1 Wählen Sie die Registerkarte **Produkte** und klicken Sie auf **Hinzufügen**.

2 Geben Sie die Namen der RAC-Geräte oder RAC-Gerätegruppen ein und klicken Sie auf **OK**.

3 Im Fenster **Eigenschaften** klicken Sie auf **Anwenden** und dann auf **OK**.

Klicken Sie auf das Register **Produkte**, um der Zuordnung ein oder mehrere RAC-Geräte hinzuzufügen. Die zugeordneten Geräte geben die an das Netzwerk angeschlossenen RAC-Geräte an, die für die festgelegten Benutzer oder Benutzergruppen verfügbar sind. Einem Zuordnungsobjekt können mehrere RAC-Geräte hinzugefügt werden.

Active Directory mit erweitertem Schema unter Verwendung der CMC-Webschnittstelle konfigurieren

So konfigurieren Sie Active Directory mit erweitertem Schema über die CMC-Webschnittstelle:

ANMERKUNG: Weitere Informationen zu den verschiedenen Feldern finden Sie in der *Online-Hilfe*.

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Benutzerauthentifizierung** > **Gehäuseübersicht** > **Verzeichnisdienste**.

2 Wählen Sie **Microsoft Active Directory (Erweitertes Schema)** aus.

Die Einstellungen, die für das erweiterte Schema vorzunehmen sind, werden auf derselben Seite angezeigt.

3 Legen Sie im Abschnitt **Allgemeine Einstellungen** Folgendes fest:

- Wählen Sie **Active Directory aktivieren** aus, und geben Sie den Zeitüberschreitungswert für Active Directory in das Feld **AD-Zeitüberschreitung** ein.
- Um den Active Directory-Domänen-Controller über eine DNS-Suche abzurufen, wählen Sie **Domänen-Controller mit DNS suchen**, und wählen Sie dann eine der folgenden Optionen aus:
  - **Benutzerdomäne der Anmeldung** – Wählen Sie diese Option aus, um die DNS-Suche mit dem Domänennamen des Anmeldungsbenutzers auszuführen.
  - Wählen Sie ansonsten **Eine Domäne angeben** aus, und geben Sie den Domänennamen für die DNS-Suche ein.
- Um den CMC zu Verwendung der festgelegten Active Directory-Domänen-Controller-Serveradressen zu aktivieren, wählen Sie die Option **Domänen-Controller-Adressen angeben** aus. Dies sind die Adressen der Domänen-Controller, auf denen sich das CMC-Geräteobjekt und die zugeordneten Objekte befinden.

4 Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

ANMERKUNG: Sie müssen die Einstellungen anwenden, bevor Sie fortfahren. Wenn Sie die Einstellungen nicht anwenden, verlieren Sie die eingegebenen Einstellungen, wenn Sie zur nächsten Seite wechseln.

5 Im Abschnitt **Erweiterte Schemaeinstellungen** geben Sie den CMC-Gerätenamen und den Domänennamen ein.

6 Falls Sie die Zertifikatsvalidierung aktiviert haben, müssen Sie das von der Zertifizierungsstelle signierte Root-Zertifikat der Domänengesamtstruktur auf den CMC hochladen. Geben Sie im Abschnitt **Zertifikate verwalten** den Dateipfad des Zertifikats ein oder suchen Sie nach der Zertifikatsdatei. Klicken Sie auf **Hochladen**, um die Datei auf den CMC hochzuladen.

ANMERKUNG: Der Wert `File Path` (Dateipfad) zeigt den relativen Dateipfad des Zertifikats an, das Sie hochladen. Sie müssen den absoluten Dateipfad eingeben, der den vollständigen Pfad und den vollständigen Dateinamen sowie die Dateierweiterung enthält.

Die SSL-Zertifikate für die Domänen-Controller müssen von dem von der Root-Zertifizierungsstelle signierten Zertifikat signiert werden. Das von der Root-Zertifizierungsstelle signierte Zertifikat muss auf der Management Station verfügbar sein, die auf den CMC zugreift.

VORSICHT: Die SSL-Zertifikatüberprüfung ist standardmäßig erforderlich. Das Deaktivieren dieses Zertifikats wird nicht empfohlen.

7 Falls Sie die Option „Einmalige Anmeldung“ (Single Sign-On, SSO) aktiviert haben, klicken Sie im Abschnitt „Kerberos-Keytab“ auf **Durchsuchen**, geben Sie die Keytab-Datei an, und klicken Sie auf **Hochladen**. Wenn der Vorgang beendet ist, wird ein Meldungsfenster eingeblendet, das anzeigt, ob der Upload erfolgreich oder fehlerhaft war.

8 Klicken Sie auf **Apply (Anwenden)**.

Der CMC-Webserver startet automatisch neu, wenn Sie auf **Anwenden** klicken.

9 Melden Sie sich bei der CMC-Web-Schnittstelle an.

10 Wählen Sie in der Systemstruktur **Gehäuse** aus, klicken Sie auf die Registerkarte **Netzwerk**, und klicken Sie anschließend auf die Unterregisterkarte **Netzwerk**. Die Seite **Netzwerkkonfiguration** wird angezeigt.

11 Wenn **DHCP verwenden** für Netzwerkschnittstellen-IP-Adresse aktiviert ist, wählen Sie eine der folgenden Vorgehensweisen aus:

- Wählen Sie **DHCP zum Abrufen der DNS-Serveradresse verwenden**, um den DHCP-Server zum automatischen Abrufen der DNS-Server-Adressen zu aktivieren.

- Konfigurieren Sie manuell eine DNS-Server-IP-Adresse, indem Sie das Kontrollkästchen **DHCP zum Abrufen von DNS-Serveradressen verwenden** frei lassen und dann die IP-Adresse des primären und des alternativen DNS-Servers in die entsprechenden Felder eingeben.

12 Klicken Sie auf **Änderungen anwenden**.

Die Active Directory-Einstellungen für den Modus „Erweitertes Schema“ sind nun konfiguriert.

Konfiguration des Active Directory mit erweitertem Schema unter Verwendung von RACADM

Um die CMC-Active Directory-Funktion mit erweitertem Schema mit Hilfe des RACADM-Befehls zu konfigurieren, öffnen Sie eine Befehlszeile und geben Sie bei Eingabeaufforderung die folgenden Befehle ein:

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1
racadm config -g cfgActiveDirectory -o cfgADType 1
racadm config -g cfgActiveDirectory -o cfgADRacName <RAC common name>
racadm config -g cfgActiveDirectory -o cfgADRacDomain < fully qualified rac domain name >
racadm config -g cfgActiveDirectory -o cfgADDomainController1 < fully qualified domain name or
IP Address of the domain controller >
racadm config -g cfgActiveDirectory -o cfgADDomainController2 < fully qualified domain name or
IP Address of the domain controller >
racadm config -g cfgActiveDirectory -o cfgADDomainController3 < fully qualified domain name or
IP Address of the domain controller >
```

ANMERKUNG: Sie müssen mindestens eine der drei Adressen konfigurieren. CMC versucht so lange, nacheinander mit jeder der konfigurierten Adressen eine Verbindung herzustellen, bis eine Verbindung hergestellt werden konnte. Mit erweitertem Schema sind dies der FQDN oder die IP-Adresse des Domänen-Controllers, auf dem sich das CMC-Gerät befindet.

So deaktivieren Sie die Zertifikatvalidierung während eines Handshake (optional):

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0
```

ANMERKUNG: In diesem Fall brauchen Sie kein CA-Zertifikat zu laden.

So erzwingen Sie die Zertifikatvalidierung während eines SSL-Handshake (optional):

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
```

In diesem Fall müssen Sie ein Zertifizierungsstellenzertifikat hochladen:

```
racadm sslcertupload -t 0x2 -f < ADS root CA certificate >
```

ANMERKUNG: Wenn die Zertifikatvalidierung aktiviert ist, geben Sie die Adressen für den Domain Controller Server und FQDN an. Stellen Sie sicher, dass DNS korrekt konfiguriert ist unter.

Die Verwendung des folgenden RACADM-Befehls kann optional sein.

```
racadm sslcertdownload -t 0x1 -f < RAC SSL certificate >
```

Generische LDAP-Benutzer konfigurieren

CMC bietet eine allgemeine Lösung zur Unterstützung LDAP-basierter Authentifizierung (Lightweight Directory Access Protocol). Für diese Funktion ist auf Ihren Verzeichnisdiensten keine Schemaeweiterung erforderlich.

Ein CMC-Administrator kann nun die LDAP-Server-Benutzeranmeldungen in den CMC integrieren. Diese Integration erfordert die Konfiguration sowohl des LDAP-Servers wie auch des CMC. Auf der Seite des LDAP-Servers wird ein Standardgruppenobjekt als Rollengruppe verwendet. Ein Benutzer, der Zugang zum CMC hat, wird ein Mitglied der Rollengruppe. Berechtigungen sind weiterhin auf dem CMC für die Authentifizierung gespeichert, ähnlich wie bei der Standardschema-Einrichtung mit Active Directory-Unterstützung.

Damit der LDAP-Benutzer auf eine bestimmte CMC-Karte zugreifen kann, müssen der Rollengruppenname und dessen Domänenname auf der spezifischen CMC-Karte konfiguriert werden. Sie können maximal fünf Rollengruppen für jeden CMC konfigurieren. Ein Benutzer hat

die Möglichkeit, zu mehreren Gruppen innerhalb des Verzeichnisdienstes hinzugefügt zu werden. Wenn der Benutzer ein Mitglied mehrerer Gruppen ist, dann erhält der Benutzer die Berechtigungen aller dieser Gruppen.

Für Informationen über Zugriffsebene der Rollengruppen und die standardmäßigen Einstellungen der Rollengruppen, gehen Sie zu Typen von Benutzern.

Allgemeines LDAP-Verzeichnis für Zugriff auf CMC konfigurieren

Die allgemeine LDAP-Implementierung des CMC verwendet zwei Phasen, um einem Benutzer Zugriff zu gewähren – Benutzerauthentifizierung und dann Benutzerautorisierung.

Authentifizierung von LDAP-Benutzern

Manche Verzeichnisserver erfordern eine Bindung, bevor eine Suche auf einem spezifischen LDAP-Server durchgeführt werden kann.
So authentifizieren Sie einen Benutzer:

1 Stellen Sie optional eine Bindung zum Verzeichnisdienst her. Die Standardeinstellung ist eine anonyme Bindung.

ANMERKUNG: Die Windows-basierten Verzeichnisserver gestatten keine anonyme Anmeldung. Geben Sie daher den DN.-Namen und das zugehörige Kennwort der Bindung ein.

2 Suchen Sie anhand der Benutzeranmeldung nach dem Benutzer. Das Standardattribut lautet `uid`. Wenn mehr als ein Objekt gefunden wird, dann meldet der Prozess einen Fehler.

3 Bindung lösen und Bindung mit dem DN und Kennwort des Benutzers herstellen. Wenn das System keine Bindung herstellen kann, ist eine erfolgreiche Anmeldung nicht möglich.

4 Wenn diese Schritte erfolgreich sind, ist der Benutzer authentifiziert.

Autorisierung von LDAP-Benutzern

So autorisieren Sie einen Benutzer:

1 Durchsuchen Sie alle konfigurierten Gruppen nach dem Domänenname des Benutzers und zwar innerhalb der Attribute `member or uniqueMember`. Ein Administrator kann eine Benutzerdomäne konfigurieren.

2 Geben Sie dem Bentuzer die entsprechenden Zugriffsberechtigungen und Berechtigungen für jede Benutzergruppe, der der Benutzer angehört.

Konfiguration des allgemeinen LDAP-Verzeichnisdienstes mit der CMC-Webschnittstelle

So konfigurieren Sie den allgemeinen LDAP-Verzeichnisdienst:

ANMERKUNG: Sie müssen die Berechtigung als Gehäusekonfiguration-Administrator besitzen.

1 Klicken Sie im linken Fensterbereich auf **Gehäuse-Übersicht** > **Benutzerauthentifizierung** > **Verzeichnisdienste**.

2 Wahlen Sie **Allgemeines LDAP** aus.
Die Einstellungen, die für Standardschema konfiguriert werden sollen, werden auf derselben Seite angezeigt.

3 Geben Sie folgendes an:

ANMERKUNG: Weitere Informationen zu den verschiedenen Feldern finden Sie in der *Online-Hilfe*.

- Allgemeine Einstellungen
- Für LDAP zu verwendenden Server:
  - Statischer Server – Geben Sie den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse und die LDAP-Schnittstellennummer ein.
  - DNS-Server – Geben Sie den DNS-Server an, um eine Liste von LDAP-Servern durch Suchen nach deren SRV-Einträgen im DNS abzurufen.

    Die folgende DNS-Abfrage wird für SRV-Einträge durchgeführt:

    ```
    _[Dienstname]._tcp.[Suchdomäne]
    ```

    wobei <*Search Domain*> die root-Ebenendomäne ist, die für die Abfrage verwendet wird, und <*Service Name*> der Dienstname, der für die Abfrage verwendet wird.

    Beispiel:

    ```
    _ldap._tcp.dell.com
    ```

    wobei `ldap` der Dienstname ist und `dell.com` die Suchdomäne.

4 Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

ANMERKUNG: Sie müssen die Einstellungen anwenden, bevor Sie fortfahren. Wenn Sie die Einstellungen nicht anwenden, verlieren Sie die eingegebenen Einstellungen, wenn Sie zur nächsten Seite wechseln.

5 Klicken Sie im Abschnitt **Gruppeneinstellungen** auf eine **Rollengruppe**.

6 Geben Sie auf der Seite **LDAP-Rollengruppe konfigurieren** den Gruppendomänenname und die Rollengruppen-Berechtigungen ein.

7 Klicken Sie auf **Anwenden**, um die Einstellungen der Rollengruppe zu speichern, Klicken Sie auf **Zurück zur Seite Konfiguration**, und dann wählen Sie **Generisches LDAP**.

8 Wenn Sie **Überprüfung des Zertifikats aktiviert** gewählt haben, geben Sie das CA-Zertifikat im Abschnitt **Zertifikate verwalten** an, um das LDAP-Serverzertifikat während des Secure Socket Layer (SSL)-Handshake zu validieren. Klicken Sie auf **Hochladen**. Das Zertifikat wird auf den CMC heraufgeladen und weitere Details werden angezeigt.

9 Klicken Sie auf **Anwenden**.

Der allgemeine LDAP-Verzeichnisdienst ist damit konfiguriert.

Konfiguration des allgemeinen LDAP-Verzeichnisdienstes mittels RACADM

Um den LDAP-Verzeichnisdienst zu konfigurieren, verwenden Sie die Objekte in `cfgLdap` und `cfgLdapRoleGroup` RACADM-Gruppen.

Es gibt viele Möglichkeiten zur Konfiguration von LDAP-Anmeldungen. Meistens können einige Optionen in der Standardeinstellung verwendet werden.

ANMERKUNG: Wir empfehlen dringend die Verwendung des Befehls racadm `testfeature -f LDAP`, um die LDAP-Einstellungen bei Ersteinrichtungen zu testen. Diese Funktion unterstützt sowohl IPv4 wie auch IPv6.

Die erforderlichen Eigenschaftenänderungen sind zum Beispiel die Aktivierung von LDAP-Anmeldungen, die Einstellung des Server-FQDN oder der -IP und die Konfiguration der Base-DN des LDAP-Servers.

- ```
  $ racadm config -g cfgLDAP -o cfgLDAPEnable 1
  ```
- ```
  $ racadm config -g cfgLDAP -o cfgLDAPServer 192.168.0.1
  ```
- ```
  $ racadm config -g cfgLDAP -o cfgLDAPBaseDN dc=
  company,dc=com
  ```
  ```

Der CMC kann so konfiguriert werden, dass er optional einen DNS-Server auf SRV-Einträge abfragt. Falls die Eigenschaft `cfgLDAPSRVLookupEnable` aktiviert ist, wird die Eigenschaft `cfgLDAPServer` ignoriert. Die folgende Abfrage wird für die Suche nach SRV-Einträgen im DNS verwendet:

```
_ldap._tcp.domainname.com
```

`ldap` in der obigen Abfrage ist die Eigenschaft `cfgLDAPSRVLookupServiceName`.

`cfgLDAPSRVLookupDomainName` ist als **domainname.com** konfiguriert.

Weitere Informationen zu RACADM-Befehlen finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX), verfügbar unter **dell.com/support/manuals**.

10

CMC für die einfache Anmeldung oder Smart Card-Anmeldung konfigurieren

Dieser Abschnitt enthält Informationen zum Konfigurieren von CMC für die Smart Card-Anmeldung sowie für die einfache Anmeldung (Single Sign-On, SSO) von Active Directory-Benutzern.

SSO verwendet Kerberos als Authentifizierungsmethode, die Benutzern, die sich mit automatischer oder einfacher Anmeldung angemeldet haben, nachfolgende Anwendungen wie Exchange ermöglicht. Bei der einfachen Anmeldung verwendet der CMC die Anmeldeinformationen des Clientsystems, die im Betriebssystem zwischengespeichert werden, nachdem Sie sich mit einem gültigen Active Directory-Konto angemeldet haben.

Die Zweifaktor-Authentifizierung bietet eine höhere Sicherheitsstufe, indem Benutzer aufgefordert werden, ein Kennwort oder eine PIN sowie eine physische Karte mit einem privaten Schlüssel oder einem digitalen Zertifikat bereitzustellen. Kerberos verwendet diesen Zweifaktor-Authentifizierungsmechanismus und ermöglicht es Systemen, ihre Authentizität zu beweisen.

ANMERKUNG: Die Auswahl einer Anmeldemethode legt keine Richtlinienattribute hinsichtlich anderer Anmeldeschnittstellen, z. B. SSH, fest. Sie müssen auch sonstige Richtlinienattribute für andere Anmeldeschnittstellen festlegen. Falls Sie alle anderen Anmeldeschnittstellen deaktivieren möchten, navigieren Sie zur Seite Dienste und deaktivieren Sie alle (oder bestimmte) Anmeldeschnittstellen.

Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7 und Windows Server 2008 können Kerberos als Authentifizierungsmethode für SSO- und Smart Card-Anmeldung verwenden.

Weitere Informationen über Kerberos finden Sie auf der Microsoft-Website.

Themen:

Systemanforderungen

Zur Verwendung der Kerberos-Authentifizierung muss Ihr Netzwerk Folgendes enthalten:

- DNS-Server
- Microsoft Active Directory-Server

ANMERKUNG: Falls Sie Active Directory unter Microsoft Windows 2003 verwenden, müssen Sie sicherstellen, dass die neuesten Service-Packs auf dem Clientsystem installiert sind. Falls Sie Active Directory unter Microsoft Windows 2008 verwenden, müssen Sie sicherstellen, dass SP1 sowie die folgenden Hotfixes installiert sind:

Windows6.0-KB951191-x86.msu für das Dienstprogramm KTPASS. Ohne dieses Patch erzeugt das Dienstprogramm fehlerhafte Keytab-Dateien.

Windows6.0-KB957072-x86.msu für Verwendung von GSS_API- und SSL-Transaktionen während einer LDAP-Bindung.

- Kerberos-Schlüsselverteilungscenter – KDC (mit der Active Directory-Serversoftware)
- DHCP-Server (empfohlen).
- Die DNS-Server-Reverse-Zone muss einen Eintrag für den Active Directory-Server und den CMC enthalten.

Client-Systeme

- Für reine Smart Card-Anmeldung muss das Clientsystem die verteilbare Komponente von Microsoft Visual C++ 2005 enthalten. Weitere Informationen finden Sie unter **www.microsoft.com/downloads/details.aspx?FamilyID=32BC1BEEA3F9-4C13-9C99-220B62A191EE&displaylang=en**
- Für einfache Anmeldung oder Smart Card-Anmeldung muss das Clientsystem ein Teil der Active Directory-Domäne und des Kerberos-Bereichs sein.

CMC

- Jeder CMC muss ein Active Directory-Konto haben.
- Der CMC muss ein Teil der Active Directory-Domäne und des Kerberos-Bereichs sein.

Vorbedingungen für die einfache Anmeldung oder Smart Card-Anmeldung

Die Voraussetzungen für die Konfiguration der SSO- oder Smart Card-Anmeldungen lauten wie folgt:

- Einrichtung des Kerberos-Bereichs und Key Distribution Centers (KDC)) für Active Directory (ksetup).
- Gewährleisten Sie eine robuste NTP- und DNS-Infrastruktur zur Vermeidung von Problemen mit Clock-Drift und Reverse-Lookup.
- Konfiguration des CMC mit der Standardschema-Rollengruppe mit autorisierten Mitgliedern.
- Erstellen Sie für Smart Card „Active Directory-Benutzer“ für jeden CMC und konfigurieren Sie Kerberos-DES-Verschlüsselung, jedoch nicht Vorauthentifizierung.
- Browser für SSO oder Smart Card-Anmeldung konfigurieren
- Registrieren Sie die CMC-Benutzer mit Ktpass beim Schlüsselverteilungscenter (dies erzeugt auch einen Schlüssel zum Hochladen auf den CMC).

Kerberos Keytab-Datei generieren

Zur Unterstützung der SSO- und Smart Card-Anmeldungs-Authentifizierung unterstützt CMC das Windows-Kerberos-Netzwerk. Mit dem ktpass-Hilfsprogramm (wird von Microsoft als Teil der Server-Installations-CD/DVD bereitgestellt) werden die Bindungen des Dienstprinzipalnamens (SPN =Service Principal Name) zu einem Benutzerkonto erstellt und die Vertrauensinformationen in eine MIT-artige Kerberos-Keytab-Datei exportiert. Weitere Informationen zum Dienstprogramm ktpass finden Sie auf der Microsoft-Website.

Sie müssen vor dem Erstellen einer Keytab-Datei ein Active Directory-Benutzerkonto zur Benutzung mit der Option **-mapuser** des Befehls ktpass einrichten. Außerdem müssen Sie denselben Namen verwenden wie den CMC-DNS-Namen, zu dem Sie die erstellte Keytab-Datei hochladen.

So generieren Sie eine Keytab-Datei mithilfe des ktpass-Tools:

1 Führen Sie das Dienstprogramm *ktpass* auf dem Domänen-Controller (Active Directory-Server) aus, auf dem Sie den CMC einem Benutzerkonto in Active Directory zuordnen möchten.

2 Verwenden Sie den folgenden `ktpass`-Befehl, um die Kerberos-Keytab-Datei zu erstellen:

```
ktpass -princ HTTP/cmcname.domainname.com@DOMAINNAME.COM -mapuser keytabuser -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -pass * -out c:\krbkeytab
```

ANMERKUNG: Der `cmcname.domainname.com` muss gemäß RFC in Kleinbuchstaben und der `@REALM_NAME` muss in Großbuchstaben angegeben werden. Darüber hinaus unterstützt der CMC die DES-CBC-MD5- und AES256–SHA1-Typen von Kryptographie für Kerberos-Authentifizierung.

Dieses Verfahren erstellt eine Keytab-Datei, die Sie zum CMC hochladen müssen.

ANMERKUNG: Das Keytab enthält einen Verschlüsselungsschlüssel und muss an einem sicheren Ort aufbewahrt werden. Weitere Informationen zum Dienstprogramm *ktpass* finden Sie auf der Microsoft-Website.

Konfigurieren des CMC für das Active Directory-Schema

Weitere Informationen über die Konfiguration des CMC für das Active Directory-Standardschema finden Sie unter Active Directory-Standardschema konfigurieren.

Weitere Informationen über die Konfiguration des CMC für Erweitertes Schema für Active Directory finden Sie unter Übersicht des Active Directory mit erweitertem Schema.

Browser für SSO-Anmeldung konfigurieren

Einfache Anmeldung (SSO) wird von Internet Explorer Version 6.0 und höher und Firefox Version 3.0 und höher unterstützt.

ANMERKUNG: Die folgenden Anweisungen gelten nur, wenn der CMC die einfache Anmeldung mit Kerberos-Authentifizierung verwendet.

Internet Explorer

So konfigurieren Sie Internet Explorer für die einfache Anmeldung:

1 Wählen Sie in Internet Explorer **Extras** > **Internetoptionen** aus.

2 Wählen Sie im Register **Sicherheit** unter **Wählen Sie eine Zone aus, um deren Sicherheitseinstellungen festzulegen** die Option **Lokales Intranet** aus.

3 Klicken Sie auf **Sites**.

Das Dialogfeld **Lokales Intranet** wird angezeigt.

4 Klicken Sie auf **Erweitert**.

Das Dialogfeld **Lokales Intranet – Erweiterte Einstellungen** wird angezeigt.

5 Geben Sie im Feld **Diese Website zur Zone hinzufügen** den Namen des CMC und dessen Domäne ein und klicken Sie auf **Hinzufügen**.

ANMERKUNG: Sie können einen Platzhalter (*) verwenden, um alle Geräte/Benutzer in dieser Domäne anzugeben.

Mozilla Firefox

1 Geben Sie in Firefox **about:config** in die Adressleiste ein.

ANMERKUNG: Wenn der Browser die Warnung Das kann Ihre Garantie ungültig machen anzeigt, klicken Sie auf I'll be careful. I promise.

2 Im Textfeld **Filter** geben Sie **negotiate** (verhandeln) ein.

Der Browser zeigt eine Liste bevorzugter Namen an, die alle das Wort „negotiate“ enthalten.

3 Doppelklicken Sie in der Liste auf **network.negotiate-auth.trusted-uris**.

4 Geben Sie im Dialogfeld **Enter string value** (Zeichenfolgewert eingeben) den Domänennamen des CMC ein und klicken Sie auf **OK**.

Browser für Smart Card-Anmeldung konfigurieren

Internet Explorer – Stellen Sie sicher, dass der Webbrowser zum Herunterladen von Active-X-Plug-Ins konfiguriert ist.

CMC SSO oder Smart Card-Anmeldung für Active Directory-Benutzer konfigurieren

Sie können die CMC-Webschnittstelle oder RACADM zum konfigurieren von CMC SSO oder Smart Card-Anmeldung benutzen.

Konfiguration der CMC SSO- oder Smart Card-Anmeldung für Active Directory-Benutzer über die Webschnittstelle

So konfigurieren Sie Active Directory SSO- oder Smart Card-Anmeldung für CMC:

ANMERKUNG: Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe*.

1 Führen Sie beim Konfigurieren von Active Directory zum Einstellen des Benutzerkontos die folgenden zusätzlichen Schritte aus:

- Laden Sie die Keytab-Datei hoch.
- Um SSO (Single Sign-On) zu aktivieren, wählen Sie die Option **Einfache Anmeldung aktivieren** aus.
- Um Smart Card-Anmeldung zu aktivieren, wählen Sie die Option **Smart-Card-Anmeldung aktivieren** aus.

ANMERKUNG: Wenn diese zwei Schritte ausgewählt werden, bleiben alle bandexternen Schnittstellen, einschließlich Secure Shell (SSH), Telnet, Seriell und Remote-RACADM für diese Option unverändert.

2 Klicken Sie auf **Anwenden**.

Die Einstellungen werden gespeichert.

Sie können das Active Directory mit Kerberos-Authentifizierung testen, indem Sie den RACADM-Befehl verwenden:

```
testfeature -f adkrb -u <user>@<domain>
```

wobei *<user>* für ein gültiges Active Directory-Benutzerkonto steht.

Wenn der Befehl erfolgreich durchgeführt wird, bedeutet das, dass der CMC Kerberos-Anmeldeinformationen beschaffen und auf das Active Directory-Konto des Benutzers zugreifen kann. Wenn der Befehl nicht erfolgreich ist, müssen Sie den Fehler beseitigen und den Befehl erneut ausführen. Weitere Informationen finden Sie unter *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX) auf dell.com/support/manuals.

Keytab-Datei hochladen

Die Kerberos-Keytab-Datei liefert die CMC-Benutzername-Kennwort-Anmeldeinformationen für das KDC (Kerberos Data Center), das wiederum Zugriff auf das Active Directory ermöglicht. Jeder CMC im Kerberos-Bereich muss beim Active Directory registriert sein und eine eindeutige Keytab-Datei aufweisen.

Sie können einen Kerberos-Keytab hochladen, der auf dem zugeordneten Active Directory-Server erstellt wurde. Sie können die Kerberos-Keytab-Datei vom Active Directory-Server aus erzeugen, indem Sie das Dienstprogramm **ktpass.exe** ausführen. Diese Keytab-Datei stellt eine Vertrauensstellung zwischen dem Active Directory-Server und dem CMC her.

So laden Sie die Keytab-Datei hoch:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Benutzerauthentifizierung** > **Verzeichnisdienst**.
2 Wählen Sie **Microsoft Active Directory (Standardschema)** aus.
3 Klicken Sie im Abschnitt **Kerberos-Keytab** auf **Durchsuchen**, wählen Sie eine Keytab-Datei aus und klicken Sie auf **Hochladen**.
Wenn der Vorgang beendet ist, wird eine Meldung angezeigt, die anzeigt ob die Keytab-Datei erfolgreich hochgeladen wurde.

Konfigurieren der CMC SSO- oder Smart-Card-Anmeldung für Active Directory-Benutzer über RACADM

Neben den im Rahmen der Konfiguration von Active Directory ausgeführten Schritten führen Sie zum Aktivieren von SSO den folgenden Befehl aus:

```
racadm config -g cfgActiveDirectory -o cfgADSSOEnable 1
```

Neben den im Rahmen der Konfiguration von Active Directory ausgeführten Schritten verwenden Sie zum Aktivieren der Smart Card-Anmeldung die folgenden Objekte:

- `cfgSmartCardLogonEnable`
- `cfgSmartCardCRLEnable`

11

CMC zur Verwendung von Befehlszeilenkonsolen konfigurieren

Dieser Abschnitt enthält Informationen über die Funktionen der CMC-Befehlszeilenkonsole (bzw. der serielle/Telnet-/Secure Shell-Konsole) und erklärt, wie das System eingerichtet wird, sodass Systemverwaltungsmaßnahmen über die Konsole ausgeführt werden können. Weitere Informationen zur Verwendung der RACADM-Befehle im CMC über die Befehlszeilenkonsole finden Sie unter *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

Themen:

Funktionen der CMC-Befehlszeilenkonsolenverbindung

Der CMC unterstützt die folgenden Funktionen von seriellen, Telnet- und SSH-Konsolen:

- Eine serielle Client-Verbindung und bis zu vier gleichzeitige Telnet-Client-Verbindungen.
- Bis zu vier gleichzeitige Secure Shell- (SSH-) Client-Verbindungen.
- RACADM-Befehlsunterstützung.
- Integrierter connect-Befehl zum Anschließen an die serielle Konsole von Servern und E/A-Modulen; auch als `racadm connect`-Befehl verfügbar.
- Befehlszeilenbearbeitung und Verlauf
- Steuerung der Sitzungszeitüberschreitung auf allen Konsolen-Schnittstellen.

CMC-Befehlszeilenoberflächenbefehle

Wenn Sie zur CMC-Befehlszeile verbinden, können Sie folgende Befehle eingeben:

Tabelle 31. CMC-Befehlszeilenbefehle

Befehl	Beschreibung
`racadm`	RACADM-Befehle beginnen mit dem Stichwort `racadm` und werden von einem Unterbefehl gefolgt. Weitere Informationen finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-

Befehl	Beschreibung
	Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).
`connect`	Verbindet sich mit der seriellen Konsole eines Servers oder eines E/A-Moduls. Weitere Informationen finden Sie unter Verbindung zu Servern oder E/A-Modul mit dem connect-Befehl . **ANMERKUNG: Sie können auch den RACADM Befehl `connect` verwenden.**
`exit`, `logout` und `quit`	Alle diese Befehle führen die gleiche Maßnahme aus. Sie beenden die aktuelle Sitzung und kehren zu einer Anmeldungsbefehlszeilenschnittstelle zurück.

Telnet-Konsole mit dem CMC verwenden

Mit CMC können Sie bis zu vier Telnet-Sitzungen gleichzeitig durchführen.

Wenn Ihre Management Station Microsoft Windows XP oder Microsoft Windows Server 2003 ausführt, kann ein Problem mit den Zeichen in einer CMC-Telnet-Sitzung auftreten. Dieses Problem kann sich als eingefrorene Anmeldung äußern, bei der die Eingabetaste nicht reagiert und keine Kennworteingabeaufforderung erscheint.

Um dieses Problem zu beheben, laden Sie Hotfix 824810 von **support.microsoft.com** herunter. Weitere Informationen finden Sie im Microsoft Knowledge Base-Artikel 824810.

In der Befehlszeilenschnittstelle können Sie Sitzungszeitüberschreitung mit dem RACADM-Befehl `racadm getconfig -g cfgSessionManagement` verwalten. Weitere Informationen finden Sie im *Chassis Management Controller Version for Dell PowerEdge VRTX Command Line Reference Guide* (VRTX-Befehlszeilen-Referenzhandbuch für Chassis Management Controller Version für Dell PowerEdge).

SSH mit dem CMC verwenden

SSH ist eine Befehlszeilensitzung, die über die gleichen Merkmale wie eine Telnet-Sitzung verfügt, allerdings mit Sitzungsverhandlung und Verschlüsselung für verbesserte Sicherheit. CMC unterstützt SSH Version 2 mit Kennwortauthentifizierung. SSH ist beim CMC standardmäßig aktiviert.

ANMERKUNG: Der CMC unterstützt die SSH-Version 1 nicht.

Wenn während des Anmeldeverfahrens ein Fehler auftritt, gibt der SSH-Client eine Fehlermeldung aus. Der Meldungstext ist vom Client abhängig und wird nicht vom CMC gesteuert. Überprüfen Sie die RACLog-Meldungen, um die Ursache für den Fehler zu bestimmen.

ANMERKUNG: `OpenSSH` muss unter Windows von einem VT100 oder ANSI-Terminalemulator ausgeführt werden. Sie können `OpenSSH` auch mithilfe von Putty.exe ausführen. Das Ausführen von `OpenSSH` an der Windows-Eingabeaufforderung ergibt keine vollständige Funktionalität (d. h. einige Tasten reagieren nicht, und es werden keine Grafiken angezeigt). Führen Sie auf Servern, die Linux ausführen, SSH-Client-Dienste aus, um über beliebige Shells eine Verbindung zum CMC herzustellen.

Vier gleichzeitige SSH-Sitzungen werden jeweils zu einem gegebenen Zeitpunkt unterstützt. Die Sitzungszeitüberschreitung wird durch die Eigenschaft `cfgSsnMgtSshIdleTimeout` gesteuert. Sie können die verschiedenen Sitzungszeitüberschreitungen mit dem RACADM-Befehl `getconfig -g cfgSessionManagement` überprüfen.

```
$ racadm getconfig -g cfgSessionManagement
cfgSsnMgtWebserverTimeout=1800
cfgSsnMgtTelnetIdleTimeout=1800
cfgSsnMgtSshIdleTimeout=1800
cfgSsnMgtRacadmTimeout=60
```

Weitere Informationen zu RACADM-Befehlen finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX), das unter dell.com/support/Manuals verfügbar ist.

Der CMC unterstützt auch Authentifizierung mit öffentlichem Schlüssel (PKA) über SSH. Diese Authentifizierungsmethode verbessert SSH-Scripting-Automatisierung durch Beseitigung des Bedarfs, Benutzer-ID/Kennwort einzubetten bzw. anzufordern. Weitere Informationen finden Sie unter Konfigurieren der Authentifizierung mit öffentlichem Schlüssel über SSH.

SSH ist standardmäßig aktiviert. Falls SSH deaktiviert ist, können Sie die Option mit jeder anderen unterstützten Schnittstelle aktivieren.

Zur Konfiguration von SSH gehen Sie zu Dienste konfigurieren.

Unterstützte SSH-Verschlüsselungssysteme

Um mit CMC über das SSH-Protokoll zu kommunizieren, unterstützt es verschiedene Verschlüsselungsschemas, die in der folgenden Tabelle aufgelistet sind.

Tabelle 32. Verschlüsselungsschemata

Schematyp	Schema
Asymmetrische Verschlüsselung	Diffie-Hellman DSA/DSS 512-1024 (zufallsbestimmt) Bits gemäß NIST-Spezifikation
Symmetrische Verschlüsselung	• AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
Meldungsintegrität	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
Authentifizierung	Kennwort

Authentifizierung mit öffentlichem Schlüssel über SSH

Sie können bis zu 6 öffentliche Schlüssel konfigurieren, die mit dem Dienst-Benutzernamen über eine SSH-Schnittstelle verwendet werden können. Verwenden Sie vor dem Hinzufügen oder Löschen öffentlicher Schlüssel unbedingt den `view`befehl, um zu sehen, welche Schlüssel bereits eingerichtet sind, sodass kein Schlüssel versehentlich überschrieben oder gelöscht wird. Der Dienst-Benutzername ist ein spezielles Benutzerkonto, das für den Zugriff auf den CMC über SSH verwendet werden kann. Wenn der PKA über SSH eingerichtet ist und korrekt verwendet wird, dann müssen Sie den Benutzernamen und das Kennwort nicht mehr eingeben, wenn Sie sich beim CMC anmelden. Es kann sehr hilfreich sein, automatisierte Skripts einzurichten, um verschiedene Funktionen auszuführen.

ANMERKUNG: Es gibt keine GUI-Unterstützung zur Verwaltung dieser Funktionen; Sie können nur RACADM verwenden.

Beim Hinzufügen neuer öffentlicher Schlüssel müssen Sie sicherstellen, dass bestehende Schlüssel nicht bereits den Index belegen, zu dem der neue Schlüssel hinzugefügt werden soll. Der CMC führt vor dem Hinzufügen eines Schlüssels keine Prüfungen durch, um sicherzustellen, dass keine vorherigen Schlüssel gelöscht werden. Sobald ein neuer Schlüssel hinzugefügt wurde, tritt er automatisch in Kraft, solange die SSH-Schnittstelle aktiviert ist.

Beachten Sie bei Verwendung des Anmerkungsabschnitts des öffentlichen Schlüssels, dass nur die ersten 16 Zeichen vom CMC verwendet werden. Die Anmerkung des öffentlichen Schlüssels wird vom CMC verwendet, um SSH-Benutzer bei Verwendung des RACADM-Befehls `getssninfo` zu unterscheiden, weil alle PKA-Benutzer den Dienst-Benutzernamen zur Anmeldung verwenden.

Beispiel: zwei öffentliche Schlüssel, einer mit Anmerkung PC1 und einer mit Anmerkung PC2:

```
racadm getssninfo
Type       User   IP Address   Login
Date/Time
SSH        PC1    x.x.x.x      06/16/2009
09:00:00
SSH        PC2    x.x.x.x      06/16/2009
09:00:00
```

Lesen Sie für weitere Informationen zu `sshpkauth`, das *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

Generieren öffentlicher Schlüssel für Systeme, die Windows ausführen

Vor dem Hinzufügen eines Kontos ist ein öffentlicher Schlüssel von dem System erforderlich, das über SSH auf den CMC zugreift. Es gibt zwei Möglichkeiten, das öffentliche/private Schlüsselpaar zu generieren: mit der Schlüsselgeneratoranwendung PuTTY für Clients unter Windows bzw. mit ssh-keygen CLI für Clients unter Linux.

Dieser Abschnitt enthält einfache Anweisungen zum Generieren eines öffentlichen/privaten Schlüsselpaars für beide Anwendungen. Weitere Informationen über erweiterte Funktionen dieser Hilfsprogramme finden Sie in der Anwendungshilfe.

So verwenden Sie den PuTTY-Schlüsselgenerator für Clients, die Windows ausführen, zum Erstellen eines Grundschlüssels:

1 Starten Sie die Anwendung und wählen Sie entweder SSH-2 RSA oder SSH-2 DSA als Typ des zu generierenden Schlüssels aus (SSH-1 wird nicht unterstützt).

2 Geben Sie die Anzahl an Bits für den Schlüssel ein. Stellen Sie sicher, dass die RSA-Schlüsselgröße zwischen 1024 und 4096 liegt.

ANMERKUNG:

- Die empfohlene DSA-Schlüssellänge ist 1024.
- CMC blendet möglicherweise keine Meldung ein, wenn Sie Schlüssel mit einem Wert kleiner als 1024 oder größer als 4096 hinzufügen, doch wenn Sie versuchen, sich mit diesen Schlüsseln anzumelden, antwortet CMC nicht mehr.
- Verwenden Sie für Schlüssel mit einer Größe von über 2048 den folgenden RACADM-Befehl. CMC akzeptiert RSA-Schlüssel bis einer Größe von 4096, die empfohlene Schlüsselgröße ist jedoch 1024.

```
racadm -r 192.168.8.14 -u root -p calvin sshpkauth -i svcacct -k 1 -p 0xfff -f
dsa_2048.pub
```

3 Klicken Sie auf **Generieren**, und bewegen Sie die Maus gemäß der Anleitung im Fenster.

Nachdem der Schlüssel erstellt wurde, können Sie das Schlüsselanmerkungsfeld ändern.

Sie können auch eine Passphrase eingeben, um den Schüssel sicher zu machen. Stellen Sie sicher, dass Sie den privaten Schüssel speichern.

4 Sie haben zwei Optionen, den öffentlichen Schlüssel zu verwenden:

- Speichern des öffentlichen Schlüssels in eine Datei, die später hochgeladen werden kann.
- Kopieren und Einfügen des Texts aus dem Fenster **Öffentlicher Schlüssel zum Einfügen** beim Hinzufügen des Kontos mit der Textoption.

Generieren öffentlicher Schlüssel für Linux

Die Anwendung ssh-keygen für Linux-Clients ist ein Befehlszeilendienstprogramm ohne grafische Benutzeroberfläche. Öffnen Sie ein Terminalfenster und geben Sie bei der Shell-Eingabeaufforderung Folgendes ein:

```
ssh-keygen -t rsa -b 1024 -C testing
```

wobei

`-t-` „dsa“ oder „rsa“ sein muss.

`-b` die Bit-Verschlüsselungsgröße zwischen 768 und 4096 angibt.

`-c` das Ändern der Anmerkung des öffentlichen Schlüssels ermöglicht und optional ist.

Die <*passphrase*> ist optional. Wenn der Befehl beendet ist, verwenden Sie die öffentliche Datei zur Übergabe an den RACADM zum Hochladen der Datei.

Hinweise zur RACADM-Syntax für CMC

Wenn Sie den Befehl `racadm sshpkauth` verwenden, stellen Sie Folgendes sicher:

- Bei der Option `-i` muss der Parameter `svcacct` sein. Alle anderen Parameter für `-i` schlagen bei CMC fehl. `svcacct` ist ein besonderes Konto für die Authentifizierung öffentlicher Schlüssel über SSH bei CMC.
- Um sich am CMC anzumelden, muss der Benutzer der Kategorie service angehören. Benutzer anderer Kategorien können auf die eingegebenen öffentlichen Schlüssel mithilfe des Befehls `sshpkauth` zugreifen.

Öffentliche Schlüssel anzeigen

Um öffentliche Schlüssel anzuzeigen, die Sie zum CMC hinzugefügt haben, geben Sie Folgendes ein:

```
racadm sshpkauth -I svcacct -k all -v
```

Um jeweils nur einen Schlüssel anzuzeigen, ersetzen Sie `all` durch eine Zahl zwischen 1 und 6. Um zum Beispiel Schlüssel 2 anzuzeigen, geben Sie Folgendes ein:

```
racadm sshpkauth -I svcacct -k 2 -v
```

Öffentliche Schlüssel hinzufügen

Um CMC einen öffentlichen Schlüssel mit der Datei-Hochladen-Option `-f` der Konsole der Befehlszeilenschnittstelle hinzuzufügen, geben Sie Folgendes ein:

```
racadm sshpkauth -I svcacct -k 1 -p 0xfff -f <Dateiname des öffentlichen Schlüssels>
```

ANMERKUNG: Sie können nur die Datei-Hochladen-Option mit Remote-RACADM verwenden. Weitere Informationen finden Sie unter *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

Um einen öffentlichen Schlüssel mit der Text-Hochladen-Option hinzuzufügen, geben Sie Folgendes ein:

```
racadm sshpkauth -I svcacct -k 1 -p 0xfff -t "<Text des öffentlichen Schlüssels>"
```

Öffentliche Schlüssel löschen

Führen Sie den folgenden Befehl aus, um einen öffentlichen Schlüssel zu löschen:

```
racadm sshpkauth -i svcacct -k 1 -d
```

Führen Sie den folgenden Befehl aus, um alle öffentlichen Schlüssel zu löschen:

```
racadm sshpkauth -i svcacct -k all -d
```

Terminalemulationssoftware konfigurieren

CMC unterstützt eine serielle Textkonsole einer Management Station, auf der einer der folgenden Typen der Terminalemulationssoftware ausgeführt wird:

- Linux Minicom
- Hilgraeve HyperTerminal Private Edition (Version 6.3)

Um den erforderlichen Typ der Terminalsoftware zu konfigurieren, beenden Sie die in den folgenden Unterabschnitten aufgeführten Tasks.

Konfigurieren von Linux Minicom

Minicom ist ein serielles Dienstprogramm für Schnittstellenzugriff unter Linux. Die folgenden Schritte beziehen sich auf die Konfiguration von Minicom Version 2.0. Andere Versionen von Minicom können geringfügig abweichen, erfordern jedoch die selben grundlegenden Einstellungen. Zur Konfiguration anderer Minicom-Versionen, verwenden Sie die Informationen im Abschnitt „Erforderliche Minicom-Einstellungen“ dieses Benutzerhandbuchs.

Minicom Version 2.0 konfigurieren

ANMERKUNG: Für beste Ergebnisse stellen Sie die Eigenschaft cfgSerialConsoleColumns so ein, dass sie der Anzahl der Spalten entspricht. Beachten Sie, dass die Eingabeaufforderung zwei Zeichen beansprucht. Geben Sie zum Beispiel für ein 80-Spalten-Terminalfenster folgendes ein:

```
racadm config -g cfgSerial -o cfgSerialConsoleColumns 80.
```

1. Wenn Sie keine Minicom-Konfigurationsdatei haben, fahren Sie mit dem nächsten Schritt fort. Wenn Sie eine Minicom-Konfigurationsdatei haben, geben Sie `minicom<Minicom config file name>` ein und fahren Sie mit Schritt 12 fort.
2. Geben Sie bei der Linux-Eingabeaufforderung `minicom -s` ein.
3. Wählen Sie die Option **Seriellen Anschluss einrichten** aus und drücken Sie die Taste <Eingabe>.
4. Drücken Sie <a> und wählen Sie dann das entsprechende serielle Gerät aus (Beispiel: `/dev/ttyS0`).
5. Drücken Sie <e> und stellen Sie dann die Option **Bps/Par/Bits** auf **115200 8N1** ein.
6. Drücken Sie <f> und stellen Sie dann die **Hardware-Datenflusssteuerung** auf **Ja** und die **Software-Datenflusssteuerung** auf **Nein** ein. Um das Menü **Seriellen Anschluss einrichten** zu beenden, drücken Sie die Taste <Eingabe>.
7. Wählen Sie **Modem und Wählen** aus und drücken Sie die Taste <Eingabe>.
8. Im Menü **Modem-Wählen und Parameter-Setup** drücken Sie die <Rücktaste>, um die Einstellungen bei **init**, **reset**, **connect** und **hangup** zu löschen, damit diese leer sind, und drücken dann die Taste <Eingabe>, um den jeweiligen Leerwert zu speichern.
9. Wenn alle angegebenen Felder gelöscht sind, drücken Sie die Taste <Eingabe>, um das Menü **Modem-Wählen und Parameter-Setup** zu beenden.
10. Wählen Sie **Minicom beenden** aus und drücken Sie die Taste <Eingabe>.
11. An der Befehls-Shell-Eingabeaufforderung geben Sie `minicom <Minicom config file name>`.
12. Um Minicom zu beenden, drücken Sie <Strg><a>, <x>, <Eingabetaste>.

    Stellen Sie sicher, dass das Minicom-Fenster eine Anmeldeaufforderung anzeigt. Wenn die Anmeldeaufforderung angezeigt wird, wurde Ihre Verbindung erfolgreich hergestellt. Sie können sich jetzt anmelden und auf die CMC-Befehlszeilenschnittstelle zugreifen.

Erforderliche Minicom-Einstellungen

Verwenden Sie die folgende Tabelle zum Konfigurieren einer beliebigen Minicom-Version.

Tabelle 33. Minicom-Einstellungen

Beschreibung der Einstellung	Erforderliche Einstellung
Bit/s/Par/Bit	115200 8N1
Hardware-Datenflusssteuerung	Ja
Software-Datenflusssteuerung	Nein
Terminalemulation	ANSI
Einwahl per Modem und Parameter-Einstellungen	Löschen Sie die Einstellungen **init**, **reset**, **connect** und **hangup**, sodass sie leer sind.

Herstellen einer Verbindung zu Servern oder E/A-Modulen mit dem connect-Befehl

Der CMC kann eine Verbindung herstellen, um die serielle Konsole von Servern oder E/A-Modulen umzuleiten.

Für Server kann die serielle Konsolenumleitung so erreicht werden:

- Mit der CMC-Befehlszeilenschnittstelle (CLI) oder dem RACADM-Befehl `connect`. Weitere Informationen über das Ausführen von RACADM-Befehlen finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).
- Serielle Konsolenumleitungsfunktion der iDRAC-Webschnittstelle.
- iDRAC-Seriell-über-LAN (SOL)-Funktionalität.

In einer seriellen, Telnet- oder SSH-Konsole unterstützt der CMC den Befehl `connect` zum Herstellen einer seriellen Verbindung zu einem Server oder E/A-Modul. Die serielle Serverkonsole umfasst sowohl die BIOS-Start- und Setup-Bildschirme als auch die serielle Betriebssystemkonsole. Für E/A-Module steht die serielle Switch-Konsole zur Verfügung. Auf dem Gehäuse befindet sich ein einziges EAM.

VORSICHT: Bei Ausführung der Befehlsoption `connect -b` in der seriellen CMC-Konsole bleibt die Verbindung bestehen, bis der CMC zurückgesetzt wird. Diese Verbindung stellt ein potenzielles Sicherheitsrisiko dar.

ANMERKUNG: Der Befehl `connect` bietet die Option `-b` (binär). Mit der Option `-b` werden reine Binärdaten weitergegeben und `cfgSerialConsoleQuitKey` wird nicht verwendet. Zudem führen Übergänge beim DTR-Signal (z. B. wenn das serielle Kabel entfernt wird, um eine Verbindung mit einem Debugger herzustellen) nicht zum Beenden der Anwendung, wenn eine Verbindung zu einem Server über die serielle CMC-Konsole hergestellt wird.

ANMERKUNG: Wenn das EAM die Konsolenumleitung nicht unterstützt, wird beim Befehl `connect` eine leere Konsole angezeigt. Wenn Sie in diesem Fall zur CMC-Konsole zurückkehren möchten, geben Sie die Escape-Sequenz ein. Die Standard-Escape-Sequenz für die Konsole ist <Strg><\>.

Um eine Verbindung zu einem EAM herzustellen, geben Sie Folgendes ein:

```
connect switch-n
```

wobei `n` eine EAM-Kennzeichnung A1 ist.

Wenn Sie sich beim connect-Befehl auf die EAMs beziehen, werden den EAMs-Switches zugeordnet, wie in der folgenden Tabelle dargestellt.

Tabelle 34. E/A-Module zu Switches zuordnen

E/A-Modulkennzeichnung	Switch
A1	switch-a1 oder switch-1

ANMERKUNG: Es kann jeweils nur eine EAM-Verbindung pro Gehäuse aktiv sein.

ANMERKUNG: Von der seriellen Konsole aus kann keine Verbindung zu Passthroughs hergestellt werden.

Um eine Verbindung zu einer seriellen Konsole eines verwalteten Servers herzustellen, führen Sie den Befehl `connect server-n` aus, wobei *n* 1-4 entspricht. Sie können auch den Befehl `racadm connect server-n` verwenden. Wenn Sie mithilfe der Option `-b` eine Verbindung zu einem Server herstellen, wird eine binäre Datenübertragung vorausgesetzt und das Escape-Zeichen deaktiviert. Wenn der iDRAC nicht verfügbar ist, wird die Fehlermeldung `No route to host` angezeigt.

Der Befehl `connect server-n` ermöglicht dem Benutzer den Zugriff auf die serielle Schnittstelle des Servers. Sobald diese Verbindung hergestellt ist, kann der Benutzer die Konsolenumleitung des Servers über die serielle Schnittstelle des CMC sehen, die sowohl die serielle BIOS-Konsole als auch die serielle Betriebssystemkonsole umfasst.

ANMERKUNG: Um die BIOS-Startbildschirme anzuzeigen, muss die serielle Umleitung im BIOS-Setup des Servers aktiviert werden. Außerdem muss das Terminal-Emulationsfenster auf 80 x 25 eingestellt werden. Andernfalls werden die Zeichen auf der Seite nicht einwandfrei dargestellt.

ANMERKUNG: Sämtliche Schlüssel funktionieren nicht auf den BIOS-Setup-Seiten. Stellen Sie daher geeignete Tastenkombinationen für <Strg>, <Alt>, <Löschen> und andere bereit. Auf dem anfänglichen Umleitungsbildschirm werden die benötigten Tastenkombinationen angezeigt.

BIOS des verwalteten Servers für die serielle Konsolenumleitung konfigurieren

Sie können eine Remote-Konsolensitzung verwenden, um sich mit dem verwalteten System unter Verwendung der iDRAC-Webschnittstelle zu verbinden. Weitere Informationen finden Sie im *iDRAC User's Guide* (iDRAC7-Benutzerhandbuch) unter **dell.com/support/manuals**.

Die serielle Kommunikation ist im BIOS standardmäßig ausgeschaltet. Um die Daten der Hosttextkonsole zu „Seriell über LAN" umzuleiten, müssen Sie die Konsolenumleitung über COM1 aktivieren. So ändern Sie die BIOS-Einstellung:

1. Schalten Sie den Verwaltungsserver ein.
2. Drücken Sie auf die Schaltfläche <F2>, um das BIOS-Setup-Dienstprogramm während POST einzugeben.
3. Gehen Sie zu **Serielle Kommunikation** und drücken Sie die Taste <Eingabe>. Im Dialogfeld wird die Liste der seriellen Kommunikation mit den folgenden Optionen angezeigt:
   - **off**
   - **Ein ohne Konsolenumleitung**
   - **Ein mit Konsolenumleitung über COM1**

   Um zwischen Optionen hin und her zu navigieren, verwenden Sie die entsprechenden Pfeiltasten.

   ANMERKUNG: Achten Sie darauf, dass die Option Ein mit Konsolenumleitung über COM1 ausgewählt ist.
4. Aktivieren Sie **Umleitung nach Start** (Standardwert ist **deaktiviert**). Durch diese Option wird die BIOS-Konsolenumleitung für nachfolgende Neustarts aktiviert.
5. Zum Speichern der Änderungen und Beenden.

   Das verwaltete System wird neu gestartet.

Windows für serielle Konsolenumleitung konfigurieren

Es ist keine Konfiguration erforderlich für Server, die unter den Microsoft Windows Server-Versionen laufen, beginnend mit Windows Server 2003. Windows erhält Informationen vom BIOS und aktiviert die spezielle Verwaltungskonsole (SAC) auf COM1.

Linux während des Starts für die Umleitung der seriellen Konsole konfigurieren

Die folgenden Schritte beziehen sich speziell auf den Linux Grand Unified Bootloader (GRUB). Ähnliche Änderungen sind erforderlich, um einen anderen Bootloader zu verwenden.

ANMERKUNG: Beim Konfigurieren des Client-VT100-Emulationsfensters stellen Sie das Fenster bzw. die Anwendung, die die umgeleitete virtuelle Konsole anzeigt, auf 25 Reihen x 80 Spalten ein, um eine ordnungsgemäße Textanzeige sicherzustellen. Andernfalls werden einige Textanzeigen möglicherweise nicht richtig dargestellt.

Bearbeiten Sie die Datei **/etc/grub.conf** wie folgt:

1 Suchen Sie die allgemeinen Einstellungsabschnitte in der Datei und geben Sie die folgenden zwei Zeilen ein:

```
serial --unit=1 --speed=57600 terminal --timeout=10 serial
```

2 Hängen Sie zwei Optionen an die Kernel-Zeile an:

```
kernel console=ttyS1,57600
```

3 Wenn **/etc/grub.conf** eine `splashimage`-Direktive enthält, kommentieren Sie sie aus.

Im folgenden Beispiel sind die Änderungen zu sehen, die in diesem Verfahren beschrieben werden.

```
# grub.conf, erstellt durch anaconda # # Beachten Sie, dass grub nicht erneut ausgeführt
werden muss, nachdem Sie Änderungen an # dieser Datei # vorgenommen haben. HINWEIS: Sie
haben keine /boot-Partition. Dies bedeutet, dass # alle Kernel und initrd-Pfade relativ zu /
sind, z. B. # root (hd0,0) # kernel /boot/vmlinuz-version ro root=/dev/sdal # initrd /boot/
initrd-version.img #boot=/dev/sda default=0 timeout=10 #splashimage=(hd0,2)/grub/
splash.xpm.gz serial --unit=1 --speed=57600 terminal --timeout=10 serial title Red Hat Linux
Advanced Server (2.4.9-e.3smp) root (hd0,0) kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/
sda1 hda=ide-scsi console=ttyS0 console=ttyS1,115200n8r initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3) root (hd0,00) kernel /boot/vmlinuz-2.4.9-
e.3 ro root=/dev/sda1 s initrd /boot/initrd-2.4.9-e.3.im
```

Folgen Sie beim Bearbeiten der Datei **/etc/grub.conf** diesen Richtlinien:

- Deaktivieren Sie die GRUB-Grafikschnittstelle und verwenden Sie die textbasierte Schnittstelle. Ansonsten wird der GRUB-Bildschirm nicht in der Konsolenumleitung angezeigt. Zum Deaktivieren der grafischen Schnittstelle kommentieren Sie die Zeile aus, die mit `splashimage` beginnt.
- Zum Starten mehrerer GRUB-Optionen, um Konsolensitzungen über die serielle Verbindung zu beginnen, fügen Sie allen Optionen die folgende Zeile hinzu:

  ```
  console=ttyS1,57600
  ```

  Das Beispiel zeigt, dass `console=ttyS1,57600` nur zur ersten Option hinzugefügt wurde.

Linux für die Umleitung der seriellen Konsole nach Start konfigurieren

Bearbeiten Sie die Datei **/etc/inittab** wie folgt:

Fügen Sie eine neue Zeile hinzu, um `agetty` auf der seriellen COM2-Schnittstelle zu konfigurieren:

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

Das folgende Beispiel zeigt die Datei mit der neuen Zeile.

```
# # inittab This file describes how the INIT process # should set up the system in a certain #
run-level. # # Author: Miquel van Smoorenburg # Modified for RHS Linux by Marc Ewing and #
Donnie Barnes # # Default runlevel. The runlevels used by RHS are: # 0 - halt (Do NOT set
initdefault to this) # 1 - Single user mode # 2 - Multiuser, without NFS (The same as 3, if you
# do not have networking) # 3 - Full multiuser mode # 4 - unused # 5 - X11 # 6 - reboot (Do NOT
```

```
set initdefault to this) # id:3:initdefault: # System initialization. si::sysinit:/etc/rc.d/
rc.sysinit l0:0:wait:/etc/rc.d/rc 0 l1:1:wait:/etc/rc.d/rc 1 l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3 l4:4:wait:/etc/rc.d/rc 4 l5:5:wait:/etc/rc.d/rc 5 l6:6:wait:/etc/
rc.d/rc 6 # Things to run in every runlevel. ud::once:/sbin/update # Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now # When our UPS tells us power has failed, assume we
have a few # minutes of power left. Schedule a shutdown for 2 minutes from now. # This does, of
course, assume you have power installed and your # UPS is connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down" # If power was
restored before the shutdown kicked in, cancel it. pr:12345:powerokwait:/sbin/shutdown -c
"Power Restored; Shutdown Cancelled" # Run gettys in standard runlevels co:2345:respawn:/sbin/
agetty -h -L 57600 ttyS1 ansi 1:2345:respawn:/sbin/mingetty tty1 2:2345:respawn:/sbin/mingetty
tty2 3:2345:respawn:/sbin/mingetty tty3 4:2345:respawn:/sbin/mingetty tty4 5:2345:respawn:/sbin/
mingetty tty5 6:2345:respawn:/sbin/mingetty tty6 # Run xdm in runlevel 5 # xdm is now a
separate service x:5:respawn:/etc/X11/prefdm -nodaemon
```

Edit the **/etc/securetty**file as follows:

Fügen Sie eine neue Zeile mit dem Namen des seriellen tty für COM2 hinzu:

```
ttyS1
```

Das folgende Beispiel zeigt eine Beispieldatei mit der neuen Zeile.

```
vc/1 vc/2 vc/3 vc/4 vc/5 vc/6 vc/7 vc/8 vc/9 vc/10 vc/11 tty1 tty2 tty3 tty4 tty5 tty6 tty7
tty8 tty9 tty10 tty11 ttyS1
```

12

Verwenden von FlexAddress und FlexAdress Plus

Dieser Abschnitt enthält Informationen über FlexAddress, FlexAddress Plus und die Konfiguration.

ANMERKUNG: Auf dem CMC muss eine Enterprise-Lizenz installiert sein, um die FlexAddress-Funktion verwenden zu können.

Themen:

Über FlexAddress

Wird ein Server ausgetauscht, bleibt die FlexAddress für den Steckplatz für den entsprechenden Serversteckplatz erhalten. Wenn der Server in einen neuen Steckplatz oder ein neues Gehäuse eingesetzt wird, wird die dem Server zugewiesene WWN/MAC-Adresse so lange verwendet, bis das Gehäuse über die aktivierte FlexAddress-Funktion für den neuen Steckplatz verfügt. Falls Sie den Server entfernen, wechselt er wieder zur Server-zugewiesenen Adresse. Sie müssen die Bereitstellungs-Frameworks, DHCP-Server und Router für verschiedene Strukturen zur Identifizierung des neuen Servers nicht erneut konfigurieren.

Jedem Servermodul werden im Zuge der Herstellung eindeutige WWN- und/oder MAC-Adressen zugewiesen. Ohne FlexAddress, wenn ein Server mit einem anderen Servermodul ausgetauscht werden musste, änderten sich die WWN/MAC-Adressen, und die Ethernet-Netzwerkverwaltungsinstrumente sowie SAN-Ressourcen mussten neu konfiguriert werden, um das neue Servermodul erkennen zu können.

FlexAddress ermöglicht es dem CMC, WWN/MAC-Adressen einem bestimmten Steckplatz zuzuweisen und die werkseitigen Adressen außer Kraft zu setzen. Wird das Servermodul ausgetauscht, bleiben die steckplatzbasierten WWN/MAC-Adressen erhalten. Dank dieser Funktion ist es nicht mehr notwendig, die Ethernet-Netzwerkverwaltungsinstrumente und die SAN-Ressourcen für ein neues Servermodul neu zu konfigurieren.

Außerdem erfolgt das *Überschreiben* nur, wenn ein Servermodul in ein FlexAddress-aktiviertes Gehäuse eingesetzt wird. Es werden keine permanenten Änderungen am Servermodul vorgenommen. Wird ein Servermodul in ein Gehäuse eingesetzt, das FlexAddress nicht unterstützt, werden die werkseitig zugewiesenen WWN/MAC-Adressen verwendet.

Das CMC VRTX-Gehäuse wird mit einer SD-Karte geliefert, die FlexAddress-, FlexAddress Plus- und Extended Storage-Funktionen unterstützt. Wird das VRTX-Gehäuse mit einem optionalen zweiten CMC geliefert, verfügt der zweite CMC über eine SD-Karte, die nur Extended Storage unterstützt.

ANMERKUNG:

- Auf der SD-Karte befindliche Daten sind verschlüsselt und dürfen auf keine Weise vervielfältigt oder verändert werden, da dies die Systemfunktion beeinträchtigen und zu Fehlfunktionen des Systems führen könnte.
- Die SD-Karte kann nur für ein einzelnes Gehäuse verwendet werden. Sie können die gleiche SD-Karte auf keinem anderen Gehäuse verwenden.

Die FlexAddress-Funktionskarte enthält einen Bereich von MAC-Adressen. Vor der Installation von FlexAddress können Sie den MAC-Adressenbereich, der auf einer FlexAddress-Funktionskarte enthalten ist, feststellen, indem Sie die SD-Karte in einen USB-Speicherkartenleser einsetzen und die Datei **pwwn_mac.xml** anzeigen. Diese Klartext-XML-Datei auf der SD-Karte beinhaltet die XML-Kennung *mac_start*. Diese Kennung ist die hexadezimale MAC-Start-Adresse für diesen eindeutigen MAC-Adressbereich. Das Tag *mac_count* ist die Gesamtzahl der MAC-Adressen, die die SD-Karte zuweist. Der gesamte zugewiesen MAC-Bereich kann wie folgt bestimmt werden:

```
<mac_start> + <mac_count>  - 1 = <mac_end>
```

Beispiel:

```
(starting_mac)00188BFFDCFA + (mac_count)0xCF - 1 = (ending_mac)00188BFFDDC8
```

.

ANMERKUNG: Sperren Sie die SD-Karte vor dem Einsetzen in den USB-Speicherkartenleser, um versehentliches Ändern des Inhalts zu verhindern. Entsperren Sie die SD-Karte, bevor Sie sie in den CMC einsetzen.

Über FlexAddress Plus

FlexAddress Plus ist eine neue Funktion bei der Kartenversion 2.0. Es ist eine Erweiterung der FlexAddress-Funktionskarte Version 1.0. FlexAddress Plus enthält mehr MAC-Adressen als die FlexAddress-Funktion. Beide Funktionen ermöglichen es dem Gehäuse, WWN/MAC-Adressen (World Wide Name/Media Access Control) für Fibre Channel- und Ethernet-Geräte zuzuweisen. Gehäusezugewiesene WWN/MAC-Adressen sind global eindeutig und für jeden Serversteckplatz spezifisch.

Anzeigen des FlexAddress-Aktivierungsstatus

Eine Funktionskarte enthält eine oder mehrere der folgenden Funktionen: FlexAddress, FlexAddress Plus und/oder Erweiterter Speicher.

Um den FlexAddress-Status für das Gehäuse mithilfe der CMC-Webschnittstelle anzuzeigen, gehen Sie zu **Gehäuseübersicht** > **Setup**.

Die Seite **Allgemeine Gehäuseeinstellungen** wird angezeigt.

Der Eintrag für **FlexAddress** weist den Wert **Aktiv** oder **Nicht Aktiv** auf. Der Wert **Aktiv** bedeutet, dass die Funktion für das Gehäuse installiert ist, während **Nicht aktiv** bedeutet, dass die Funktion für das Gehäuse nicht installiert wurde und daher nicht verfügbar ist.

Verwenden Sie den folgenden RACADM-Befehl, um den Status der SD-Funktionskarte anzuzeigen:

```
racadm featurecard -s
```

Die folgende Meldung wird angezeigt:

```
Active CMC:
The feature card inserted is valid, serial number CN0H871T1374036T00MXA00
The feature card contains the following feature(s)
       FlexAddress: bound
       FlexAddressPlus: bound
       ExtendedStorage: bound
Standby CMC:
The feature card contains the following feature(s)
       ExtendedStorage: bound
```

ANMERKUNG: Der sekundäre CMC ist optional, und die Ausgabe des Standby-CMCs wird nur angezeigt, wenn der Standby-CMC im Gehäuse verfügbar ist.

Tabelle 35. Statusmeldungen, zurückgegeben vom Befehl featurecard -s

Statusmeldung	Maßnahmen
`No feature card inserted.`	Prüfen Sie den CMC um sicherzustellen, dass die SD-Karte korrekt eingesetzt wurde. Stellen Sie in einer redundanten CMC-Konfiguration sicher, dass der CMC mit der installierten SD-Funktionskarte der aktive CMC ist und nicht der Standby-CMC.
`The feature card inserted is valid and contains the following feature(s) FlexAddress: bound.`	Keine Maßnahme erforderlich.
`The feature card inserted is valid and contains the following feature(s) FlexAddress: bound to another chassis, svctag=ABC1234, SD card SN = 1122334455.`	Entfernen Sie die SD-Karte; bestimmen und installieren Sie die SD-Karte für das aktuelle Gehäuse.
`The feature card inserted is valid and contains the following feature(s) FlexAddress: not bound.`	Die Funktionskarte kann in ein anderes Gehäuse eingesetzt oder für das aktuelle Gehäuse neu reaktiviert werden. Um sie für das aktuelle Gehäuse zu reaktivieren, geben Sie `racadm racreset` ein, bis das CMC-Modul mit der installierten SD-Karte aktiv wird.

Verwenden Sie den folgenden RACADM-Befehl, um alle aktivierten Funktionen dieses Gehäuses anzuzeigen:

```
racadm feature -s
```

Der Befehl gibt die folgende Statusmeldung aus:

```
Feature Name = FlexAddress
       Date/time Activated = 05 Oct 2013 - 11:50:49
       Feature installed from SD-card serial number = CN0H871T1374036T00MXA00

       Feature Name = FlexAddressPlus
       Date/time Activated = 05 Oct 2013 - 11:50:49
       Feature installed from SD-card serial number = CN0H871T1374036T00MXA00

       Feature Name = ExtendedStorage
       Current Status = redundant, active
       Date/time Activated = 05 Oct 2013 - 11:50:58
       Feature installed from SD-card serial number = CN0H871T1374036T00MXA00
```

Wenn es keine aktiven Funktionen auf dem Gehäuse gibt, gibt der Befehl eine Meldung zurück:

```
racadm feature -s
No features active on the chassis
```

Dell-Funktionskarten können mehr als eine Funktion enthalten. Sobald eine auf einer Dell-Funktionskarte enthaltene Funktion auf einem Gehäuse aktiviert ist, können keine anderen Funktionen, die möglicherweise auf der Dell-Funktionskarte enthalten sind, auf einem anderen Gehäuse aktiviert werden. In diesem Fall zeigt der Befehl `racadm feature -s` die folgende Meldung für die betroffenen Funktionen an:

```
ERROR: One or more features on the SD card are active on another chassis
```

Weitere Informationen über die Befehle `feature` und `featurecard` finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX), das auf der Support-Webseite verfügbar ist.

FlexAddress konfigurieren

FlexAddress ist eine optionale Erweiterung, die es ermöglicht, die werkseitig zugewiesenen WWN/MAC-Adressen der Servermodule mit einer WWN/MAC-Adresse des Gehäuses zu ersetzen.

ANMERKUNG: In diesem Bereich bedeutet der Begriff FlexAddress auch FlexAddress Plus.

ANMERKUNG: Mithilfe des `racresetcfg`-Unterbefehls können Sie die Flex-Adresse eines CMC auf die Standardwerkseinstellung „Deaktiviert“ zurücksetzen. Die RACADM-Syntax ist:

```
racadm racresetcfg -c flex
```

Weitere Informationen über RACADM-Befehle, die sich auf die FlexAddress beziehen, sowie Daten über andere werksseitig eingestellte Eigenschaften finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX), das unter dell.com/support/manuals verfügbar ist.

Der Server muss ausgeschaltet sein, bevor Sie mit der Konfiguration beginnen. Sie können „FlexAddress“ für einzelne Strukturen aktivieren oder deaktivieren. Zusätzlich können Sie die Funktion für einzelne Steckplätze aktivieren oder deaktivieren. Nachdem Sie die Funktion für einzelne Strukturen aktiviert haben, können Sie Steckplätze auswählen, die aktiviert werden sollen. Wenn z. B. Struktur A aktiviert ist, ist FlexAddress bei allen aktivierten Steckplätzen nur in Struktur A aktiviert. In allen anderen Strukturen werden die werkseitig zugewiesenen WWN/MAC-Adressen auf dem Server verwendet.

ANMERKUNG: FlexAddress wirkt sich erst beim nächsten Neustart auf ein Servermodul aus. Wenn die FlexAddress-Funktion zum ersten Mal auf einem Servermodul bereitgestellt wird, ist es erforderlich, herunter- und danach wieder hochzufahren, damit FlexAddress wirksam wird. FlexAddress auf Ethernet-Geräten wird vom BIOS des Systemmoduls programmiert. Damit das BIOS des Servermoduls die Adresse programmieren kann, muss es in Betrieb sein, sodass das Servermodul eingeschaltet sein muss. Ist das Herunter-/Hochfahren abgeschlossen, stehen die gehäusezugewiesenen MAC-Adressen für die Wake-On-LAN (WOL)-Funktion zur Verfügung.

Konfiguration der FlexAddress Struktur und Steckplatz auf Gehäuseebene

Auf Gehäuseebene können Sie FlexAddress für Strukturen und Steckplätze aktivieren oder deaktivieren. FlexAddress ist jeweils für eine Struktur aktiviert, und dann werden die Steckplätze ausgewählt, die davon betroffen sein sollen. Sowohl Strukturen, als auch Steckplätze müssen für eine erfolgreiche FlexAddress-Konfiguration aktiviert sein.

FlexAddress für Struktur und Steckplatz auf Gehäuseebene über die CMC-Webschnittstelle konfigurieren

Ist ein Server im Steckplatz vorhanden, schalten Sie ihn aus, bevor Sie die Funktion FlexAddress für diesen Steckplatz aktivieren.

So aktivieren oder deaktivieren Sie Struktur und Steckplätze für die Verwendung mit der FlexAddress-Funktion mithilfe der CMC-Webschnittstelle:

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Setup** > **FlexAddress**.
2. Wählen Sie auf der Seite **FlexAddress bereitstellen** im Abschnitt **Struktur für gehäusezugewiesene WWN/MACs auswählen** den Strukturtyp (Struktur**-A** oder **iDRAC**) aus, mit dem Sie FlexAddress aktivieren wollen. Zum Deaktivieren heben Sie die Auswahl der Option auf.
3. Wählen Sie auf der Seite **Steckplätze für gehäusezugewiesene WWN/MACs auswählen** die Option **Aktiviert** für den Steckplatz aus, auf dem Sie FlexAddress aktivieren möchten. Zum Deaktivieren heben Sie die Auswahl der Option auf.

ANMERKUNG: Beachten Sie Folgendes:

- Wirk kein Steckplatz ausgewählt, wird FlexAddress für die ausgewählten Strukturen nicht aktiviert.
- Wenn keine Strukturen ausgewählt wurden und ein Serversteckplatz ausgewählt und angewendet wurde, wird die folgende Meldung angezeigt: `No fabrics selected! FlexAddress will not be used on this chassis.` Wählen Sie die Struktur und den Steckplatz für eine erfolgreiche FlexAddress-Konfiguration aus.
- Die Konfiguration von FlexAddress für den Slave-Anschluss ist nicht zulässig. Diese Option wird in der CMC-Webschnittstelle ausgegraut dargestellt. Die Ethernet-Geräte, die mit dem Slave-Anschluss des Servers verbunden sind, übernehmen die Rolle der Master-Steckplatz-Konfiguration.

4 Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

FlexAddress für Struktur und Steckplatz auf Gehäuseebene über RADACM konfigurieren

Verwenden Sie zum Aktivieren oder Deaktivieren von Strukturen die folgenden RACADM-Befehle:

```
racadm setflexaddr [-f <fabricName> <state>]
```

wobei `<fabricName> = A or iDRAC` und `<state> = 0 or 1`

0 bedeutet deaktiviert und 1 bedeutet aktiviert.

Verwenden Sie zum Aktivieren oder Deaktivieren von Steckplätzen die folgenden RACADM-Befehle:

```
racadm setflexaddr [-i <slot#> <state>
```

wobei `<slot#> = 1 or 4` und `<state> = 0 or 1`

0 bedeutet deaktiviert und 1 bedeutet aktiviert.

Weitere Informationen über den Befehl **setflexaddr** finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

ANMERKUNG: Wenn Sie die FlexAddress- oder FlexAddressPlus-Funktion mit Ihrem Dell PowerEdge VTRX erwerben, ist sie vorinstalliert und für alle Steckplätze und Strukturen aktiviert. Um diese Funktion zu erwerben, kontaktieren Sie Dell unter dell.com.

ANMERKUNG: Mithilfe des `racresetcfg`-Unterbefehls können Sie die Flex-Adresse eines CMC zur Standardwerkseinstellung „Deaktiviert“ zurücksetzen. Die RACADM-Syntax ist:

```
racadm racresetcfg -c flex
```

Weitere Informationen über RACADM-Befehle, die sich auf die FlexAddress beziehen, sowie Daten über andere werksseitig eingestellte Eigenschaften finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX), das unter dell.com/support/manuals verfügbar ist.

Anzeigen von World Wide Name- oder Media Access Control-Adressen

Auf der Seite **WWN/MAC-Zusammenfassung** können Sie die World Wide Name (WWN)-Konfiguration und die Media Access Control (MAC)-Adresse eines Steckplatzes im Gehäuse einsehen.

Strukturkonfiguration

Der Abschnitt **Strukturkonfiguration** zeigt den Typ der Eingabe/Ausgabe-Struktur an, der für Struktur A installiert ist. Ein grünes Häkchen zeigt an, dass die Struktur für FlexAddress aktiviert ist. Die Funktion FlexAddress wird verwendet, um gehäusezugewiesene und steckplatzgebundene WWN/MAC-Adressen verschiedenen Strukturen und Steckplätzen innerhalb des Gehäuses bereitzustellen. Diese Funktion ist pro Struktur und pro Steckplatz aktiviert.

ANMERKUNG: Weitere Informationen zur FlexAddress-Funktion finden Sie unter Über FlexAddress.

Anzeigen von WWN- oder MAC-Adressinformationen

Sie können die WWW/MAC-Adressen-Bestandsaufnahme der Netzwerkadapter für jeden Serversteckplatz oder alle Server in einem Gehäuse anzeigen. Die Bestandsliste enthält folgende Daten:

- Strukturkonfiguration

  ANMERKUNG:
  - Struktur A zeigt den Typ der installierten Eingabe/Ausgabe-Struktur an. Wenn Struktur A aktiviert ist, werden für die nicht bestückten Steckplätze Gehäuse-zugewiesene MAC-Adressen für Struktur A angezeigt.
  - Der iDRAC-Management-Controller ist keine Struktur, doch wird seine FlexAddress als Struktur betrachtet.
  - Wenn das mit einer Komponente verknüpfte Kontrollkästchen aktiviert ist, bedeutet dies, dass die Struktur für FlexAddress oder FlexAddressPlus aktiviert ist.
- Protokoll, das am NIC-Adapteranschluss verwendet wird. Beispiel: LAN, iSCSI und FCoE.
- Fibre Channel World Wide Name (WWN) Konfiguration und MAC (Media Access Control)-Adressen eines Steckplatzes im Gehäuse.
- Typ der MAC-Adresszuweisung und der aktuell aktive Adresstyp – Serverzugewiesen, FlexAddress oder E/A-Identität. Ein schwarzes Häkchen zeigt den aktiven Adresstyp an, entweder serverzugewiesen, gehäusezugewiesen oder remote zugewiesen.
- Status von NIC-Partitionen für Geräte, die Partitionierung unterstützen.

Sie können den Bestand der WWN/MAC-Adressen über die Webschnittstelle oder die RACADM-Befehlszeilenschnittstelle (CLI) anzeigen. Auf Basis der Schnittstelle können Sie die MAC-Adresse filtern und feststellen, welche WWN/MAC-Adresse für diese Funktion oder Partition verwendet wird. Wenn NPAR für den Adapter aktiviert ist, kann angezeigt werden, welche Partitionen aktiviert oder deaktiviert sind.

Bei Verwendung der Web-Schnittstelle können Sie die WWN/MAC-Adresseninformationen anzeigen:

- Bestimmte Steckplätze – Öffnen Sie die Seite **FlexAddress**, indem Sie auf **Server-Übersicht** > **Steckplatz <x>** > **Setup** > **FlexAddress** klicken.
- Alle Steckplätze und Server – Öffnen Sie die Seite **WWN/MAC-Zusammenfassung**, indem Sie auf **Server-Übersicht** > **Eigenschaften** > **WWN/MAC** klicken.

Auf beiden Seiten können Sie die WWN/MAC-Adresseninformationen im Standardmodus oder im erweiterten Modus anzeigen:

- **Grundlegender Modus** - In diesem Modus können Sie Serversteckplatz, Struktur, Protokoll, WWN/MAC-Adressen und Partitionsstatus anzeigen. Im WWN/MAC-Adressfeld werden nur aktive MAC-Adressen angezeigt. Sie können filtern, indem Sie einzelne oder alle angezeigten Felder verwenden:
- **Erweiterter Modus** – In diesem Modus werden alle Felder, die im grundlegenden Modus angezeigt werden, und alle MAC-Typen (Server-zugewiesen, Flex Address und E/A-Identität) angezeigt. Sie können filtern, indem Sie einzelne oder alle angezeigten Felder verwenden.

Sowohl im grundlegenden Modus als auch im erweiterten Modus werden die WWN/MAC-Adressinformationen in reduzierter Form angezeigt. Klicken Sie auf das Pluszeichen neben einem Steckplatz oder auf **Alle erweitern/reduzieren**, um die Informationen für einen bestimmten Steckplatz oder alle Steckplätze anzuzeigen.

Zudem können Sie die WWN/MAC-Adressen für alle Server im Gehäuse in einen lokalen Ordner exportieren.

Weitere Informationen zu den Feldern finden Sie in der *Online-Hilfe*.

Anzeigen von grundlegenden WWN/MAC-Adressinformationen unter Verwendung der Webschnittstelle

Um die WWN/MAC-Adressen-Informationen für jeden Serversteckplatz oder für alle Server in einem Gehäuse anzuzeigen, gehen Sie im Basismodus folgendermaßen vor:

1 Klicken Sie auf **Server-Übersicht** > **Eigenschaften** > **WWN/MAC**

Auf der Seite **WWN/MAC-Zusammenfassung** werden die WWN/MAC-Adressinformationen angezeigt.

Klicken Sie alternativ auf **Serverübersicht** > **Steckplatz <x>** > **Setup** > **FlexAddress**, um die WWN/MAC-Adressinformationen für einen spezifischen Serversteckplatz anzuzeigen. Die Seite **FlexAddress** wird angezeigt.

2 Klicken Sie in der Tabelle **WWN/MAC-Adressen** auf **Exportieren**, um die WWN/MAC-Adressen lokal zu speichern.

3 Klicken Sie auf das Pluszeichen neben einem Steckplatz oder auf **Alle erweitern/reduzieren**, um die Attribute für einen bestimmten Steckplatz oder für alle Steckplätze in der Tabelle der WWN/MAC Adressen zu erweitern oder zu reduzieren.

4 Wählen Sie aus dem Drop-Down-Menü **Ansicht Grundlegend** aus, um die Attribute der WWN/MAC-Adressen in der Systemstruktur anzuzeigen.

5 Wählen Sie aus dem Drop-Down-Menü **Serversteckplatz Alle Server** oder einen spezifischen Steckplatz aus, um die Attribute der WWN/MAC-Adressen für alle Server bzw. nur für Server in spezifischen Steckplätzen anzuzeigen.

6 Wählen Sie aus dem Drop-Down-Menü **Struktur** einen der Strukturtypen aus, um Einzelheiten zu allen oder zu spezifischen Verwaltungstypen oder zur mit den Servern verknüpften E/A-Struktur anzuzeigen.

7 Wählen Sie aus dem Drop-Down-Menü **Protokoll** die Option **Alle Protokolle** oder eines der aufgeführten Netzwerkprotokolle aus, um alle MACS oder die mit dem ausgewählten Protokoll verbundenen MACs anzuzeigen.

8 Geben Sie im Feld **WWN/MAC-Adressen** den Teil einer MAC-Adresse oder die vollständige MAC-Adresse ein, um nur die mit der spezifischen MAC-Adresse verbundenen Steckplätze anzuzeigen.

9 Wählen Sie aus dem Drop-Down-Menü **Partitionsstatus** den Status der Partitionen aus, um Server mit dem ausgewählten Partitionsstatus anzuzeigen.

Weitere Informationen zu den Feldern finden Sie in der *Online-Hilfe*.

Anzeigen von erweiterten WWN- oder MAC-Adressinformationen unter Verwendung der Webschnittstelle

Um die WWN/MAC-Adressinformationen für jeden Serversteckplatz oder für alle Server in einem Gehäuse anzuzeigen, gehen Sie im erweiterten Modus folgendermaßen vor:

1 Klicken Sie auf **Server-Übersicht** > **Eigenschaften** > **WWN/MAC**

Auf der Seite **WWN/MAC-Zusammenfassung** werden die WWN/MAC-Adressinformationen angezeigt.

2 Wählen Sie aus dem Drop-Down-Menü **Ansicht Erweitert** aus, um die Attribute der WWN/MAC-Adressen ausführlich anzuzeigen.

In der Tabelle **WWN/MAC-Adressen** werden Serversteckplatz, Struktur, Protokoll, WWN/MAC-Adressen, Partitionsstatus und der Typ der MAC-Adresszuweisung angezeigt – Serverzugewiesen, FlexAddress oder E/A-Identität. Ein schwarzes Häkchen zeigt den aktiven Adresstyp an, entweder serverzugewiesen, gehäusezugewiesen oder remote zugewiesen. MAC.

3 Klicken Sie in der Tabelle **WWN/MAC-Adressen** auf **Exportieren**, um die WWN/MAC-Adressen lokal zu speichern.

4 Klicken Sie auf das + vor einem Steckplatz oder klicken Sie auf **Alle erweitern/reduzieren**, um die Attribute für einen bestimmten Steckplatz oder für alle Steckplätze in der Tabelle der WWN/MAC Adressen zu erweitern oder zu reduzieren.

5 Wählen Sie aus dem Drop-Down-Menü **Serversteckplatz Alle Server** oder einen spezifischen Steckplatz aus, um die Attribute der WWN/MAC-Adressen für alle Server bzw. nur für Server in spezifischen Steckplätzen anzuzeigen.

6 Wählen Sie aus dem Drop-Down-Menü **Struktur** einen der Strukturtypen aus, um Einzelheiten zu allen oder zu spezifischen Verwaltungstypen oder zur mit den Servern verknüpften E/A-Struktur anzuzeigen.

7 Wählen Sie aus dem Drop-Down-Menü **Protokoll** die Option **Alle Protokolle** oder eines der aufgeführten Netzwerkprotokolle aus, um alle MACS oder die mit dem ausgewählten Protokoll verbundenen MACs anzuzeigen.

8 Geben Sie im Feld **WWN/MAC-Adressen** die MAC-Adresse ein, um nur die mit der spezifischen MAC-Adresse verbundenen Steckplätze anzuzeigen.

9 Wählen Sie aus dem Drop-Down-Menü **Partitionsstatus** den Status der Partitionen aus, um Server mit dem ausgewählten Partitionsstatus anzuzeigen.

Wenn eine bestimmte Partition deaktiviert ist, wird der Status **Deaktiviert** angezeigt, und die Zeile, die die Partition anzeigt, wird ausgegraut.

Weitere Informationen zu den Feldern finden Sie in der *Online-Hilfe*.

Anzeigen von WWN- oder MAC-Adressinformationen unter Verwendung von RACADM

Um WWN/MAC-Adressinformationen für alle Server oder spezifische Server unter Verwendung von RACADM anzuzeigen, verwenden Sie die Unterbefehle `getflexaddr` und `getmacaddress`.

Um die Flexaddress für das gesamte Gehäuse anzuzeigen, verwenden Sie den folgenden RACADM-Befehl:

```
racadm getflexaddr
```

Um den FlexAddress-Status für einen bestimmten Steckplatz anzuzeigen, verwenden Sie den folgenden RACADM-Befehl:

```
racadm getflexaddr [-i <slot#>]
```

wobei *<slot #>* ein Wert von 1 bis 4 ist.

Um die NDC- oder LOM-MAC-Adresse anzuzeigen, verwenden Sie den folgenden RACADM-Befehl:

```
racadm getmacaddress
```

Um die MAC-Adresse für das Gehäuse anzuzeigen, verwenden Sie den folgenden RACADM-Befehl:

```
racadm getmacaddress -m chassis
```

Um die iSCSI-MAC-Adressen für alle Server anzuzeigen, verwenden Sie den folgenden RACADM-Befehl:

```
racadm getmacaddress -t iscsi
```

Um die iSCSI-MAC-Adresse für einen spezifischen Server anzuzeigen, verwenden Sie den folgenden RACADM-Befehl:

```
racadm getmacaddress [-m <module> [-x]] [-t iscsi]
```

Um die benutzerdefinierte MAC- und WWN-Adresse anzuzeigen, verwenden Sie den folgenden RACADM-Befehl:

```
racadm getmacaddress -c io-identity
```

```
racadm getmacaddress -c io-identity -m server -2
```

Um die Konsolen-zugewiesene MAC/WWN für alle LOMs oder Mezzanine-Karten anzuzeigen, verwenden Sie den folgenden RACADM-Befehl:

```
racadm getmacaddress -c all
```

Um die Gehäuse-zugewiesene WWN/MAC-Adresse anzuzeigen, verwenden Sie den folgenden RACADM-Befehl:

```
racadm getmacaddress -c flexaddress
```

Um die MAC/WWN-Adressen für alle LOMs oder Mezzanine-Karten anzuzeigen, verwenden Sie den folgenden RACADM-Befehl:

```
racadm getmacaddress -c factory
```

Um die Ethernet- und iSCSI-MAC/WWN-Adressen für alle iDRAC/LOMs/Mezzanine-Karten anzuzeigen, verwenden Sie den folgenden RACADM-Befehl:

```
racadm getmacaddress -a
```

Weitere Informationen über die Unterbefehle **getflexaddr** und **getmacaddress** finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

Befehlsmeldungen

In der folgenden Tabelle werden RACADM-Befehle und -Ausgaben für häufig auftretende FlexAddress-Situationen aufgelistet.

Tabelle 36. FlexAddress-Befehle und -Ausgaben

Situation	Befehl	Ausgabe

SD-Karte im aktiven CMC-Modul ist an eine andere Service-Tag-Nummer gebunden.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)`
		
		`FlexAddress: bound to another chassis, svctag = <Service tag Number> SD card SN = <Valid flex address serial number>`

SD-Karte im aktiven CMC-Modul ist an die gleiche Service-Tag-Nummer gebunden.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)`
		
		`FlexAddress: bound`

Die SD-Karte im aktiven CMC-Modul ist an keine Service-Tag-Nummer gebunden.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)`
		
		`FlexAddress:not bound`

Die Funktion FlexAddress ist auf dem Gehäuse aus irgendeinem Grund (keine SD-Karte eingesetzt / beschädigte SD-Karte / Funktion deaktiviert / SD-Karte an anderes Gehäuse gebunden) nicht aktiv.	`$racadm setflexaddr [-f <fabricName> <slotState>]`
	
	`$racadm setflexaddr [-i <<slot#> <slotstate>]`
		`ERROR: Flexaddress feature is not active on the chassis`

Gastbenutzer versucht FlexAddress für Steckplätze/Strukturen festzulegen	`$racadm setflexaddr [-f <fabricName> <slotState>]`
	
	`$racadm setflexaddr [-i <<slot#> <slotstate>]`
		`ERROR: Insufficient user privileges to perform operation`

Situation	Befehl	Ausgabe
Die Funktion FlexAddress bei eingeschaltetem Gehäuse deaktivieren.	`$racadm feature -d -c flexaddress`	`ERROR: Unable to deactivate the feature because the chassis is powered ON`
Gastbenutzer versucht die Funktion auf dem Gehäuse zu deaktivieren.	`$racadm feature -d -c flexaddress`	`ERROR: Insufficient user privileges to perform operation`
Ändern der FlexAddress-Einstellungen für einen Steckplatz/eine Struktur, während die Servermodule eingeschaltet sind.	`$racadm setflexaddr -i 1 1`	`ERROR: Unable to perform the set operation because it affects a powered ON server`
Flexaddress-Einstellungen auf Steckplatz oder Struktur ändern, wenn die CMC Enterprise-Lizenz nicht installiert ist.	`$racadm setflexaddr -i<slotnum> <status>` `$racadm setflexaddr -f<FabricName> <status>`	`FEHLER: SWC0242 : Eine erforderliche Lizenz fehlt oder ist abgelaufen. Rufen Sie eine entsprechende Lizenz ab und versuchen Sie es erneut, oder bitten Sie Ihren Dienstanbieter um weitere Details.`

ANMERKUNG: Um dieses Problem zu beheben, müssen Sie eine FlexAddress-Aktivierungs-Lizenz aufweisen.

FlexAddress DELL SOFTWARE-LIZENZVEREINBARUNG

Dies ist ein rechtlich bindender Vertrag zwischen Ihnen, dem Benutzer, und Dell Products L.P oder Dell Global B.V. ("Dell"). Diese Vereinbarung erstreckt sich auf jede Software (zusammenfassend als „Software“ bezeichnet), die mit dem Dell-Produkt geliefert wird und für die keine separate Lizenzvereinbarung zwischen Ihnen und dem Hersteller bzw. dem Eigentümer der Software besteht. Diese Vereinbarung ist nicht für den Verkauf von Software oder von anderem geistigen Eigentum bestimmt. Alle Eigentumsrechte und Rechte an geistigem Eigentum sind im Besitz des Herstellers oder Eigentümers der Software. Alle Rechte, die in dieser Vereinbarung nicht ausdrücklich übertragen werden, sind im Besitz des Herstellers oder Eigentümers der Software. Durch Öffnen bzw. Aufbrechen des Siegels am bzw. an den Softwarepaket(en), Installieren oder Herunterladen der Software oder Verwenden der Software, die bereits im Computer geladen oder im Produkt integriert ist, erkennen Sie die Bestimmungen dieser Vereinbarung an. Wenn Sie diesen Bestimmungen nicht zustimmen, geben Sie bitte die gesamte Software inklusive Begleitmaterial (Disketten, CDs, gedrucktes Material und Verpackungen) unverzüglich zurück, und löschen Sie die bereits geladene oder integrierte Software.

Sie sind berechtigt, eine Kopie der Software auf einem einzigen Computer zu installieren und zu verwenden. Wenn Sie über mehrere Lizenzen der Software verfügen, ist es Ihnen gestattet, so viele Kopien der Software gleichzeitig zu verwenden, wie Sie Lizenzen haben. Die Software wird auf einem Computer „verwendet“, wenn sie in einen temporären Speicher geladen oder auf einem permanenten Speicher des Computers installiert ist. Die Installation auf einem Netzwerkserver nur zum Zweck der internen Verteilung stellt jedoch keine „Verwendung“ dar, wenn (und nur wenn) Sie für jeden Computer, an den die Software verteilt wird, über eine gesonderte Lizenz verfügen. Sie müssen sicherstellen, dass die Anzahl der Personen, die die auf einem Netzwerkserver installierte Software verwenden, nicht die Anzahl der vorhandenen Lizenzen übersteigt. Wenn mehr Personen die Software verwenden, die auf einem Netzwerkserver installiert ist, als Lizenzen vorhanden sind, müssen Sie erst so viele zusätzliche Lizenzen erwerben, bis die Anzahl der Lizenzen der Anzahl der Benutzer entspricht, bevor Sie weiteren Benutzern die Verwendung der Software gestatten dürfen. Als gewerblicher Kunde oder als Dell-Tochtergesellschaft gewähren Sie hiermit Dell oder einem von Dell bestimmten Vertreter das Recht, während der normalen Geschäftszeiten ein Audit der Softwareverwendung durchzuführen; außerdem erklären Sie sich damit einverstanden, Dell bei einem solchen Audit zu unterstützen und Dell alle Aufzeichnungen zur Verfügung zu stellen, die billigerweise mit der Verwendung der Software in Beziehung stehen. Das Audit beschränkt sich auf die Überprüfung der Einhaltung der Bestimmungen dieser Vereinbarung.

Die Software ist durch US-amerikanische Urheberrechtsgesetze und Bestimmungen internationaler Verträge geschützt. Sie sind berechtigt, eine Kopie der Software ausschließlich zu Sicherungs- oder Archivierungszwecken zu erstellen oder die Software auf eine

einzige Festplatte zu übertragen, wenn Sie das Original ausschließlich zu Sicherungs- und Archivierungszwecken aufbewahren. Sie sind nicht berechtigt, die Software 240 bei Benutzung von FlexAddress and FlexAdress Plus Karten durch Vermietung oder Leasing zu veräußern oder die schriftlichen Begleitmaterialien zu kopieren; Sie sind jedoch berechtigt, die Software mit sämtlichen Begleitmaterialien dauerhaft als Teil eines Verkaufs des Dell-Produkts zu übertragen, vorausgesetzt, Sie behalten keine Kopien zurück, und der Empfänger stimmt den Bestimmungen dieser Vereinbarung zu. Jede Übertragung muss die neueste Aktualisierung und alle früheren Versionen enthalten. Sie sind nicht berechtigt, die Software zurückzuentwickeln, zu dekompilieren oder zu disassemblieren. Wenn das Paket, das mit dem Computer geliefert wird, CDs, 3,5-Zoll- und/oder 5,25-Zoll-Disketten enthält, dürfen Sie nur die Datenträger verwenden, die für Ihren Computer geeignet sind. Sie sind nicht berechtigt, die Datenträger auf einem anderen Computer oder auf einem anderen Netzwerk zu verwenden oder sie zu verleihen, zu vermieten, zu verleasen oder an andere Benutzer zu übertragen, außer innerhalb der Grenzen dieses Vertrages.

BESCHRÄNKTE GARANTIE

Dell garantiert, dass die Software für einen Zeitraum von 90 Tagen ab Erhalt bei normalem Gebrauch frei von Material- und Verarbeitungsfehlern sein wird. Diese Garantie ist auf Ihre Person beschränkt und nicht übertragbar. Jegliche konkludente Garantie ist ab dem Erhalt der Software auf neunzig (90) Tage beschränkt. Da einige Staaten oder Rechtsordnungen die Begrenzung der Gültigkeitsdauer von konkludenten Garantien nicht gestatten, gilt die vorstehende Einschränkung für Sie möglicherweise nicht. Die gesamte Haftung von Dell und seinen Lieferanten und Ihr ausschließlicher Anspruch beschränkt sich auf (a) Rückerstattung des Kaufpreises der Software oder (b) den Ersatz von Datenträgern, die der vorstehenden Garantie nicht genügen, sofern diese unter Angabe einer Rücksendegenehmigungsnummer an Dell geschickt werden, wobei Sie das Risiko und die Kosten tragen. Diese eingeschränkte Garantie gilt nicht, wenn Disketten durch einen Unfall oder durch falsche und unsachgemäße Anwendung beschädigt wurden oder an ihnen von anderen Parteien als Dell Reparaturen oder Veränderungen vorgenommen wurden. Der Garantiezeitraum für Ersatzdisketten ist auf die verbleibende ursprüngliche Garantiedauer oder dreißig (30) Tage beschränkt, je nachdem welcher der beiden Zeiträume länger ist.

Dell kann NICHT garantieren, dass die Software Ihren Anforderungen entspricht oder die Software ohne Unterbrechung bzw. fehlerfrei funktioniert. Sie übernehmen selbst die Verantwortung für die Auswahl der Software, um die von Ihnen gewünschten Ergebnisse zu erzielen, und für die Verwendung sowie die Ergebnisse, die durch den Gebrauch der Software erzielt werden.

DELL LEHNT AUCH IM NAMEN SEINER LIEFERANTEN ALLE ANDEREN AUSDRÜCKLICHEN ODER KONKLUDENTEN GARANTIEN FÜR DIE SOFTWARE SOWIE DIE GESAMTEN BEILIEGENDEN GEDRUCKTEN MATERIALIEN AB, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF JEGLICHE KONKLUDENTEN GARANTIEN FÜR MARKTGÄNGIGE QUALITÄT UND TAUGLICHKEIT FÜR EINEN BESTIMMTEN ZWECK. Diese beschränkte Garantie verleiht Ihnen bestimmte Rechte; möglicherweise haben Sie weitere Rechte, die je nach Staat, Land oder Rechtsordnung unterschiedlich sein können.

DELL HAFTET NICHT FÜR DIREKTE ODER INDIREKTE SCHÄDEN (DIES GILT UNTER ANDEREM AUCH OHNE BESCHRÄNKUNG FÜR FOLGESCHÄDEN JEGLICHER ART, FÜR SCHÄDEN DURCH ENTGANGENE GEWINNE, BETRIEBSUNTERBRECHUNGEN, VERLUST VON GESCHÄFTSDATEN ODER SONSTIGE PEKUNIÄRE VERLUSTE), DIE AUS DER VERWENDUNG ODER DER FEHLENDEN MÖGLICHKEIT, DIE SOFTWARE ZU VERWENDEN, ENTSTEHEN, AUCH WENN AUF DIE MÖGLICHKEIT DES ENTSTEHENS SOLCHER SCHÄDEN HINGEWIESEN WURDE. In einigen Staaten oder Gerichtsbarkeiten ist ein Ausschluss oder eine Beschränkung der Haftung für Folgeschäden oder beiläufig entstandene Schäden nicht zulässig, deshalb gilt die oben aufgeführte Beschränkung für Sie möglicherweise nicht.

OPEN-SOURCE-SOFTWARE

Ein Teil dieser CD enthält eventuell Open-Source-Software, die Sie gemäß den Bedingungen der spezifischen Lizenz verwenden können, unter der die Open-Source-Software veröffentlicht wird.

Die Veröffentlichung dieser Open-Source-Software erfolgt in der Hoffnung, dass sie Ihnen von Nutzen sein wird, WIRD JEDOCH „OHNE MÄNGELGEWÄHR“ ZUR VERFÜGUNG GESTELLT, OHNE IRGENDEINE AUSDRÜCKLICHE ODER IMPLIZITE GARANTIE, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE IMPLIZITE GARANTIE FÜR MARKTREIFE ODER DIE VERWENDBARKEIT FÜR EINEN BESTIMMTEN ZWECK. DELL, DIE URHEBERRECHTSINHABER ODER BETEILIGTE HAFTEN IN KEINER WEISE FÜR DIREKTE, INDIREKTE, BESONDERE, VERSCHÄRFTE, ZUFALLS- ODER FOLGESCHÄDEN (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZGÜTERN ODER -DIENSTEN, ENTGANGENE NUTZUNG ODER GEWINNE, DATENVERLUSTE BZW. BETRIEBSUNTERBRECHUNG), DIE SICH AUS DER VERWENDUNG DIESER SOFTWARE ERGEBEN, UND ZWAR UNABHÄNGIG DAVON, WIE DIESE VERURSACHT WERDEN BZW. AUF WELCHER HAFTUNGSTHEORIE SIE BASIEREN UND OB SIE AUF VERTRAG,

VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER UNERLAUBTER HANDLUNG (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF FAHRLÄSSIGKEIT) BERUHEN. DIES GILT SELBST DANN, WENN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE.

U.S.-REGIERUNG EINGESCHRÄNKTE RECHTE

Die Software und die Dokumentation verstehen sich als Handelswaren ("commercial items") im Sinne von 48 C.F.R. 2,101 (Code of Federal Regulations), bestehend aus "kommerzieller Computersoftware" und "kommerzieller Computersoftwaredokumentation" gemäß 48 C.F.R. 12,212. Im Einklang mit 48 C.F.R. 12,212 und 48 C.F.R. 227,7202-1 bis 227,7202-4 beziehen sämtliche U.S. Regierungs-Endnutzer die Software und die Dokumentation ausschließlich mit den hierin festgelegten Rechten.

Vertragsnehmer bzw. Hersteller ist Dell Products, L.P., One Dell Way, Round Rock, Texas 78682.

ALLGEMEIN

Diese Lizenzvereinbarung gilt bis zu einer Kündigung. Sie gilt gemäß oben genannten Bedingungen oder wenn Sie gegen irgendeine der Bestimmungen verstoßen, als gekündigt. Im Fall der Kündigung sind Sie verpflichtet, die Software und das Begleitmaterial sowie sämtliche Kopien davon zu vernichten. Diese Vereinbarung unterliegt den Gesetzen des US-Bundesstaates Texas. Jede Bestimmung dieser Vereinbarung ist unabhängig von den anderen Bestimmungen gültig. Wenn es sich herausstellt, dass eine Bestimmung der vorliegenden Vereinbarung nicht durchsetzbar ist, so wird die Gültigkeit und Durchsetzbarkeit der übrigen Bestimmungen und Bedingungen davon nicht berührt. Diese Vereinbarung ist für Rechtsnachfolger und Abtretungsempfänger bindend. Dell und Sie selbst erklären sich einverstanden, in dem höchstmöglichen rechtlich erlaubten Maße auf alle Rechte auf ein Gerichtsverfahren im Hinblick auf die Software und diese Vereinbarung zu verzichten. Da in einigen Rechtsordnungen diese Verzichtserklärung nicht rechtsgültig ist, gilt die Verzichtserklärung für Sie möglicherweise nicht. Sie bestätigen hiermit, dass Sie diese Vereinbarung gelesen und verstanden haben, dass Sie sich an die vorgenannten Bestimmungen halten und dass diese Vereinbarung hinsichtlich der Software die vollständige und exklusive Vereinbarung zwischen Ihnen und Dell darstellt.

13

Verwalten von Strukturen

Das Gehäuse unterstützt einen Strukturtyp: Struktur A. Struktur A wird von dem einen E/A Modul verwendet, und ist stets mit den integrierten Ethernet-Adaptern der Server verbunden.

Das Gehäuse enthält nur ein E/A-Module (EAM), das entweder ein Switch- oder Passthrough-Modul sein kann. Das E/A-Modul wird als Gruppe A klassifiziert.

Der Gehäuse EAM verwendet einen diskrete Datenpfad: **Struktur**, und wird A genannt. Struktur A unterstützt nur Ethernet. Jeder Server-E/A-Adapter (Mezzanine-Karte oder LOM) kann entweder zwei oder vier Schnittstellen haben, je nach Kapazität. Die Zusatzkartensteckplätze sind mit PCIe-Erweiterungskarten bestückt, die mit PCIe-Karten (keinen EAM-Modulen) verbunden sind. Wenn Sie die Ethernet-, iSCSI- oder FibreChannel-Netzwerke bereitstellen, sollten Sie deren redundante Links über die Bänke eins und zwei spannen, um maximale Verfügbarkeit zu erzielen. Das diskrete E/A-Modul ist mit der Strukturkennung und der Banknummer gekennzeichnet.

ANMERKUNG: In der CMC-Befehlszeilenschnittstelle werden die EAMs mit der Konvention Schalter bezeichnet.

Themen:

Neues Einschaltszenario

Wenn das Gehäuse eingesteckt und eingeschaltet ist, hat das E/A-Modul gegenüber den Servern Priorität. Das EAM darf vor den Anderen eingeschaltet werden. Zu diesem Zeitpunkt wird keine Überprüfung der Strukturtypen durchgeführt.

Nachdem sich die EAMs eingeschaltet haben, schalten sich die Server ein, und der CMC überprüft die Server auf Strukturkonsistenz.

Ein Passthrough-Modul und ein Switch sind in der gleichen Gruppe zugelassen, wenn deren Struktur identisch ist. Switches und Passthrough-Module können in derselben Gruppe existieren, auch wenn Sie von unterschiedlichen Herstellern stammen.

EAM-Funktionszustand überwachen

Weitere Informationen zur Überwachung des EAM-Funktionszustands finden Sie unter Informationen und Funktionszustand der EAMs anzeigen.

Netzwerkeinstellungen für EAM(s) konfigurieren

Sie können die Netzwerkeinstellungen der zur Verwaltung der EAM verwendeten Schnittstelle angeben. Für Ethernet-Switches wird die bandexterne Verwaltungsschnittstelle (IP-Adresse) konfiguriert. Die bandinterne Verwaltungsschnittstelle (das heißt VLAN1) wird nicht mittels dieser Schnittstelle konfiguriert.

Stellen Sie vor der Konfiguration der Netzwerkeinstellungen für EAM(s) sicher, dass das EAM eingeschaltet ist.

Um die Netzwerkeinstellungen für IOM in Gruppe A konfigurieren zu können, müssen Sie die Berechtigungen als Struktur A-Administrator aufweisen.

ANMERKUNG: Für Ethernet-Switches können weder die bandinternen (VLAN1) noch die bandexterne Verwaltungs-IP-Adressen gleich sein bzw. sich im gleichen Netzwerk befinden; dies führt dazu, dass die bandexterne IP-Adresse nicht vergeben wird. Beachten Sie die EAM-Dokumentation für die standardmäßige bandinterne Verwaltungs-IP-Adresse.

ANMERKUNG: Die Netzwerkeinstellungen des E/A-Moduls für Ethernet-Passthrough und Infiniband-Schalter dürfen nicht konfiguriert werden.

Konfigurieren der Netzwerkeinstellungen für EAM über die CMC-Webschnittstelle

So konfigurieren Sie die Netzwerksicherheitseinstellungen für E/A-Module:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht**, dann auf **E/A-Modul-Übersicht** und klicken Sie dann auf **Setup**. Alternativ, um die Netzwerkeinstellungen des einzigen verfügbaren E/A-Moduls, welches mit **A** bezeichnet ist zu konfigurieren, klicken Sie auf **A Gigabit-Ethernet** und klicken Sie dann auf **Setup**.

   Geben Sie auf der Seite **E/A-Modul-Netzwerkeinstellungen konfigurieren** die entsprechenden Daten ein, und klicken Sie dann auf **Anwenden**.

2 Falls zugelassen, geben Sie das Stammkennwort, die SNMP RO Community-Zeichenkette und die SysLog Server IP-Adresse für das EAM ein. Weitere Informationen über die Feldbeschreibungen auf dieser Seite finden Sie in der *Online-Hilfe*.

   ANMERKUNG: Die auf den EAMs festgelegte IP-Adresse vom CMC wird nicht in die permanente Startkonfiguration des Switch übertragen. Um die IP-Adressenkonfiguration permanent zu speichern, müssen Sie den Befehl `connect switch` oder den RACADM-Befehl `racadm connect switch` eingeben oder eine direkte Schnittstelle zum GUI des EAMs verwenden, um diese Adresse in der Startkonfiguration zu speichern.

   ANMERKUNG: Die Länge der SNMP-Community-Zeichenfolge kann innerhalb des ASCII-Wertebereichs von 33 bis 125 Zeichen liegen.

3 Klicken Sie auf **Apply (Anwenden)**.

   Die Netzwerkeinstellungen sind für das IOM konfiguriert.

   ANMERKUNG: Falls zugelassen, können Sie die VLANs, Netzwerkeigenschaften und E/A-Schnittstellen auf die Standardkonfiguration zurückzusetzen..

Konfigurieren von Netzwerkeinstellungen für EAMs unter Verwendung von RACADM

Um die Netzwerkeinstellungen für EAMs mit RACADM zu konfigurieren, stellen Sie das Datum und die Uhrzeit ein. Siehe den Abschnitt „Befehl bereitstellen“ im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

Sie können den Benutzernamen, das Kennwort und die SNMP-Zeichenkette für das EAM mithilfe des Befehls „RACADM bereitstellen“ einstellen:

```
racadm deploy -m switch-<n> -u <Benutzername> -p <Kennwort>
racadm deploy -m switch-<n> -u -p <Kennwort> -v SNMPv2 <snmpCommunityString> ro
racadm deploy -a [server|switch] -u <Benutzername> -p <Kennwort>
```

Energiesteuerungsvorgang für EAMs verwalten

Weitere Informationen zum Einstellen des Energiesteuerungsvorgangs für EAMs finden Sie unter Stromsteuerungsvorgänge für ein E/A-Modul ausführen.

Aktivieren oder Deaktivieren von LED-Blinken für EAMs

Weitere Informationen zur Aktivierung des LED-Blinkens für EAMs finden Sie unter LEDs zum Identifizieren von Komponenten im Gehäuse konfigurieren.

14

Energieverwaltung und -überwachung

Das PowerEdge VRTX-Gehäuse ist das energieeffizienteste modulare Servergehäuse auf dem Markt. Es ist für hocheffiziente Netzteile und Lüfter konzipiert, verfügt über ein optimiertes Layout, sodass die Luft leichter durch das System strömen kann, und verfügt im gesamten Gehäuse über energieoptimierte Komponenten. Das verbesserte Hardware-Design ist mit fortschrittlichen Stromverwaltungsfunktionen gekoppelt, die im CMC (Chassis Management Controller), in Netzteilen und im iDRAC integriert sind. Sie können damit die Stromeffizienz weiter verbessern.

Die Stromverwaltungsfunktionen des PowerEdge VRTX helfen Administratoren, das Gehäuse zu konfigurieren, um den Stromverbrauch zu reduzieren und die Stromverwaltung ggf. auf die bestimmte Umgebung zuzuschneiden.

Das modulare PowerEdge VRTX-Gehäuse verbraucht Wechselstrom und verteilt die Last auf alle aktiven Netzteile (PSUs). Das System kann bis zu 4800 Watt Wechselstrom übertragen, der den Servermodulen und der damit verbundenen Gehäuseinfrastruktur zugeteilt wird. Diese Kapazität variiert jedoch auf Grundlage der von Ihnen ausgewählten Stromredundanzregel.

Das PowerEdge VRTX kann für eine von zwei Redundanzregeln konfiguriert werden, die das Netzteileinheit-Verhalten beeinflussen und bestimmen, wie der Gehäuse-Redundanzstatus Administratoren gemeldet wird.

Sie können die Energieverwaltung auch über die **OpenManage Power Center (OMPC)** steuern. Wenn die Energie über OMPC extern gesteuert wird, setzt CMC die Verwaltung der folgenden Aktivitäten fort:

- Redundanzregel
- Remote-Stromprotokollierung
- Dynamische Netzteilzuschaltung (DPSE)

OMPC verwaltet dann:

- Server-Stromversorgung
- Serverpriorität
- Eingangsstromkapazität des Systems
- Maximaler Stromsparmodus

ANMERKUNG: Die tatsächliche Stromzuteilung hängt von der Konfiguration und der Auslastung ab.

Sie können die CMC-Webschnittstelle oder RACADM verwenden, um Stromsteuerungen auf CMC zu verwalten und zu konfigurieren:

- Stromzuteilungen, Verbrauch und Status des Gehäuses, der Server und der Netzteile anzeigen
- Strombudget und Redundanzregel für das Gehäuse konfigurieren
- Stromsteuerungsvorgänge (Einschalten, Ausschalten, System-Reset, Aus- und Einschalten) für das Gehäuse ausführen.

Themen:

- Zuweisung der Prioritätsstufen an Server unter Verwendung der CMC-Webschnittstelle
- Vergabe von Prioritätsstufen an Server, die RACADM benutzen
- Anzeige des Stromverbrauchsstatus
- Strombudgetstatus über die CMC-Webschnittstelle anzeigen
- Redundanzstatus und allgemeiner Stromzustand
- Konfigurieren von Strombudget und Redundanz
- Stromsteuerungsvorgänge ausführen
- Durchführen von Energieverwaltungsmaßnahmen an einem Server
- Stromsteuerungsvorgänge für mehrere Server unter Verwendung der CMC-Webschnittstelle ausführen
- Stromsteuerungsvorgänge für ein E/A-Modul ausführen

Redundanzregeln

Eine Redundanzregel ist ein konfigurierbarer Satz von Eigenschaften, die festlegen, wie der CMC den Strom im Gehäuse verwaltet. Die folgenden Redundanzregeln sind mit oder ohne dynamische Zuschaltung von Netzteileinheiten konfigurierbar:

- Netzredundanz
- Netzteilredundanz

Netzredundanzregeln

Die Netzredundanzregel macht es möglich, dass ein modulares Gehäusesystem in einem Modus betrieben wird, in dem es Netzstromausfälle überbrücken kann. Diese Ausfälle können ihren Ursprung im Wechselstromnetz, in der Verkabelung oder in einer Netzteileinheit selbst haben.

Wenn ein System für Netzredundanz konfiguriert wird, dann werden die Netzteileinheiten in Netze aufgeteilt: die Netzteileinheiten in den Steckplätzen 1 und 2 befinden sich im ersten Netz und die Netzteileinheiten in den Steckplätzen 3 und 4 befinden sich im zweiten Netz. Der CMC verwaltet den Strom damit, dass, wenn eines der Netze ausfällt, das System ohne irgendeine Herabsetzung weiterarbeitet. Die Netzredundanz toleriert auch den Ausfall einzelner Netzteileinheiten.

ANMERKUNG: Eine der Aufgaben der Netzredundanz ist es, für nahtlosen Serverbetrieb zu sorgen, selbst bei Ausfall eines ganzen Stromnetzes, aber der meiste Strom ist für die Aufrechterhaltung der Netzredundanz verfügbar, wenn die Kapazitäten der beiden Netze etwa gleich sind.

ANMERKUNG: Netzredundanz besteht nur dann, wenn die Ladungsanforderungen nicht die Kapazität des schwächeren Stromnetzes übersteigen.

Netzredundanzstufen

Eine Netzteileinheit in jedem Netz ist die Minimalkonfiguration, die für die Verwendung als Netzredundanz notwendig ist. Zusätzliche Konfigurationen sind bei jeder Kombination möglich, die mindestens eine Netzteileinheit in jedem Netz aufweist. Um den maximal verfügbaren Strom jedoch nutzbar zu machen, sollte der Gesamtstrom der Netzteileinheiten in jedem Teil möglichst gleich sein. Die Stromobergrenze bei der Aufrechterhaltung der Wechselstromredundanz ist der Strom, der im schwächeren der beiden Netze verfügbar ist.

Falls der CMC aus irgendeinem Grund die Netzredundanz nicht aufrechterhalten kann, werden E-Mail- bzw. SNMP-Warnungen an die Administratoren gesendet, wenn das Ereignis „Redundanz verloren“ für Warnungen konfiguriert ist.

Wenn ein einzelnes Netzteil in dieser Konfiguration ausfällt, werden die verbleibenden Netzteile des ausgefallenen Netzes als „Online“ markiert. In diesem Zustand helfen die Netzteile, die sich im Status „Netzredundanz“ oder gar „Ausgefallen“ befinden, bei der Aufrechterhaltung eines unterbrechungsfreien Systembetriebs. Wenn ein Netzteil ausfällt, wird der Gehäusezustand als „Nicht kritisch“

markiert. Wenn das kleinere Netz die Summe der Gehäusestromzuteilungen nicht unterstützen kann, wird für den Wechselstromredundanzstatus **Keiner**, gemeldet, und der Gehäusezustand wird als **Kritisch** angezeigt.

Die Netzteilredundanz-Richtlinie

Der Netzteilredundanz-Richtlinie ist nützlich, wenn keine redundanten Stromnetze zur Verfügung stehen und Schutz gegen den Ausfall einer einzelnen Netzteileinheit erwünscht ist, um den Ausfall der Server in einem modularen Gehäuse zu vermeiden. Für diesen Zweck wird die Netzteileinheit mit der größten Kapazität als Onlinereserve gehalten. Das bildet einen Netzteilredundanzpool.

Etwaige über die für die Stromversorgung und Redundanz erforderlichen Netzteileinheiten sind weiterhin verfügbar und werden dem Pool im Falle eines Ausfalls hinzugefügt.

Im Gegensatz zur Netzredundanz erfordert der CMC bei ausgewählter Netzteilredundanz nicht, dass die Netzteile bestimmte Steckplatzpositionen einnehmen müssen.

ANMERKUNG: Dynamische Netzteilzuschaltung (DPSE) ermöglicht, dass Netzteileinheiten als Standby eingesetzt werden. Der Standby-Zustand zeigt einen physischen Zustand an (dass kein Strom geliefert wird). Bei Aktivierung von DPSE werden die zusätzlichen Netzteileinheiten in den Standby-Modus gesetzt, um die Effizienz zu erhöhen und Energie zu sparen.

ANMERKUNG: Ändern Sie die modulare Gehäuseredundanzregel, während das Gehäuse ausgeschaltet ist.

Dynamische Netzteil-Einsatzfähigkeit

Der Modus „Dynamische Zuschaltung von Netzteileinheiten“ (DPSE) ist standardmäßig deaktiviert. DPSE spart Strom, indem die Stromeffizienz der Netzteileinheiten optimiert wird, die das Gehäuse mit Strom versorgen. Dies führt zudem zu einer längeren Lebensdauer der Netzteileinheiten und geringerer Hitzeentwicklung. Um diese Funktion zu verwenden, müssen Sie eine Enterprise-Lizenz aufweisen.

Der CMC überwacht die Gesamtstromzuteilung des Gehäuses und versetzt die Netzteileinheiten in den Zustand Standby. So wird die Gesamtstromzuteilung des Gehäuses über weniger Netzteileinheiten erbracht. Da die Online-Netzteileinheiten effizienter sind, wenn sie mit höherer Ausnutzung laufen, verbessert dies ihre Effizienz. Außerdem erhöht sich die Lebensdauer der Standby-Netzteileinheiten.

Zum Betreiben der verbleibenden Netzteileinheiten mit maximaler Effizienz, verwenden Sie die folgenden Stromredundanzmodi:

- Der **Netzteilredundanz**modus mit dynamischer Zuschaltung von Netzteileinheiten (DPSE) bietet Energieeffizienz. Mindestens zwei Netzteileinheiten sind aktiv, wobei eine Netzteileinheit die Konfiguration versorgt und eine andere für Redundanz sorgt, falls eine Netzteileinheit ausfällt. Der Netzteileinheitredundanzmodus schützt vor dem Ausfall beliebiger Netzteileinheiten, bietet aber keinen Schutz bei einem Ausfall des Wechselstromnetzes.
- Beim Modus **Netzredundanz** mit dynamischer Zuschaltung von Netzteileinheiten (DPSE) sind mindestens zwei Netzteileinheiten aktiv, eine in jedem Stromnetz. Bei Netzredundanz besteht auch ein guter Ausgleich zwischen Effizienz und maximaler Verfügbarkeit für eine teilbelastete modulare Gehäusekonfiguration.
- Das Deaktivieren der dynamischen Zuschaltung von Netzteileinheiten bietet die geringste Effizienz, da alle vier Netzteileinheiten aktiv sind und die Last teilen. Dies führt zu einer schlechteren Ausnutzung der einzelnen Netzteile.

Die dynamische Zuschaltung von Netzteileinheiten (DPSE) kann für alle zwei oben erläuterten Redundanzkonfigurationen aktiviert werden – **Netzteilredundanz** und **Netzredundanz**.

ANMERKUNG: In einer Konfiguration mit zwei Netzteileinheiten kann die Serverlast verhindern, dass Netzteileinheiten in den Standbymodus gesetzt werden.

- In einer **Netzteilredundanz-**Konfiguration lässt das Gehäuse, neben den für die Versorgung des Gehäuses erforderlichen Netzteileinheiten, immer eine zusätzliche Netzteileinheit eingeschaltet und als **Online** markiert. Der Stromverbrauch wird überwacht. Je nach Gesamtsystemlast kann eine Netzteileinheit in den Standby-Zustand gesetzt werden. In einer Konfiguration mit vier Netzteileinheiten sind immer mindestens zwei Netzteileinheiten eingeschaltet.

  Da bei einem Gehäuse in der **Netzteilredundanz**-Konfiguration immer eine weitere Netzteileinheit eingeschaltet ist, kann das Gehäuse mit dem Verlust einer Online-Netzteileinheit auskommen und dennoch genügend Strom für die installierten Servermodule zur Verfügung haben. Der Verlust der Online-Netzteileinheit führt dazu, dass eine Standby-Netzteileinheit einspringt. Gleichzeitiges

Versagen mehrerer Netzteileinheiten kann zu Stromverlust für einige Servermodule führen, während die Standby-Netzteileinheiten eingeschaltet werden.

- Bei der Konfiguration **Netzredundanz** werden beim Einschalten des Gehäuses alle Netzteileinheiten in Betrieb genommen. Die Stromauslastung wird überwacht, und wenn es die Systemkonfiguration und die Stromauslastung erlauben, werden Netzteileinheiten in den **Standby**-Zustand versetzt. Da der **Online**-Status von Netzteileinheiten in einem Netz den des anderen Netzes widerspiegelt, kann das Gehäuse den Stromverlust eines gesamten Netzes ausgleichen, ohne die Stromversorgung des Gehäuses zu unterbrechen.

  Ein höherer Strombedarf in der Konfiguration **Netzredundanz** sorgt für die Zuschaltung von Netzteilen, die sich im **Standby**-Zustand befinden. So wird die gespiegelte Konfiguration beibehalten, die für die Doppelnetzredundanz notwendig ist.

ANMERKUNG: Wenn dynamische Zuschaltung von Netzteileinheiten (DPSE) aktiviert ist, werden die Standby-Netzteileinheiten Online genommen, um bei erhöhtem Bedarf in allen zwei Wechselstromredundanzmodi Strom anzufordern.

Standard-Redundanzkonfiguration

Wie in der folgenden Tabelle dargestellt, hängt die Standard-Redundanzkonfiguration eines Gehäuses von der Zahl der enthaltenen Netzteileinheiten ab

Tabelle 37. Standard-Redundanzkonfiguration

Konfiguration der Netzteileinheiten	Standard-Redundanzregel	Standardeinstellung für die dynamische Zuschaltung von Netzteileinheiten
Zwei Netzteile	Gleichstromredundanz	Deaktiviert
Vier Netzteile	Gleichstromredundanz	Deaktiviert

Netzredundanz

Im Netzredundanzmodus mit vier Netzteileinheiten sind alle vier Netzteileinheiten aktiv. Die zwei Netzteileinheiten müssen mit einen Wechselstromnetz verbunden sein, während die anderen zwei Netzteileinheiten mit dem anderen Wechselstromnetz verbunden sind.

VORSICHT: Um einen Systemfehler zu vermeiden und effizient funktionierende Netzredundanz zu gewährleisten, muss sichergestellt werden, dass es einen ausgeglichenen Satz von Netzteileinheiten gibt, der mit separaten Wechselstromkreisen verkabelt ist.

Falls ein Wechselstromnetz ausfällt, übernehmen die Netzteileinheiten des funktionierenden Wechselstromnetzes die Funktion, ohne dass Unterbrechungen für Server oder Infrastruktur auftreten.

VORSICHT: Im Netzredundanzmodus muss ein ausgeglichener Satz von Netzteileinheiten (mindestens eine Netzteileinheit pro Stromnetz) vorhanden sein. Wenn diese Bedingung nicht erfüllt wird, ist keine Netzredundanz möglich.

Netzteil-Redundanz

Wenn Netzteilredundanz aktiviert ist, befindet sich eine Ersatz-Netzteileinheit im Gehäuse. Diese stellt sicher, dass der Ausfall einer anderen Netzteileinheit nicht dazu führt, dass die Stromversorgung der Server oder des Gehäuses unterbrochen wird. Der Netzteilredundanzmodus erfordert mindestens zwei Netzteileinheiten. Weitere Netzteileinheiten, falls vorhanden, werden zur Verbesserung der Energieeffizienz des Systems eingesetzt, falls dynamische Zuschaltung von Netzteileinheiten (DPSE) aktiviert ist. Der Ausfall von Netzteilen nach Redundanzverlust kann ein Herunterfahren der Server im Gehäuse bewirken.

Strombudget für Hardwaremodule

Der CMC bietet einen Strombudgetdienst, mit dem Sie Strombudget, Redundanz sowie eine dynamische Stromversorgung für das Gehäuse konfigurieren können.

Mit dem Stromverwaltungsdienst kann der Stromverbrauch optimiert werden; den verschiedenen Modulen kann je nach Bedarf Strom neu zugewiesen werden.

Der CMC hält ein Strombudget für das Gehäuse ein, das die für alle installierten Server und Komponenten notwendige Wattleistung reserviert.

Der CMC teilt der CMC-Infrastruktur und den Servern im Gehäuse Strom zu. Die CMC-Infrastruktur besteht aus Komponenten im Gehäuse, z. B. Lüfter, E/A-Module, Speicheradapter, PCIe-Karten, physische Festplatten und Hauptplatine. Das Gehäuse kann bis zu vier Server aufweisen, die über den iDRAC mit dem Gehäuse kommunizieren. Weitere Informationen finden Sie im *iDRAC User's Guide* (iDRAC7-Benutzerhandbuch) unter **dell.com/support/manuals**.

Der iDRAC liefert dem CMC seine Strombereichsanforderungen vor Einschalten des Servers. Der Strombereich besteht aus den maximalen und minimalen Stromanforderungen, die für den Betrieb des Servers erforderlich sind. Die erste Schätzung vom iDRAC basiert auf seinem anfänglichen Verständnis der Komponenten im Server. Nach dem Start und wenn weitere Komponenten erkannt werden, kann iDRAC seine anfänglichen Stromanforderungen erhöhen oder verringern.

Wenn ein Server in einem Gehäuse eingeschaltet wird, schätzt die iDRAC-Software die Stromanforderungen neu ein und fordert eine nachfolgende Änderung des Strombereichs an.

CMC liefert dem Server den angeforderten Strom und die zugeteilte Wattleistung wird vom verfügbaren Budget abgezogen. Sobald dem Server eine Stromanforderung gewährt wurde, kontrolliert die iDRAC-Software des Servers fortlaufend den tatsächlichen Stromverbrauch. Der iDRAC-Strombereich kann, basierend auf den tatsächlichen Stromanforderungen, sich im Lauf der Zeit ändern. Der iDRAC verlangt eine Stromerhöhung, wenn die Server den zugeteilten Strom vollständig verbrauchen.

Bei starker Belastung kann die Leistung des Serverprozessors herabgesetzt werden, um sicherzustellen, dass der Stromverbrauch unter der vom Benutzer konfigurierten Systemeingangsstromobergrenze bleibt.

Das PowerEdge VRTX-Gehäuse kann ausreichend Strom für die Spitzenleistung der meisten Serverkonfigurationen bereitstellen, aber viele verfügbare Serverkonfigurationen verbrauchen nicht die maximale Strommenge, die das Gehäuse liefern kann. Um Rechenzentren bei der Stromzuweisung für ihre Gehäuse zu unterstützen, erlaubt VRTX dem Benutzer, eine Systemeingangsstromobergrenze anzugeben. Damit kann sichergestellt werden, dass der Gesamt-Wechselstromverbrauch des Gehäuses innerhalb eines festgelegten Schwellenwerts bleibt. Zunächst stellt der CMC sicher, dass ausreichend Strom für die Lüfter, E/A-Module, Speicheradapter, physisches Festplattenlaufwerk, Hauptplatine, und den CMC selbst verfügbar ist. Diese Stromzuteilung wird als der Gehäuseinfrastruktur zugewiesener Eingangsstrom bezeichnet. Nach der Gehäuseinfrastruktur werden die Server in einem Gehäuse eingeschaltet. Jeder Versuch, die Systemeingangsstromobergrenze unter der „Strombelastung" anzusetzen, schlägt fehl. „Strombelastung" ist die Stromsumme, die der Gehäuseinfrastruktur zugeteilt wurde und der Mindeststrom, der den eingeschalteten Servern zugeteilt wurde.

ANMERKUNG: Um die Funktion „Stromobergrenze" zu aktivieren, müssen Sie eineEnterprise-Lizenz aufweisen.

Wenn es für das Gesamtstrombudget erforderlich ist, unter dem Wert der *Systemeingangsstromobergrenze* zu bleiben, teilt der CMC den Servern einen Wert zu, der unter der maximal angeforderten Strommenge liegt. Strom wird den Servern basierend auf ihrer *Server-Priorität* zugeteilt: Server der Priorität 1 erhalten die maximale Strommenge vor Servern der Priorität 2 usw. Server mit niedrigerer Priorität erhalten basierend auf der Einstellung *Maximale Systemeingangskapazität* und der benutzerdefinierten Einstellung *Systemeingangsstromobergrenze* möglicherweise weniger Strom als Server der Priorität 1.

Konfigurationsänderungen, z. B. ein zusätzlicher Server, freigegebene HDDs oder PCIe-Karten iim Gehäuse erfordern u. U., dass die *Systemeingangsstromobergrenze* erhöht wird. Der Strombedarf in einem modularen Gehäuse steigt ebenfalls, wenn sich die Temperatur ändert und die Lüfter mit höherer Geschwindigkeit laufen müssen, wodurch sie mehr Strom verbrauchen. Der Einbau vonE/A-Modulen und Speicheradaptern, PCIe-Karten, physischer Festplatte, Hauptplatine; auch die Nummer, der Typ und die Konfiguration von PSUs erhöht den Strombedarf des modularen Gehäuses ebenfalls. Eine geringe Menge Strom wird selbst von ausgeschalteten Servern verbraucht, um die Funktion des Management-Controllers aufrechtzuerhalten.

Zusätzliche Server können nur dann in einem modularen Gehäuse gestartet werden, wenn ausreichend Strom verfügbar ist. Die *Systemeingangsstromgrenze* kann jederzeit bis zu einem Maximalwert von 5000 Watt erhöht werden, um das Einschalten von zusätzlichen Servern zu ermöglichen.

Änderungen im modularen Gehäuse, die die Stromzuteilung verringern, sind:

- Server ausgeschaltet
- E/A Modul ausgeschaltet
- Speicheradapter, PCIe-Karten, physisches Festplattenlaufwerk und Hauptplatine ausgeschaltet
- Gehäuse in einen ausgeschalteten Zustand versetzen

Die *Systemeingangsstromobergrenze* kann neu konfiguriert werden, wenn das Gehäuse eingeschaltet oder ausgeschaltet ist.

Serversteckplatz-Stromprioritätseinstellungen

Der CMC ermöglicht es Ihnen, eine Strompriorität für jeden der vier Serversteckplätze eines Gehäuses festzulegen. Die Prioritätseinstellungen gehen von 1 (höchste) bis 9 (niedrigste). Diese Einstellungen werden Steckplätzen des Gehäuses zugewiesen. Die Priorität des Steckplatzes trifft für jeden Server zu, der diesen Steckplatz später belegt. Der CMC verwendet die Steckplatzpriorität, um vorzugsweise den Servern mit der höchsten Priorität Strom zuzuweisen.

Der Strom wird gemäß der Standard-Serversteckplatzpriorität gleichmäßig auf alle Steckplätze verteilt. Durch die Änderung der Steckplatzpriorität können Administratoren festlegen, welche Server bei der Stromzuteilung bevorzugt werden sollen. Wenn für die kritischeren Servermodule die Standard-Steckplatzpriorität von 1 beibehalten wird und die Priorität der weniger kritischen Servermodule auf den Prioritätswert 2 oder niedriger gesetzt werden, werden die Servermodule mit der Priorität 1 zuerst hochgefahren. Diese Server mit höherer Priorität erhalten ihre maximale Stromzuteilung, während die Server mit niedrigerer Priorität eventuell nicht genug Strom erhalten, um ihre maximale Leistung zu erbringen. Sie könnten sogar ausgeschaltet bleiben, je nachdem, wie niedrig der Wert für die Systemeingangsstromobergrenze gesetzt ist und wie die Stromanforderung des Servers lauten.

Wenn ein Administrator die Server mit niedriger Priorität manuell vor denen mit höherer Priorität einschaltet, dann wird die Stromzuteilung der Server mit niedriger Priorität als erstes auf deren Mindestwert zurückgefahren, damit die Server mit höherer Priorität versorgt werden können. Wenn der verfügbare Strom aufgebraucht ist, fordert der CMC den Strom von den Servern mit niedriger oder gleicher Priorität zurück, bis sie an ihrem Mindestleistungsniveau angelangt sind.

ANMERKUNG: E/A-Module, Lüfter und Hauptplatine, physische Festplattenlaufwerke und Speicheradapter erhalten die höchste Priorität. Der CMC fordert Strom nur von Geräten mit niedrigerer Priorität zurück, um den Strombedarf eines Geräts mit höherer Priorität oder eines Servers zu erfüllen.

Vergabe von Prioritätsstufen an Server

Über Server-Prioritätsstufen wird festgelegt, von welchen Servern das CMC-Modul bei zusätzlichem Strombedarf Strom bezieht.

ANMERKUNG: Die Priorität, die Sie einem Server zuweisen, ist nicht an den Server selbst, sondern an den Serversteckplatz gekoppelt. Wenn der Server an einen anderen Steckplatz verlegt wird, müssen Sie die Priorität für den neuen Steckplatz erneut konfigurieren.

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, müssen Sie die Berechtigung als Gehäusekonfigurations-Administrator besitzen.

Zuweisung der Prioritätsstufen an Server unter Verwendung der CMC-Webschnittstelle

So weisen Sie Prioritätsstufen zu:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Strom** > **Priorität**.
Die Seite **Serverpriorität** führt alle Server in dem Gehäuse auf.

2 Wählen Sie aus dem Drop-Down-Menü **Priorität** für einen, mehrere oder alle Server eine Prioritätsstufe von 1 bis 9 aus, wobei 1 die höchste Prioritätsstufe ist. Der Standardwert ist 1. Sie können mehreren Servern dieselbe Prioritätsstufe zuweisen.

3 Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

Vergabe von Prioritätsstufen an Server, die RACADM benutzen

Öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC, melden Sie sich an und geben Sie Folgendes ein:

```
racadm config -g cfgServerInfo -o cfgServer Priority -i <Steckplatznummer> <Prioritätsstufe>
```

wobei sich <*Steckplatznummer*> (1-4) auf die Position des Servers bezieht und der Wert für die <*Prioritätsstufe*> zwischen 1 und 9 liegt.

Beispiel: Um die Prioritätsstufe 1 für den Server in Steckplatz 4 einzustellen, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgServerInfo -o cfgServerPriority -i 4 1
```

Anzeige des Stromverbrauchsstatus

Der CMC zeigt den tatsächlichen Eingangsstromverbrauch für das gesamte System auf der Seite Stromverbrauchsstatus an.

Anzeigen von Stromverbrauchsstatus über die CMC-Webschnittstelle

Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Strom** > **Stromüberwachung**. Die Seite „Stromüberwachung“ zeigt Stromfunktionszustand, Systemstromstatus, Stromstatistik in Echtzeit und Energiestatistik in Echtzeit an. Weitere Informationen finden Sie in der *Online-Hilfe*.

ANMERKUNG: Der Stromredundanzstatus wird auch unter Netzteile angezeigt.

Anzeigen des Stromverbrauchsstatus mithilfe von RACADM

So zeigen Sie den Stromverbrauchsstatus mithilfe von RACADM an:

Öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC, melden Sie sich an und geben Sie Folgendes ein:

```
racadm getpminfo
```

AC Power Recovery (Netzstromwiederherstellung)

Falls die Netzstromversorgung eines Systems unterbrochen wird, wird das Gehäuse in den Stromzustand zurückversetzt, in dem es sich vor dem Ausfall der Netzstromversorgung befand. Die Wiederherstellung des vorherigen Stromzustandes entspricht dem Standard-Funktionszustand. Die nachfolgenden Faktoren können zu einer Unterbrechung führen:

- Stromausfall
- Trennen der Netzkabel von den Netzteileinheiten (PSUs)
- Ausfall der Stromverteilungseinheit (PDU)

Wenn die Optionen **Budget/Redundanzkonfiguration** > **Netzstromwiederherstellung deaktivieren** ausgewählt sind, bleibt das Gehäuse nach der Wiederherstellung der Netzstromversorgung ausgeschaltet.

Falls die Blade-Server nicht für das automatische Einschalten konfiguriert sind, müssen Sie sie manuell einschalten.

Strombudgetstatus über die CMC-Webschnittstelle anzeigen

Um Strombudgetstatus über die CMC-Webschnittstelle anzuzeigen, wählen Sie im linken Fensterbereich **Gehäuse-Übersicht** aus und klicken Sie auf **Strom** > **Budgetstatus**. Auf der Seite **Strombudgetstatus** werden die Regelkonfiguration des Systemstroms, Strombudgetdetails, Budgetzuweisung für die Servermodule und Informationen über das Netzteil des Gehäuses angezeigt. Weitere Informationen finden Sie unter *Online-Hilfe*.

Stromverbrauchsstatus mithilfe von RACADM anzeigen

Öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC, melden Sie sich an und geben Sie Folgendes ein:

```
racadm getpbinfo
```

Weitere Informationen über **getpbinfo**, einschließlich Ausgabedetails finden Sie im Befehlsabschnitt **getpbinfo** im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

Redundanzstatus und allgemeiner Stromzustand

Der Redundanzstatus ist ein Faktor beim Bestimmen des allgemeinen Stromzustands. Wenn die Stromredundanzregel festgelegt ist, zum Beispiel auf Netzredundanz, und der Redundanzstatus anzeigt, dass das System mit Redundanz arbeitet, ist der allgemeine Stromzustand in der Regel **OK**. Wenn das auf einem Gehäuse installierte Netzteil aus irgendeinem Grund ausfällt, wird der allgemeine Stromzustand des Gehäuses als **Non-Critical** (Nicht-kritisch) angezeigt. Wenn jedoch die Bedingungen für den Betrieb mit Netzredundanz nicht erfüllt werden können, ist der Redundanzstatus **No** (Keine) und der allgemeine Stromzustand **Critical** (Kritisch). Der Grund dafür ist, dass das System nicht in Übereinstimmung mit der konfigurierten Redundanzregel funktionieren kann.

ANMERKUNG: Der CMC führt keine Vorabprüfung dieser Bedingungen durch, wenn Sie die Redundanzregel auf oder von „Netzredundanz“ ändern. Das Konfigurieren der Redundanzregel kann demzufolge unverzüglich zu Redundanzverlust oder zu einer wiedererlangten Bedingung führen.

Stromverwaltung nach Entdeckung von Netzteilfehlern

Wenn das Ereignis „unzureichende Stromversorgung“ auftritt, z. B. der Ausfall einer Netzteileinheit, verringert der CMC die Stromzufuhr zu Servern. Nachdem der Strom verringert wurde, berechnet der CMC den Strombedarf des Gehäuses neu. Falls die Stromanforderungen nach wie vor nicht erfüllt werden, schaltet der CMC die Server mit niedriger Priorität aus. Dies wird jedoch auf Grundlage der Stromredundanzregel, die sie auf Ihrem CMC eingestellt haben, ausgeführt. Ein redundanter Server kann Stromverlust ohne Beeinträchtigung der Leistung der Server verkraften.

Der Strom für Server mit höherer Priorität wird stufenweise wiederhergestellt, wobei der Strombedarf innerhalb des Strombudgets verbleibt. Informationen, um die Redundanzregel festzulegen, finden Sie unter Konfiguration von Stromversorgungsbudget und Redundanz.

Stromverwaltung nach Entfernung des Netzteils

Der CMC kann beginnen, Strom zu sparen, wenn Sie eine Netzteileinheit entfernen oder ein Netzteileinheit-Stromkabel entfernen. Der CMC verringert die Stromzufuhr zu den Servern mit niedriger Priorität, bis der Stromverbrauch von den verbleibenden Netzteileinheiten im Gehäuse unterstützt wird. Wenn Sie mehr als eine Netzteileinheit entfernen, berechnet der CMC den Strombedarf neu, wenn die zweite Netzteileinheit entfernt wird, um die Reaktion der Firmware zu bestimmen. Falls die Stromanforderungen nach wie vor nicht erfüllt werden, schaltet der CMC u. U. auch die Server mit niedriger Priorität aus.

Grenzen

- Der CMC unterstützt ein *automatisches* Herunterfahren von Servern mit niedriger Priorität nicht, um einen Server mit höherer Priorität einzuschalten; ein Ausschalten kann jedoch vom Benutzer initiiert und ausgeführt werden.
- Änderungen der Redundanzregel der Netzteileinheiten sind durch die Anzahl der Netzteileinheiten im Gehäuse begrenzt. Sie können eine beliebige der zwei in der Liste aufgeführten Redundanzkonfigurationseinstellungen von Netzteileinheiten unter Standard-Redundanzkonfiguration auswählen.

Regel zur Zuschaltung neuer Server

Wenn ein neuer Server eingeschaltet wird, der den verfügbaren Strom für das Gehäuse überschreitet, kann der CMC die Stromzufuhr zu Servern mit niedriger Priorität verringern. Dies kann eintreten, wenn der Administrator eine Stromgrenze für das Gehäuse konfiguriert hat, die unter dem Wert liegt, der für eine vollständige Stromzuweisung für den Server nötig wäre, oder wenn unzureichend Strom verfügbar ist im Falle von höheren Stromanforderungen von allen Servern im Gehäuse. Wenn durch die Reduktion des zugewiesenen Stroms der Server mit niedriger Priorität nicht genügend Strom freigesetzt werden kann, kann der neue Server nicht gestartet werden.

Dies kann eintreten, wenn der Administrator eine Stromgrenze für das Gehäuse konfiguriert hat, die unter dem Wert liegt, der für eine vollständige Stromzuweisung für die Server nötig wäre, oder wenn unzureichend Strom für Server, die hohen Strom erfordern, verfügbar ist.

Die folgende Tabelle beschreibt die vom CMC ergriffenen Maßnahmen, wenn ein neuer Server im oben beschriebenen Szenario eingeschaltet wird.

Tabelle 38. CMC-Reaktion, beim Einschaltversuch eines Servers

Strom für den ungünstigsten Fall ist verfügbar	CMC-Reaktion	Server einschalten
Ja	Keine Stromeinsparung erforderlich	Zugelassen
Nein	Stromeinsparung ausführen:	Zugelassen
	• Für neuen Server benötigter Strom ist verfügbar • Für neuen Server benötigter Strom ist nicht verfügbar	Nicht zulässig

Wenn eine Netzteileinheit ausfällt, ergibt sich ein nicht-kritischer Funktionszustand und es wird ein Netzteileinheit-Ausfallereignis erzeugt. Die Entfernung einer Netzteileinheit führt zu einem Netzteileinheiten-Entfernungsereignis.

Wenn eines der beiden Ereignisse aufgrund von Stromzuteilungen zu Redundanzverlust führt, wird ein *Redundanzverlust*-Ereignis erzeugt.

Wenn nachfolgend die Stromkapazität oder die Benutzer-Stromkapazität größer ist als die Serverzuteilungen, werden Server geringere Leistung erbringen oder können im extremen Fall ausgeschaltet werden. Beide Bedingungen wirken sich zuerst auf Server mit niedriger Priorität aus, welches bedeutet, dass die Server mit niedriger Priorität zuerst ausgeschaltet werden.

Die folgende Tabelle beschreibt die Firmware-Reaktion, wenn eine Netzteileinheit ausgeschaltet oder entfernt wird, hinsichtlich verschiedener Redundanzkonfigurationen von Netzteileinheiten.

Tabelle 39. Auswirkung auf das Gehäuse bei Ausfall oder Entfernung einer Netzteileinheit

Konfiguration der Netzteileinheiten	Dynamische Zuschaltung von Netzteileinheiten	Firmware-Reaktion
Netzredundanz	Disabled (Deaktiviert)	Der CMC alarmiert Sie über den Verlust der Netzredundanz.
Netzteil-Redundanz	Disabled (Deaktiviert)	Der CMC alarmiert Sie über den Verlust der Netzteilredundanz.

Konfiguration der Netzteileinheiten	Dynamische Zuschaltung von Netzteileinheiten	Firmware-Reaktion
Netzredundanz	Enabled (Aktiviert)	Der CMC alarmiert Sie über den Verlust der Netzredundanz. Netzteile im Standby-Modus (wenn vorhanden) werden eingeschaltet, um den Stromverlust in Folge eines Netzteileinheitfehlers oder -ausfalls zu kompensieren.
Netzteil-Redundanz	Enabled (Aktiviert)	Der CMC alarmiert bei Verlust der Netzteilredundanz. Netzteile im Standby-Modus (wenn vorhanden) werden eingeschaltet, um den Stromverlust in Folge eines Netzteileinheitfehlers oder -ausfalls zu kompensieren.

Netzteil- und Redundanzregeländerungen im Systemereignisprotokoll

Änderungen des Netzteilzustands und der Stromredundanzregeln werden als Ereignisse protokolliert. Ereignisse, die mit den Netzteilen zusammenhängen und Einträge im Systemereignisprotokoll (SEL) verursachen, sind Hinzufügen und Entfernen von Netzteilen, Hinzufügen und Entfernen der Netzteileingangsleistung sowie Aussagen zur Netzteilausgangsleistung sowie deren Rücknahme.

Die folgende Tabelle listet die SEL-Einträge auf, die mit Netzteiländerungen zusammenhängen:

Tabelle 40. SEL-Ereignisse für Netzteiländerungen

Netzteilereignis	Systemereignisprotokoll (SEL)-Eintrag
Einfügen	Netzteil ist vorhanden.
Entfernung	Netzteil ist nicht vorhanden.
Wechselstromeingang	Die Stromzufuhr vom Netzteil wurde wiederhergestellt.
Wechselstrom-Eingangsverlust	Verlust der Stromzufuhr vom Netzteil.
Gleichstromausgabe hergestellt	Netzteil funktioniert normal.
Gleichstromausgabeverlust	Netzteil fehlerhaft.

Ereignisse, die mit Änderungen des Stromredundanzstatus zusammenhängen und Einträge im SEL verursachen, sind Redundanzverlust und Redundanzwiederherstellung für das modulare Gehäuse, das entweder für eine **Netzredundanz**regel oder eine **Netzteilredundanz**regel konfiguriert ist. Die folgende Tabelle listet die SEL-Einträge auf, die mit Änderungen der Stromredundanzregeln zusammenhängen.

Tabelle 41. SEL-Ereignisse für Änderungen der Stromredundanzregeln

Stromregelereignis	Systemereignisprotokoll (SEL)-Eintrag
Redundanzverlust	Verlust der Netzteilredundanz.
Redundanz wiederhergestellt	Die Netzteile sind redundant.

Konfigurieren von Strombudget und Redundanz

Sie können das Strombudget, die Redundanz und die dynamische Energie des gesamten Gehäuses (Gehäuse, Server, E/A-Modul, KVM, CMC und Netzteile) konfigurieren, das vier Netzteileinheiten (PSUs) verwendet. Der Stromverwaltungsdienst optimiert den Stromverbrauch und weist den verschiedenen Modulen entsprechend den Anforderungen Strom zu.

Sie können Folgendes konfigurieren:

- Systemeingangsstrom-Obergrenze

- Redundanzregel
- Dynamische Netzteil-Einsatzfähigkeit aktivieren
- Netzschalter des Gehäuses deaktivieren
- Max. Stromkonservierungsmodus
- Remote-Stromprotokollierung
- Remote-Stromverbrauchsprotokollierungszeitraum
- Serverbasierte Stromverwaltung
- Netzstromwiederherstellung deaktivieren

Stromeinsparung und Strombudget

Der CMC kann Strom einsparen, wenn die vom Benutzer konfigurierte maximale Stromgrenze erreicht ist. Wenn der Strombedarf die benutzerdefinierte Systemeingangsstromobergrenze überschreitet, verringert der CMC die Stromzufuhr zu den Servern mit niedriger Priorität, um Strom für Server und andere Module mit höherer Priorität im Gehäuse freizugeben.

Wenn alle oder mehrere Steckplätze im Gehäuse mit derselben Prioritätsstufe konfiguriert sind, verringert der CMC die Stromzufuhr zu den Servern in aufsteigender Steckplatznummernfolge. Beispiel: Wenn die Server in Steckplatz 1 und 2 dieselbe Prioritätsstufe haben, wird die Stromzufuhr für den Server in Steckplatz 1 verringert, bevor die Stromzufuhr für den Server in Steckplatz 2 verringert wird.

ANMERKUNG: Sie können jedem der Server im Gehäuse eine Prioritätsstufe zuweisen, indem Sie ihm eine Nummer von 1 bis einschließlich 9 geben. Die Standardprioritätsstufe für alle Server ist 1. Je niedriger die Zahl, desto höher die Prioritätsstufe.

Das Strombudget ist auf einen Maximalwert begrenzt, der anhand des jeweils schwächsten Satzes von zwei Netzteileinheiten bestimmt wird. Wenn versucht wird, einen Wechselstrombudgetwert festzulegen, der die *Systemeingangsstromobergrenze* überschreitet, zeigt das CMC-Modul eine Meldung an. Das Strombudget ist auf 4800W begrenzt.

Maximaler Stromsparmodus

Dieser ist aktiviert für den Netzredundanz- oder den Netzteilredundanzmodus. Der CMC sorgt für maximale Stromeinsparung, wenn:

- Der maximale Stromsparmodus aktiviert ist.
- Ein von einem UPS-Gerät automatisch ausgegebenes Befehlszeilenskript den maximalen Sparmodus aktiviert.

Im maximalen Stromsparmodus starten alle Server mit Minimalstrom und alle nachfolgenden Stromzuteilungsanforderungen von Servern werden abgelehnt. In diesem Modus kann es sein, dass die Leistung der eingeschalteten Server herabgesetzt ist. Zusätzliche Server können nicht eingeschaltet werden, unabhängig von deren Priorität.

Die volle Systemleistung wird wieder hergestellt, wenn der maximale Stromsparmodus aufgehoben wird.

ANMERKUNG: Wenn der maximale Stromsparmodus (Maximum Power Conversation Mode, MPCM) auf dem Gehäuse aktiviert wird, werden alle Energieanforderungen von einem Blade-Server verweigert. Der Blade-Server wird nicht eingeschaltet, wenn eine Aktion im iDRAC oder Blade-Server vorliegt, die verlangt, dass der Host den Energiezyklus startet.

Herabsetzen des Serverstroms zur Einhaltung des Strombudgets

Der CMC reduziert Stromzuteilungen von Servern mit niedriger Priorität, wenn zusätzlicher Strom erforderlich ist, um den Systemstromverbrauch unterhalb der benutzerdefinierten *Systemeingangsstromobergrenze* zu halten. Wenn beispielsweise ein neuer Server zugeschaltet wird, kann der CMC die Stromzufuhr zu Servern mit niedriger Priorität verringern, um den neuen Server mit mehr Strom zu versorgen. Wenn die Strommenge nach der Verringerung der Stromzuteilung zu Servern mit niedriger Priorität nach wie vor nicht

ausreicht, drosselt der CMC die Server mit höherer Priorität bis ausreichend Strom freigegeben ist, um den neuen Server mit Strom zu versorgen.

Der CMC reduziert Server-Stromzuteilung in zwei Fällen:

- Der Gesamtstromverbrauch übersteigt die konfigurierbare *Systemeingangsstromobergrenze*.
- Ein Stromausfall tritt in einer nicht-redundanten Konfiguration auf.

110V Netzteileinheiten Wechselstrom-Betrieb

Standardmäßig ist die Netzteilbetriebsfunktion von 110V Wechselstrom verfügbar. Ein Mischbetrieb bei 110 V und 220 V wird jedoch nicht unterstützt. Wenn der CMC erkennt, dass beide Spannungen verwendet werden, dann wird eine ausgewählt und die Netzteile, die an die andere Spannung angeschlossen sind, werden ausgeschaltet und als „Fehlgeschlagen" markiert.

Remote-Protokollierung

Der Stromverbrauch kann einem Remote-Syslog-Server gemeldet werden. Es kann der Gesamtstromverbrauch des Gehäuses, der mimimale, maximale und der durchschnittliche Stromverbrauch über einen Erfassungszeitraum hinweg protokolliert werden. Lesen Sie für weitere Informationen zur Aktivierung dieser Funktion und zur Konfiguration des Erfassungs- oder Protokollierungszeitraums Energieverwaltung und -überwachung.

Externe Energieverwaltung

Die CMC-Energieverwaltung wird optional über die OpenManage Stromverwaltung (OMPC) gesteuert. Weitere Informationen finden Sie im *OMPC User's Guide* (OMPC Benutzerhandbuch).

Wenn eine externe Energieverwaltung aktiviert ist, verwaltet OMPC die folgenden Aktivitäten:

- Server-Stromversorgung für unterstützte VRTX-Server
- Server-Priorität unterstützter VRTX-Server
- Eingangsstromkapazität des Systems
- Maximaler Stromsparmodus

CMC setzt die Aufrechterhaltung oder Verwaltung der folgenden Aktivitäten fort:

- Redundanzregel
- Remote-Stromprotokollierung
- Serverleistung über Stromredundanz
- Dynamische Netzteil-Einsatzfähigkeit

OPMC verwaltet daraufhin die Priorisierung und die Stromversorgung für unterstützte VRTX-Server-Knoten mithilfe des Budgets, das nach der Zuteilung der Energie auf die Gehäuseinfrastruktur und vor der Generierung von Server-Knoten zur Verfügung steht. Die Remote-Energieprotokollierung ist von der externen Energieverwaltung nicht betroffen.

Nachdem der serverbasierte Energieverwaltungsmodus aktiviert wurde, ist das Gehäuse auf die PM3-Verwaltung vorbereitet. Die Prioritäten für alle unterstützten VRTX-Server sind auf „1" (Hoch) gesetzt. PM3 verwaltet die Server-Stromversorgung und die Prioritäten direkt. Da PM3 kompatible Serverstromversorgungszuweisungen steuert, steuert CMC nicht mehr den maximalen Stromsparmodus. Damit ist diese Option nicht mehr auswählbar.

Wenn der **maximale Stromsparmodus** aktiviert ist, setzt CMC die Eingangsstromkapazität des Systems auf den Maximalwert, den das Gehäuse verarbeiten kann. Bei CMC darf die Stromversorgung die höchst mögliche Kapazität nicht überschreiten. PM3 verarbeitet jedoch alle anderen Beschränkungen bei der Stromkapazität.

Wenn die Stromversorgung über die PM3-Verwaltung deaktiviert ist, geht CMC zu den Serverprioritätseinstellungen zurück, die vor der Aktivierung der externen Verwaltung gültig waren.

ANMERKUNG: Wenn die Verwaltung über PM3 deaktiviert ist, geht CMC nicht zur einer älteren Einstellung für die maximale Stromversorgung des Gehäuses zurück. Weitere Informationen zur früheren Einstellung für die manuelle Wiederherstellung des Wertes finden Sie im CMC-Protokoll.

Konfigurieren von Stromversorgungsbudget und Redundanz über die CMC-Webschnittstelle

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, müssen Sie die Berechtigung als Gehäusekonfigurations-Administrator besitzen.

So konfigurieren Sie das Strombudget

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Strom** > **Konfiguration**.

2 Wählen Sie auf der Seite **Budget/Redundanzkonfiguration** jede oder alle der folgenden Eigenschaften, Ihren Anforderungen entsprechend, aus. Weitere Informationen zu den Feldbeschreibungen finden Sie in der *Online-Hilfe*.

- **Serverbasierte Stromverwaltung aktivieren**
- **Systemeingangsstrom-Obergrenze**
- **Redundanzregel**
- **Dynamische Netzteil-Einsatzfähigkeit aktivieren**
- **Netzschalter des Gehäuses deaktivieren**
- **Max. Stromkonservierungsmodus**
- **Remote-Stromprotokollierung aktivieren**
- **Remote-Stromverbrauchsprotokollierungszeitraum**

3 Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

Strombudget und Redundanz unter Verwendung von RACADM konfigurieren

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, müssen Sie die Berechtigung als Gehäusekonfigurations-Administrator besitzen.

So aktivieren Sie die Redundanz und legen die Redundanzregel fest:

1 Öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC und melden Sie sich an.

2 Legen Sie die Eigenschaften nach Bedarf fest:

- Um eine Redundanzregel auszuwählen, geben Sie Folgendes ein:

```
racadm config -g cfgChassisPower -o
cfgChassisRedundancyPolicy <value>
```

wobei <*Wert*> = 1 (Grid-Redundanz) und 2 (Netzteilredundanz) lautet. Der Standardwert ist 2.

Zum Beispiel legt der folgende Befehl die Redundanzregel auf 1 fest:

```
racadm config -g cfgChassisPower -o
cfgChassisRedundancyPolicy 1
```

- Um einen Wechselstrombudgetwert festzulegen, geben Sie Folgendes ein:

```
racadm config -g cfgChassisPower -o
cfgChassisPowerCap <value>
```

wobei <*value*> eine Zahl zwischen 938 W – 4800 W ist und die maximale Stromgrenze in Watt angibt. Die Standardeinstellung ist 4800.

Der folgende Befehl setzt zum Beispiel das maximale Strombudget mit 4800 Watt fest:

```
racadm config -g cfgChassisPower -o
cfgChassisPowerCap 4800
```

- Um die dynamische Zuschaltung von Netzteileinheiten zu aktivieren oder deaktivieren, geben Sie Folgendes ein:

```
racadm config -g cfgChassisPower -o
cfgChassisDynamicPSUEngagementEnable <value>
```

wobei der <*Wert*> 0 für „deaktivieren“ und 1 für „aktivieren“ steht. Der Standardwert ist 0.

Der folgende Befehl deaktiviert zum Beispiel die dynamische Zuschaltung von Netzteileinheiten:

```
racadm config -g cfgChassisPower -o
cfgChassisDynamicPSUEngagementEnable 0
```

- Um den Modus für maximalen Stromverbrauch zu aktivieren, geben Sie Folgendes ein:

```
racadm config -g cfgChassisPower -o
cfgChassisMaxPowerConservationMode 1
```

- Um den Normalbetrieb wiederherzustellen, geben Sie Folgendes ein:

```
racadm config -g cfgChassisPower -o
cfgChassisMaxPowerConservationMode 0
```

- Geben Sie zur Aktivierung der Remote-Stromverbrauchsprotokollierungsfunktion den folgenden Befehl ein:

```
racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogPowerLoggingEnabled 1
```

- Geben Sie zur Angabe des gewünschten Protokollierungszeitraums den folgenden Befehl ein:

```
racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogPowerLoggingInterval n
```

wobei *n* 1-1440 Minuten sein kann.

- Geben Sie zur Bestimmung dessen, ob die Remote-Stromverbrauchsprotokollierungsfunktion aktiviert ist den folgenden Befehl ein:

```
racadm getconfig -g cfgRemoteHosts -o
cfgRhostsSyslogPowerLoggingEnabled
```

- Geben Sie zur Bestimmung des Remote-Stromverbrauchsprotokollierungszeitraums den folgenden Befehl ein:

```
racadm getconfig -g cfgRemoteHosts -o
cfgRhostsSyslogPowerLoggingInterval
```

Die Remote-Stromverbrauchsprotokollierungsfunktion hängt von den bereits konfigurierten Remote-Syslog-Hosts ab. Die Protokollierung auf einem oder mehreren Remote-Syslog-Hosts muss aktiviert sein, anderenfalls wird der Stromverbrauch nicht protokolliert. Dies kann entweder mittels der Web-GUI oder RACADM-CLI erfolgen. Weitere Informationen finden Sie in der Anleitung zur Remote-Syslog-Konfiguration.

- Um die Remote-Energieverwaltung durch Open Manage Power Center (OPMC) zu aktivieren, geben Sie Folgendes ein:

```
racadm config -g cfgChassisPower -o
cfgChassisServerBasedPowerMgmtMode 1
```

- Um die CMC-Energieverwaltung wiederherzustellen, geben Sie Folgendes ein:

```
racadm config -g cfgChassisPower -o
cfgChassisServerBasedPowerMgmtMode 0
```

Weitere Informationen zu den RACADM-Befehlen für die Gehäusestromversorgung finden Sie in den Abschnitten **config**, **getconfig**, **getpbinfo** und **cfgChassisPower** im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

Stromsteuerungsvorgänge ausführen

Sie können den folgenden Stromsteuerungsvorgang für das Gehäuse, Server und die E/A-Module ausführen.

ANMERKUNG: Stromsteuerungsvorgänge wirken sich auf das gesamte Gehäuse aus.

Durchführen von Energieverwaltungsmaßnahmen am Gehäuse

Mit dem CMC können Sie im Remote-Zugriff verschiedene Stromverwaltungsmaßnahmen auf dem gesamten Gehäuse (Gehäuse, Server, E/A-Module und Netzteileinheiten) ausführen, z. B. ordnungsgemäßes Herunterfahren.

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, müssen Sie die Berechtigung als Gehäusekonfigurations-Administrator besitzen.

Energieverwaltungsmaßnahmen am Gehäuse über die Webschnittstelle durchführen

So führen Sie auf dem Gehäuse Stromsteuerungsvorgänge unter Verwendung der CMC-Webschnittstelle durch:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Strom** > **Steuerung**.
Die Seite **Gehäuse-Stromsteuerung** wird angezeigt.

2 Wählen Sie eine der folgenden Stromsteuerungsoptionen aus.
Weitere Informationen zu jeder Option finden Sie in der *Online-Hilfe*.
- **System einschalten**
- **System ausschalten**
- **System aus- und wieder einschalten (Hardwareneustart)**
- **Reset CMC (Warmstart)**
- **Nicht-ordentliches Herunterfahren**

3 Klicken Sie auf **Anwenden**.
Ein Dialogfeld wird eingeblendet, das Sie zur Bestätigung auffordert.

4 Klicken Sie auf **OK**, um die Energieverwaltungsmaßnahme auszuführen (z. B. das System zurückzusetzen).

Energieverwaltungsmaßnahmen am Gehäuse über RACADM durchführen

Öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC, melden Sie sich an und geben Sie Folgendes ein:

```
racadm chassisaction -m chassis <Maßnahme>
```

wobei <*Maßnahme*> powerup, powerdown, powercycle, nongraceshutdown oder reset ist.

Durchführen von Energieverwaltungsmaßnahmen an einem Server

Sie können im Remote-Zugriff Stromverwaltungsmaßnahmen für mehrere Server gleichzeitig oder einen individuellen Server im Gehäuse durchführen.

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, müssen Sie die Berechtigung als Gehäusekonfigurations-Administrator besitzen.

Stromsteuerungsvorgänge für mehrere Server unter Verwendung der CMC-Webschnittstelle ausführen

So führen Sie Stromsteuerungsvorgänge unter Verwendung der Webschnittstelle für mehrere Server durch:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Strom**.

Die Seite **Energiesteuerung** wird angezeigt.

2 Wählen Sie in der Spalte **Vorgänge** des Drop-Down-Menüs einen der nachfolgenden Stromsteuerungsvorgänge für die notwendingen Server aus.

- **Kein Vorgang**
- **Server einschalten**
- **Server ausschalten**
- **Ordentliches Herunterfahren**
- **Server zurücksetzen (Softwareneustart)**
- **Server aus- und einschalten (Hardwareneustart)**

Weitere Informationen zu den verfügbaren Optionen finden Sie in der *Online-Hilfe*.

3 Klicken Sie auf **Anwenden**.

Daraufhin werden Sie über ein Dialogfeld zur Bestätigung des Vorgangs aufgefordert.

4 Klicken Sie auf **OK**, um die Stromverwaltungsmaßnahme durchzuführen (z. B. den Server zurückzusetzen).

Stromsteuerungsvorgänge für ein E/A-Modul ausführen

Sie können im Remote-Zugriff ein E/A-Modul zurücksetzen oder einschalten.

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, müssen Sie die Berechtigung als Gehäusekonfigurations-Administrator besitzen.

Stromsteuerungsvorgänge auf EAM unter Verwendung der CMC-Webschnittstelle ausführen

So führen Sie auf einem E/A-Modul Stromsteuerungsvorgänge aus:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **E/A-Modul-Übersicht** > **Strom**.

2 Wählen Sie auf der Seite **Stromsteuerung** für EAM aus dem Drop-Down-Menü den Vorgang aus, den Sie ausführen möchten (Aus- und einschalten).

3 Klicken Sie auf **Anwenden**.

Energieverwaltungsmaßnahmen am EAM über RACADM durchführen

Um auf einem EAM Stromsteuerungsvorgänge unter Verwendung von RACADM auszuführen, öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole zum CMC, melden Sie sich an und geben Sie Folgendes ein:

```
racadm chassisaction -m switch<Maßnahme>
```

wobei <*Maßnahme*> den Vorgang anzeigt, den Sie ausführen möchten: Aus- und Einschalten.

15

Verwaltung von Gehäusespeichern

Sie können auf Dell PowerEdge VRTX folgende Aufgaben ausführen:

- Den Status von physischen Festplattenlaufwerken und Speicher-Controllern anzeigen.
- Die Eigenschaften von Controllern, physischen Festplattenlaufwerken, virtuellen Festplatten und Gehäusen anzeigen.
- Controller, physische Festplattenlaufwerke und virtuelle Festplatten einrichten.
- Virtuelle Adapter zuweisen.
- Fehler von Controllern, physischen Festplattenlaufwerken und virtuellen Festplatten beheben.
- Speicherkomponenten aktualisieren.
- Gemeinsamen Speicher-Controller im Fehlertoleranzmodus verwenden
- Aktivieren oder Deaktivieren des freigegebenen PERC8 (Integriert 2)

ANMERKUNG: „Schnell initialisieren“ oder „Vollständig initialisieren“ wird nicht angezeigt, wenn virtuelle Festplatten erstmals erstellt werden.

Themen:

- Entsperren von Fremdkonfigurationen
- Kryptografischer Löschvorgang
- Zugangsrichtlinie für virtuelle Adapter auf virtuelle Festplatten anwenden
- Ändern der Eigenschaften von virtuellen Festplatten unter Verwendung der CMC Web-Schnittstelle
- Gehäuseverwaltungsmodul
- Anzeigen von Gehäuseeigenschaften unter Verwendung der CMC-Webschnittstelle

Den Status der Speicherkomponenten anzeigen

So zeigen Sie den Status der Speicherkomponenten an:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Speicher** > **Eigenschaften** > **Speicherübersicht**.

2 Auf der Seite **Speicherübersicht** können Sie:

- Die graphische Übersicht der physischen Festplattenlaufwerke, die im Gehäuse installiert sind und deren Status anzeigen.
- Die Zusammenfassung aller Speicherkomponenten mit Links zu deren entsprechenden Seiten anzeigen.
- Die verwendete Kapazität und die Gesamtkapazitätof der Speicher anzeigen.
- Controller-Informationen anzeigen.

  ANMERKUNG: Im Falle eines fehlertoleranten Controllers lautet das Namensformat wie folgt: Gemeinsam genutzter <*PERC - Nummer* (Integriert <Nummer>). Beispiel: Der aktive Controller ist „Gemeinsam genutzer PERC8“ (Integrierter 1), und der Peer-Controller ist „Gemeinsam genutzer PERC8“ (Integrierter 2).

  ANMERKUNG: Wenn der sekundäre PERC deaktiviert ist, wird der Name wie folgt angezeigt: Deaktivierter PERC (Integriert 2).
- Vor kurzem protokolliere Speicherereignisse anzeigen.

ANMERKUNG: Weitere Informationen finden Sie in der *Online-Hilfe*.

Anzeigen der Speichertopologie

So zeigen Sie die Speichertopologie an:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Speicher** > **Eigenschaften** > **Topologie**.

2 Klicken sie auf der Seite **Topologie** auf **<Controllername>**, um die entsprechenden Seiten anzuzeigen.

ANMERKUNG: Sie können den Namen des Controllers anzeigen, der sich aktiv an der Steuerung der Speichergeräte im Zusammenhang mit dem CMC beteiligt, und auch die passiven Controller, die als Stand-by fungieren.

3 Klicken Sie unter jedem installieren Controller die Links **Virtuelle Festplatten anzeigen**, **<Gehäusename>** und **Physische Festplatten anzeigen**, um die entsprechenden Seiten zu öffnen.

Anzeigen von Informationen zur fehlertoleranten Fehlerbehebung von SPERC über die CMC-Webschnittstelle

Gehen Sie wie folgt vor, um die Attribute anzuzeigen, die die korrekte Funktionsweise der Fehlertoleranzfunktionen eines SPERC anzeigen.

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Speicher** > **Fehlerbehebung** > **Fehlerbehebung einrichten**.
Die Seite **Speicherfehlerbehebung** wird angezeigt.

2 Auf der Seite **Speicherfehlerbehebung** können Sie:

- Klicken Sie auf + So zeigen Sie die folgenden Attribute an, wenn sich der integrierte Controller im Fehlertoleranzmodus befindet:

- Zwei gemeinsam genutzte PERCs erkannt.
- Zwei Erweiterungen erkannt
- Gemeinsam genutzte PERCs und Erweiterungen korrekt verkabelt
- Korrekte Firmware auf gemeinsam genutzten PERCs
- Korrekte Firmware auf Erweiterungen
- Korrekte Firmware auf der Gehäuseinfrastruktur
- Gemeinsam genutzte PERCs mit den gleichen Einstellungen: Zeigt an, ob die SPERCs die gleichen Einstellungen aufweisen.

• Klicken Sie auf + So zeigen Sie die folgenden Attribute an, wenn sich der integrierte Controller nicht im Fehlertoleranzmodus befindet:
  - Ein gemeinsam genutzter PERC erkannt
  - Eine Erweiterung erkannt.
  - Gemeinsam genutzte PERC und Erweiterungen korrekt verkabelt

• Klicken Sie auf + So zeigen Sie die folgenden Attribute an, wenn sich der externe Controller im Fehlertoleranzmodus befindet:
  - Zwei gemeinsam genutzte PERCs erkannt
  - Freigegebene PERCs sind in unterschiedlichen Fabrics installiert
  - Freigegebene PERCs und EMMs sind ordnungsgemäß angeschlossen
  - Korrekte Firmware auf freigegebenen PERCs
  - Freigegebene PERCs weisen die gleichen Einstellungen auf

• Klicken Sie auf + So zeigen Sie die folgenden Attribute an, wenn sich der externe Controller nicht im Fehlertoleranzmodus befindet:
  - Ein gemeinsam genutzter PERC erkannt
  - Eine Erweiterung erkannt.
  - Gemeinsam genutzte PERC und Erweiterungen korrekt verkabelt

• Zeigen Sie den Status für jedes Attribut an, das anzeigt, ob das Fehlertoleranzkriterium erfüllt ist.

ANMERKUNG: Wenn das Attribut in einer fehlertoleranten Umgebung nicht mit dem Kriterium übereinstimmt, wird die Option Jetzt aktualisieren für dieses Attribut angezeigt.

ANMERKUNG: Die Option Vorgehensweise wird für einige der angezeigten Attribute angezeigt. Weitere Informationen über dieses Attribut erhalten Sie durch einen Klick auf Vorgehensweise.

3 Zur Erfüllung eines Kriteriums für ein Attribut klicken Sie auf **Jetzt aktualisieren**.

Die Seite **Speicherkomponentenaktualisierung** wird angezeigt. Hier können Sie die gewünschte Speicherkomponente aktualisieren, um das Kriterium für das Attribut zu erfüllen.

Zuweisen von virtuellen Adaptern auf Steckplätze über die CMC-Webschnittstelle

Mithilfe der Funktion für virtuelle Adapter können Sie den installierten Speicher mit den vier Servern gemeinsam nutzen. Sie können einem Serversteckplatz eine virtuelle Festplatte so zuordnen: zuerst ordnen Sie eine virtuelle Festplatte einem virtuellen Adapter (VA) zu, und dann ordnen Sie einen virtuellen Adapter (VA) einem Serversteckplatz zu.

- Stellen Sie vor dem Zuweisen eines VA auf einen Serversteckplatz Folgendes sicher:
  - Der Serversteckplatz ist leer, oder der Server im Steckplatz ist ausgeschaltet.
  - Die Zuordnung eines virtuellen Adapters wird von einem Server oder einem Steckplatz aufgehoben.
  - Alle betroffenen Server sind ausgeschaltet.
- Virtuelle Laufwerke werden erstellt und als **Virtueller Adapter 1**, **Virtueller Adapter 2**, **Virtueller Adapter 3** oder **Virtueller Adapter 4** zugewiesen. Weitere Informationen finden Sie unter Zugriffsrichtlinie für virtuelle Adapter auf virtuelle Laufwerke anwenden.

ANMERKUNG:

- Sie können nur einen virtuellen Adapter auf einmal einem Server zuordnen.
- Ohne eine entsprechende Lizenz können Sie die Zuordnung einer Server-Zuweisung für einen virtuellen Adapter nicht aufheben oder den vituellen Adapter nur dem Standardserver zuordnen.
- Die Standardzuordnung ist VA1-Server-Steckplatz 1, VA2-Server-Steckplatz 2, VA3-Server-Steckplatz 3 und VA4-Server-Steckplatz 4.
- Wenn ein Server mit voller Bauhöhe eingesetzt wird, ist dem oberen Steckplatz ein VA zugeordnet, während der untere Steckplatz weiterhin ohne Zuordnung ist. Bei einem Server mit voller Höhe in Steckplatz 1 ist VA1 z. B. dem Steckplatz 1 zugewiesen, während VA3 weiterhin nicht zugeordnet ist.
- Wenn das System eine Enterprise-Lizenz besitzt, können Sie jede der vier virtuellen Adapter einem Serversteckplatz zuweisen. Sie können einem Server jedoch nur einen virtuellen Adapter auf einmal zuordnen.
- Virtuelle Adapterregeln werden an den externen und integrierten freigegebenen Speicheradaptern angewendet.

Gehen Sie wie folgt vor, um einen virtuellen Adapter einem Serversteckplatz zuzuordnen oder die Zuordnung aufzuheben:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Speicher** > **Setup** > **Virtualization**.

Die Seite **Speichervirtualisierung** wird angezeigt.

2 Für die Auswahl des erforderlichen Zuweisungstyps wählen Sie in der Tabelle **Zuweisungsmodus: Virtuelle Festplatten auf virtuelle Adapter** Folgendes aus:

- **Einfache Zuweisung** – Wählen Sie diese Option aus, um eine virtuelle Festplatte einem virtuellen Adapter zuzuweisen.
- **Mehrfachzuweisung** – Wählen Sie diese Option aus, um eine virtuelle Festplatte mehreren virtuellen Adaptern zuzuweisen. Lesen Sie die am Bildschirm angezeigten Anweisungen, bevor sie diese Option auswählen.

ANMERKUNG: Wählen Sie den Modus Mehrfachzuweisung nur dann aus, wenn die Cluster-Dienste auf den Servern installiert sind. Die Verwendung dieses Modus ohne Cluster-Dienste könnte zu einer Beschädigung oder einem Verlust von Daten führen.

ANMERKUNG: Sie können ein virtuelles Laufwerk über die Befehlsschnittstelle des CMC mehreren virtuellen Adaptern zuweisen, auch wenn der Zuweisungsmodus in der CMC-Webschnittstelle auf Einfache Zuweisung eingestellt ist.

3 Wählen Sie in der Tabelle **Zuordnung virtueller Netzwerkadapter** aus der Dropdown-Liste **Aktion** eine der folgenden Optionen aus und klicken Sie dann auf **Anwenden**.

- **<Steckplatz-Nr.>** – Wählen Sie den Steckplatz aus, dem der virtuelle Adapter zugewiesen werden muss.
- **Zuordnung aufheben** – Wählen Sie aus, die Zuweisung des virtuellen Adapters zu einem Steckplatz zu entfernen.

Der virtuelle Adapter wird vom ausgewählten Serversteckplatz aus zugeordnet, oder die Zuordnung wird entsprechend aufgehoben. Maßgeblich dafür ist die ausgewählte Aktion.

ANMERKUNG: Ziehen Sie in Betracht, einem Server im unteren Steckplatz (3 oder 4) einen virtuellen Adapter zuzuweisen. Wenn ein Server mit halber Bauhöhe (Steckplatz 3 oder 4) gegen einen Server mit voller Bauhöhe austauschen, greift der Server mit voller Bauhöhe nicht auf den virtuellen Adapter zu, der unteren Steckplätzen zugewiesen wurde. Wenn Sie erneut einen Server mit halber Bauhöhe einfügen, erhalten Sie Zugriff auf den virtuellen Adapter.

Zuordnen oder Aufheben der Zuordnung eines virtuellen PERC-Controllers zu einem Blade:

- Jede externe freigegebene PERC 8-Karte verfügt über vier virtuelle Adapter (VA). Wenn eine oder zwei externe freigegebene PERC 8-Karten im System vorhanden sind, können Sie einen der vier virtuellen Adapter im freigegebenen Modus zuordnen oder die Zuordnung aufheben.
- Wenn ein externer PCIE-Steckplatz durch einen freigegebenen Adapter belegt ist, kann die Zuordnung des virtuellen Adapters die aktuellen Details oder Informationen für die VA-Zuordnung des freigegebenen VA-Speicherpools ermitteln.
- Ein freigegebenes Gerät wird nicht unterstützt, wenn der externe PCIE-Steckplatz von einem freigegebenen Adapter belegt ist. Mithilfe des freigegebenen Adapters können Sie ein freigegebenes Gerät unterstützen, indem Sie den freigegebenen VA-Speicherpool ändern.

Fehlertoleranz in Speicher-Controllern

Hochverfügbarkeit (HA) in Speichern ermöglicht die Verfügbarkeit von mehreren integierten Komponenten und mehreren Zugriffspunkten auf Speicherressourcen. Wenn eine Speicherkomponente nicht funktioniert, wird der Server durch eine zweite wichtige Komponente oder einen zweiten wichtigen Pfad zu den verfügbaren Daten unterstützt. Hochverfügbarkeit minimiert nur die Ausfallzeiten durch das Wiederherstellen der Services hinter den Kulissen, in den meisten Fällen, bevor das Nichtfunktionieren sichtbar wird, die Ausfallzeiten werden jedoch nicht eliminiert. Fehlertoleranz (FT) nutzt redundante Komponenten in einem Speichersystem, die so konfiguriert werden, dass sie als Backup-Komponenten und im Standby-Modus laufen. Die Speicher-Controller im Fehlertoleranzmodus verhindern Störungen von Speicherservices und übernehmen automatisch die Services einer Komponente, die nicht mehr funktioniert. Die Leistung bleibt während dieses Failover-Prozesses konsistent, da die redundanten Komponenten (Controller) im normalen Betrieb nicht verwendet werden.

Hochverfügbarkeit mit Fehlertoleranz bietet die folgenden Vorteile:

- Verfügbarkeit für alle Speicheranwendungen, selbst wenn der Controller nicht mehr ordnungsgemäß funktioniert.
- Jederzeit Zugriff auf wichtige Funktionen des Gehäuses.
- Server können Situationen lösen, in denen der Controller nicht mehr funktionsfähig ist und Fehler auftreten.
- Verwendung von Komponentenredundanz

Mithilfe der Fehlertoleranzfunktionen von Controllern können Sie die Aufgaben im Zusammenhang mit gemeinsam genutztem Speicher, die durch einen aktiven und einen passiven (Peer-)Controller erreicht werden, verwalten. Der aktive Controller ist aktiviert und überwacht alle speicherrelevanten Prozesse. Der Status beider Controller wird zwischen den Controllern mitgeteilt, so dass bei Ausfall des aktiven Controllers der passive Controller als Peer-Hotspare dessen Funktion nahtlos übernimmt.

ANMERKUNG: CMC zeigt fehlertolerante Daten für gemeinsam genutzte PERC 8-Komponenten mit einer SR-IOV-fähigen Firmware. Wenn keine SR-IOV-Karte den gemeinsam genutzten Speichersteckplätzen zugeordnet ist, wird die Karte nicht eingeschaltet, und es wird ein Alarm ausgegeben.

ANMERKUNG: Vorgänge wie z. B. das Zurücksetzen des CMC, mit dem die CMC-Konfiguration zurückgesetzt wird, setzen auch die externe fehlertolerante Konfiguration zurück. Dies hat zur Folge, dass sich der PERC-Modus auf den „Abgesicherten Modus“ ändert. Deaktivieren Sie die Fehlertoleranz im externen PERC.

Nichtübereinstimmung der Sicherheitsschlüssel

Sie können einen Sicherheitsschlüssel auf einem Controller unter Verwendung einer **Encryption-KeyID** und einer **Passphrase** erstellen. Der Controller vergleicht beim Erstellen des Sicherheitsschlüssels nur die benutzte **Passphrase**, um festzustellen, ob die zwei Controller über die gleichen Sicherheitsschlüssel verfügen. Daher sind zwei Controller, die einem Cluster beitreten, auch dann fehlertolerant, wenn sie unterschiedliche **Encryption-KeyIDs** aufweisen, jedoch über die gleiche Passphrase verfügen.

Wenn eine Nichtübereinstimmung der Sicherheitsschlüssel auf zwei Peer-Controllern festgestellt wird, ändert sich der fehlertolerante Modus auf „Herabgesetzt“. Ein kritischer Warnhinweis wird auf der Seite **Gehäusefunktionszustand** angezeigt, und die Überwachung zeigt möglicherweise keine korrekte Laufwerkszuordnung an.

Wenn eine Nichtübereinstimmung festgestellt wird, können Sie diese durch Erstellen, Ändern oder Löschen des Sicherheitsschlüssels auf einem der Controller beheben, bevor Sie weitere Aktionen zur Speichersicherheit auf dem Controller durchführen. Schalten Sie das Gehäuse nach Behebung der Nichtübereinstimmung aus und wieder ein. Bevor Sie zwei nicht-hochverfügbare Controller kombinieren, ändern Sie die Schlüssel, damit diese übereinstimmen. Diese Maßnahme vereinfacht den Import von sicheren Laufwerken, die den jeweiligen Controllern zugeordnet werden, die dem Cluster beitreten.

Ändern Sie bei externen Controllern die Schlüssel, damit diese aus Gründen der Fehlertoleranz vor der Verkabelung übereinstimmen. Die Änderung von Sicherheitsschlüsseln vereinfacht den Import von sicheren Laufwerken, die den jeweiligen Controllern zugeordnet werden, die dem Cluster beitreten.

Beheben der Nichtübereinstimmung der Sicherheitsschlüssel unter Verwendung der CMC Web-Schnittstelle

So beheben Sie die Nichtübereinstimmung der Sicherheitsschlüssel unter Verwendung der CMC Web-Schnittstelle:

1 Schalten Sie die Servermodule aus.
2 Klicken Sie auf **Server-Übersicht** > **Strom** > **Steuerung** > **Server ausschalten**.
3 Ändern Sie den Sicherheitsschlüssel auf einem oder beiden der vorhandenen nicht-fehlertoleranten Controller, damit diese übereinstimmen.
4 Schalten Sie das Gehäuse aus und wieder ein.
5 Überprüfen Sie, ob die Schlüssel der Controller übereinstimmen.

Anzeigen von Gehäuseeigenschaften unter Verwendung der CMC-Webschnittstelle

So können Sie die Controller-Eigenschaften anzeigen:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Controller**.
2 Sie können auf der Seite **Controller**, unter dem Abschnitt **Controller** die grundlegenden Eigenschaften der Controller anzeigen. Um jedoch die erweiterten Eigenschaften anzuzeigen, klicken Sie auf das +.

ANMERKUNG: Wenn sich der Controller im fehlertoleranten Modus befindet, werden die folgenden Informationen zum Fehlertoleranzstatus und -modus ebenfalls angezeigt:

- Fehlertoleranzmodus – Gemeinsam genutzt, Aktiv/Passiv
- Fehlertoleranzstatus – Funktionsfähig/Normal oder Verloren/Herabgesetzt
- Peer-Controller – Zeigt den Namen des Controllers an, der als Peer (Stand-by) im Falle eines Fehlertoleranzmodus fungiert; unterstützt durch zwei Controller.

ANMERKUNG: Wenn der Peer-Controller deaktiviert ist, wird der Name als PERC deaktiviert (Integriert 2) oder PERC deaktiviert (SPERC-Steckplatz 6) angezeigt, und der Status wird als Unbekannt angezeigt, was bedeutet, dass der Peer-Controller ausgeschaltet ist.

Weitere Informationen über Controller finden Sie in der *Online-Hilfe*.

Anzeigen der Controller-Eigenschaften unter Verwendung von RACADM

Um die Controller-Eigenschaften unter Verwendung von RACADM anzuzeigen, führen Sie den Befehl `racadm raid get controllers -o` aus.

Weitere Informationen finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

Importieren oder Löschen einer Fremdkonfiguration

Eine fremde Festplatte muss in das Gehäuse eingesetzt werden.
So importieren oder löschen Sie die Fremdkonfiguration:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Speicher** > **Controller** > **Setup**.
2 Klicken Sie auf der Seite **Controller-Setup** im Abschnitt **Fremdkonfiguration** für den entsprechenden Controller auf:

- **Fremdkonfiguration löschen**, um die bestehende Konfiguration der Festplatte zu löschen.
- **Importieren/Wiederherstellen**, um die Festplatte mit der Fremdkonfiguration zu importieren.

ANMERKUNG: Wenn Sie die Laufwerke einer bestimmten virtuellen Festplatte entfernen, den Controller zurücksetzen und die Laufwerke nacheinander wieder einsetzen, werden auf der Seite Fremdkonfiguration mehrere virtuelle Festplatteninstanzen verschiedener Größen und Zustände angezeigt. Nachdem der Importvorgang abgeschlossen wurde, werden der richtige Zustand und die richtige Größe der virtuellen Festplatte angezeigt.

Konfigurieren von Speicher-Controller-Einstellungen

Sie können die Eigenschaften eines vorhandenen Speicher-Controllers ändern oder die Eigenschaften eines neu installierten Speicher-Controllers konfigurieren.

Konfigurieren von Speicher-Controller-Einstellungen über die CMC-Webschnittstelle

Stellen Sie sicher, dass mindestens ein Speicher-Controller im Gehäuse installiert ist.
So konfigurieren Sie die Speicher-Controller-Einstellungen:

1 Gehen Sie in der CMC-Webschnittstelle zu **Gehäuseübersicht** > **Speicher** > **Controller** > **Setup**.

2 Wählen Sie auf der Seite **Controller-Setup** aus dem Drop-Down-Menü **Controller** den Controller aus.

ANMERKUNG: Beachten Sie Folgendes:

- Wenn es sich um Speicher-Controller im fehlertoleranten Modus handelt und wenn beide die gleiche Firmware-Version haben, werden beide Controller als ein einziges Gerät im Drop-Down-Menü angezeigt. Beispiel: Freigegebener PERC8 (Integrierter 1) oder freigegebener PERC8 (Integrierter 2) oder freigegebener PERC8 (SPERC-Steckplatz 5) oder freigegebener PERC8 (SPERC-Steckplatz 6). Wenn die Einstellungen für die beiden Controller nicht identisch sind, wird die Meldung **Einstellungen inkompatibel** angezeigt. Sie können die Eigenschaften der fehlertoleranten Controller so festlegen, dass die Eigenschaften auf beiden Controllern identisch sind. Controller in diesem Modus dürfen keine unterschiedlichen Eigenschaften aufweisen.
- Wenn ein zweiter Speicher-Controller mit einer anderen Firmware-Version installiert ist, werden die Controller als zwei verschiedene Komponenten im Dropdown-Menü angezeigt. Beispiel: Freigegebener PERC8 (Integrierter 1), freigegebener PERC8 (Integrierter 2), freigegebener PERC8 (SPERC-Steckplatz 5) und freigegebener PERC8 (SPERC-Steckplatz 6).

Die Attributwerte für den ausgewählten Controller werden in der Tabelle aktualisiert.

3 Geben Sie die Daten ein, oder wählen Sie sie aus, und klicken Sie dann auf **Anwenden**.

ANMERKUNG: Weitere Informationen zu den Attributen und anderen Feldbeschreibungen finden Sie in der *Online-Hilfe*.

Die neu festgelegten Eigenschaften werden auf die ausgewählten Controller angewendet, und das Feld **Aktueller Wert** zeigt die aktualisierten Werte für die Attribute an.

Konfigurieren der Speicher-Controller-Einstellungen mit RACADM

Um einen Speicher-Controller durch das Ausführen eines RACADM-Befehls einzurichten, verwenden Sie die folgende Syntax:

```
racadm raid ctrlprop:RAID.ChassisIntegrated.1-1 [-rebuild <value>] [-bgi <value>] [-reconstruct
<value>] [-checkconsistency <value>] [-ccmode {abortonerror | normal}] [-copybackmode {off | on
| onwithsmart}] [-lb {auto | disabled}] [-prunconfigured {yes | no}]
```

Weitere Informationen finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

Freigegebener PERC-Controller

Für Systeme mit zwei integrierten freigegebenen PERC können Sie den Betriebsmodus zwischen den Modi **Fehlertolerant** und **Nicht-Fehlertolerant** wechseln. Verwenden Sie hierzu die Web-Schnittstelle oder die RACADM-Befehlszeilenschnittstelle, indem Sie den zweiten internen freigegebenen PERC 8-Controller aktivieren oder deaktivieren.

Für interne freigegebene PERC8-Controller können Sie den zweiten integrierten Controller deaktivieren. Nach dem Deaktivieren des zweiten integrierten Controllers, ist der erste integrierte Controller nicht im fehlertoleranten Modus. Wenn der zweite integrierte Controller aktiviert ist, sind die beiden integrierten Controllern standardmäßig im fehlertoleranten Modus. Der zweite integrierte Controller kann mithilfe des Befehls `racadm raid disableperc:RAID.ChassisIntegrated.2-1` deaktiviert werden.

Für externe Gehäuse können sowohl die externe freigegebene PERC 8-Karte in Steckplatz 5 und Steckplatz 6 mithilfe des Befehls `racadm raid disableperc: RAID.ChassisSlot.5-1 and racadm raid disableperc: RAID.ChassisSlot.6-1` deaktiviert werden.

Führen Sie von der RACADM-Befehlszeilenschnittstelle den Befehl `racadm raid get controllers` aus, um die Anzahl der freigegebenen PERC-Controller auf dem System aufzulisten. Wenn der Befehl nur `RAID.ChassisIntegrated.1-1` auslistet, weist das System einen einzigen freigegebenen PERC-Controller auf. Wenn der Befehl `RAID.ChassisIntegrated.1-1`, `RAID.ChassisIntegrated.2-1` auflistet, verfügt Ihr System über zwei freigegebene PERC-Controller.

Die zweite integrierte freigegebene PERC 8- und die externe freigegebene PERC 8-Karten in Steckplatz 5 und Steckplatz 6 können aktiviert oder deaktiviert werden.

Wechseln Sie zum Ändern des Betriebsmodus mithilfe der CMC Web-Schnittstelle zur Seite **Controller-Fehlerbehebung** indem Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Speicher-Controller** wechseln und die Option **Raid-Controller deaktivieren** oder **Raid-Controller aktivieren** auswählen.

So ändern Sie den Betriebsmodus mithilfe der RACADM-CLI:

- Führen Sie den Befehl `racadm raid enableperc:RAID.ChassisIntegrated.2-1` zum Aktivieren der Modi **Integrierte 2 freigegebene PERC 8** und **Fehlertolerant** aus, wenn die zweite integrierte freigegebene PERC8 deaktiviert ist.
- Führen Sie den Befehl `racadm raid enableperc:RAID.ChassisSlot.6-1` zum Aktivieren des **externen freigegebenen PERC8** in Steckplatz 6 aus.
- Führen Sie den Befehl `racadm raid disableperc:RAID.ChassisIntegrated.2-1` zum Deaktivieren des **zweiten integrierten freigegebenen PERC8** und des **fehlertoleranten** Modus aus.

ANMERKUNG:

- Das Gehäuse muss eingeschaltet und alle Servermodule müssen ausgeschaltet sein, bevor Sie die Befehle zum Aktivieren oder Deaktivieren ausführen. Das Gehäuse wird bei diesem Vorgang automatisch aus- und wieder eingeschaltet. Nachdem Sie den Betriebsmodus des freigegebenen PERC geändert haben, sollten Sie den CMC zurücksetzen, indem Sie die Seite **Fehlerbehebung** oder den Befehl `racadm racreset` verwenden.
- Standardmäßig wird der Modus „Hohe Verfügbarkeit“ angezeigt, wenn zweite integrierte PERC 8-Karten erkannt wurden.
- Das Aktivieren des SPERC in externen Steckplätzen aktiviert die Fehlertoleranz nicht.
- Informationen zum Aktivieren des fehlertoleranten Modus für externe freigegebene PERC8 finden Sie im Abschnitt *Aktivieren oder Deaktivieren der Fehlertoleranz von externem RAID-Controller unter Verwendung von RACADM*.

RAID-Controller über die CMC-Web-Schnittstelle aktivieren oder deaktivieren

Bei einem VRTX-Gehäuse mit zwei freigegebenen PERC8-Controllern, kann der Integrierte 2 PERC-Adapter aktiviert oder deaktiviert werden, wenn der Integrierte 1 PERC-Adapter aktiv ist und die Servermodule ausgeschaltet sind. Beide Adapter müssen für Fehlertoleranz aktiviert sein. Auf der Seite **Controller-Fehlerbehebung** können Sie den Peer-Controller aktivieren oder deaktivieren.

ANMERKUNG: Um Datenverlust zu verhindern, führen Sie Folgendes aus, bevor Sie Controller aktivieren oder deaktivieren:

- Führen Sie alle Daten-Vorgänge wie Neuerstellung oder Rückkopieren aus.
- Stellen Sie sicher, dass sich die Datenträger in einem optimalen Zustand befinden.

ANMERKUNG: Während der Aktivierung des zweiten PERC-Adapters wird eine Warnmeldung angezeigt, und der Fehlertoleranz-Status ist in folgenden Fällen herabgestuft:

- Wenn PERC-Adapter-Einstellungen geändert werden.
- Wenn die Firmware aktualisiert wird.

Stellen Sie sicher, dass die Firmware und die Einstellungen des freigegebenen PERC übereinstimmen, wenn Sie die fehlertolerante System-Konfiguration in den Fehlertoleranz-Modus versetzen.

Sie können einen Peer-Controller nur dann deaktivieren, wenn Folgendes zutrifft:

- Alle Server, die sich im Gehäuse befinden, werden heruntergefahren.
- Der PERC-Controller mit der Bezeichnung „Integriert 1“ ist derzeit der aktive Controller.

  ANMERKUNG: Wenn der PERC-Controller mit der Bezeichnung „Integriert 1“ derzeit nicht der aktive Controller ist, dann schalten Sie das Gehäuse aus und wieder ein, um diesen Controller zum aktiven Controller zu machen.
- Beide CMCs verfügen über dieselbe Firmware-Version, die diese Funktion unterstützt.

ANMERKUNG: Nach der Deaktivierung des PERC-Controllers mit der Bezeichnung „Integriert 2“ als Ersatz einer CMC-Karte wird empfohlen, die CMC-Karte mit der Firmware ab Version 1.35 zu aktualisieren, bevor die Karte als aktiver CMC-Controller im System zugewiesen wird. Es wird eine Warnung angezeigt, bevor Sie diese Maßnahme durchführen.

So aktivieren oder deaktivieren Sie einen Peer-Controller im fehlertoleranten Modus über die CMC-Web-Schnittstelle:

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Speicher-** > **Controller** > **Fehlerbehebung**.
2. Wählen Sie auf der Seite **Controller-Fehlerbehebung** aus der Drop-Down-Liste **Maßnahmen** für „Integriert 2 PERC“ eine der folgenden Optionen aus, und klicken Sie dann auf **Anwenden**.
   - **RAID-Controller deaktivieren** – Deaktiviert den Peer-Controller im Fehlertoleranz-Modus.
   - **RAID-Controller aktivieren** – Aktiviert den Peer-Controller im Fehlertoleranz-Modus. Wenn „Integrierter 2 PERC“ bereits deaktiviert ist, dann ist im Drop-Down-Menü die Option **Raid-Controller aktivieren** vorhanden.
   - So aktivieren oder deaktivieren Sie externe freigegebene PERC 8-Karten-Controller:
     - Wählen Sie auf der Seite **Controller-Fehlerbehebung** aus der Drop-Down-Liste **Maßnahmen** für externe freigegebene PERC 8-Karten in Steckplatz 5 oder Steckplatz 6 eine der folgenden Optionen aus, und klicken Sie dann auf **Anwenden**.
       - **RAID-Controller deaktivieren** – Deaktiviert den RAID-Controller.
       - **RAID-Controller aktivieren** – Aktiviert den RAID-Controller. Wenn der PERC bereits deaktiviert ist, dann ist im Drop-Down-Menü die Option **Raid-Controller aktivieren** vorhanden.
   - **Konfiguration zurücksetzen** – Wählen Sie diese Option aus, um virtuelle Laufwerke zu löschen und die Zuweisung aller Hotspares, die mit dem Controller verbunden sind, aufzuheben. Dadurch werden jedoch lediglich die Laufwerke aus der Konfiguration entfernt; es werden keine Daten gelöscht. ANMERKUNG: „Konfiguration zurücksetzen“ entfernt keine Fremdkonfigurationen. Verwenden Sie dazu die Option „Fremdkonfiguration löschen“.
   - **TTY-Protokoll exportieren** – Wählen Sie diese Option aus, um das TTY-Protokoll auf dem lokalen System zu exportieren. HINWEIS: Das vom Controller erfasste TTY-Protokoll enthält keine Daten von den Festplatten. Es kann jedoch ggf. Daten wie z.B. SAS-Adressen enthalten.
   - **Fehlertoleranz aktivieren** – Wählen Sie diese Option aus, um den Fehlertoleranzmodus des externen SPERC zu aktivieren. Durch diesen Vorgang erfolgt außerdem ein Rücksetzen der externen freigegebenen PERC 8-Karte.
   - **Fehlertoleranz deaktivieren** – Wählen Sie diese Option aus, um den Fehlertoleranzmodus des externen SPERC zu deaktivieren. Durch diesen Vorgang erfolgt außerdem ein Rücksetzen der externen freigegebenen PERC 8-Karte.

ANMERKUNG:

- Wenn PERC deaktiviert ist, sind die Optionen „Konfigurations-Reset“, „TTY-Protokoll exportieren“, „Pinned Cache verwerfen“ und „RAID-Controller deaktivieren“ im Drop-Down-Menü vorhanden.
- Standardmäßig werden die beiden integrierten freigegebenen Speicheradapter mit hohem Verfügbarkeitsmodus erkannt.
- Sie müssen den **Fehlertoleranzmodus** auf dem externen freigegebenen Controller aktivieren, nachdem er verkabelt wurde.
- **Fehlertoleranz aktivieren** und **Fehlertoleranz deaktivieren** werden nur für die externen freigegebenen PERC 8-Karten angezeigt. Der Standardmodus der externen freigegebenen PERC 8-Karten ist der nicht-fehlertolerante Modus.

ANMERKUNG: Durch das Aktivieren oder Deaktivieren eines Peer-Controllers wird das Aus- und Einschalten des Gehäuses eingeleitet. Die Änderungen werden erst wirksam, nachdem das System aus- und wieder eingeschaltet wurde.

Aktivieren oder Deaktivieren von RAID-Controllern mit RACADM

Um einen Peer-Controller mit RACADM zu aktivieren, öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole zum CMC, melden Sie sich an und geben Sie Folgendes ein:

```
racadm raid enableperc:<AdapterFQDD>
```

Geben Sie zum Deaktivieren des Peer-Controllers Folgendes ein:

```
racadm raid disableperc:<AdapterFQDD>
```

ANMERKUNG: Informationen zu dieser Funktion unter Verwendung der RACADM-Schnittstelle finden Sie im *RACADM Command Line Reference Guide for iDRAC and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC und CMC).

Aktivieren oder Deaktivieren der Fehlertoleranz von externen RAID-Controllern unter Verwendung von RACADM

So aktivieren Sie die Fehlertoleranz:

```
racadm raid controllers: <FQDD of External Shared PERC8> -p HighAvailabilityMode ha
```

So deaktivieren Sie die Fehlertoleranz:

```
racadm raid set controllers: <FQDD of External Shared PERC8> -p HighAvailabilityMode None
```

Anzeigen der Eigenschaften von physischen Festplatten unter Verwendung der CMC Web-Schnittstelle

Achten Sie darauf, dass physische Festplatten im Gehäuse installiert sind.
So zeigen Sie die Eigenschaften physischer Festplattenlaufwerke an:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Speicher** > **Physische Festplatten**.
Die Seite **Eigenschaften** wird angezeigt.

2 Um die Eigenschaften aller physischer Festplattenlaufwerke anzuzeigen, klicken sie im Abschnitt **Physische Festplatten** auf das ⊞.

ANMERKUNG: Die folgenden Attribute werden für den Fehlertoleranzmodus von integrierten freigegebenen Adaptern angezeigt:

- Aktiver Controller – Gemeinsam genutzter PERC8 (Integrierter 1)
- Redundanz-/Failover-Controller – Gemeinsam genutzter PERC8 (Integrierter 2)

Die folgenden Attribute werden für den Fehlertoleranzmodus von externen freigegebenen Adaptern angezeigt:

- Aktiver Controller – Freigegebener PERC8 (SPERC-Steckplatz 5)
- Redundanz-/ Failover-Controller – Freigegebener PERC8 (SPERC-Steckplatz 6)

Sie können auch die folgenden Filter verwenden, um spezifische Eigenschaften für physische Festplattenlaufwerke anzuzeigen:

- Wählen Sie unter der Option **Grundlegender physischer Festplattenfilter** aus dem Drop-Down-Menü **Gruppieren nach Virtuelle Festplatte**, **Controller** oder **Gehäuse** aus, und klicken Sie dann auf **Anwenden**.
- Klicken Sie auf **Erweiterter Filter**, wählen Sie die Werte für verschiedene Attribute und klicken Sie dann auf **Anwenden**.

Anzeigen der Eigenschaften von physischen Festplatten unter Verwendung von RACADM

Um die Eigenschaften von physischen Festplatten unter Verwendung von RACADM anzuzeigen, führen Sie den Befehl `racadm raid get pdisks –o` aus.

Lesen Sie für weitere Informationen das *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

Physische Festplatten und virtuelle Festplatten identifizieren

Weitere Informationen zum Aktivieren oder Deaktivieren der LED-Blinkfunktion finden Sie unter:

- Konfigurieren von LED-Blinken über die CMC-Webschnittstelle
- LED-Blinken mittels RACADM konfigurieren

Zuweisen von globalen Hotspares unter Verwendung der CMC Web-Schnittstelle

Zuweisen und Aufheben der Zuweisung von globalen Hotspares:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Speicher** > **Physische Festplatte** > **Setup**.
Die Seite **Physische Festplatten konfigurieren** wird angezeigt.

2 Wählen Sie unter dem Abschnitt **Physische Festplatten konfigurieren** im Drop-Down-Menü **Maßnahmen für physische Festplatten** die Option **Nicht zugewiesen** oder **Globale Hotspare** für jede der physischen Festplatten aus und klicken Sie dann auf **Anwenden**.

ANMERKUNG: Die Zuweisung des globalen Hotspare ist nur erlaubt, wenn mindestens ein virtuelles Laufwerk auf dem entsprechenden Controller vorhanden ist.

Globalen Hotspare unter Verwendung von RACADM zuweisen

Um globale Hotspare unter Verwendung von RACADM zuzuweisen, führen Sie den Befehl `racadm raid hotspare: -assign yes -type ghs` aus.

Weitere Informationen über RACADM-Befehle finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

Wiederherstellung von physischen Festplatten

So stellen Sie physische Festplatten wieder her:

1 Gehen Sie in der CMC-Webschnittstelle zu **Gehäuseübersicht** > **Speicher** > **Physische Festplatten** > **Setup**.

2 Wählen Sie auf der Seite **Setup** unter **Physische Festplatten wiederherstellen** die physische Festplatte aus, die wiederhergestellt werden muss, und wählen Sie aus dem Drop-Down-Menü die Option **Laufwerk neu erstellen Neuerstellung abbrechen** oder **Online erzwingen** aus. Klicken Sie abschließend auf **Anwenden**.

Eigenschaften von virtuellen Festplatten unter Verwendung der CMC-Webschnittstelle anzeigen

Stellen Sie sicher, dass die virtuellen Festplatten erstellt wurden.
So zeigen Sie die Eigenschaften virtueller Festplatten an:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Speicher** > **Virtuelle Festplatten** > **Eigenschaften**.

2 Auf der Seite **Eigenschaften**, im Abschnitt **Virtuelle Festplatten** klicken Sie auf das  . Sie können auch die folgenden Filter verwenden, um spezifische Eigenschaften virtueller Festplatten anzuzeigen:

- Wählen Sie im Abschnitt **Grundlegender Filter für virtuelle Festplatten** aus dem Drop-Down-Menü **Controller** den Controllernamen und klicken Sie dann auf **Anwenden**.
- Klicken Sie auf **Erweiterter Filter**, wählen Sie die Werte für verschiedene Attribute und klicken Sie dann auf **Anwenden**.

Anzeigen der Eigenschaften von virtuellen Festplatten unter Verwendung von RACADM

Um die Eigenschaften von virtuellen Festplatten unter Verwendung von RACADM anzuzeigen, führen Sie den Befehl `racadm raid get vdisks -o` aus.

Weitere Informationen finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

Erstellung von virtuellen Festplatten unter Verwendung der CMC-Webschnittstelle

Standardmäßig erstellt CMC virtuelle Festplatten, ohne diese zu initialisieren. Sie können jedoch die Option der schnellen Initialisierung für virtuelle Festplatten auswählen, die ohne Initialisierung erstellt werden. Durch den Vorgang der schnellen Initialisierung werden die ersten und letzten 8 MB der virtuellen Festplatte entfernt und somit alle Boot-Records oder Partitionsdaten gelöscht. Sie müssen über die Rechte eines **Gehäusekonfigurations-Administrators** verfügen, um die schnelle Initialisierung durchzuführen.
Achten Sie darauf, dass die physische Festplatte im Gehäuse installiert ist.

ANMERKUNG: Das Löschen einer virtuellen Festplatte entfernt die virtuelle Festplatte aus der Konfiguration des Controllers.

So erstellen Sie eine virtuelle Festplatte:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Speicher** > **Virtuelle Festplatten** > **Erstellen**.

2 Wählen Sie auf der Seite **Virtuelle Festplatte erstellen** im Abschnitt **RAID-Stufe** die gewünschte RAID-Stufe aus.

3 Wählen Sie im Abschnitt **Physische Festplatten auswählen** die Anzahl der physischen Festplattenlaufwerke aus, die auf der gewählten RAID-Stufe basieren.

4 Geben Sie im Abschnitt **Einstellungen konfigurieren** die entsprechenden Daten ein, wählen Sie die Optionen **Initialisieren** und **Virtuelle Festplatte verschlüsseln** aus, und klicken Sie dann auf **Virtuelle Festplatte erstellen**.

CMC bietet mit der Initialisierung eine neue Option bei der Erstellung von virtuellen Festplatten. Mit dieser Option können Sie virtuelle Festplatten ohne schnelle Initialisierung erstellen. Standardmäßig wird die virtuelle Festplatte mit schneller Initialisierung erstellt.

Mit der Option **Initialisieren** können Sie virtuelle Festplatten ohne Initialisierung erstellen. Diese Option überschreibt den Standard-Funktionszustand, bei dem der schnelle Initialisierungsvorgang bei Erstellung einer virtuellen Festplatte gestartet wird.

Mit der Option **Virtuelle Festplatte verschlüsseln** können Sie sichere virtuelle Festplatten auf selbstverschlüsselnden Laufwerken (SEDs) erstellen.

ANMERKUNG: Die Option Virtuelle Festplatte verschlüsseln ist nur dann aktiviert, wenn der Verschlüsselungsschlüssel für den spezifischen Controller auf der Seite Controller-Einstellungen konfiguriert ist.

Verwalten von Verschlüsselungsschlüsseln

Ein Verschlüsselungs- oder Sicherheitsschlüssel, der auf einem Controller erstellt wird, wird zum Sperren oder Entsperren des Zugriffs auf sichere virtuelle Laufwerke verwendet, die auf SEDs erstellt werden. Sie können jeweils nur einen Verschlüsselungsschlüssel für einen verschlüsselungsfähigen Controller erstellen. Sie können Verschlüsselungsschlüssel erstellen, indem Sie eine Verschlüsselungsschlüssel-Kennung und die Passphrase auf der Seite **Controller-Setup** eingeben. Der CMC ermöglicht es auch, die Verschlüsselungsschlüssel-Passphrasen zu ändern und die Verschlüsselungsschlüsseln zu löschen.

Erstellen von Verschlüsselungsschlüsseln unter Verwendung der CMC Web-Schnittstelle

Sie können Verschlüsselungs- oder Sicherheitsschlüssel für Controller erstellen, wenn der Verschlüsselungsschlüssel **Nicht konfiguriert** ist. So erstellen Sie einen Verschlüsselungsschlüssel:

1. Wechseln Sie im linken Fensterbereich auf **Speicher** > **Controller** > **Setup**.
2. Im Drop-Down-Menü **Sicherheitsschlüssel** wählen Sie **Sicherheitsschlüssel erstellen** aus.
   Es wird ein Popup-Fenster angezeigt.
3. Geben Sie den Sicherheitsschlüssel und das Kennwort ein, und klicken Sie auf **OK**.
4. Klicken Sie auf der Seite **Controller-Setup** auf **Anwenden**.
   Sobald der Verschlüsselungsschlüssel erstellt wurde, wechselt der Status des **Sicherheitsschlüssels** auf **Aktiviert**.

Erstellen von Verschlüsselungsschlüsseln unter Verwendung von RACADM

Um einen Verschlüsselungsschlüssel durch Ausführung eines RACADM-Befehls zu erstellen, verwenden Sie die folgende Syntax:

```
racadm raid createsecuritykey:RAID.ChassisIntegrated.1-1 -key <Key id> -passwd <passphrase>
```

Weitere Informationen finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

Ändern der Verschlüsselungsschlüssel-Kennung unter Verwendung der CMC Web-Schnittstelle

Sie können die Verschlüsselungsschlüssel-Kennung und die Passphrase für Controller ändern.

So ändern Sie die Verschlüsselungsschlüssel-Kennung und die Passphrase:

1 Wechseln Sie im linken Fensterbereich auf **Speicher** > **Controller** > **Setup**.
2 Wählen Sie aus dem Drop-Down-Menü **Sicherheitsschlüssel** die Option **Sicherheitsschlüssel ändern** aus.
Es wird ein Popup-Fenster angezeigt.
3 Geben Sie die neue Kennung des Verschlüsselungsschlüssels sowie die vorhandene und neue Passphrase ein, und klicken Sie auf **OK**.
4 Klicken Sie auf der Seite **Controller-Setup** auf **Anwenden**.

Ändern der Verschlüsselungsschlüssel-Kennung unter Verwendung von RACADM

Um eine Verschlüsselungsschlüssel-Kennung und die Passphrase durch Ausführung eines RACADM-Befehls zu ändern, verwenden Sie die folgende Syntax:

```
racadm raid modifysecuritykey:RAID.ChassisIntegrated.1-1 -key <Key id> -oldpasswd
<oldpassphrase> -newpasswd <newpassphrase>
```

Weitere Informationen finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

Löschen von Verschlüsselungsschlüsseln unter Verwendung der CMC Web-Schnittstelle

Sie können Verschlüsselungsschlüssel für einen Controller nur löschen, wenn keine gesicherten virtuellen Festplatten damit verknüpft sind. So löschen Sie einen Verschlüsselungsschlüssel:

1 Wechseln Sie im linken Fensterbereich auf **Speicher** > **Controller** > **Setup**.
2 Wählen Sie aus dem Drop-Down-Menü **Sicherheitsschlüssel** die Option **Sicherheitsschlüssel löschen** aus.
Es wird eine Bestätigungsmeldung angezeigt.
3 Klicken Sie auf **OK**, um fortzufahren.
Nachdem Sie den Verschlüsselungsschlüssel gelöscht haben, werden alle SEDs sicher gelöscht, die nicht zu den virtuellen Festplatten gehören. Weitere Informationen finden Sie in der *Online-Hilfe*.

Löschen von Verschlüsselungsschlüsseln unter Verwendung von RACADM

Um einen Verschlüsselungsschlüssel durch Ausführen eines RACADM-Befehls zu löschen, verwenden Sie die folgende Syntax:

```
racadm raid deletesecuritykey:RAID.ChassisIntegrated.1-1
```

Weitere Informationen finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

Verschlüsseln der virtuellen Laufwerke

Nach der Konfiguration eines Verschlüsselungsschlüssels auf dem Controller können Sie virtuelle Laufwerke, die auf SEDs erstellt wurden, verschlüsseln. Jedesmal, wenn Sie eine Verschlüsselung ausführen, wird eine Meldung im `CMC-Protokoll` protokolliert. Sie können virtuelle Laufwerke verschlüsseln:

- Der Sicherheitsschlüssel wird auf dem Controller konfiguriert.

- Alle Laufwerke auf dem virtuellen Laufwerk sind SEDs.

Durch Verschlüsseln eines virtuellen Laufwerks wird die Verschlüsselung für alle virtuellen Laufwerke auf derselben Laufwerksgruppe aktiviert.

Sie müssen über die Rechte eines **Gehäusekonfigurations-Administrators** verfügen, um virtuelle Laufwerke zu verschlüsseln.

Verschlüsseln von virtuellen Festplatten unter Verwendung der CMC Web-Schnittstelle

So verschlüsseln Sie eine vorhandene virtuelle Festplatte:

1 Wechseln Sie im linken Fensterbereich auf **Speicher** > **Virtuelle Festplatten** > **Verwalten**.
2 Wählen Sie im Drop-Down-Menü **Virtuelle Maßnahmen** die Option **Virtuelle Festplatte verschlüsseln** aus, und klicken Sie auf **Anwenden**.

ANMERKUNG: Die Option Virtuelle Festplatte verschlüsseln ist nur verfügbar, wenn nicht gesicherte virtuelle Festplatten im SED konfiguriert sind.

Verschlüsseln von virtuellen Festplatten unter Verwendung von RACADM

Um virtuelle Festplatten durch Ausführen eines RACADM-Befehls zu verschlüsseln, verwenden Sie die folgende Syntax:

```
racadm raid encryptvd:Disk.Virtual.0:RAID.ChassisIntegrated.1-1
```

Weitere Informationen finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

Entsperren von Fremdkonfigurationen

Laufwerke, die Teil von sicheren virtuellen Laufwerken sind, werden als gesicherte Laufwerke bezeichnet. Gesicherte Laufwerke können von einem Controller auf einen anderen Controller migriert werden. Falls für den Zielcontroller eine andere Verschlüsselung oder ein anderer Sicherheitsschlüssel konfiguriert ist, wird der Sicherheitsstatus diese Laufwerke als „gesperrt“ angezeigt und lässt sich nicht als Teil der „Fremdkonfigurations-Vorschau“ einsehen. Die Funktion „Fremdkonfiguration importieren“ erkennt diese Fremdlaufwerke nicht.

Geben Sie während der Ausführung des Befehls zum Entsperren die Quellcontroller-Passphrase und die Schlüssel-ID für diese Laufwerke an. Auch nach dem Entsperren werden diese Laufwerke weiterhin vom „Fremdcontroller-Schlüssel“ gesichert. Sie können diese Laufwerke jedoch anzeigen, während Sie in der vorhandenen „Fremdkonfigurations-Vorschau“ nach Fremdlaufwerken suchen. Sie können die Fremdkonfiguration auf diese sichere Laufwerke importieren oder sie löschen.

Wenn Fremdlaufwerke mit unterschiedlicher Sicherheitsschlüsseln von mehr als einem Controller migriert werden, müssen Sie den Satz von Laufwerken von einem Fremdcontroller entsperren und importieren oder löschen, bevor die Laufwerke entsperrt werden, die von einem anderen Controller migriert wurden. Diese Maßnahme gewährleistet, dass das Entsperren auf einem Controller nicht zugelassen wird, wenn der Controller über Laufwerke verfügt, die zwar entsperrt, aber nicht importiert oder gelöscht wurden.

Sobald Laufwerke entsperrt sind, können Sie die Fremdkonfiguration unter Verwendung der CMC Web-Schnittstelle oder RACADM importieren.

Wenn der Controller nach dem Entsperren und vor dem Importieren aus- und wieder eingeschaltet wird, werden die Laufwerke erneut gesperrt.

Wenn das System über mehrere Fremdkonfigurationen verfügt, müssen Sie jede Fremdkonfiguration entsperren und importieren, bevor Sie die Fremdkonfiguration entsperren.

Die beim Entsperren verwendete Schlüssel-ID dient nur zur Identifizierung der Laufwerke durch Abgleich der Schlüssel-ID. Nachdem die passenden Laufwerke gefunden wurden, werden sie mithilfe der Passphrase entsperrt.

Entsperren von Fremdkonfigurationen über die CMC-Webschnittstelle

So wird die Fremdkonfiguration entsperrt:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Speicher** > **Controller** > **Setup**.
2 Wechseln Sie zur Seite **Setup**.
3 Klicken Sie auf **Zum Entsperren hier klicken**.
Die Seite **Physische Festplatten** wird angezeigt.
4 Wählen Sie die physischen Festplatten aus, die Sie entsperren möchten.
5 Überprüfen Sie, ob die physische Festplatte mit der Schlüsselkennung verknüpft ist.
6 Wählen Sie in der Dropdown-Liste **Aktionen** den Eintrag **Laufwerk entsperren** aus.
Ein Dialogfeld wird angezeigt, das Sie dazu auffordert, das Sicherheitsschlüsselwort einzugeben.
7 Geben Sie eine Passphrase in das Textfeld **Sicherheitsschlüssel-Passphrase** ein.
8 Geben Sie die Passphrase erneut ein und klicken Sie auf **Entsperren**.
Das physikalische Laufwerk wird entsperrt und nicht mehr in der Liste **Physische Laufwerke wiederherstellen** angezeigt.

Entsperren von Fremdkonfigurationen unter Verwendung von RACADM

Um Fremdkonfigurationen durch Ausführen eines RACADM-Befehls zu entsperren, verwenden Sie die folgende Syntax:

```
racadm raid unlock:<Controller FQDD> -key <Key id> -passwd <passphrase>
```

Weitere Informationen finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

Kryptografischer Löschvorgang

Sie können die kryptografische Löschoption verwenden, um Daten auf gesicherten SEDs auf sichere Weise zu löschen. Da sichere Daten auch nach dem Löschen von virtuellen Laufwerken auf Festplatten vorhanden bleiben, sind sie potenziellen Gefahren ausgesetzt. Der kryptografische Löschvorgang kann in den folgenden Situationen durchgeführt werden:

- Daten löschen, um sichere Laufwerke auszumustern/wiederzuverwenden.
- Daten sicher löschen, wenn gesicherte und gesperrte Fremdkonfigurationen nicht importiert werden dürfen.
- Gesperrte Laufwerke wiederherstellen, wenn die Passphrase verloren geht.

Sie können den kryptografischen Löschvorgang auf einem oder mehreren physischen SED-Laufwerken durchführen.

VORSICHT: Bei Durchführung des kryptografischen Löschvorgangs werden alle Daten auf der physischen Festplatte gelöscht.

Durchführen des kryptografischen Löschvorgangs

Wenn die physische Festplatte zu einem virtuellen Laufwerk gehört, müssen Sie sie zuerst vom virtuellen Laufwerk trennen, bevor Sie den kryptografischen Löschvorgang durchführen können.
So führen Sie einen kryptografischen Löschvorgang aus:

1 Wechseln Sie im linken Fensterbereich auf **Speicher** > **Physische Festplatten** > **Setup**.

Die Seite **Physische Festplatten konfigurieren** wird angezeigt.

2 Wählen Sie die physische Festplatte aus, von der Sie die Daten löschen möchten.

3 Wählen Sie im Drop-Down-Menü **Maßnahmen für physische Festplatten** die Option **Kryptografischer Löschvorgang** aus, und klicken Sie auf **Anwenden**.

Es wird eine Meldung angezeigt, die Sie dazu auffordert, den Vorgang zu bestätigen.

4 Klicken Sie auf **Ja**, um fortzufahren.

Alle Daten von der ausgewählten physischen Festplatte werden gelöscht.

Zugangsrichtlinie für virtuelle Adapter auf virtuelle Festplatten anwenden

Achten Sie darauf, dass physische Festplatten im Gehäuse installiert sind und die virtuellen Festplatten erstellt sind.
So wenden Sie die Zugangsrichtlinie für virtuelle Adapter an:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Speicher** > **Virtuelle Festplatten** > **Verwalten**.

2 Wählen Sie auf der Seite **Virtuelle Festplatten zuweisen** im Abschnitt **Zugangsrichtlinie für virtuelle Adapter** aus dem Drop-Down-Menü **Virtuelle Adapter <Nummer>** für jedes physische Festplattenlaufwerk **Voller Zugriff** aus.

3 Klicken Sie auf **Anwenden**.

Sie können nun virtuelle Adapter auf Server-Steckplätze zuweisen. Weitere Informationen finden Sie im Abschnitt „Zuweisen von virtuellen Adaptern auf Steckplätze“ in diesem Benutzerhandbuch.

Ändern der Eigenschaften von virtuellen Festplatten unter Verwendung der CMC Web-Schnittstelle

So ändern Sie die Eigenschaften virtueller Festplatten:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Speicher** > **Virtuelle Festplatten** > **Verwalten**.

2 Wählen Sie aus der Seite **Virtuelle Laufwerke verwalten** das Drop-Down-Menü **Maßnahmen für virtuelle Festplatten** aus, wählen Sie eine der folgenden Maßnahmen, und klicken Sie dann auf **Anwenden**.

- **Umbenennen**
- **„Löschen“**

ANMERKUNG: Wenn Sie Löschen auswählen, wird die folgende Meldung angezeigt, die angibt, dass durch das Löschen einer virtuellen Festplatte die Daten auf dieser Festplatte dauerhaft gelöscht werden.

```
Deleting the virtual disk removes the virtual disk from the controller's configuration.
Initializing the virtual disk permanently erases data from the virtual disk.
```

- **Richtlinie bearbeiten: Lese-Cache**
- **Richtlinie bearbeiten: Schreib-Cache**
- **Richtlinie bearbeiten: Festplatten-Cache**
- **Initialisieren: Schnell**
- **Initialisieren: Voll**

- **Virtuelle Festplatte verschlüsseln**

Gehäuseverwaltungsmodul

Das Gehäuseverwaltungsmodul (EMM) stellt Datenpfad- und Gehäuseverwaltungsaufgaben für Gehäuse bereit. EMM überwacht und steuert Gehäusekomponenten und Zugriff auf die Laufwerke.

EMM kommuniziert Gehäuseattribute und -zustände an den Host-Server. EMM-Module überwachen die folgenden Komponenten des Gehäuses:

- Lüfter
- Netzteile
- Temperatursonden
- Einsetzen oder Entfernen einer physischen Festplatte
- LED-Anzeigen am Gehäuse

Anzeigen von EMM-Status und -Attributen

Der EMM-Status zeigt den Zustand des EMM an. EMMs enthalten einen eindeutigen Statuswert vom Gehäuse. Sie können über bis zu zwei EMMs verfügen. Die Gehäuse-Firmware erstellt einen Status für jedes EMM.

Anzeigen von EMM-Status und -Attributen unter Verwendung der Web-Schnittstelle

So zeigen Sie den Status und die Attribute des EMM an:

Klicken Sie auf **Gehäuseübersicht** → **Speicher** → **Gehäuse** → **Eigenschaften**. Die Seite **Gehäuse** stellt den EMM-Status und die Attribute der Gehäuse im Gehäuse bereit. Erweitern Sie das integrierte Gehäuse oder externe Gehäuse zum Anzeigen des Status und der Attribute des EMM. Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.

Anzeigen von EMM-Status und -Attributen unter Verwendung von RACADM

Zum Anzeigen des Status von EMM verwenden Sie den Befehl `racadm raid get emms -o -p Status`.

Verwenden Sie zur Anzeige der Attribute von EMM den Befehl `racadm raid get emms -o`.

Weitere Informationen finden Sie im *Chassis Management Controller für PowerEdge VRTX RACADM-Befehlszeilen-Referenzhandbuch* unter **dell.com/support/manuals**.

Anzeigen des Status und der Attribute des Gehäuses

Der CMC zeigt den Funktionszustand des Gehäuses basierend auf dem physikalischen Komponenten an. Daten von den am freigegebenen Speicher angeschlossenen Gehäusen werden im CMC angezeigt, aber die externen ein einigen wenigen PCIe-Karten angeschlossenen Gehäuse werden nicht angezeigt. Sie müssen über CMC-Anmeldeberechtigungen zum Anzeigen des Status und der Attribute der Gehäuse verfügen.

Anzeigen des Gehäusestatus und der Attribute über die Webschnittstelle

So zeigen Sie den Status und die Attribute des Gehäuses an:

Klicken Sie auf **Gehäuseübersicht** → **Speicher** → **Gehäuse** → **Eigenschaften**. Die Seite **Gehäuse** stellt den Funktionszustand der Gehäuse im Gehäuse bereit. Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.

ANMERKUNG: Der Rollup-Status des Gehäuses wird kritisch, wenn das EMM, das Netzteil oder der Lüfter entfernt wird, aber der primäre Status bleibt unverändert. Nachdem der CMC oder das Gehäuse aus- und wieder eingeschaltet wurde, ändert sich auch der primäre Status zu kritisch.

Anzeigen von Status und Attributen des Gehäuses unter Verwendung von RACADM

Zum Anzeigen des Status des Gehäuses verwenden Sie den Befehl `racadm raid get enclosures -o -p Status`.

Zum Anzeigen der Attribute des Gehäuses verwenden Sie den Befehl `racadm raid get enclosures -o`.

Weitere Informationen finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX* unter **dell.com/support/manuals**.

Melden von bis zu zwei Gehäusen pro Konnektor

Jede externe freigegebene PERC 8-Karte unterstützt bis zu zwei Gehäuse pro Konnektor. Es gibt jedoch zwei unterschiedliche Konfigurationen mit unterschiedlichen Einschränkungen. In einer (nicht fehlertoleranten) Konfiguration mit einem einzelnen PERC können Sie bis zu zwei Gehäuse pro Karte anschließen. Wegen einer redundanten Verkabelung unterstützt eine fehlertolerante externe freigegebene PERC 8-Kartenlösung bis zu zwei Gehäuse pro fehlertolerantem Paar.

Wenn mehr als zwei Gehäuse auf einem beliebigen Anschluss erkannt werden, wird eine Warnmeldung im Gehäuseprotokoll protokolliert. Dies wirkt sich auf den Funktionszustand des Gehäuses aus und stellt eine aktive Warnung oder einen Gehäuse-Protokolleintrag bereit.

Einstellung von Systemkennnummer und Bestandsname des Gehäuses

Zur Identifizierung der Gehäuse stellen Sie den Bestandsnamen und die Systemkennnummer der Gehäuse ein.

ANMERKUNG:

- Ein Fehler wird angezeigt, wenn Sie einen ungültigen Wert eingeben.
- Anfänglich wird der Wert, der in der Firmware gespeichert wurde, angezeigt.
- Sie müssen die Berechtigung zur Gehäusekonfiguration haben, um die Systemkennnummer und den Bestandsnamen des Gehäuses einzustellen.
- Sie können Systemkennnummer und Bestandsname nur für externe Gehäuse festlegen.

Einstellen von Systemkennnummer und der Bestandsname des Gehäuses unter Verwendung der Web-Schnittstelle

Zum Festlegen einer Systemkennnummer und eines Bestandsnamens des Gehäuses klicken Sie auf **Gehäuseübersicht** → **Speicher** → **Gehäuse** → **Setup**. Geben Sie die **Systemkennnummer** und den **Bestandsnamen** in die entsprechenden Felder ein, und klicken Sie dann auf **Anwenden**. Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.

Einstellen von Systemkennnummer und der Bestandsname des Gehäuses unter Verwendung von RACADM

Verwenden Sie zum Einstellen der Systemkennnummer des Gehäuses den Befehl `racadm raid set enclosures: Enclosure.External.0-0:RAID.ChassisSlot.5-1 -p AssetTag <value>`.

Verwenden Sie zum Einstellen des Bestandsnamens des Gehäuses den Befehl `racadm raid set enclosures: Enclosure.External.0-0:RAID.ChassisSlot.5-1 -p AssetName <value>`.

Weitere Informationen finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX* unter **dell.com/support/manuals**.

Anzeigen des Temperatursondenstatus und der Attribute des Gehäuses

Der Temperatursondenstatus zeigt den Status der Temperatursensoren des Gehäuses an. Sensoren enthalten einen eindeutigen Statuswert vom Gehäuse. Sie können bis zu vier Temperatursensoren oder Sonden haben, und die Gehäuse-Firmware erstellt einen Status für jeden Sensor. Sie müssen zum Anzeigen des Temperatursondenstatus über CMC-Anmeldeberechtigungen verfügen.

Anzeigen des Temperatursondenstatus und der Attribute des Gehäuses unter Verwendung der Web-Schnittstelle

So zeigen Sie den Temperatursondenstatus und die Attribute des Gehäuses an:

Klicken Sie auf **Gehäuseübersicht** → **Speicher** → **Gehäuse** → **Eigenschaften**. Die Seite **Gehäuse** bietet eine Übersicht über den Funktionszustand und die Attribute für die Temperatursonde des Gehäuses im Gehäuse. Erweitern Sie das externe Gehäuse zur Anzeige des Status für den Netzteil der Gehäuse. Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.

Anzeigen von Temperatursondenattributen des Gehäuses unter Verwendung von RACADM

Um Temperatursondenattribute des Gehäuses anzuzeigen, verwenden Sie den Befehl `racadm raid get tempprobes -o`. Weitere Informationen finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX) unter **dell.com/support/manuals**.

Einstellen des Temperaturwarnungsschwellenwerts des Gehäuses

Der Temperaturwarnungsschwellenwert ermöglicht Ihnen das Ändern des Schwellenwerts, bei dem eine Gehäusetemperatur eine Warnung erzeugt.

ANMERKUNG:

- Ein Fehler wird angezeigt, wenn Sie einen ungültigen Wert eingeben.
- Anfänglich wird der Wert, der in der Firmware gespeichert wurde, angezeigt.
- Sie müssen die Berechtigung zur Gehäusekonfiguration haben, um die Systemkennnummer und den Bestandsnamen des Gehäuses einzustellen.

Einstellen des Temperaturwarnungsschwellenwerts des Gehäuses unter Verwendung der Web-Schnittstelle

So stellen Sie den Temperaturwarnungsschwellenwert des Gehäuses ein.

Klicken Sie auf **Gehäuseübersicht** → **Speicher** → **Gehäuse** → **Setup**. Wählen Sie das Gehäuse aus dem Dropdown-Menü **Gehäuse**, dann geben Sie die entsprechenden Mindest- und Höchstwerte für die Warnungsschwellenwert-Temperaturen von Temp-Sensor 2 und 3 ein. Geben Sie die **Systemkennnummer** und den **Bestandsnamen** in die entsprechenden Felder ein, und klicken Sie dann auf **Anwenden**. Weitere Informationen finden Sie in der *CMC- Online-Hilfe*.

Einstellen des Temperaturwarnungsschwellenwerts des Gehäuses unter Verwendung von RACADM

Um den minimalen Warnungsschwellenwert der Temperatursonde im Gehäuse festzulegen, verwenden Sie den Befehl `racadm raid set tempprobes:TempSensor.Embedded.0:Enclosure.External.1-0:RAID.ChassisSlot.6-1 -p MinimumWarningThreshold <value>`.

Für das Einstellen des maximalen Warnungsschwellenwerts der Temperatursonde im Gehäuse verwenden Sie den Befehl `racadm raid set tempprobes:TempSensor.Embedded.0:Enclosure.External.1-0:RAID.ChassisSlot.6-1 -p MaximumWarningThreshold <value>`.

Weitere Informationen finden Sie im *Chassis Management Controller für PowerEdge VRTX RACADM-Befehlszeilen-Referenzhandbuch* unter **dell.com/support/manuals**.

Anzeigen des Lüfterstatus und der Attribute des Gehäuses

Lüfterstatus und Attribute zeigen den Status des Gehäuselüfters an und enthalten einen einmaligen Statuswert vom Gehäuse. Sie können bis zu zwei Lüfter haben, und die Gehäuse-Firmware erstellt einen Status für jeden Lüfter. Sie müssen über CMC-Anmeldeberechtigungen zum Anzeigen des Lüfterstatus verfügen.

ANMERKUNG: Wenn ein Netzteil fehlt, zeigt der zugehörige Lüfter des Netzteils einen kritischen Status an.

Anzeigen des Lüfterstatus und der Attribute des Gehäuses unter Verwendung der Web-Schnittstelle

So zeigen Sie den Status und die Attribute der Netzteile an:

Klicken Sie auf **Gehäuseübersicht** → **Speicher** → **Gehäuse** → **Eigenschaften**. Die Seite **Gehäuse** bietet eine Übersicht über den Funktionszustand und Attribute für den Lüfter des Gehäuses. Erweitern Sie das externen Gehäuse zur Anzeige des Status für den Lüfter des Gehäuses. Weitere Informationen finden Sie in der *CMC- Online-Hilfe*.

Anzeigen des Lüfterstatus und der Attribute des Gehäuses unter Verwendung von RACADM

Zum Anzeigen des Lüfterstatus verwenden Sie den Befehl `racadm raid get fans -o -p Status`.

Verwenden Sie zur Anzeige der Attribute des Lüfters den Befehl `racadm raid get fans -o`.

Weitere Informationen finden Sie im *Chassis Management Controller für PowerEdge VRTX RACADM-Befehlszeilen-Referenzhandbuch* unter **dell.com/support/manuals**.

Anzeigen von Gehäuseeigenschaften unter Verwendung der CMC-Webschnittstelle

So zeigen Sie die Gehäuseeigenschaften an:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Speicher** > **Gehäuse** > **Eigenschaften**.

2 Klicken Sie auf der Seite **Eigenschaften** unter dem Abschnitt **Gehäuse** auf das , um eine graphische Ansicht der physischen Festplattenlaufwerke und deren Zustände, eine Zusammenfassung der Steckplätze der physischen Festplattenlaufwerke und von erweiterten Eigenschaften anzuzeigen.

16

PCIe-Steckplätze.verwalten

Standardmäßig sind keine Steckplätze zugewiesen. Sie können Folgendes ausführen:

- Sie können den Status aller PCIe-Steckplätze im Gehäuse anzeigen.
- Weisen Sie den Servern einen zugewiesenen PCIe-Steckplatz zu, oder heben Sie die Zuweisung auf.

Berücksichtigen Sie die folgenden Faktoren, bevor Sie einem Server einen PCIe-Steckplatz zuweisen:

- Ein leerer PCIe-Steckplatz kann einem Server, der eingeschaltet ist, nicht zugewiesen werden.
- Ein PCIe-Steckplatz mit einem Adapter, der einem Server zugewiesen ist, kann keinem anderen Server zugewiesen werden, wenn der zurzeit zugewiesene Server (Quelle) eingeschaltet ist.
- Ein PCIe-Steckplatz mit einem Adapter, der einem Server zugewiesen ist, kann keinem anderen Server (Ziel) zugewiesen werden, wenn der Server eingeschaltet ist.

Berücksichtigen Sie die folgenden Schritte, bevor Sie einen zugewiesenen PCIe-Steckplatz von einem Servern entfernen:

- Wenn ein PCIe-Steckplatz leer ist, kann die Zuweisung eines Steckplatzes zu einem Server aufgehoben werden, selbst wenn der Server eingeschaltet ist.
- Wenn ein PCIe-Steckplatz Adapter hat und nicht eingeschaltet ist, kann seine Zuweisung zu einem Server aufgehoben werden, selbst wenn der Server eingeschaltet ist. Dies kann vorkommen, wenn ein Steckplatz leer ist und der zugewiesene Server eingeschaltet ist, und wenn dann ein Benutzer einen Adaper in den leeren Steckplatz einsetzt.

Zuordnen oder Aufheben der Zuordnung des externen PCIe Adapters zu einem Blade:

- Als nicht freigegebenes Gerät ist ein Adapter immer eingeschaltet. Von jetzt an wird ein Adapter einem einzigen Server zugewiesen.
- Wenn ein externer PCIE-Steckplatz durch einen freigegebenen Adapter belegt ist, bleibt die Zuweisung vor dem eingesetzten Adapter unverändert.
- Wenn ein externer PCIE-Steckplatz von einem freigegebenen Adapter belegt ist, kann der PCIE-Steckplatz möglicherweise nicht einem Blade-Server zugeordnet werden, und diese Zuordnung kann auch nicht aufgehoben werden. Wenn ein Benutzer versucht, einen freigegebenen Adapter zuzuordnen bzw. die Zuordnung aufzuheben, wird eine EEMI-Meldung protokolliert.

Weitere Informationen zum Zuweisen zum oder zum Entfernen der Zuweisung für einen zugewiesenen PCIe-Steckplatz von einem Servern finden Sie in der *Online-Hilfe*.

ANMERKUNG:

- Ohne Lizenz können Sie maximal vier PCIe-Steckplätze mit voller Bauhöhe zuweisen und zwar zwei an den oberen Steckplatz und zwei an den Erweiterungssteckplatz oder zwei PCIe-Geräte an einen Server mit halber Bauhöhe.
- Sie können die Eigenschaften von externen PCIE-Steckplätzen mit externen freigegebenen PERC 8-Kartengeräten von dedizierten Geräten unterscheiden, diese freigegebenen Geräte besitzen andere Eigenschaften als dedizierte Geräte.
- Im Falle eines externen SPERC wird der Status „Freigegeben“ angezeigt. Die Optionen zum Zuordnen bzw. Aufheben der Zuordnung der externen freigegebenen PERC 8-Karte sind nicht verfügbar.

Themen:

Anzeigen von PCIe-Steckplatz-Eigenschaften unter Verwendung der CMC Web-Schnittstelle

- Um die Informationen über alle acht PCIe-Steckplätze im linken Fensterbereich anzuzeigen, klicken Sie auf **Gehäuseübersicht** > **PCIe-Übersicht**. Klicken Sie auf das , um alle Eigenschaften für den erforderlichen Steckplatz anzuzeigen.
- Um die Informationen eines PCIe-Steckplatzes anzuzeigen, klicken Sie auf **Gehäuseübersicht** > **PCIe-Steckplatz <Nummer>** > **Eigenschaften** > **Status**.

ANMERKUNG: Die Benutzeroberfläche differenziert die externen PCIe-Steckplätze, die SPERC- (oder freigegebene) Geräte enthalten, die von externen PCIe-Steckplätzen aus mit dedizierten Adaptern installiert wurden, da diese freigegebenen Geräte unterschiedliche Eigenschaften besitzen.

Zuweisung von PCIe-Steckplätzen an Server unter Verwendung der CMC-Webschnittstelle

So können Sie den Servern PCIe-Steckplätze zuweisen:

- Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **PCIe-Übersicht** > **Setup** > **Zuordnung: PCIe-Steckplätze zu Server-Steckplätzen**. Wählen Sie auf der Seite **Zuordnung: PCIe-Steckplätze zu Server-Steckplätzen** in der Spalte **Maßnahme** aus dem Drop-Down-Menü **Maßnahme** den entsprechenden Servernamen aus, und klicken Sie dann auf **Anwenden**.

Beachten Sie Folgendes:

- Ohne Lizenz können Sie einem Server mit halber Höhe maximal zwei PCIe-Slots zuordnen. Wenn ein Server in voller Bauhöhe installiert ist, können Sie dem oberen Server-Steckplatz zwei PCIe-Steckplätze und dem unteren (erweiterten) Server-Steckplatz zwei PCIe-Steckplätze zuordnen, also insgesamt vier PCIe-Steckplätze pro Server mit voller Höhe**.**
- Sie können die Server-Steckplätze beliebigen der acht PCIe-Steckplätze zuordnen.
- Bei einem Server mit voller Höhe sind sowohl die oberen als auch die unteren Mezzanines ausgefüllt. Andernfalls werden sie während des POST angehalten, wenn die Tasten <F1> oder <F2> auf der Seite angezeigt und Sie aufgefordert werden, eine beliebige Taste zu drücken.
- Für Server voller Höhe können Sie maximal zwei PCIe-Steckplätze den oberen und zwei den unteren Mezzanines zuordnen. Standardmäßig gehen alle PCIe-Zuweisungen auf Serversteckplatz 3 auf die unteren Mezzanines.
- Server-Steckplatz wird als Slot-01, Slot-02 usw. angezeigt. Bei einem Server mit voller Höhe wird der Steckplatzname als Erweiterung, also Ext. von Slot-01, Ext. von Slot-02 usw. angezeigt.
- Wenn Sie den Host-Namen auswählen, wird statt des Steckplatznamens der Host-Name angezeigt.
- CMC bietet Warnmöglichkeiten durch das Systemereignisprotokoll (System Event Log, SEL), SNMP und E-Mail-Schnittstellen.

Weitere Informationen über das Zuweisen von PCIe-Geräten finden Sie in der *Online-Hilfe*.

PCIe-Steckplätze unter Verwendung von RACADM verwalten

Sie können einen PCIe-Steckplatz unter Verwendung der RACADM-Befehle einem Server zuweisen oder die Zuweisung aufheben. Einige der Befehle werden hier angegeben. Weitere Informationen über RACADM-Befehle finden Sie unter *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX), verfügbar unter dell.com/support/manuals.

- Führen Sie zum Anzeigen der aktuellen Zuweisung der PCIe-Geräte zu Servern den folgenden Befehl aus:

```
racadm getpiecfg -a
```

- Führen Sie zum Anzeigen der Eigenschaften für PCIe-Geräte mithilfe von FQDD den folgenden Befehl aus:

  ```
  racadm getpciecfg [-c <FQDD>]
  ```

  Um zum Beispiel die Eigenschaften von PCIe-Gerät 1 anzuzeigen, führen Sie den folgenden Befehl aus.

  ```
  racadm getpciecfg -c PCIE.ChassisSlot.1
  ```

- Um einen PCIe-Adaptersteckplatz einem Servers teckplatz zuzuweisen, führen Sie den folgenden Befehl aus:

  ```
  racadm setpciecfg assign [-c <FQDD>] [i <server slot>]
  ```

- Um zum Beispiel PCIe-Steckplatz 5 dem Servers teckplatz 2 zuzuweisen, führen Sie den folgenden Befehl aus.

  ```
  racadm setpciecfg assign -c PCIE.ChassisSlot.5 -i 2
  ```

- Um die Zuweisung von PCIe-Steckplatz 3 von einem Server rückgängig zu machen, führen Sie den folgenden Befehl aus:

  ```
  racadm setpciecfg unassign -c pcie.chassisslot.3
  ```

PCIe-Energieüberbrückung

Die neu zugewiesenen PCIe-Karten in CMC VRTX müssen ermittelt und initialisiert werden, bevor ein Server-Knoten eingeschaltet wird. Die Ermittlung und Initialisierung umfasst die folgenden Schritte:

- Bestandsaufnahme und Ermittlung von installierten Karten
- Vorbereiten einer PCIe-Karte für ein Servermodul
- Vorbereiten mehrerer Karten für die Konfiguration durch das Server-BIOS
- Initialisieren aller Karten vor dem Einschalten eines Blade-Knotens

All diese Prozesse benötigen eine Laufzeit von wenigen Sekunden, dies führt zu Verzögerungen bei der Initialisierung der PCIe-Karten. Die PCIe-Überbrückungsfunktion in CMC VRTX reduziert diese Prozesszykluszeit. Die PCIe-Überbrückungsfunktion ermöglicht die folgenden Schritte:

- Die Server-Knoten werden schnell eingeschaltet, so dass die PCIe-Karten ebenfalls neu eingeschaltet werden.
- Der eingeschaltete Status der PCIe-Karten wird für einen vordefinierten Zeitraum in den folgenden Szenarien verlängert:
  - Nachdem der entsprechende Server ausgeschaltet ist.
  - Nachdem der Adapter-Ermittlungsprozess abgeschlossen ist.
- Der Einschaltbereitschaftsstatus der Karten wird nach der Ermittlung für einen vordefinierten Zeitraum verlängert. Diese Erweiterung eliminiert die Verzögerungen bei gängigen Einschaltszenarien. Die Karten bleiben im Bereitschaftsstatus und warten auf die Zuweisung und das Einschalten der Knoten. Die Karten werden nach Ablauf des Zeitraums heruntergefahren.

.

ANMERKUNG: Am Ende des Zeitraums werden die PCIe-Karten ausschalten. Alle Adapter im Überbrückungsmodus werden ebenfalls ausgeschaltet, sobald die Gehäuseabdeckung geöffnet wird.

ANMERKUNG:

- Wenn der CMC nicht über ausreichend Strom verfügt, werden alle Adapter ausgeschaltet, die sich im Überbrückungsmodus befinden, wodurch die gesamte diesen Adaptern zugewiesene Stromversorgung freigegeben wird. Sobald die Stromversorgung wiederhergestellt wird, wird den PCIe-Steckplätzen erneut Strom zugewiesen. Durch diese Wiederherstellung sind die Karten ohne Verzögerung bereit für die Server-Zuweisung.
- Alle externen PCIe-Adapter, die im Freigabemodus eingeschaltet werden, sind aus den Überbrückungsprozessen ausgeschlossen. Nachdem ein freigegebener Adapter als freigegebenes Gerät eingeschaltet wurde, bleibt er eingeschaltet, bis das Gehäuse ausgeschaltet wird.

Anzeigen von PCIe-Überbrückungseigenschaften über die CMC Webschnittstelle

Klicken Sie zum Anzeigen der PCIe-Überbrückungseigenschaften im linken Fenster auf **Gehäuseübersicht** > **PCIe-Übersicht**. Daraufhin wird die Seite **PCIe-Status** angezeigt. In Abschnitt **Allgemeinen Einstellungen** werden die folgenden PCIe-Überbrückungseigenschaftsstatus angezeigt:

- **Überbrückungsstatus** – Aktiviert oder Deaktiviert
- **Überbrückung - Zeitüberschreitung** – Gibt die Zeit an, für die die Überbrückungsfunktion aktiviert ist.

Anzeigen des Status der PCIe-Überbrückungseigenschaften über RACADM

Um die Informationen zu den PCIe-Überbrückungseigenschaften anzuzeigen, geben Sie den folgenden Befehl ein:

```
racadm getpciecfg –r
```

Weitere Informationen finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

Konfigurieren von PCIe-Überbrückungseigenschaften unter Verwendung der CMC-Webschnittstelle

So konfigurieren Sie die PCIe-Überbrückungseigenschaften für den CMC VRTX:

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Einrichtung** > **Überbrückung**.
   Daraufhin wird die Seite **PCIe-Überbrückungseinstellungen** angezeigt.
2. Um die PCIe-Überbrückungsfunktion zu aktivieren oder zu deaktivieren, aktivieren oder deaktivieren Sie die Option **PCIe-Überbrückung aktivieren**.

   ANMERKUNG: Standardmäßig ist die Überbrückungsfunktion aktiviert, und der Zeitraum ist mit 300 Sekunden festgelegt.
3. Geben Sie in das Feld **Zeitüberschreitung** die Zeit ein, für die die Überbrückungsfunktion aktiviert werden soll.
   Geben Sie entweder null (0) oder einen Wert zwischen 60 und 1.800 Sekunden ein. Null steht für eine nicht definierte Zeitüberschreitung.
4. Klicken Sie auf **Apply** (Anwenden).

Konfigurieren des Status für PCIe-Überbrückungseigenschaften über RACADM

Sie können die Eigenschaften der PCIe-Energieüberbrückung konfigurieren, indem Sie die folgenden Befehle ausführen:

- Führen Sie zum Deaktivieren der Überbrückungsfunktion den Befehl `racadm setpciecfg ridethru –d` aus.
- Führen Sie zum Aktivieren der Überbrückungsfunktion den Befehl `racadm setpciecfg ridethru –e` aus.
- Führen Sie zum Zurücksetzen der Eigenschaft für die Überbrückungszeitüberschreitung den Befehl `racadm setpciecfg ridethru –t <timeout>` aus.

- Führen Sie zum Festlegen eines akzeptablen Zeitüberschreitungsbereichs den Befehl `racadm setpciecfg help ridethru` aus.

Weitere Informationen finden Sie im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

17

Fehlerbehebung und Wiederherstellung

Dieser Abschnitt erklärt, wie Tasks unter Verwendung der CMC-Webschnittstelle ausgeführt werden, die sich auf die Wiederherstellung und Behebung eines Problems auf dem Remote-System beziehen.

- Gehäuseinformationen anzeigen.
- Ereignisprotokolle anzeigen.
- Konfigurationsinformationen, Fehlerstatus und Fehlerprotokolle sammeln.
- Diagnosekonsole verwenden.
- Strom auf einem Remote-System verwalten.
- Lifecycle Controller-Jobs auf einem Remote-System verwalten.
- Komponenten zurücksetzen.
- Fehlerbehebung bei Network Time Protocol (NTP)-Problemen.
- Fehlerbehebung bei Netzwerkproblemen.
- Fehlerbehebung bei Warnmeldungsproblemen.
- Vergessenes Administratorkennwort zurücksetzen.
- Gehäusekonfigurationseinstellungen und Zertifikate speichern und wiederherstellen.
- Fehlercodes und -protokolle anzeigen.

ANMERKUNG: WinRM-Support für Microsoft ist nicht für Windows 10 Client verfügbar. Verwenden Sie Power Shell anstelle von WinRM.

Themen:

Vergessenes Administratorkennwort zurücksetzen

Im folgenden Verfahren wird erklärt, wie das vergessene Administratorkennwort zurückgesetzt wird:

- Entfernen Sie das CMC-Modul aus dem Gehäuse.

- Verkürzen Sie die Header-Pins **Kennwortwiederherstellung** unter Verwendung von Jumper
- Setzen Sie das CMC-Modul wieder in das Gehäuse ein. Nachdem sich der CMC im Onlinestatus befindet, sind die Standard-Anmeldeinformationen aktiv (Benutzername: root/Kennwort: calvin)
- Melden Sie sich am CMC unter Verwendung der Standard-Anmeldeinformationen an, und ändern Sie das Kennwort
- Nachdem das Kennwort geändert wurde, entfernen Sie das CMC-Modul und den Jumper aus dem Header **Kennwortwiederherstellung**
- Setzen Sie das CMC-Modul wieder in das Gehäuse ein. Nachdem sich der CMC im Onlinestatus befindet, sind die neuen Anmeldeinformationen aktiv

Konfigurationsinformationen und Gehäusestatus und Protokolle unter Verwendung von RACDUMP sammeln

Der Unterbefehl `racdump` bietet die Möglichkeit, mit einem einzigen Befehl umfassende Informationen zu Gehäusestatus, Konfigurationsstatus und den historischen Ereignisprotokollen abzufragen.

Der `racdump`-Unterbefehl zeigt die folgenden Informationen an:

- Allgemeine System-/RAC-Informationen
- CMC-Informationen
- Gehäuseinformationen
- Sitzungsinformationen
- Sensorinformationen
- Firmware-Build-Informationen

Unterstützte Schnittstellen

- CLI-RACADM
- Remote-RACADM
- Telnet-RACADM

`racdump` beinhaltet die folgenden Untersysteme und verbindet die folgenden RACADM-Befehle: Weitere Informationen zu `racdump` finden Sie im *RACADM Command Line Reference Guide for CMC in PowerEdge VRTX* (RACADM-Befehlszeilen-Referenzhandbuch für CMC in PowerEdge VRTX).

Tabelle 42. RACADM-Befehle für Subsysteme

Untersystem	RACADM-Befehl
Allgemeine System-/RAC-Informationen	`getsysinfo`
Sitzungsinformationen	`getssninfo`
Sensorinformationen	`getsensorinfo`
Switches-Informationen (EA-Modul)	`getioinfo`
Mezzanine-Karteninformationen (Tochterkarte)	`getdcinfo`
Informationen zu allen Modulen	`getmodinfo`
Strombudgetinformationen	`getpbinfo`
KVM-Informationen	`getkvminfo`

Untersystem	RACADM-Befehl
NIC-Informationen (CMC-Modul)	`getniccfg`
Redundanzinformationen	`getredundancymode`
Ablaufverfolgungsprotokollinformationen	`gettracelog`
RAC-Ereignisprotokoll	`getraclog`
System-Ereignisprotokoll	`getsel`

Herunterladen der Datei für die SNMP-Verwaltungsinformationsbasis

Die SNMP-MIB-Datei (Management Information Base, Verwaltungsinformationsbasis) des CMC definiert die Gehäusetypen, Ereignisse und Anzeigen. Mit CMC können Sie die MIB-Datei über die Webschnittstelle herunterladen.

So laden Sie die SNMP-MIB-Datei des CMC über die Webschnittstelle herunter:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Netzwerk** > **Dienste** > **SNMP**.

2 Klicken Sie im Abschnitt **SNMP-Konfiguration** auf **Speichern**, um die CMC-MIB-Datei auf Ihr lokales System herunterzuladen.
Weitere Informationen zur SNMP-MIB-Datei finden Sie im *Dell OpenManage Server Administrator SNMP Reference Guide* (Dell OpenManage Server Administrator-SNMP-Referenzhandbuch) unter **dell.com/support/manuals**.

Erste Schritte, um Störungen an einem Remote-System zu beheben

Die folgenden Fragen werden häufig für die Fehlerbehebung bei Problemen auf hoher Ebene auf dem verwalteten System gestellt:

- Ist das System ein- oder ausgeschaltet?
- Wenn eingeschaltet, funktioniert das Betriebssystem, antwortet es nicht oder reagiert es nicht mehr?
- Wenn ausgeschaltet, wurde der Strom unerwartet ausgeschaltet?

Strombezogene Fehlerbehebung

Die folgenden Informationen sind Ihnen bei der Fehlerbehebung bei Netzteilen und bei der Stromversorgung hilfreich:

- **Problem:** Die **Stromredundanzregel** ist auf **Netzredundanz** eingestellt und es wurde ein Keine-Netzteilredundanz-Ereignis gemeldet.
  - **Lösung A**: Diese Konfiguration erfordert mindestens ein Netzteil auf Seite 1 (die linken zwei Steckplätze) und ein Netzteil auf Seite 2 (die rechten zwei Steckplätze), um im modularen Gehäuse vorhanden und funktionsfähig zu sein. Außerdem muss die Kapazität jeder Seite groß genug sein, um die gesamte Stromzuteilung für das Gehäuse zu unterstützen und die **Netzredundanz** zu erhalten. (Bei vollständigem Netzredundanzbetrieb sollten Sie sicherstellen, dass eine vollständige Netzteileinheitskonfiguration mit vier Netzteilen verfügbar ist.)
  - **Lösung B:** Prüfen Sie, ob alle Netzteile ordnungsgemäß an die beiden Wechselstromnetze angeschlossen sind; die Netzteile auf Seite 1 müssen mit dem einen Wechselstromnetz verbunden sein, und die Netzteile auf Seite 2 müssen mit dem anderen Wechselstromnetz verbunden sein. Beide Wechselstromnetze müssen funktionieren. **Netzredundanz** fällt aus, wenn eines der Wechselstromnetze nicht funktioniert.
- **Problem:** Der Zustand der Netzteileinheit wird als **Fehlgeschlagen (Kein Wechselstrom)** angezeigt, selbst wenn ein Netzkabel angeschlossen ist und der Stromverteiler ausreichenden Wechselstromausgang erzeugt.
  - **Lösung A:** Das Netzkabel prüfen und ersetzen. Prüfen und verifizieren Sie, dass der Stromverteiler, der Strom an das Netzteil liefert, ordnungsgemäß funktioniert. Falls der Fehler nach wie vor besteht, rufen Sie den Dell-Kundendienst an, um das Netzteil zu ersetzen.

- **Lösung B:** Überprüfen Sie, ob die Netzteileinheit an dieselbe Spannung angeschlossen ist wie die anderen Netzteileinheiten. Wenn der CMC feststellt, dass eine Netzteileinheit mit einer anderen Spannung arbeitet, dann wird die Netzteileinheit ausgeschaltet und als „Fehlerhaft“ markiert.

- **Problem:** Dynamische Netzteilzuschaltung (DPSE) ist aktiviert, doch keines der Netzteile wird im **Standby**-Modus angezeigt.
  - **Lösung A:** Es werden nur dann Netzteile in den Standby-Zustand versetzt, wenn der im Gehäuse verfügbare Überschussstrom die Kapazität von mindestens einem Netzteil übersteigt.
  - **Lösung B:** Die Dynamische Netzteilzuschaltung (DPSE) kann mit den Netzteileinheiten, die im Gehäuse vorhanden sind, nicht vollständig unterstützt werden. Um zu prüfen, ob dies der Fall ist, schalten Sie die Dynamische Netzteilzuschaltung mithilfe der Webschnittstelle aus und dann wieder ein. Es wird eine Meldung angezeigt, wenn die Dynamische Netzteilzuschaltung (DPSE) nicht voll unterstützt werden kann.
- **Problem:** Es wurde ein neuer Server in das Gehäuse mit ausreichend Netzteilen eingesetzt, doch der Server schaltet nicht ein.
  - **Lösung A:** Prüfen Sie die Eingangsleistungsgrenze des Systems. Die Einstellung ist u. U. zu niedrig konfiguriert, um ein Einschalten weiterer Server zu ermöglichen.
  - **Lösung B:** Überprüfen Sie die Einstellungen zum maximalen Stromsparmodus. Wenn dieser aktiviert ist, tritt dieses Problem auf. Weitere Einzelheiten dazu finden Sie in den Stromkonfigurationseinstellungen.
  - **Lösung C:** Prüfen Sie die Stromprioritäten des Serversteckplatzes, die dem neu eingesetzten Server zugewiesen ist, und stellen Sie sicher, dass die Priorität nicht niedriger ist als die Stromprioritäten aller übrigen Serversteckplätze.
- **Problem:** Verfügbare Leistung schwankt, selbst wenn die modulare Gehäusekonfiguration nicht verändert wurde.
  - **Lösung:** CMC verfügt über dynamisches Lüfterleistungsmanagement, das Serverstromzuweisungen kurzzeitig verringert, wenn das Gehäuse im Bereich der benutzerseitig konfigurierten maximalen Leistungsgrenze (Spitze) betrieben wird; es bewirkt, dass den Lüftern Strom durch Verringerung von Serverleistung zugewiesen wird, so dass die Eingangsleistungsaufnahme unterhalb der **Eingangsleistungsgrenze des Systems** gehalten werden kann. Dieses Verhalten ist normal.
- **Problem:** <Nummer> W wird als **Überschuss für Systemspitzen** gemeldet.
  - **Lösung:** Das Gehäuse hat in der derzeitigen Konfiguration <Nummer> W Überschussstrom verfügbar, und die **Eingangsleistungsgrenze des Systems** kann sicher um diesen gemeldeten Wert verringert werden, ohne dass die Serverleistung beeinträchtigt wird.
- **Problem:** Eine Teilmenge der Server hat nach einem Ausfall eines Wechselstromnetzes einen Stromausfall erfahren, obwohl das Gehäuse in der **Netzredundanz**-Konfiguration mit vier Netzteilen betrieben wurde.
  - **Lösung:** Dies kann auftreten, wenn die Netzteile zum Zeitpunkt, an dem das Wechselstromnetz ausfällt, nicht korrekt an die redundanten Wechselstromnetze angeschlossen sind. Die **Netzredundanz**-Richtlinie schreibt vor, dass die zwei Netzteile auf der linken Seite an ein Wechselstromnetz angeschlossen werden und die zwei Netzteile auf der rechten Seite an ein anderes Wechselstromnetz angeschlossen werden. Wenn zwei Netzteileinheiten nicht korrekt angeschlossen sind (z. B. Netzteileinheit 2 und Netzteileinheit 3 an die falschen Wechselstromnetze), bewirkt der Ausfall des Wechselstromnetzes einen Ausfall der Stromversorgung zu den Servern niedrigster Priorität.
- **Problem:** Die Server niedrigster Priorität haben nach einem Ausfall der Netzteileinheit einen Stromausfall erfahren.
  - **Lösung:** Um weitere Netzteilfehler und ein nachfolgendes Abschalten der Server zu vermeiden, stellen Sie sicher, dass das Gehäuse mindestens drei Netzteile aufweist und für die **Netzteilredundanz**-Richtlinie konfiguriert ist, sodass ein Ausfall der Netzteileinheit den Serverbetrieb nicht beeinträchtigt.
- **Problem:** Die Gesamtserverleistung verringert sich, wenn die Umgebungstemperatur im Rechenzentrum ansteigt.
  - **Lösung:** Dies kann auftreten, wenn die **Eingangsleistungsgrenze** des Systems auf einen Wert konfiguriert wurde, der zu einem erhöhten Strombedarf durch die Lüfter führt und durch Verringerung in der Stromzuweisung zu den Servern wettgemacht werden muss. Der Benutzer kann die **Eingangsleistungsgrenze des Systems** auf einen höheren Wert setzen, der zusätzliche Stromzuweisung zu den Lüftern ermöglicht, ohne die Serverleistung zu beeinträchtigen.

Fehlerbehebungs-Alarme

Verwenden Sie das CMC- und das Ablaufverfolgungsprotokoll, um CMC-Fehlermeldungen zu behandeln. Der Erfolg oder das Fehlschlagen jedes einzelnen E-Mail- und/oder SNMP-Trap-Sendeversuches wird im CMC-Protokoll gespeichert. Zusätzliche Informationen, die die speziellen Fehler beschreiben, werden im Ablaufverfolgungsprotokoll gespeichert. Da SNMP jedoch die Übergabe von Traps nicht bestätigt, ist es am besten, die Pakete auf dem verwalteten System mit Hilfe eines Netzwerkanalysators oder eines Hilfsprogramms wie snmputil von Microsoft zu verfolgen.

Ereignisprotokolle anzeigen

Sie können Hardware- und Gehäuseprotokolle für Informationen über systemkritische Ereignisse, die auf dem verwalteten System auftreten, anzeigen.

Hardwareprotokoll anzeigen

Der CMC erstellt ein Hardwareprotokoll von Ereignissen, die im Gehäuse auftreten. Sie können das Hardwareprotokoll über die Webschnittstelle und Remote-RACADM anzeigen.

ANMERKUNG: Um das Hardwareprotokoll zu löschen, müssen Sie die Berechtigung als Administrator zum Löschen von Protokollen besitzen.

ANMERKUNG: Sie können den CMC so konfigurieren, dass E-Mail- oder SNMP-Traps gesendet werden, wenn bestimmte Ereignisse auftreten. Informationen zur Konfiguration des CMC zum Aussenden von Warnungen finden Sie unter Konfigurieren von CMC zum Senden von Warnungen.

Beispiele von Hardwareprotokolleinträgen

```
critical System Software event: redundancy lost
Wed May 09 15:26:28 2007 normal System Software
event: log cleared was asserted
Wed May 09 16:06:00 2007 warning System Software
event: predictive failure was asserted
Wed May 09 15:26:31 2007 critical System Software
event: log full was asserted
Wed May 09 15:47:23 2007 unknown System Software
event: unknown event
```

Anzeigen von Hardwareprotokollen unter Verwendung der CMC-Webschnittstelle

Sie können das Hardwareprotokoll anzeigen, löschen oder als Textdatei speichern. Sie können die Protokolleinträge nach Schweregrad, Datum/Uhrzeit oder Beschreibung sortieren, indem Sie auf die Spaltenüberschrift klicken. Wenn Sie wiederholt auf eine Spaltenüberschrift klicken, wird die Sortierung rückgängig gemacht.

Um die Hardware-Protokolle unter Verwendung der CMC-Webschnittstelle im linken Fensterbereich anzuzeigen, klicken Sie auf **Gehäuseübersicht** > **Protokolle**. Die Seite **Hardwareprotokoll** wird angezeigt. Um eine Kope des Hardwareprotokolls auf Ihre verwaltete Station oder auf Ihr Netzwerk zu speichern, klicken Sie auf **Protokoll speichern** und dann wählen Sie einen Speicherort für eine Textdatei des Protokolls aus.

ANMERKUNG: Weil das Protokoll als Textdatei gespeichert wurde, werden die Grafiken, die zur Kennzeichnung des Schweregrads in der Benutzeroberfläche verwendet werden, nicht angezeigt. In der Textdatei wird der Schweregrad mit den Worten OK, Zur Information, Unbekannt, Warnung und Schwerwiegend angezeigt. Die Einträge von Datum und Uhrzeit erscheinen in aufsteigender Reihenfolge. Wenn <SYSTEMSTART> in der Spalte Datum/Uhrzeit erscheint, bedeutet dies, dass das Ereignis während des Einschaltens oder des Ausschaltens eines Moduls aufgetreten ist, wenn Datum und Uhrzeit nicht verfügbar sind.

Um das Hardwareprotokoll zu löschen, klicken Sie auf **Protokoll löschen**.

ANMERKUNG: Der CMC erstellt einen neuen Protokolleintrag, der darauf hinweist, dass das Protokoll gelöscht wurde.

ANMERKUNG: Um das Hardwareprotokoll zu löschen, müssen Sie die Berechtigungen als Administrator zum Löschen von Protokollen aufweisen.

Hardware-Protokoll unter Verwendung von RACADM anzeigen

Um das Hardware-Protokoll mit RACADM anzuzeigen, öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole zum CMC, melden Sie sich an und geben Sie Folgendes ein:

```
racadm getsel
```

Um das Hardwareprotokoll zu löschen, geben Sie Folgendes ein:

```
racadm clrsel
```

Gehäuseprotokoll anzeigen

CMC erstellt ein Protokoll der mit dem Gehäuse verbundenen Ereignisse. CMC bietet Warnmöglichkeiten durch das Systemereignisprotokoll (System Event Log, SEL), SNMP und E-Mail-Schnittstellen.

SPERC wird eingesetzt, während ein oder mehrere PowerEdge-Server eingeschaltet werden.

ANMERKUNG:

- Um das Gehäuseprotokoll zu löschen, müssen Sie die Berechtigungen als **Administrator zum Löschen von Protokollen** aufweisen.

Gehäuseprotokolle unter Verwendung von RACADM anzeigen

Um die Gehäuseprotokollinformationen unter Verwendung von RACADM anzuzeigen, öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole zum CMC, melden Sie sich an und geben Sie Folgendes ein:

```
racadm chassislog view
```

Dieser Befehl zeigt die letzten 25 Gehäuseprotokolleinträge an.

Um die Optionen, die zur Anzeige der Gehäuseprotokolle verfügbar sind, anzuzeigen, führen Sie den folgenden Befehl aus:

```
racadm chassislog help view
```

Gehäuseprotokolle über die Webschnittstelle anzeigen

Sie können das Gehäuseprotokoll anzeigen, speichern und löschen. Sie können die Protokolle auf der Basis des Protokolltyps und des Filters filtern. Zusätzlich können Sie eine Suche, basieren auf ein Stichwort ausführen oder die Protokolle an bestimmten Tagen anzeigen.

Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Protokolle** > **Gehäuseprotokoll**. Die Seite **Gehäuseprotokoll** wird angezeigt.

Um eine Kopie des Gehäuseprotokolls auf Ihrer verwalteten Station oder im Netzwerk zu speichern, klicken Sie auf **Protokoll speichern** und dann geben Sie einen Speicherort an, um die Protokolldatei zu speichern.

Diagnosekonsole verwenden

Wenn Sie ein fortgeschrittener Benutzer oder ein Benutzer unter der Leitung des technischen Supports sind, können Sie Probleme im Zusammenhang mit der Gehäuse-Hardware unter Verwendung von CLI-Befehlen diagnostizieren.

ANMERKUNG: Um diese Einstellungen zu ändern, müssen Sie Berechtigungen als Administrator für Debug-Befehle haben.

So greifen Sie auf die Seite „Diagnosekonsole“ zu:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Fehlerbehebung** > **Diagnose**.

Die Seite **Diagnosekonsole** wird angezeigt.

2 Geben Sie im Textfeld **Befehl** einen Befehl ein und klicken Sie auf **Senden.**

Weitere Informationen zu den Befehlen finden Sie in der *Online-Hilfe*.

Es wird eine Seite mit Diagnoseergebnissen eingeblendet.

Komponenten zurücksetzen

Sie können den aktiven CMC zurücksetzen oder Server virtuell neu einsetzen und somit bewirken, dass diese sich so verhalten, als seien sie herausgenommen und wieder eingesetzt worden. Falls das Gehäuse einen Standby-CMC aufweist, bewirkt das Zurücksetzen des aktiven CMC einen Failover, und der Standby-CMC wird aktiviert.

ANMERKUNG: Zum Zurücksetzen von Komponenten müssen Sie die Berechtigung als Debug-Befehl-Administrator besitzen.

So setzen Sie die Komponenten bei Verwendung der CMC-Webschnittstelle zurück:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Fehlerbehebung** > **Komponenten zurücksetzen**.

Die Seite **Aktualisierbare Komponenten** wird angezeigt.

2 Um den aktiven CMC zurückzusetzen, klicken Sie im Abschnitt **CMC-Status** auf **CMC zurücksetzen/Failover**. Wenn ein Standby-CMC vorhanden ist und ein Gehäuse vollständig redundant ist, tritt ein Failover auf und bewirkt, dass der Standby-CMC aktiv wird. Wenn jedoch ein Standby-CMC nicht vorhanden ist, wird der vorhandene CMC neu gestartet.

3 Um den Server virtuell neu einzusetzen, wählen Sie im Abschnitt **Virtuelles Neueinsetzen von Servern** neu einzusetzende Server und klicken Sie dann auf **Auswahl anwenden**.

Weitere Informationen finden Sie in der *Online-Hilfe*.

Dieser Vorgang simuliert das Entfernen und Wiedereinsetzen eines Servers.

Gehäusekonfiguration speichern oder wiederherstellen.

Dies ist eine lizenzierte Funktion. So führen Sie eine Speicherung oder Wiederherstellung einer Gehäusekonfiguration unter Verwendung der CMC Webschnittstelle durch:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Setup** > **Gehäuse-Backup**. Die Seite **Gehäuse-Backup** wird angezeigt. Klicken Sie auf **Speichern**, um die Gehäusekonfiguration zu speichern. Überschreiben Sie den Standarddateipfad (optional) und klicken Sie auf **OK**, um die Datei zu speichern. Der standardmäßige Sicherungsdateiname enthält die Service-Tag-Nummer des Gehäuses. Diese Sicherungsdatei kann später verwendet werden, um die Einstellungen und Zertifikate für dieses eine Gehäuse wiederherzustellen.

2 Klicken Sie zum Wiederherstellen der Gehäusekonfiguration im Abschnitt „Wiederherstellen“ auf **Durchsuchen**, geben Sie die Sicherungsdatei an, und klicken Sie dann auf **Wiederherstellen**.

ANMERKUNG:

- CMC wird beim Wiederherstellen der Konfiguration nicht zurückgesetzt, jedoch kann es einige Zeit dauern, bis jedwede geänderte oder neue Konfiguration effektiv durch die CMC-Dienste durchgesetzt wird. Nach der erfolgreichen Fertigstellung werden alle aktuellen Sitzungen beendet.
- Flexaddress-Informationen, Server-Profile und erweiterte Speicher werden nicht mit der Gehäusekonfiguration gespeichert oder wiederhergestellt.

Fehlerbehebung bei Network Time Protocol (NTP)-Fehlern

Nach der Konfiguration des CMC zur Synchronisierung der Uhr mit einem Remote-Zeitserver über das Netzwerk kann es 2-3 Minuten dauern, bevor eine Änderung des Datums und der Uhrzeit in Kraft tritt. Falls nach Ablauf dieser Zeit immer noch keine Änderung erfolgt ist, handelt es sich möglicherweise um ein Problem, das behoben werden muss. Der CMC kann seine Uhr möglicherweise aus folgenden Gründen nicht synchronisieren:

- Es könnte ein Problem mit den Network Time Protocol (NTP)-Server 1-, NTP-Server 2- und NTP-Server 3-Einstellungen vorliegen.
- Es wurden versehentlich ein ungültiger Hostname oder eine ungültige IP-Adresse eingegeben.
- Es könnte ein Netzwerkverbindungsproblem geben, das verhindert, dass der CMC mit den konfigurierten NTP-Servern kommunizieren kann.
- Es könnte ein DNS-Problem geben, das verhindert, dass NTP-Server-Hostnamen aufgelöst werden können.

Überprüfen Sie zur Behebung von Fehlern, die mit NTP in Verbindung stehen, die Informationen im CMC-Ablaufverfolgungsprotokoll. Dieses Protokoll enthält eine Fehlermeldung für Ausfälle im Zusammenhang mit NTP. Falls der CMC keine Synchronisierung mit einem der konfigurierten Remote-NTP-Server vornehmen kann, wird die CMC-Zeit mit der lokalen Systemuhr synchronisiert und das Ablaufverfolgungsprotokoll enthält einen Eintrag der folgenden Art:

```
Jan 8 20:02:40 cmc ntpd[1423]: synchronized to LOCAL(0), stratum 10
```

Sie können den ntpd-Status auch prüfen, indem Sie den folgenden racadm-Befehl eingeben:

```
racadm getractime –n
```

Die Ausgabe dieses Befehls enthält detaillierte NTP-Statistikdaten, die für die Lösung des Problems nützlich sein können.

Wenn Sie versuchen, einen Windows-basierten NTP-Server zu konfigurieren, kann es hilfreich sein, den Parameter `MaxDist` für `ntpd` zu erhöhen. Bevor Sie diesen Parameter ändern, sollten Sie alle Auswirkungen einer solchen Änderung verstehen, da die Standardeinstellung ausreichend hoch sein muss, damit sie mit den meisten NTP-Servern funktioniert.

Um den Parameter zu ändern, geben Sie folgenden Befehl ein:

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpMaxDist 32
```

Nach Durchführung der Änderung deaktivieren Sie NTP, warten Sie 5-10 Sekunden und dann aktivieren Sie den NTP neu.

ANMERKUNG: NTP könnte drei zusätzliche Minuten benötigen, um neu zu synchronisieren.

Um NPT zu deaktivieren, geben Sie Folgendes ein:

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpEnable 0
```

Um NPT zu aktivieren, geben Sie Folgendes ein:

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpEnable 1
```

Wenn die NTP-Server richtig konfiguriert sind und dieser Eintrag im Ablaufverfolgungsprotokoll steht, dann bestätigt dies, dass sich der CMC nicht mit einem der konfigurierten NTP-Server synchronisieren kann.

Wenn die NTP-Server-IP-Adresse nicht konfiguriert ist, könnte ein Eintrag der folgenden Art vorhanden sein:

```
Jan 8 19:59:24 cmc ntpd[1423]: Cannot find existing interface for address 1.2.3.4 Jan 8
19:59:24 cmc ntpd[1423]: configuration of 1.2.3.4 failed
```

Falls eine NTP-Server-Einstellung mit einem ungültigen Hostnamen konfiguriert wurde, enthält das Ablaufverfolgungsprotokoll u. U. einen Eintrag der folgenden Art:

```
Aug 21 14:34:27 cmc ntpd_initres[1298]: host name not found: blabla Aug 21 14:34:27 cmc
ntpd_initres[1298]: couldn't resolve `blabla', giving up on it
```

Weitere Informationen zur Eingabe des Befehls `gettracelog` zur Prüfung des Ablaufverfolgungsprotokolls über die CMC-Webschnittstelle finden Sie unter Diagnosekonsole verwenden.

LED-Farben und Blinkmuster interpretieren

Die LEDs im Gehäuse geben den folgenden Status einer Komponente an:

- Beständig grün leuchtende LEDs zeigen an, dass die Komponente eingeschaltet ist. Wenn die grüne LED blinkt, weist dies auf ein kritisches, aber routinemäßiges Ereignis hin, wie etwa einen Firmware-Upload, währenddessen das Gerät nicht betriebsbereit ist. Dies weist nicht auf einen Fehler hin.
- Eine blinkende gelbe LED an einem Modul weist auf einen Fehler in diesem Modul hin.
- Blaue, blinkende LEDs können vom Benutzer konfiguriert und zur Identifizierung genutzt werden. Weitere Informationen zur Konfiguration finden Sie unter LEDs zum Identifizieren von Komponenten im Gehäuse konfigurieren.

Tabelle 43. LED-Farbe und Blinkmuster

Komponente	LED-Farbe, Blinkmuster	Status
CMC	Grün, beständig leuchtend	Eingeschaltet
	Grün, blinkend	Firmware wird hochgeladen
	Grün, dunkel	Ausgeschaltet
	Blau, beständig leuchtend	Aktiv
	Blau blinkend	Vom Benutzer aktivierte Modulidentifizierung
	Gelb, beständig leuchtend	Nicht verwendet
	Gelb blinkend	Fehler
	Blau, dunkel	Standby
Server	Grün, beständig leuchtend	Eingeschaltet
	Grün, blinkend	Firmware wird hochgeladen
	Grün, dunkel	Ausgeschaltet
	Blau, beständig leuchtend	Normal
	Blau blinkend	Vom Benutzer aktivierte Modulidentifizierung
	Gelb, beständig leuchtend	Nicht verwendet
	Gelb blinkend	Fehler
	Blau, dunkel	Kein Fehler
E/A-Modul (Allgemein)	Grün, beständig leuchtend	Eingeschaltet
	Grün, blinkend	Firmware wird hochgeladen
	Grün, dunkel	Ausgeschaltet
	Blau, beständig leuchtend	Normal/übergeordneter Stapel
	Blau blinkend	Vom Benutzer aktivierte Modulidentifizierung
	Gelb, beständig leuchtend	Nicht verwendet
	Gelb blinkend	Fehler
	Blau, dunkel	Kein Fehler/untergeordneter Stapel
E/A (Passthrough)	Grün, beständig leuchtend	Eingeschaltet

Komponente	LED-Farbe, Blinkmuster	Status
	Grün, blinkend	Nicht verwendet
	Grün, dunkel	Ausgeschaltet
	Blau, beständig leuchtend	Normal
	Blau blinkend	Vom Benutzer aktivierte Modulidentifizierung
	Gelb, beständig leuchtend	Nicht verwendet
	Gelb blinkend	Fehler
	Blau, dunkel	Kein Fehler
Gebläse	Grün, beständig leuchtend	Lüfter arbeitet
	Grün, blinkend	Nicht verwendet
	Grün, dunkel	Ausgeschaltet
	Gelb, beständig leuchtend	Lüftertyp nicht erkannt, aktualisieren Sie die CMC-Firmware
	Gelb blinkend	Lüfterfehler; außerhalb Drehzahlmessbereich
	Gelb, dunkel	Nicht verwendet
Netzteil	(Oval) Grün, beständig leuchtend	Wechselstrom OK
	(Oval) Grün, blinkend	Nicht verwendet
	(Oval) Grün, dunkel	Wechselstrom nicht OK
	Gelb, beständig leuchtend	Nicht verwendet
	Gelb blinkend	Fehler
	Gelb, dunkel	Kein Fehler
	(Kreis) Grün, beständig leuchtend	Gleichstrom OK
	(Kreis) Grün, dunkel	Gleichstrom nicht OK
schrank	Blau	Wenn der Hostserver das Gehäuse identifiziert
	Gelb	Eingeschaltet oder zurücksetzen, Störzustand

Fehlerbehebung an einem CMC, der nicht mehr reagiert

Wenn Sie sich nicht über eine der Schnittstellen beim CMC anmelden können (Webschnittstelle, Telnet, SSH, Remote-RACADM oder seriell), können Sie die Funktionsfähigkeit des CMC durch Beobachtung der LEDs auf dem CMC überprüfen, Wiederherstellungsinformationen über die serielle DB-9-Schnittstelle abrufen oder das CMC-Firmware-Abbild wiederherstellen.

ANMERKUNG: Es ist nicht möglich, sich über eine serielle Konsole beim Standby-CMC anzumelden.

Problem durch Beobachtung der LEDs erkennen

Es gibt zwei LEDs links auf der Karte:

- Die LED oben links – Zeigt den Stromstatus an. Wenn sie nicht eingeschaltet ist:
  - Überprüfen Sie, dass mindestens ein Netzteil mit Netzstrom versorgt wird.

- Überprüfen Sie, dass die CMC-Karte korrekt eingesetzt ist. Sie können die Entriegelung betätigen, den CMC entfernen, den CMC neu installieren und sicherstellen, dass die Platine vollständig eingeschoben ist und der Riegel richtig einrastet.

- Die LED unten links – Die untere LED ist mehrfarbig. Wenn der CMC aktiv ist und ausgeführt wird und keine Probleme vorliegen, leuchtet die untere LED blau. Wenn die LED gelb leuchtet, wurde ein Fehler erkannt. Der Fehler kann durch jedes der drei folgenden Ereignisse verursacht worden sein:
  - Kernfehler. In diesem Fall muss die CMC-Platine ausgetauscht werden.
  - Selbsttestfehler. In diesem Fall muss die CMC-Platine ausgetauscht werden.
  - Beschädigung des Image. In diesem Fall können Sie den CMC durch Hochladen des CMC-Firmware-Image wiederherstellen.

ANMERKUNG: Ein normaler CMC-Start/Reset dauert mehr als eine Minute, um das Betriebssystem vollständig hochzufahren und die Anmeldebereitschaft zu erreichen. Die blaue LED ist auf dem aktiven CMC aktiviert. In einer redundanten Konfiguration mit zwei CMCs ist nur die grüne LED oben rechts auf dem Standby-CMC aktiviert.

Wiederherstellungsinformationen über die serielle DB-9-Schnittstelle abrufen

Wenn die untere LED gelb leuchtet, stehen über die serielle DB-9-Schnittstelle, die sich an der Vorderseite des CMC befindet, Wiederherstellungsinformationen zur Verfügung.

So rufen Sie Wiederherstellungsinformationen ab:

1. Installieren Sie ein NULL-Modemkabel zwischen einem CMC-System und einem Client-Computer.
2. Öffnen Sie einen Terminalemulator Ihrer Wahl (z. B. HyperTerminal oder Minicom). Stellen Sie Folgendes ein,wenn Sie dazu aufgefordert werden: 8 Bit, keine Parität, keine Ablaufsteuerung, Baudrate 115200.
3. Drücken Sie die Eingabetaste.

   Wenn die Eingabeaufforderung Wiederherstellung angezeigt wird, stehen zusätzliche Informationen zur Verfügung. Die Eingabeaufforderung zeigt die CMC-Steckplatznummer und den Fehlertyp an.

   Um die Ursache des Fehlers und die Syntax für einige Befehle anzuzeigen, geben Sie `recover` ein und dann drücken Sie die Taste <Eingabe>.

   Beispiele von Eingabeaufforderungen:

   ```
   recover1[self test] CMC 1 self test failure
   ```

   ```
   recover2[Bad FW images] CMC2 has corrupted images
   ```

   - Wenn die Eingabeaufforderung auf einen Selbsttestfehler hinweist, befinden sich keine betriebsfähigen Komponenten auf dem CMC. Der CMC ist unbrauchbar und muss zu Dell zurückgesendet werden.
   - Wenn die Eingabeaufforderung **Beschädigte Firmware-Images** anzeigt, führen Sie die Tasks in Firmware-Image wiederherstellen aus.

Firmware-Image wiederherstellen

Der CMC geht in den Wiederherstellungsmodus über, wenn ein normaler Start des CMC-Betriebssystems nicht möglich ist. Im Wiederherstellungsmodus steht ein kleiner Teilsatz an Befehlen zur Verfügung, mit denen Sie Flash-Geräte durch Hochladen der Firmware-Aktualisierungsdatei **vrtx_cmc.bin** neu programmieren können. Dies ist dieselbe Firmware-Image-Datei, die auch für normale Firmware-Aktualisierungen verwendet wird. Der Wiederherstellungsvorgang zeigt die laufende Aktivität an und startet am Ende das CMC-Betriebssystem.

Wenn Sie recover eingeben und dann bei der Eingabeaufforderung zur Wiederherstellung die Taste <Eingabe> drücken, werden der Wiederherstellungsgrund und die verfügbaren Unterbefehle angezeigt. Ein Beispiel einer Wiederherstellungsabfolge könnte folgendermaßen lauten:

```
recover getniccfg
recover setniccfg 192.168.0.120 255.255.255.0
```

```
192.168.0.1
recover ping 192.168.0.100
recover fwupdate -g -a 192.168.0.100
```

ANMERKUNG: Schließen Sie das Netzwerkkabel an den RJ45 ganz links an.

ANMERKUNG: Im Wiederherstellungsmodus können Sie den CMC normalerweise nicht pingen, da kein aktiver Netzwerkstapel vorhanden ist. Mit dem Befehl `recover ping <TFTP server IP>` können Sie den TFTP-Server pingen, um die LAN-Verbindung zu überprüfen. Möglicherweise müssen Sie auf einigen Systemen den Befehl `recover reset` nach `setniccfg` verwenden.

Fehlerbehebung bei Netzwerkproblemen

Mit dem integierten CMC-Ablaufverfolgungsprotokoll können Sie CMC-Warnmeldungen und den CMC-Netzwerkbetrieb debuggen. Sie können auf das Verlaufsprotokoll mittels CMC-Webschnittstelle oder RACADM zugreifen. Weitere Informationen finden Sie im Abschnitt zum `gettracelog`-Befehl im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

Das Ablaufverfolgungsprotokoll verfolgt die folgenden Informationen:

- DHCP - Verfolgt Pakete, die an einen DHCP-Server gesendet und von ihm empfangen werden.
- DDNS - Verfolgt dynamische Aktualisierungsanfragen und Antworten des DNS-Servers.
- Konfigurationsänderungen an den Netzwerkschnittstellen.

Das Ablaufverfolgungsprotokoll kann auch spezifische Fehlercodes der CMC-Firmware enthalten, die sich auf die integierte CMC-Firmware beziehen und nicht auf das Betriebssystem des verwalteten Systems.

Fehlerbehebung: Controller

So führen Sie eine Fehlerbehebung an einem Controller aus:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** > **Speicher-** > **Controller** > **Fehlerbehebung**.

2 Wählen Sie auf der Seite **Controller – Fehlerbehebung** aus der Drop-Down-Liste **Maßnahmen** für den entsprechenden Controller eines der Folgenden aus und klicken Sie dann auf **Anwenden**.

- **Konfigurations-Reset** – Löscht die virtuellen Festplatten und die Hot Spares. Die Daten auf den Festplatten werden jedoch nicht gelöscht.

  ANMERKUNG: Durch Zurücksetzen der PERC-Konfiguration wird das Pinned Cache, falls vorhanden, am PERC-Controller verworfen.

- **TTY-Protokoll exportieren** – Das TTY-Debug-Protokoll vom Speichercontroller wird auf Ihr lokales System exportiert.
- **Pinned Cache verwerfen** – Löscht die Daten vom RAID-Controller-Cache.

  ANMERKUNG: Wenn ein Pinned Cache vorliegt, ist die Option zum Löschen vorhanden. Wenn kein Pinned Cache vorhanden ist, wird diese Option nicht angezeigt.

- **RAID-Controller deaktivieren** — Deaktiviert den Peer-Controller. Diese Option steht im Drop-Down-Menü nur für freigegebene PERC8 (Integriert 2) und externe freigegebene PERC8s zur Verfügung.
- **RAID-Controller aktivieren** — Aktiviert den Peer-Controller. Die Option **RAID-Controller aktivieren** steht im Drop-Down-Menü zur Verfügung.

  ANMERKUNG:

  Wenn PERC deaktiviert ist, sind die Optionen „Konfigurations-Reset“, „TTY-Protokoll exportieren“, „Pinned Cache verwerfen“ und „RAID-Controller deaktivieren“ im Drop-Down-Menü vorhanden.

- **Fehlertoleranz aktivieren** — Aktiviert den Fehlertoleranzmodus der externen freigegebenen PERC 8-Karte.
- **Fehlertoleranz deaktivieren** — Deaktiviert den Fehlertoleranzmodus der externen freigegebenen PERC 8-Karte.

  ANMERKUNG: „Fehlertoleranz aktivieren“ und „Fehlertoleranz deaktivieren“ werden nur für die externen freigegebenen PERC 8-Karten angezeigt. Der Standardmodus der externen freigegebenen PERC 8-Karten ist der nicht-fehlertolerante Modus.

ANMERKUNG:

- Es wird eine Fehlermeldung angezeigt, wenn die Blades eingeschaltet werden.
- Der Befehl schlägt fehl, wenn der Blade eingeschaltet wird.

Hot-Plug-fähige Gehäuse im fehlertoleranten Gehäuse

1 Stellen Sie sicher, dass die Steckplätze 5 und 6 im Gehäuse nicht fehlertolerant sind.
2 Trennen Sie die Gehäuse.
3 Ändern Sie den Status der Steckplätze 5 und 6 auf den fehlertoleranten Modus.
4 Schließen Sie die Gehäuse wieder mit einer fehlertoleranten Verkabelung an.

Schalten Sie das Gehäuse nach dem Trennen und vor dem erneuten Anschließen der Gehäuse aus und wieder ein, da die Laufwerke die vorherige SCSI-3-Reservierung beibehalten, bis das Gehäuse aus- und wieder eingeschaltet wurde.

18

LCD-Schnittstelle verwenden

Über das LCD-Bedienfeld des Gehäuses können Sie Konfigurationen und Diagnosen durchführen und Statusinformationen zum Gehäuse und dessen Inhalt abrufen.

In der folgenden Abbildung wird das LCD Bedienfelt veranschaulicht. Auf dem LCD-Bildschirm werden Menüs, Symbole, Bilder und Meldungen angezeigt.

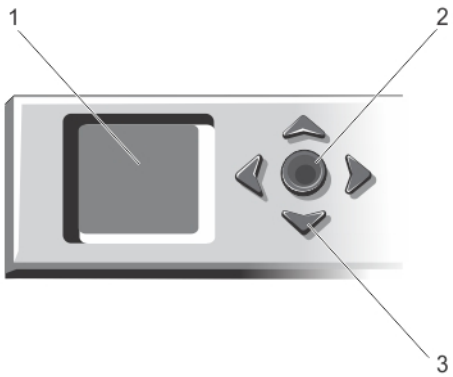


Abbildung 4. LCD-Anzeige

1	LCD-Bildschirm	2	Auswahlschaltfläche zum Markieren
3	Scrolltasten (4)		

Themen:

- LCD-Navigation
- Diagnose
- Frontblenden-LCD-Meldungen
- LCD-Modul- und Serverstatusinformationen

LCD-Navigation

Die rechte Seite des LCD-Bedienfelds umfasst fünf Schaltflächen: vier Pfeilschaltflächen (nach oben, unten, links und rechts) und eine Schaltfläche in der Mitte.

- *Um zwischen Bildschirmen zu wechseln, verwenden Sie die Pfeilschaltflächen nach rechts (nächster) und nach links (vorhergehender). Während Sie das Bedienfeld verwenden, können Sie jederzeit zum vorhergehenden Bildschirm zurückkehren.*
- *Um auf einem Bildschirm zwischen Optionen zu wechseln, verwenden Sie die Pfeilschaltfläche nach unten und nach oben.*
- *Um auf einem Bildschirm ein Element auszuwählen und zu speichern und zum nächsten Bildschirm zu wechseln, verwenden Sie die Pfeilschaltfläche in der Mitte.*

Anhand der Schaltflächen Nach oben, Nach unten, Nach links und Nach rechts können Sie die ausgewählten Menüelemente oder Symbole auf dem Bildschirm ändern. Das ausgewählte Element wird mit einem hellblauen Hintergrund oder Rahmen dargestellt.

Wenn die auf dem LCD-Bildschirm angezeigten Meldungen nicht auf den Bildschirm passen, führen Sie anhand der Schaltflächen Nach links bzw. Nach rechts einen Bildlauf nach links und rechts durch.

Die in der folgenden Tabelle beschriebenen Symbole werden zum Wechseln zwischen LCD-Bildschirmen verwendet.

Tabelle 44. LCD-Bedienfeld-Navigationssymbole

Symbol Normal	Symbol markiert	Symbolname und -beschreibung
		**Zurück** – Markieren und drücken Sie die mittlere Schaltfläche, um zum vorhergehenden Bildschirm zurückzukehren.
		**Annehmen/Ja** – Markieren und drücken Sie die mittlere Schaltfläche, um eine Änderung anzunehmen und zum vorhergehenden Bildschirm zurückzukehren.
		**Überspringen/Weiter** – Markieren und drücken Sie die mittlere Schaltfläche, um Änderungen zu überspringen und zum nächsten Bildschirm fortzufahren.
		**Nein** – Markieren und drücken Sie die mittlere Schaltfläche, um auf eine Frage mit „Nein“ zu antworten und zum nächsten Bildschirm fortzufahren.
		**Komponente identifizieren** – Bringt blaue LED an einem Bauteil zum Blinken. **ANMERKUNG: Um dieses Symbol herum ist ein blinkendes, blaues Rechteck vorhanden, wenn Komponenten identifizieren aktiviert ist.**

Eine LED-Statusanzeige auf dem LCD-Bedienfeld zeigt den Gesamtfunktionszustand des Gehäuses und seiner Komponenten an.

- Beständig leuchtendes Blau zeigt einen guten Funktionszustand an.
- Blinkendes Gelb zeigt an, dass sich mindestens eine Komponente in einem fehlerhaften Betriebszustand befindet.
- Blinkendes Blau ist ein ID-Signal, das zur Identifikation eines einzelnen Gehäuses in einer Gruppe von Gehäusen verwendet wird.

Hauptmenü

Vom **Hauptmenü** aus können Sie zu den folgenden Bildschirmen wechseln:

- **KVM-Zuordnung** – Enthält die Optionen, den Servern den KVM zuzuordnen bzw. die Zuordnung aufzuheben.
- **DVD-Zuordnung** – Diese Option wird auf dem Bildschirm **Hauptmenü** nur angezeigt, wenn Sie ein DVD-Laufwerk installiert haben.
- **Gehäuse** – Zeigt Statusinformationen für das Gehäuse an.
- **IP-Zusammenfassung** – Zeigt Informationen über CMC-IPv4, CMC-IPv6, iDRAC-IPv4 und iDRAC 4-IPv6 an.
- **Einstellungen** – Enthält Optionen wie **LCD-Sprache**, **Gehäuseausrichtung**, **Standard LCD-Bildschirm** und die **Netzwerkeinstellungen**.

KVM-Zuordnungsmenü

Von diesem Bildschirm können Sie die Informationen über die Zuordnung von KVM zu Server anzeigen, dem KVM einen anderen Server zuordnen, oder die bestehende Verbindung aufheben. Um KVM für einen Server zu verwenden, wählen Sie **KVM-Zuordnung** aus dem Hauptmenü aus, navigieren Sie zum entsprechenden Server, und drücken Sie dann auf die mittlere Schaltfläche **Überprüfen**.

DVD-Zuordnung

Unter Verwendung dieser Seite können Sie die Informationen über die Zuordnung von DVDs zu Server anzeigen, dem DVD einen anderen Server zuordnen, oder die bestehende Verbindung aufheben. Um einem Server Zugriff auf die DVD zu gewähren, wählen Sie **DVD-Zuordnung** aus dem Hauptmenü aus, navigieren Sie zum erforderlichen Server, und drücken Sie dann auf die mittlere Schaltfläche **Überprüfen**.

Das DVD-Laufwerk kann nur dem Serversteckplatz zugeordnet werden, wenn die DVD für diesen Serversteckplatz aktiviert ist. Die Zuordnung des DVD-Laufwerks kann auch aufgehoben werden, um seine Verwendung von irgenwelchen anderen Serversteckplätzen zu verhindern. Der Funktionszustand des DVD-Laufwerks wird kritisch, wenn das SATA-Kabel zwischen dem DVD-Laufwerk und der Hauptplatine nicht richtig verbunden ist. Wenn der Funktionszustand des DVD-Laufwerks kritisch ist, kann der Server nicht auf das DVD-Laufwerk zugreifen.

ANMERKUNG: Die DVD-Funktion Zuordnung wird nur auf dem Bildschirm LCD-Hauptmenü angezeigt, wenn Sie ein DVD-Laufwerk installiert haben.

Enclosure Menu (Menü Gehäuse)

Von diesem Bildschirm aus können Sie zu folgenden Bildschirmen wechseln:

- **Status der Vorderseite**
- **Status auf der Rückseite**
- **Status auf der Seite**
- **Gehäusestatus**

Markieren Sie das gewünschte Element mit den Navigationsschaltflächen (markieren Sie das **Zurück**-Symbol, um zum **Hauptmenü** zurückzukehren) und drücken Sie die mittlere Taste. Der ausgewählte Bildschirm wird angezeigt.

IP-Übersichtsmenü

Im Bildschirm **IP-Übersicht** werden IP-Informationen für den CMC (IPv4 und IPv6) und jedem Server, der im Gehäuse installiert ist, angezeigt.

Führen Sie mit den Schaltflächen Nach oben und Nach unten einen Bildlauf in der Liste durch. Mit der Linkspfeil- und Rechtspfeil-Schaltfläche können Sie in ausgewählten Meldungen, die nicht auf den Bildschirm passen, einen Bildlauf ausführen.

Wählen Sie mit den Schaltflächen Nach oben und Nach unten das **Zurück**-Symbol aus, und drücken Sie die mittlere Schaltfläche, um zum **Gehäuse**-Menü zurückzuwechseln.

Einstellungen

Im Menü **Einstellungen** wird ein Menü mit Elementen angezeigt, die konfiguriert werden können:

- **LCD-Sprache** – Wählen Sie die Sprache aus, die für LCD-Bildschirmtexte und Meldungen verwendet werden soll.
- **Gehäuseausrichtung** – Basierend auf die Installationsausrichtung des Gehäuses, wählen Sie entweder **Tower-Modus** oder **Rack-Modus** aus.
- **Standard LCD-Bildschirm** – Wählen Sie den Bildschirm aus (**Hauptmenü**, **Status der Vorderseite**, **Status derRückseite Status der Seitenansicht** oder **Benutzerdefiniert**), der angezeigt wird, wenn keine Aktivität auf dem LCD-Bereich besteht.
- **Netzwerkeinstellungen** – Wählen Sie dieses aus, um die Netzwerkeinstellungen eines CMC zu konfigurieren. Weitere Informationen zu dieser Funktion finden Sie unter CMC-Netzwerk unter Verwendung der LCD-Schnittstelle konfigurieren.

Verwenden Sie die Schaltflächen „Nach oben“ und „Nach unten“, um ein Element im Menü zu markieren, oder markieren Sie das **Zurück**-Symbol, wenn Sie zum Bildschirm **Hauptmenü** zurückkehren möchten.

Drücken Sie auf die mittlere Schaltfläche, um Ihre Auswahl zu aktivieren.

LCD-Sprache

Auf dem Bildschirm **LCD-Sprache** können Sie die Sprache auswählen, die für LCD-Bedienfeldmeldungen verwendet werden soll. Die derzeit aktive Sprache wird durch einen hellblauen Hintergrund hervorgehoben.

1 Verwenden Sie die Schaltflächen Nach oben, Nach unten, Nach links und Nach rechts, um die gewünschte Sprache zu markieren.
2 Drücken Sie die mittlere Schaltfläche. Das **Annehmen**-Symbol wird eingeblendet und ist hervorgehoben.
3 Drücken Sie die mittlere Schaltfläche, um die Änderung zu bestätigen. Das **LCD-Setup**-Menü wird aufgerufen.

Standardbildschirm

Auf dem **Standardbildschirm** können Sie den Bildschirm ändern, den das LCD-Bedienfeld anzeigt, wenn keine Aktivität auf dem Bedienfeld zu verzeichnen ist. Der werksseitige Standardbildschirm ist das **Hauptmenü**. Es stehen folgende Bildschirme zur Auswahl:

- **Hauptmenü**
- **Vorderer Status** (vordere graphische Ansicht des Gehäuses)
- **Rückwärtiger Status** (hintere graphische Ansicht des Gehäuses)
- **Seitenstatus** (linke graphische Ansicht des Gehäuses)
- **Benutzerdefiniert** (Dell-Logo mit Gehäusename)

Der derzeit aktive Standardbildschirm ist hellblau hervorgehoben.

1 Markieren Sie mit den Pfeiltasten „Nach oben“ und „Nach unten“ den Bildschirm, den Sie als Standardeinstellung festlegen möchten.
2 Drücken Sie die mittlere Schaltfläche. Das Symbol **Annehmen** ist hervorgehoben.
3 Drücken Sie erneut die mittlere Schaltfläche, um die Änderung zu bestätigen. Der **Standardbildschirm** wird angezeigt.

Diagnose

Mit dem LCD-Bedienfeld können Sie Probleme mit Servern oder Modulen im Gehäuse analysieren. Falls ein Problem oder ein Fehler beim Gehäuse oder einem Server oder anderen Modul im Gehäuse vorliegt, blinkt die LCD-Bedienfeld-Statusanzeige gelb. Im **Hauptmenü** wird ein blinkendes Symbol mit einem gelben Hintergrund neben dem Menüelement – Gehäuse – angezeigt, das zum Vorderseiten-, Rückseiten-, Seiten- oder Gehäuse-Status führt.

Indem Sie den blinkenden gelben Symbolen durch das LCD-Menüsystem hindurch folgen, können Sie die Statusbildschirm- und Fehlermeldungen für das Element anzeigen, welches das Problem aufweist.

Fehlermeldungen auf dem LCD-Bedienfeld können entfernt werden, indem das Modul bzw. der Server entfernt wird, das/der die Ursache des Problems darstellt, oder indem Sie das Hardwareprotokoll für das Modul oder den Server löschen. Für Serverfehler benutzen Sie die iDRAC Web-Schnittstelle oder Befehlszeilenschnittstelle zum Löschen des Systemereignisprotokolls (SEL/System Event Log). Verwenden Sie für Gehäusefehler die CMC-Webschnittstelle oder die Befehlszeilenschnittstelle, um das Hardwareprotokoll zu löschen.

Frontblenden-LCD-Meldungen

Dieser Abschnitt enthält zwei Unterbereiche, in denen Fehler und Statusinformationen aufgeführt werden, die auf dem Frontblenden-LCD angezeigt werden.

Fehlermeldungen auf dem LCD weisen ein Format auf, das ähnlich dem Systemereignisprotokoll (SEL) ist, wie es in der CLI oder in der Webschnittstelle angezeigt wird.

In den Tabellen im Fehlerabschnitt werden Fehler- und Warnungsmeldungen aufgeführt, die auf verschiedenen LCD-Bildschirmen angezeigt werden, sowie die mögliche Ursache der Meldung. Text, der in spitzen Klammern (< >) steht, zeigt an, dass der Text variieren kann.

Statusinformationen auf dem LCD enthalten beschreibende Informationen zu den Modulen im Gehäuse. Die Tabellen in diesem Abschnitt beschreiben die Informationen, die für jede Komponente angezeigt werden.

LCD-Modul- und Serverstatusinformationen

Die Tabellen in diesem Abschnitt beschreiben Statuselemente, die auf dem Frontblenden-LCD für jeden Komponententyp im Gehäuse angezeigt werden.

Tabelle 45. CMC-Status

Element	Beschreibung
Name/Standort.	Beispiel: CMC1, CMC2
Keine Fehler	Bei keinem Fehler wird „Keine Fehler“ angezeigt; ansonsten werden Fehlermeldungen aufgelistet, in denen die kritischen Fehler zuerst aufgelistet werden, gefolgt von den Warnungen.
Firmware-Version	Wird nur auf einem aktiven CMC angezeigt. Zeigt für den Standby-CMC Standby an.
IP4 <aktiviert, deaktiviert>	Zeigt den aktuellen IPv4-Aktivierungsstatus nur auf einem aktiven CMC an.
IP4 Adresse: <Adresse, wird bezogen>	Wird nur dann angezeigt, wenn IPv4 nur auf einem aktiven CMC aktiviert wurde.
IP6 <aktiviert, deaktiviert>	Zeigt den aktuellen IPv6-Aktivierungsstatus nur auf einem aktiven CMC an.
Lokale IP6-Adresse: <Adresse>	Wird nur dann angezeigt, wenn IPv6 nur auf einem aktiven CMC aktiviert wurde.
MAC: <Adresse>	Zeigt die MAC-Adresse des CMC an.

Tabelle 46. Gehäusestatus

Element	Beschreibung
Benutzerdefinierter Name	Beispiel: „Dell Rack System“. Es kann über die CMC-Befehlszeilenschnittstelle oder die Webschnittstelle konfiguriert werden.
Fehlermeldungen	Bei keinem Fehler wird „Keine Fehler“ angezeigt; ansonsten werden Fehlermeldungen aufgelistet, in denen die kritischen Fehler zuerst aufgelistet werden, gefolgt von den Warnungen.
Modellnummer	Beispiel „PowerEdgeM1000“.
Stromverbrauch	Aktueller Stromverbrauch in Watt.
Spitzenstrom	Spitzenstromverbrauch in Watt.
Minimaler Strom	Mindeststromverbrauch in Watt.
Umgebungstemperatur	Umgebungstemperatur in Grad Celsius.
Service Tag	Die vom Werk zugewiesene Service-Tag-Nummer.
CMC-Redundanzmodus	Nicht-redundant oder Redundant.
Netzteileinheit-Redundanzmodus	Nicht-redundant, netzredundant oder gleichstromredundant.

Tabelle 47. Lüfterstatus

Element	Beschreibung
Name/Standort.	Beispiel: Lüfter1, Lüfter2, usw.
Fehlermeldungen	Bei keinem Fehler wird „Keine Fehler“ angezeigt; ansonsten werden Fehlermeldungen aufgelistet, in denen die kritischen Fehler zuerst aufgelistet werden, gefolgt von den Warnungen.
RPM	Aktuelle Lüftergeschwindigkeit in U/Min.

Tabelle 48. Netzteileinheitstatus

Element	Beschreibung
Name/Standort.	Beispiel: Netzteileinheit1, Netzteileinheit2, usw.
Fehlermeldungen	Bei keinem Fehler wird „Keine Fehler“ angezeigt; ansonsten werden Fehlermeldungen aufgelistet, in denen die kritischen Fehler zuerst aufgelistet werden, gefolgt von den Warnungen.
Status	Offline, Online oder Standby – Zeigt den Stromstatus eines Netzteils an.
Maximale Wattzahl	Maximale Wattzahl, welche die Netzteileinheit dem System zuführen kann.

Tabelle 49. EAM-Status

Element	Beschreibung
Name/Standort.	EAM A
Fehlermeldungen	Bei keinem Fehler wird „Keine Fehler“ angezeigt; ansonsten werden Fehlermeldungen aufgelistet, in denen die kritischen Fehler zuerst aufgelistet werden, gefolgt von den Warnungen.
Status	Aus oder Ein – Zeigt an, ob das EAM funktioniert.
Modell	Modell von EAM.
Strukturtyp	Netzwerkbetriebstyp.
IP-Adresse	Nur zu sehen, wenn EAM eingeschaltet ist. Dieser Wert ist für ein EAM des Typs „Passthrough“ 0.
Service Tag	Die vom Werk zugewiesene Service-Tag-Nummer.

Tabelle 50. KVM-Zuordnungsstatus

Element	Beschreibung
Server <Nummer>	Zeigt eine Liste der Server an, denen das KVM zugeordnet werden kann.
Fehlermeldungen	Bei keinem Fehler wird „Keine Fehler“ angezeigt; ansonsten werden Fehlermeldungen aufgelistet, in denen die kritischen Fehler zuerst aufgelistet werden, gefolgt von den Warnungen.
Zugeordnet	Zeigt eine Liste der Server an, die einem KVM zugeordnet sind, falls vorhanden.
Steckplatz <Nummer>	Gibt an, welchem Serversteckplatz das KVM zugeordnet wurde. Mögliche Werte sind Steckplatz *<01 bis 04>*.
Nicht zugeordnet	Wird angezeigt, wenn das KVM-Modul keinem Server zugeordnet ist.

Tabelle 51. DVD-Zuordnungsstatus

Element	Beschreibung
Server <Nummer>	Zeigt eine Liste der Server an, denen das DVD zugeordnet werden kann.
Fehlermeldungen	Bei keinem Fehler wird „Keine Fehler“ angezeigt; ansonsten werden Fehlermeldungen aufgelistet, in denen die kritischen Fehler zuerst aufgelistet werden, gefolgt von den Warnungen.
Zugeordnet	Zeigt eine Liste der Server an, die einem DVD zugeordnet sind, falls vorhanden.
Steckplatz <Nummer>	Gibt an, welchem Servers teckplatz das DVD zugeordnet wurde. Mögliche Werte sind Steckplatz *<01 bis 04>*.
Nicht zugeordnet	Wird angezeigt, wenn das KVM-Modul keinem Server zugeordnet ist.

Tabelle 52. Lüfterstatus

Element	Beschreibung
Name/Standort.	Beispiel: Lüfter 1, Lüfter 2 usw.
Fehlermeldungen	Bei keinem Fehler wird „Keine Fehler“ angezeigt; ansonsten werden Fehlermeldungen aufgelistet, in denen die kritischen Fehler zuerst aufgelistet werden, gefolgt von den Warnungen.
RPM	Aktuelle Lüftergeschwindigkeit in U/Min.

Tabelle 53. SPERC-Status

Element	Beschreibung
SPERC: <Nummer>	Zeigt den SPERC-Namen im Format „SPERC n“, wobei „n“ die SPERC-Nummer ist. Beispiel: SPERC 1, SPERC 2 usw.
Fehlermeldungen	Bei keinem Fehler wird „Keine Fehler“ angezeigt; ansonsten werden Fehlermeldungen aufgelistet, in denen die kritischen Fehler zuerst aufgelistet werden, gefolgt von den Warnungen.
Betriebsstatus	Ein oder Aus – Zeigt an, ob der SPERC funktioniert.
Name: <Name>	Der Name des freigegebenen PERC. Beispiel: SPERC
Funktionsstatus	OK
Firmware-Version	SPERC-Version
Hersteller	Name des Herstellers
Zustand	Offline, Online oder Standby – Zeigt den Stromstatus eines SPERC an.

Tabelle 54. PCIe-Kartenstatus

Element	Beschreibung
PCIe-Karte *<Nummer>*	Zeigt den Namen der PCIe-Karte im Format „PCIe-Karte *<n>*“ an, wobei „n“ für die PCIe-Kartennummer steht. Beispiel: PCIe-Karte 1, PCIe-Karte 2 usw.
Fehlermeldungen	Bei keinem Fehler wird „Keine Fehler“ angezeigt; ansonsten werden Fehlermeldungen aufgelistet, in denen die kritischen Fehler zuerst aufgelistet werden, gefolgt von den Warnungen.

Element	Beschreibung
Betriebsstatus	Ein oder Aus – Zeigt an, ob die PCIe-Karte funktioniert.
Name: <Name>	Name der PCIe-Karte.
Dem Server zugeordnet.	Zugeordnet oder nicht zugeordnet.

Tabelle 55. Festplattenlaufwerksstatus

Element	Beschreibung
Festplattenlaufwerk: <Nummer>	Zeigt den Namen des Festplattenlaufwerks im Format „Festplattenlaufwerk *<n>*“ an, wobei „n“ die Nummer des Festplattenlaufwerks ist. Beispiel: Festplattenlaufwerk 1, Festplattenlaufwerk 2 usw.
Fehlermeldungen	Bei keinem Fehler wird „Keine Fehler“ angezeigt; ansonsten werden Fehlermeldungen aufgelistet, in denen die kritischen Fehler zuerst aufgelistet werden, gefolgt von den Warnungen.
Stromstatus	Spun-Up, Transition oder Spun-Down – Zeigt den Stromstatus eines Festplattenlaufwerks an.
Hersteller	Name des Herstellers
Kapazität	Verfügbare Speicherkapazität des Festplattenlaufwerks in Gigabyte (GB)
Firmware-Version	Die Firmware-Version des Festplattenlaufwerks.
Zustand	Offline, Online oder Standby – Zeigt den Stromstatus des Festplattenlaufwerks an.

Tabelle 56. Serverstatus

Element	Beschreibung
Name/Standort.	Beispiel: Server 1, Server 2 usw.
Keine Fehler	Bei keinem Fehler wird „Keine Fehler“ angezeigt; ansonsten werden Fehlermeldungen aufgelistet, in denen die kritischen Fehler zuerst aufgelistet werden, gefolgt von den Warnungen. Weitere Informationen finden Sie unter „LCD-Fehlermeldungen“.
Steckplatzname	Gehäuse-Steckplatzname. Zum Beispiel SLOT-01. **ANMERKUNG: Sie können diese Tabelle über die CMC-Befehlszeilenschnittstelle (CLI) oder die Webschnittstelle einstellen.**
Name	Name des Servers, dies kann durch den Benutzer über Dell OpenManage eingestellt werden. Der Name wird nur dann angezeigt, wenn iDRAC den Startvorgang abgeschlossen hat und der Server diese Funktion unterstützt, anderenfalls werden iDRAC-Startmeldungen angezeigt.
Modellnummer	Wird angezeigt, wenn der iDRAC den Bootvorgang abgeschlossen hat.
Service Tag	Wird angezeigt, wenn der iDRAC den Bootvorgang abgeschlossen hat.
BIOS Version	Firmwareversion des Server BIOS.
Letzter POST-Code	Zeigt die letzte Meldungszeichenkette mit Server-BIOS POST-Codes an.
iDRAC-Firmware-Version	Wird angezeigt, wenn der iDRAC den Bootvorgang abgeschlossen hat. **ANMERKUNG: iDRAC Version 1.01 wird als 1.1 angezeigt. Es gibt keine iDRAC-Version 1.10.**

Element	Beschreibung
IP4 <aktiviert, deaktiviert>	Zeigt den aktuellen IPv4-Aktivierungsstatus an.
IP4 Adresse: <Adresse, wird bezogen>	Wird nur bei aktiviertem IPv4 angezeigt.
IP6 <aktiviert, deaktiviert>	Wird nur dann angezeigt, wenn iDRAC IPv6 unterstützt. Zeigt den aktuellen IPv6-Aktivierungsstatus an.
Lokale IP6-Adresse: <Adresse>	Wird nur angezeigt, wenn iDRAC IPv6 unterstützt und IPv6 aktiviert ist.
Globale IP6-Adresse: <Adresse>	Wird nur angezeigt, wenn iDRAC IPv6 unterstützt und IPv6 aktiviert ist.
FlexAddress aktiviert auf Strukturen	Wird nur angezeigt, wenn die Funktion installiert ist. Listet die für diesen Server aktivierten Strukturen auf (d.h., A, B, C).

Die Informationen in der Tabelle werden dynamisch aktualisiert. Wenn der Server diese Funktion nicht unterstützt, erscheinen die folgenden Informationen nicht, andernfalls lauten die Server-Administratoroptionen wie folgt:

- Option „Keine“ = Es müssen keine Zeichenketten auf dem LCD angezeigt werden.
- Option „Standard“ = Keine Auswirkung.
- Option „Benutzerdefiniert“ = Ermöglicht Ihnen die Eingabe eines Zeichenkettennamens für den Server.

Die Informationen werden nur angezeigt, wenn der iDRAC den Startvorgang abgeschlossen hat. Weitere Informationen zu dieser Funktion finden Sie im *RACADM Command Line Reference Guide for CMC in PowerEdge VRTX* (RACADM-Befehlszeilen-Referenzhandbuch für CMC in PowerEdge VRTX).

19

Häufig gestellte Fragen

In diesem Abschnitt werden häufig gestellte Fragen zu den folgenden Themen aufgelistet:

- RACADM
- Remote-System verwalten und wiederherstellen
- Active Directory
- FlexAddress und FlexAddressPlus
- EAM

Themen:

RACADM

Nach dem Ausführen eines CMC-Resets (mithilfe des RACADM-Unterbefehls racreset), wenn ein Befehl eingegeben wird, wird die folgende Meldung angezeigt:

```
racadm <subcommand> Transport: ERROR: (RC=-1)
```

Was bedeutet diese Meldung?

Ein anderer Befehl muss nur dann ausgegeben werden, nachdem CMC-Reset abgeschlossen ist.

Durch die Verwendung der RACADM-Unterbefehle wird manchmal ein oder mehrere der folgenden Fehler angezeigt:

- Lokale RACADM-Fehlermeldungen - Probleme wie Syntax, typografische Fehler und falsche Namen. Beispiel: `ERROR: <message>`
  Verwenden Sie den RACADM-Unterbefehl `help`, um richtige Syntax- und Anwendungsinformationen anzuzeigen. Wenn Sie zum Beispiel einen Fehler im Löschen eines Gehäuseprotokolls haben, führen Sie den folgenden Unterbefehl aus.
  ```
  racadm chassislog help clear
  ```
- Fehlermeldungen, die sich auf den CMC beziehen – Probleme, bei denen der CMC keine Maßnahme durchführen kann. Die folgende Fehlermeldung wird angezeigt:
  ```
  racadm command failed.
  ```

Um Informationen über ein Gehäuse anzuzeigen, geben Sie den folgenden Befehl ein:

```
racadm gettracelog
```

Während ich Firmware-RACADM verwendet habe, wechselt die Eingabeaufforderung zu „>“ und die Eingabeaufforderung „$“ wird nicht wieder angezeigt.

Wenn ein doppeltes Anführungszeichen (") oder ein einfaches Anführungszeichen (’) nicht paarig als Teil des Befehls eingegeben wird, dann wechselt die Befehlszeile zur Aufforderung „>“ und stellt alle Befehle in die Warteschlange.

Um zur Eingabeaufforderung „$“ zurückzukehren, geben Sie <Strg>–d ein.

Eine Fehlermeldung `Not Found` wird beim Verwenden der Befehle `$ logout` und `$ quit` angezeigt.

Remote-System verwalten und wiederherstellen

Warum sind die Remote-RACADM- und webbasierten Dienste nach einer Eigenschaftsänderung nicht verfügbar?

Es kann etwa eine Minute dauern, bis die Remote-RACADM-Dienste und die Webschnittstelle nach einem Reset des CMC-Webservers wieder verfügbar sind.

Der CMC-Webserver führt nach den folgenden Ereignissen einen Reset durch:

- Änderung der Netzwerkkonfiguration oder Netzwerksicherheitseigenschaften über die CMC-Webschnittstelle.
- Die Eigenschaft cfgRacTuneHttpsPort wird geändert (einschließlich der Änderung durch eine config -f-<Konfigurationsdatei>).
- Bei Verwendung von `racresetcfg` oder Wiederherstellen einer Gehäusekonfigurationssicherung.
- CMC wird zurückgesetzt.
- Ein neues SSL-Serverzertifikat wird hochgeladen.

Warum registriert mein DNS-Server meinen CMC nicht?

Einige DNS-Server registrieren nur Namen mit höchstens 31 Zeichen.

Wenn ich auf die CMC-Webschnittstelle zugreife, erhalte ich eine Sicherheitswarnung, die aussagt, dass das SSL-Zertifikat durch eine nicht vertrauenswürdige Zertifizierungsstelle ausgegeben wurde.

Der CMC enthält ein Standard-CMC-Serverzertifikat zur Sicherung der Netzwerksicherheit für die Webschnittstelle und die Remote-RACADM-Funktionen. Dieses Zertifikat wurde nicht von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt. Um dieses Sicherheitsproblem zu beseitigen, laden Sie ein CMC-Serverzertifikat von einer vertrauenswürdigen Zertifizierungsstelle (z. B. Thawte oder Verisign) hoch.

Warum wird die folgende Meldung aus unbekannten Gründen angezeigt?

Remote Access: SNMP Authentication Failure

Als Teil der Ermittlung versucht IT Assistant, die **Get**- und **Set**-Community-Namen des Geräts zu überprüfen. Im IT Assistant ist der **Get-Community-Name = public** und der **Set-Community-Name = private**. Standardmäßig ist der Community-Name für den CMC-Agenten „public“. Wenn IT Assistant eine Set-Aufforderung sendet, erstellt der CMC-Agent den SNMP-Authentifizierungsfehler, da er nur Aufforderungen von **Community = public** akzeptiert.

Ändern des CMC-Community-Namens mit RACADM. Um den CMC Community-Namen zu sehen, verwenden Sie den folgenden Befehl:

```
racadm getconfig -g cfgOobSnmp
```

Um den CMC Community-Namen anzugeben, verwenden Sie den folgenden Befehl:

```
racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <Community-Name>
```

Um die Erzeugung von SNMP-Authentifizierungs-Traps zu verhindern, geben Sie Community-Namen ein, die vom Agenten akzeptiert werden. Da der CMC nur einen Community-Namen zulässt, geben Sie den gleichen Get- und Set-Community-Namen für das IT Assistant-Ermittlungs-Setup ein.

Wenn ich auf die CMC-Schnittstelle zugreife, erhalte ich eine Sicherheitswarnung, die besagt, dass der Host-Name des SSL-Zertifikats nicht mit dem Host-Namen des CMC übereinstimmt.

Der CMC enthält ein Standard-CMC-Serverzertifikat zur Sicherung der Netzwerksicherheit für die Webschnittstelle und die Remote-RACADM-Funktionen. Wenn dieses Zertifikat verwendet wird, zeigt der Webbrowser eine Sicherheitswarnung an, wenn das Standardzertifikat nicht mit dem Host-Namen des CMC (z. B. IP-Adresse) übereinstimmt.

Um dieses Sicherheitsproblem zu beseitigen, laden Sie ein CMC-Serverzertifikat herunter, das auf die IP-Adresse des CMC ausgestellt ist. Wenn Sie die Zertifikatsignierungsanforderung (CSR) zur Ausgabe des Zertifikats erstellen, müssen Sie sicherstellen, dass der allgemeine Name (CN) des CSR der IP-Adresse des CMC (z. B. 192.168.0.120) oder dem eingetragenen DNS-CMC-Namen entspricht.

So stellen Sie sicher, dass die CSR dem eingetragenen DNS-CMC-Namen entspricht:

1 Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht.**
2 Klicken Sie auf **Netzwerk**.
Die Seite **Netzwerkkonfiguration** wird angezeigt.
3 Wählen Sie die Option **CMC auf DNS registrieren**.
4 Geben Sie einen CMC-Namen in das Feld **DNS-CMC-Name** ein.
5 Klicken Sie auf **Änderungen anwenden**.

Active Directory

Unterstützt Active Directory CMC-Anmeldung über mehrfache Strukturen?

Ja. Der Abfragealgorithmus des CMC-Active Directory unterstützt mehrere Strukturen in einer Gesamtstruktur.

Funktioniert die Anmeldung am CMC unter Verwendung des Active Directory im gemischten Modus (d. h. die Domänen-Controller der Gesamtstruktur führen verschiedene Betriebssysteme aus, wie z. B. Microsoft Windows 2000 oder Windows Server 2003)?

Ja. Im gemischten Modus müssen sich alle Objekte, die vom CMC-Abfrageverfahren verwendet werden, (unter Benutzer, RAC-Geräteobjekt und Zuordnungsobjekt) in derselben Domäne befinden.

Das Dell-erweiterte Active Directory-Benutzer- und Computer-Snap-In überprüft den Modus und beschränkt Benutzer, um Objekte über Domänen hinweg zu erstellen (nur im gemischten Mischmodus).

Unterstützt die Verwendung des CMC mit Active Directory mehrfache Domänenumgebungen?

Ja. Die Domänen-Gesamtstrukturfunktionsebene muss sich im Native-Modus oder Windows-2003-Modus befinden. Außerdem müssen die Gruppen unter Zuordnungsobjekt, RAC-Benutzerobjekten und RAC-Geräteobjekten (einschließlich Zuordnungsobjekt) Universal-Gruppen sein.

Können diese Dell-erweiterten Objekte (Dell-Zuordnungsobjekt, Dell RAC-Gerät und Dell-Berechtigungsobjekt) in verschiedenen Domänen sein?

Das Zuordnungsobjekt und das Berechtigungsobjekt müssen sich in derselben Domäne befinden. Beim Dell-erweiterten Active Directory-Benutzer- und -Computer-Snap-In können Sie diese zwei Objekte nur in derselben Domäne erstellen. Andere Objekte können sich in verschiedenen Domänen befinden.

Gibt es Beschränkungen der Domänen-Controller SSL-Konfiguration?

Ja. Alle SSL-Zertifikate für Active Directory-Server in der Gesamtstruktur müssen von dem gleichen, von der root-Zertifizierungsstelle signierten, Zertifikat signiert werden, da der CMC nur erlaubt, ein einziges von einer vertrauenswürdigen Zertifizierungsstelle signiertes SSL-Zertifikat, hochzuladen.

Die Webschnittstelle startet nicht nach dem Erstellen und Hochladen eines neuen RAC-Zertifikats.

Wenn Sie Zertifikatsdienste von Microsoft verwenden, um das RAC-Zertifikat zu erstellen, haben Sie beim Erstellen des Zertifikats möglicherweise versehentlich Benutzerzertifikat ausgewählt anstatt Webzertifikat.

Generieren Sie zur Wiederherstellung eine CSR, erstellen Sie ein neues Webzertifikat von Microsoft Certificate Services und laden Sie es dann durch Ausführen der folgenden RACADM-Befehle hoch:

```
racadm sslcsrgen [-g] [-f {filename}]

racadm sslcertupload -t 1 -f {web_sslcert}
```

FlexAddress und FlexAddressPlus

Was geschieht bei Entfernen einer Funktionskarte?

Wenn eine Funktionskarte entfernt wird, gibt es keine sichtbare Veränderung. Funktionskarten können entfernt und aufbewahrt oder im System belassen werden.

Was passiert, wenn eine Funktionskarte, die in einem Gehäuse verwendet wurde, entfernt und in ein anderes Gehäuse gesteckt wird?

Die Webschnittstelle zeigt die folgende Fehlmeldung an:

```
This feature card was activated with a different chassis. It must be removed before accessing
the FlexAddress feature.

Current Chassis Service Tag = XXXXXXXX

Feature Card Chassis Service Tag = YYYYYYYY

An entry is added to the CMC log that states:

cmc <date timestamp> : feature 'FlexAddress@YYYYYYYY' not activated; chassis ID='XXXXXXXX'
```

Was passiert, wenn die Funktionskarte entfernt und eine Karte, die FlexAddress nicht unterstützt, eingesetzt wird?

Es findet keine Aktivierung oder Änderung der Karte statt. Die Karte wird vom CMC ignoriert. In dieser Situation gibt der Befehl **$racadm featurecard -s** folgende Meldung zurück:

```
No feature card inserted

ERROR: can't open file
```

Was passiert mit einer ans Gehäuse gebundenen Funktionskarte, wenn die Gehäuse-Service-Tag-Nummer neu programmiert wird?

- Wenn die Original-Funktionskarte im aktiven CMC auf diesem oder einem beliebigen anderen Gehäuse vorhanden ist, zeigt die Web-Schnittstelle die folgende Fehlermeldung an:
  - `This feature card was activated with a different chassis. It must be removed before accessing the FlexAddress feature.`
  - `Current Chassis Service Tag = XXXXXXXX`
  - `Feature Card Chassis Service Tag = YYYYYYYY`

  Die Original-Funktionskarte ist nicht mehr für die Deaktivierung auf diesem oder einem beliebigen anderen Gehäuse berechtigt, sofern Dell Service das Service-Tag des Original-Gehäuses nicht wieder neu in ein Gehäuse programmiert, und der CMC, der über die Original-Funktionskarte verfügt, auf diesem Gehäuse aktiviert wird.
- Die FlexAddress-Funktion bleibt auf dem ursprünglich gebundenen Gehäuse aktiviert. Die Funktion Bindung dieses Gehäuses wird aktualisiert, um das neue Service-Tag widerzuspiegeln.

Erhalte ich eine Fehlermeldung, wenn in meinem redundanten CMC-System zwei Funktionskarten installiert sind?

Eine Funktionskarte im aktiven CMC wird aktiv und im Gehäuse installiert sein. Die zweite Karte wird vom CMC ignoriert.

Hat die SD-Karte einen Schreibschutz?

Ja. Bevor Sie die SD-Karte in das CMC-Modul installieren, bestätigen Sie, dass sich die Schreibschutzsperre in der „Entsperr"-Position befindet. Die FlexAddress-Funktion kann nicht aktiviert werden, wenn die SD-Karte schreibgeschützt ist. In dieser Situation gibt der Befehl **$racadm feature -s** folgende Meldung zurück:

```
No features active on the chassis. ERROR: read only file system
```

Was passiert, wenn sich keine SD-Karte im aktiven CMC-Modul befindet?

Der Befehl **$racadm featurecard -s** wird folgende Meldung zurückgeben:

```
No feature card inserted.
```

Was passiert mit der FlexAddress-Funktion, wenn das Server-BIOS von Version 1.xx auf Version 2.xx aktualisiert wird?

Das Servermodul muss ausgeschaltet werden, bevor es mit FlexAddress verwendet werden kann. Nachdem die Server-BIOS-Aktualisierung abgeschlossen wurde, erhält das Servermodul solange keine gehäuseseitigen Adressen, bis der Server aus- und wieder eingeschaltet wurde.

Wie kann eine SD-Karte wiederhergestellt werden, wenn die SD-Karte nicht im Gehäuse war, als der Deaktivierungsbefehl auf der FlexAddress ausgeführt wurde?

Das Problem ist, dass die SD-Karte nicht zur Installation von FlexAddress auf einem anderen Gehäuse verwendet werden kann, wenn sie sich nicht im CMC befand, als FlexAddress deaktiviert wurde. Um die Nutzung der Karte wiederherzustellen, führen Sie die Karte wieder in einen CMC in dem Gehäuse ein, das damit gebunden ist, installieren Sie FlexAddress neu und deaktivieren Sie FlexAddress.

Die SD-Karte sowie sämtliche Firmware oder Software Aktualisierungen sind korrekt installiert. Die FlexAddress ist aktiv, auf dem Serverbereitstellungsbildschirm werden die Optionen zum Bereitstellen nicht angezeigt? Was ist falsch?

Das ist ein Problem des Browser-Cache; melden Sie den Browser ab und starten Sie ihn neu.

Was geschieht mit FlexAddress, wenn ich meine Gehäusekonfiguration mit dem RACADM-Befehl racresetcfg zurücksetzen muss?

Die FlexAddress-Funktion bleibt aktiviert und verfügbar. Alle Strukturen und Steckplätze werden als Standard ausgewählt.

ANMERKUNG: Es wird dringend empfohlen, dass Sie das Gehäuse ausschalten, bevor Sie den RACADM-Befehl `racresetcfg` verwenden.

Warum schlägt der Befehl racadm setflexaddr auf dem weiterhin aktiven CMC fehl, nachdem nur die FlexAddressPlus-Funktion (die FlexAddress ist weiterhin aktiv) deaktiviert wurde?

Wenn der CMC anschließend wieder aktiv ist und sich die FlexAddressPlus-Funktionskarte noch im Kartensteckplatz befindet, wird die FlexAddressPlus-Funktion reaktiviert, und die Flexaddress-Konfigurationsänderungen für den Steckplatz bzw. den Fabric können wieder aufgenommen werden.

EAM

Nach einer Konfigurationsänderung zeigt CMC manchmal die IP-Adresse als 0.0.0.0. an.

Sie müssen die **Aktualisierungs**schaltfläche betätigen, um zu sehen, ob die IP-Adresse im Switch korrekt festgelegt wurde. Wurden IP/Maske/Gateway fehlerhaft festgelegt, wird der Switch die IP-Adresse nicht vergeben und zu 0.0.0.0 in allen Feldern zurückkehren.

Häufige Fehler sind:

- Einstellen der bandexternen IP-Adresse auf die gleiche Adresse oder im gleichen Netzwerk wie die bandinterne Verwaltungs-IP-Adresse.
- Eingabe einer ungültigen Subnetzmaske.
- Einstellen des Standard-Gateway auf eine Adresse, die sich nicht in einem Netzwerk befindet, welches direkt mit dem Switch verbunden ist.