Chassis Management Controller Version 1.0 für Dell PowerEdge VRTX

Benutzerhandbuch

Anmerkungen, Vorsichtshinweise und Warnungen

ANMERKUNG: Eine ANMERKUNG liefert wichtige Informationen, mit denen Sie den Computer 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.

2013 - 06

Rev. A00

Inhaltsverzeichnis

1

Übersicht

Der Dell Chassis Management Controller (CMC) für Dell PowerEdge VRTX ist eine Systemverwaltungs-Hardware- und -Software-Lösung zur Verwaltung der **PowerEdge VRTX**-Gehäuse. Der CMC verfügt über einen eigenen Mikroprozessor und Speicher und wird vom modularen Gehäuse, an das er angeschlossen ist, mit Strom versorgt.

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. Wenn der primäre CMC in reduntanten CMC-Konfigurationen die Verbindung mit dem Gehäuse oder dem Verwaltungsnetzwerk verliert, übernimmt der Standby-CMC die Gehäuseverwaltung.

Der CMC ist mit verschiedenen Systemverwaltungsfunktionen für Server ausgestattet. Die Energie- und Temperaturverwaltung stellen die Hauptfunktionen des CMC dar, die wie folgt aufgeführt sind:

- Automatische Energie- und Temperaturverwaltung in Echtzeit für das gesamte Gehäuse.
  - CMC überwacht die Systemstromanforderungen und unterstützt den optionalen Dynamic Power Supply Engagement (DPSE)-Modus. Dieser Modus ermöglicht es dem CMC, die Stromleistung durch Einstellung der Netzteile, während sich der Server im Standby-Modus befindet und durch das dynamische Verwalten der Belastung und Redundanzanforderungen zu verbessern.
  - 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.
  - 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 für die Stromversorgungsredundanz und eine Obergrenze für den Stromverbrauch.
  - E/A-Switches und iDRAC-Netzwerkeinstellungen.
  - Das erste Startgerät auf den Serverblades.
  - Übereinstimmungsprüfungen der E/A-Struktur zwischen den E/A-Modulen und Servern. CMC deaktiviert auch wenn notwendig Komponente, um die Systemhardware zu schützen.

- Sicherheitsmerkmale für den Benutzerzugriff.
- Speicherkomponenten.
- 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.

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 Kühlungsoptionen, wie erweiterter Kühlmodus (ECM) und Lüfter-Offset kann aktiviert werden, um für zusätzliche Kühlung für eine verbesserte Leistung zu sorgen.
- Remote-Systemverwaltung und -überwachung über SNMP, eine Webschnittstelle, ein iKVM, eine Telnet- oder eine SSH-Verbindung.
- Überwachung – Bietet 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 gehäusezugewiesene WWN/MAC-Kennungen für einen bestimmten Steckplatz (optionale Erweiterung).
- 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

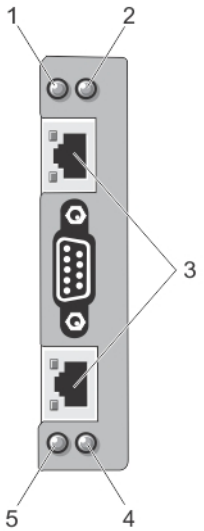
Der CMC bietet die folgenden Sicherheitsfunktionen:

- 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.

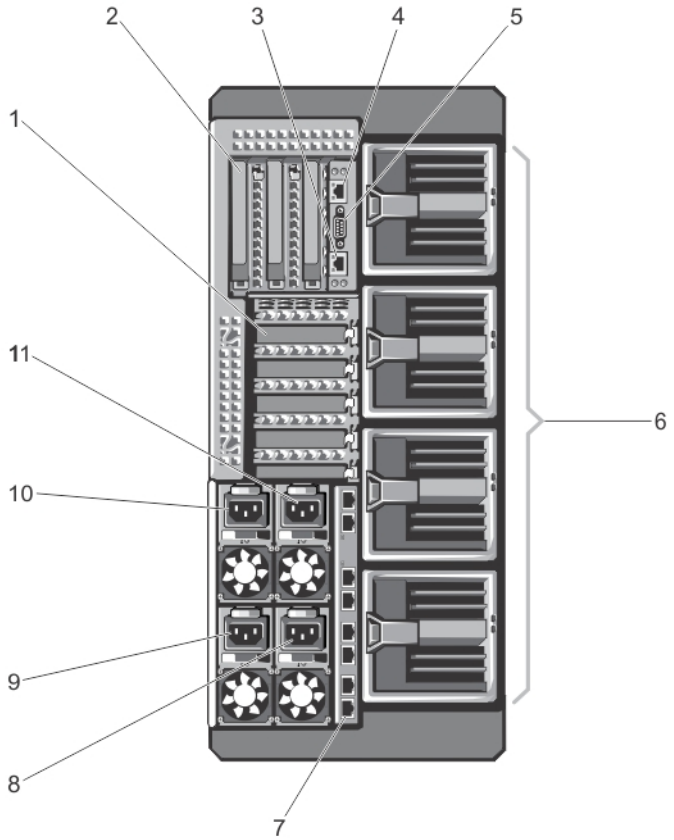
Gehäuseübersicht

Die Abbildung hier zeigt eine Ansicht der CMC-Verbindungen.



Element	Anzeige, Taste oder Anschluss
1	Status-/Identifikationsanzeiger (CMC 1)
2	Stromanzeiger (CMC 1)
3	CMC-Verbindungsschnittstellen (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.



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)

Element	Anzeige, Taste oder Anschluss
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.

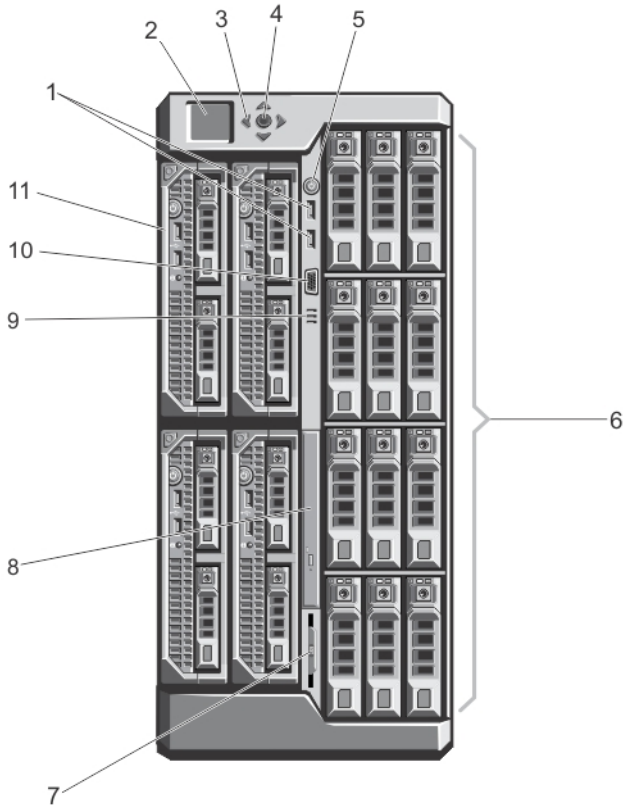


Abbildung 1. Merkmale und Anzeigen auf der Vorderseite – Gehäuse für 3,5-Zoll-Festplattenlaufwerke

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.

Element	Anzeige, Taste oder Anschluss	Beschreibung	
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 der Gehäusestrom eingeschaltet ist. Über den Netzschalter wird die Stromversorgung des Systems gesteuert.	
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	
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 oder M620 Servermodule, die besonders für das Gehäuse konfiguriert sind.	

Unterstützte Remote-Zugriffsverbindungen

Die folgende Tabelle führt die unterstützten Remote Access Controller auf.

Tabelle 1. 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). • Unterstützung für die Telnet/SSH-Befehlskonsole und RACADM CLI-Befehle einschließlich Systemstart-, Reset-, Hochfahren- und Herunterfahren-Befehle.
Serielle Schnittstelle	• Unterstützung für die 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 EAM zu kommunizieren.

Verbindung	Funktionen
	• 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

Der CMC unterstützt modulare Server, die für die PowerEdge VRTX-Plattform vorgesehen sind. Informationen über die Kompatibilität des CMC finden Sie in der Dokumentation Ihres Geräts.

Informationen über aktuell unterstützte Betriebssysteme finden Sie in den *Dell Chassis Management Controller (CMC) Version 1.00 for Dell PowerEdge VRTX Release Notes* (Dell Chassis Management Controller (CMC) Version 1.00 für Dell PowerEdge VRTX Versionshinweisen), verfügbar unter **dell.com/support/manuals**.

Unterstützte Web-Browser

Die neusten Informationen zu unterstützten Web-Browsern finden Sie in den *Dell Chassis Management Controller (CMC) Version 1.00 for Dell PowerEdge VRTX Release Notes* (Dell Chassis Management Controller (CMC) Version 1.00 für Dell PowerEdge VRTX Versionshinweisen), die unter **dell.com/support/manuals** verfügbar sind.

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.

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

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

- 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.
- 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 1. Lizenzvorgänge auf der Basis des Status oder des Zustands

Status oder Zustand von Lizenz/ Komponente	Importieren	Exportieren	Löschen	Ersetzen	Mehr erfahren
Nicht-Administrator-Anmeldung	Ja	Nein	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 CMC-Webschnittstelle zu verwalten, gehen Sie zu **Gehäuseübersicht** → **SetupGehäuseübersicht** → **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.

Funktion	Express	Enterprise	Anmerkungen
CMC-Netzwerk	Ja	Ja	
Serielle CMC-Schnittstelle	Ja	Ja	
Active Directory und LDAP	Nein	Ja	
Steckplatz- und Funktionszuweisung (PCIe und virtuelle Adapter)	Nein	Ja	
RACADM (SSH, Lokal und Remote)	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	
Gehäusewiederherstellung und -Backup	Nein	Ja	

Server-Modul-Firmware-Aktualisierung	Nein	Ja	
Remote-Syslog	Nein	Ja	
Verzeichnisdienste	Nein*	Ja	*Für Nicht-Standardverzeichnisdiensteinstellungen ist nur „Verzeichnisdienste zurücksetzen“ mit einer 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 einer 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.
Verwaltung von mehreren Gehäusen	Nein	Ja	
Erweiterte Konfiguration	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	

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 Benutzerhandbuchs

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

- Die Webschnittstelle: Hier erhalten Sie nur Informationen in Beziehung zu Tasks. Informationen über die Felder und Optionen finden Sie unter der *CMC for Dell PowerEdge VRTX Online Help* (CMC für Dell PowerEdge VRTX Online-Hilfe), die Sie von der Webschnittstelle aus öffnen können.
- Die RACADM-Befehle: Der RACADM-Befehl oder das Objekt, das Sie verwenden müssen, wird hier angezeigt. Weitere Informationen über einen RACADM-Befehl finden Sie unter *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.

Weitere nützliche Dokumente

Um auf die Dokumente auf der Dell Support-Website zuzugreifen. Zusätzlich zu dieser Anleitung können Sie auf die folgenden Anleitungen zugreifen, die hier zur Verfügung stehen: **dell.com/support/manuals**.

- Die *VRTX CMC Online Help* (VRTX CMC Online-Hilfe) enthält Informationen zur Verwendung der Webschnittstelle. Um auf diese Online-Hilfe zuzugreifen, klicken Sie auf **Hilfe** auf der CMC-Webschnittstelle.
- Im *Chassis Management Controller Version 1.0 for Dell PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller Version 1.0 für PowerEdge VRTX) finden Sie Informationen zur Verwendung der Funktionen, die mit VRTX in Beziehung stehen.
- Die *Dell Chassis Management Controller (CMC) for Dell PowerEdge VRTX Version 1.00 Release Notes* (Dell Chassis Management Controller (CMC) für Dell PowerEdge VRTX Version 1.00 Versionshinweise) geben den letzten Stand der Änderungen am System oder der Dokumentation wieder oder enthalten erweitertes technisches Referenzmaterial für erfahrene Benutzer oder Techniker.
- Das *Integrated Dell Remote Access Controller 7 (iDRAC7) User's Guide* (Integrierte Dell Remote Access Controller 7 (iDRAC7)-Benutzerhandbuch) gibt Informationen über die Installation, Konfiguration und Wartung des iDRAC auf verwalteten Systemen.
- Das *Dell OpenManage Server Administrator-Benutzerhandbuch* enthält Informationen über die Installation und Anwendung von Server Administrator.
- 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 ist online verfügbar unter dell.com/storagecontrollermanuals.
- 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-Aktualisierungen und mit dem System erworbene Komponenten. Für weitere Informationen über das System durchsuchen Sie den Quick Resource Locator (QRL) (Schnellen Ressourcenfinder), der auf Ihrem System und auf dem System-Setup-Platzset, das mit Ihrem System geliefert wurde, verfügbar ist. Laden Sie die QRL-Anwendung von Ihrer mobilen Plattform herunter, um die Anwendung auf Ihren Mobilgeräten zu aktualisieren.

Möglicherweise sind auch Aktualisierungen beigelegt, in denen Änderungen am System, an der Software und/oder an der Dokumentation beschrieben sind. Lesen Sie diese Aktualisierungen immer zuerst, da sie frühere Informationen gegebenenfalls außer Kraft setzen.

Zugriff auf Dokumente der Dell Support-Website

So greifen Sie auf die Dokumente der Dell Support-Website zu:

1. Rufen Sie die Website **dell.com/support/manuals** auf.
2. Wählen Sie im Abschnitt **Tell us about your Dell system (Sagen Sie uns, welches Dell-System Sie haben)** unter **No (Nein) Choose from a list of all Dell products (Aus einer Liste mit allen Dell-Produkten auswählen)** aus und klicken Sie auf **Continue (Fortfahren)**.
3. Klicken Sie im Abschnitt **Select your product type (Produkttyp auswählen)** auf **Software and Security (Software und Sicherheit)**.
4. Wählen Sie im Abschnitt **Choose your Dell Software (Wählen Sie Ihre Dell-Software aus)** unter den folgenden Optonen aus und klicken Sie auf den benötigten Link:
   - **Client System Management (Client-Systemverwaltung)**
   - **Enterprise System Management (Unternehmens-Systemverwaltung)**
   - **Remote Enterprise System Management (Unternehmens-Remote-Systemverwaltung)**
   - **Serviceability Tools (Tools für die Betriebsfähigkeit)**
5. Klicken Sie zur Anzeige des Dokuments auf die benötigte Produktversion.

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

- Für Unternehmens-Systemverwaltungsdokumente – **dell.com/OMConnectionsClient**
- Für Unternehmens-Remote-Systemverwaltungsdokumente – **dell.com/OMConnectionsClient**
- Für Tools für die Betriebsfähigkeitsdokumente – **dell.com/serviceabilitytools**
- Für Client-Systemverwaltungsdokumente – **dell.com/OMConnectionsClient**
- Für OpenManage Connections Enterprise-Systemverwaltungsdokumente – **dell.com/OMConnectionsEnterpriseSystemsManagement**
- Für OpenManage Connections Client-Systemverwaltungsdokumente – **dell.com/OMConnectionsClient**

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.

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 ist `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.

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**.

Zertifikatsperrliste (CRL) abrufen

Wenn der CMC nicht über einen Internetzugang verfügt, deaktivieren Sie die Abruffunktion der Zertifikatsperrliste (CRL) im Internet Explorer. Diese Funktion testet, ob ein Server wie z. B. der CMC-Webserver 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, wie 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 internen 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

Konfiguration von CMC mit Setup-Kurzanleitung (DHCP)

ANMERKUNG: Sie können die Ausrichtung einer LCD-Anzeige (für Rack- oder Tower-Modus) anpassen, indem sie die Schaltflächen Nach oben-Nach unten für zwei Sekunden gedrückt halten. Alternativ dazu können Sie auch die Schaltflächen Nach rechts-Nach links verwenden. Weitere Informationen, über die Schaltflächen, die auf einem CMC LCD-Bereich verfügbar sind, finden Sie unter LCD-Navigation.

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

1. Drücken Sie auf den Netzschalter des Gehäuses, um das Gehäuse einzuschalten. Der LCD-Bereich zeigt beim Einschalten eine Reihe von Initialisierungsbildschirmen.
2. Wählen Sie aus dem Bereich **Hauptmenü Einstellungen** aus.
3. Wählen Sie aus dem Bereich **LCD-Sprache** Ihre Sprache mit den Pfeilschaltflächen aus und drücken Sie dann auf die Schaltfläche in der Mitte. Der Bereich **Hauptmenü** wird angezeigt.
4. Wählen Sie **Einstellungen** aus und wählen Sie dann **Netzwerkeinstellungen** aus. Wenn Sie im Bereich **Netzwerkeinstellungen** aufgefordert werden, entweder den Schnell-Setup für den CMC unter Verwendung von DHCP zu wählen oder den Setup mit dem erweiterten Setup-Modus auszuführen, verwenden Sie die Pfeilschaltflächen und wählen Sie eines der Folgenden aus:
   - **Schnell-Setup (DHCP)**
   - **Erweiterter Setup**
5. Wenn Sie **Schnell-Setup (DHCP)** wählen, zeigt der Bereich die folgende Meldung an.

   ```
   Sie sind dabei, DHCP-Adressen zu bekommen. Stellen Sie sicher, dass das
   Stromkabel angeschlossen ist.
   ```

   Drücken Sie auf die mittlere Schaltfläche und warten Sie dann ein paar Minuten. Der Bereich zeigt die Meldung **Bitte Warten** an und zeigt dann die CMC IP-Nummer im Bereich **IP-Zusammenfassung** an.

   ```
   CMC-IP4: <IP-Nummer>
   ```

Drücken Sie auf die mittlere Schaltfläche und drücken Sie dann erneut auf die mittlere Schaltfläche. Der Fensterbereich **Hauptmenü** wird angezeigt.

CMC unter Verwendung von erweitertem Setup konfigurieren

1. Wenn Sie im Fensterbereich **Netzwerk-Einstellungen Erweitertes Setup** auswählen, wird die folgende Meldung angezeigt, die Sie fragt, ob Sie ein CMC konfigurieren möchten oder nicht.

   `CMC konfigurieren?`
2. Um Ihr CMC unter Verwendung von erweiterten Setup-Eigenschaften zu konfigurieren, klicken Sie auf die mittlere Schaltfläche. Fahren Sie mit Schritt 4 fort. Andernfalls fahren Sie mit Schritt 14 fort, um Ihr iDRAC zu konfigurieren.
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 Geschwindigkeit Ihrer Netzwerkkonfiguration, steigt der Verbrauch der Bandbreite und die Netzwerkkommunikation wird verlangsamt. Bestimmen Sie, ob Ihr Netzwerk die oben angegebenen Netzwerkgeschwindigkeiten unterstützt und setzen Sie diese entsprechend. Wenn die Netzwerkkonfiguration mit keinem dieser Werte übereinstimmt, wird empfohlen, die Option **Autom.(1 GB)** zu verwenden oder sich mit dem Hersteller Ihrer Netzwerkausrüstung in Verbindung zu setzen.
4. Um **Autom. (1Gb)** auszuwählen, drücken Sie auf die Schaltfläche in der Mitte, und drücken Sie erneut auf die mittlere Schaltfläche. Fahren Sie mit Schritt 7 fort. Oder wenn Sie **10 MB** oder **100 MB** ausgewählt haben, fahren Sie mit Schritt 5 fort.
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.

   ANMERKUNG: Die Netzwerkgeschwindigkeits- und Duplexmodus-Einstellungen sind nicht verfügbar, wenn die **Automatische Verhandlung** auf **Ein** eingestellt oder wenn **1000 MB** (1 GBit/s) ausgewählt ist. Wenn Automatische Verhandlung für ein Gerät eingeschaltet ist, für ein anderes jedoch nicht, kann das Gerät mit automatischer Verhandlung die Netzwerkgeschwindigkeit des anderen Geräts festlegen, den Duplexmodus jedoch nicht. In diesem Fall setzt sich der Duplexmodus während der automatischen Verhandlung auf Halbduplex. Ein derartiger Duplex-Übereinstimmungsfehler resultiert in 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 **IPv4** oder **Beide** wählen, fahren Sie mit Schritt 9 oder 10 fort, basierend auf Ihrer Wahl von **DHCP** oder **Statischer** Modus. Andernfalls wählen Sie **IPv6** und fahren Sie später währen dieser Prozedur mit Schritt 11 fort.
8. Wählen Sie den **Modus** aus, in dem der CMC die NIC-IP-Adressen abrufen soll: Wenn Sie DHCP auswählen, ruft CMC die IP-Konfiguration (IP-Adresse, Maske und Gateway) automatisch von einem DHCP-Server im Netzwerk ab. Dem CMC im Netzwerk wird eine eindeutige IP-Adresse zugewiesen. Wenn Sie **DHCP** ausgewählt haben, drücken Sie auf die mittlere Schaltfläche und drücken Sie erneut auf die mittlere Schaltfläche. Der Bereich **iDRAC Konfigurieren** wird angezeigt. Fahren Sie später währen dieser Prozedur mit Schritt 12 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 IP-Informationen, die Sie eingegeben haben, werden angezeigt. Drücken Sie auf die mittlere Schaltfläche und drücken Sie erneut auf die mittlere Schaltfläche. Der Bildschirm **CMC-Konfiguration** listet die **Statische IP - Adresse**, die **Subnetzmaske** und die **Gateway-**Einstellungen, die Sie eingegeben haben. Überprüfen Sie die Einstellungen auf Richtigkeit. Drücken Sie auf die entsprechenden Schaltflächen für eine korrekte Einstellung. Drücken Sie auf die mittlere Schaltfläche und drücken Sie erneut auf die mittlere Schaltfläche. Der Fensterbereich **DNS registrieren?** wird angezeigt.
10. Um die IP-Adresse des DNS-Servers zu registrieren, geben Sie die IP-Adresse des DNS-Servers ein und drücken Sie auf die Schaltfläche in der Mitte. Fahren Sie mit Schritt 12 fort und wählen Sie aus, ob Sie ein iDRAC konfigurieren möchten oder nicht.

11. Wenn Sie die Registrierung nicht auswählen, fahren Sie mit Schritt 12 fort.
12. Geben Sie an, ob Sie einen iDRAC konfigurieren möchten:
    - **Nein**: Fahren Sie später währen dieser Prozedur mit Schritt 17 fort.
    - **Ja**: Drücken Sie auf die mittlere Schaltfläche.

    Sie können iDRAC auch über die CMC-Web-Schnittstelle konfigurieren.
13. Wählen Sie im Bereich **Protokoll** den IP-Typ (IPv4, IPv6, oder beide) aus, den Sie für die Server verwenden wollen. Wenn Sie **IPv4** oder **Beide** ausgewählt haben, wählen Sie **DHCP** oder **Statisch** aus, und fahren Sie mit Schritt 14 fort. Andernfalls, wenn Sie **IPv6** ausgewählt haben, fahren Sie später währen dieser Prozedur mit Schritt 17 fort.

Dynamic Host Configuration Protocol (DHCP)	iDRAC ruft die IP-Konfiguration (IP-Adresse, Maske und Gateway) automatisch von einem DHCP-Server im Netzwerk ab. Dem iDRAC im Netzwerk wird eine eindeutige IP-Adresse zugewiesen. Drücken Sie auf die mittlere Schaltfläche und fahren Sie dann mit Schritt 16 dieser Prozedur fort.

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 werden automatisch nach Steckplatznummer erhöht.`
	Klicken Sie auf die mittlere Schaltfläche. Die folgende Meldung fordert Sie auf, die Steckplatz–1 IP-Nummer einzugeben.
	`Steckplatz 1 (startet) IP eingeben`
	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. Auf dem Bildschirm **Netzwerk-Zusammenfassung** sind die von Ihnen eingegebenen Einstellungen für **Statische IP-Adresse**, **Subnetzmaske** und **Gateway** aufgeführt. Überprüfen Sie die Einstellungen auf Richtigkeit. Für eine korrekte Einstellung 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.

14. Wählen Sie **Aktivieren** oder **Deaktivieren** aus, um anzugeben, ob Sie IPMI über LAN aktivieren möchten. Drücken Sie auf die mittlere Schaltfläche, um weiterzufahren.
15. Die folgende Meldung wird im Bereich **iDRAC-Konfiguration** angezeigt.

    `Einstellungen zu den installierten Servern anwenden?`

    Um alle iDRAC-Netzwerkeinstellungen auf die installierten Server anzuwenden, wählen Sie **Ja** und drücken Sie dann auf die mittlere Schaltfläche. Andernfalls wählen Sie **Nein,** drücken Sie auf die mittlere Schaltfläche und fahren Sie später währen dieser Prozedur mit Schritt 17 fort.
16. Die folgende Meldung wird im nächsten Fensterbereich **iDRAC-Konfiguration** angezeigt.

    `Einstellungen automatisch zu neu eingefügten Servern anwenden?`

    Um alle iDRAC-Netzwerkeinstellungen auf die neu installierten Server anzuwenden, wählen Sie **Ja** aus und drücken Sie auf die mittlere Schaltfläche. Wenn ein neuer Server in das Gehäuse eingesetzt wird, werden Sie auf der LCD gefragt, ob der Server unter Verwendung der zuvor konfigurierten Netzwerkeinstellungen und Richtlinien

automatisch bereitgestellt werden soll. Wenn Sie die iDRAC-Netzwerkeinstellungen nicht auf den neu installierten Servern anwenden wollen, wählen Sie **Nein** 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.

    ```
    Alle Gehäuseeinstellungen anwenden?
    ```

    Um alle Gehäuseeinstellungen anzuwenden, wählen Sie **Ja** und drücken Sie auf die mittlere Schaltfläche. Andernfalls wählen Sie **Nein** und drücken Sie auf die mittlere Schaltfläche.

18. Überprüfen Sie die von Ihnen bereitgestellten IP-Adressen im Bereich **IP-Zusammenfassung**, um sicherzustellen, dass die Adressen korrekt sind. Für eine korrekte Einstellung, drücken Sie auf die Schaltfläche **Zurück** und drücken Sie dann auf die Schaltfläche in der Mitte, um zum Bildschirm für diese Einstellung zurückzukehren. Nachdem Sie eine IP-Adresse korrigiert haben, drücken Sie auf die Schaltfläche in der Mitte.

    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. Der Fensterbereich **Hauptmenü** wir angezeigt.

    Der CMC und iDRACs sind jetzt im Netzwerk verfügbar. Sie können über die Webschnittstelle oder die CLIs, z. B. eine serielle Konsole, Telnet und SSH, auf den CMC unter der zugewiesenen IP-Adresse 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 unter Verwendung von Web, SSH oder Remote-RACADM aktivieren.

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

Tabelle 2. 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 „Supported Browsers“ (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.

Schnittstelle	Beschreibung
Gehäuse-LCD-Bedienfeld	Verwenden Sie die LCD auf der Frontblende, um die folgenden Aktivitäten auszuführen: • Warnungen, CMC-IP- oder MAC-Adresse oder benutzerprogrammierbare Zeichenfolgen anzeigen • DHCP festlegen • Statische IP-Einstellungen für CMC konfigurieren
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.
WS-MAN	Die LC-Remote Services basieren auf dem Web Services for Management (WSMAN)-Protokoll für 1-zu-n-Verwaltungsaufgaben. Sie müssen einen WS-MAN-Client verwenden, z. B. den WinRM-Client (Windows) oder den OpenWSMAN-Client (Linux), um die LC-Remote Services-Funktion zu verwenden. Sie können außerdem Power Shell- und Python-Skript verwenden, um auf die WS-MAN-Schnittstelle zu schreiben. WSMAN ist ein SOAP-basiertes (Simple Object Access Protocol) Protokoll, das für Systemverwaltung verwendet wird. CMC verwendet WS–Management zum Übermitteln von DMTF-CIM-basierten Verwaltungsinformationen (Distributed Management Task Force; Common Information Model). Die CIM-Informationen definieren die Semantik- und Informationstypen, die in einem verwalteten System geändert werden können. Die CMC WS-MAN-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/** • WS-MAN Versionshinweisdatei. • **www.wbemsolutions.com/ws_management.html** • DMTF WS-Management-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.

Schnittstelle	Beschreibung
	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 auf eine der folgenden Seiten:
  - **Gehäuseübersicht** → **Fehlerbehebung**.
  - **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**

    ANMERKUNG: Auf dieser Seite können nur physische Festplatten und virtuelle Festplatten 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 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
- `Schalter-1`
- `cmc-activ`

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 und die virtuelle Festplatte 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.

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

Ähnlich wie beim Ausfallschutz, den ein redundanter CMC bietet, aktiviert das PowerEdge VRTX-Gehäuse 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 der CMC-Ausfallzeitraums 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 mit dem Gehäuse verbunden 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**.

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**.

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.

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.

Als lokaler Benutzer, Active Directory-Benutzer oder LDAP-Benutzer bei CMC anmelden

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.

Das CMC-Modul 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. 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**.
4. 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.

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 einfacher 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.

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 3. CMC-Mehrfachsitzungen

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

4

Aktualisieren der Firmware

Sie können die Firmware für Folgendes aktualisieren:

- CMC – Aktiv und Standby
- Gehäuseinfrastruktur
- E/A-Modul
- iDRAC7

Sie können die Firmware für folgende Serverkomponenten aktualisieren:

- iDRAC
- BIOS
- Lifecycle-Controller
- 32–Bit-Diagnose
- Treiberpaket des Betriebssystems
- Netzwerkschnittstellen-Controller
- RAID-Controller

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.

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

Die CMC-Firmware kann mit der CMC-Webschnittstelle oder RACADM aktualisiert werden. Die Firmware-Aktualisierung behält standardmäßig die aktuellen CMC-Einstellungen bei. Während des Aktualisierungsvorgangs können Sie die CMC-Konfigurationseinstellungen auf die werkseitigen Voreinstellungen zurückzusetzen.

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

Wenn eine Benutzersitzung an der Webschnittstelle verwendet wird, um Systemkomponenten-Firmware zu aktualisieren, müssen die Einstellungen für die **Inaktivitätszeitüberschreitung (0, 60–10800)** auf einen höheren Wert gesetzt sein, um die Dateitransferzeit abzudecken. In einigen Fällen kann die Übertragungszeit der Firmware bis zu 30 Minuten betragen. Zur Einstellung des Wertes für die Inaktivitätszeitüberschreitung beachten Sie bitte 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.

Der aktive CMC wird zurückgesetzt und ist vorübergehend nicht verfügbar, nachdem die Firmware erfolgreich hochgeladen wurde. Wenn ein Standby-CMC vorhanden ist, dann werden die Rollen zwischen Standby und Aktiv getauscht. Der Standby-CMC wird zum aktiven CMC. Wird eine Aktualisierung lediglich für den aktiven CMC durchgeführt, wird der aktive CMC nach Abschluss des Reset nicht das aktualisierte Image ausführen; lediglich der Standby-CMC wird dieses Image haben. Allgemein wird dringend empfohlen, identische Firmware-Versionen für die aktiven und Standby-CMCs zu unterhalten.

Nachdem der Standby-CMC aktualisiert wurde, tauschen Sie die CMC-Rollen miteinander aus, sodass der neu aktualisierte CMC als aktiver CMC und der CMC mit der früheren Firmware als Standby funktioniert. Weitere Informationen zum Tausch von Rollen finden Sie im Befehlsabschnitt `cmcchangeover` im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX). Das Ausführen dieses Befehls ermöglicht Ihnen zu 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 Befehl `cmcchangeover` verwenden, um die vorhergehenden Rollen der CMCs wiederherzustellen. Die CMC Firmwareversion 2.x aktualisiert sowohl den primären CMC als auch den redundanten CMC ohne Ausführung des `cmcchangeover`-Befehls.

Um zu vermeiden, dass die Verbindung von Benutzern während des Resets unterbrochen wird, benachrichtigen Sie bitte berechtigte Benutzer, die sich am CMC anmelden könnten, und prüfen Sie auf aktive Sitzungen, indem Sie die Seite **Sitzungen** anzeigen. Um die Seite **Sitzungen** zu öffnen, wählen Sie im linken Fensterbereich **Gehäuse-Übersicht** aus, klicken Sie auf **Netzwerk** und dann auf **Sitzungen**.

Wenn Sie Dateien zum und vom CMC übertragen, dreht sich während der Übertragung das Dateiübertragungssymbol. Wenn das Symbol animiert ist, überprüfen Sie, ob der Browser so konfiguriert ist, dass Animationen zugelassen sind.

Weitere Informationen zum Zulassen von Animationen im Browser finden Sie unter Animationen im Internet Explorer zulassen.

Aktualisieren der CMC-Firmware über 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).

CMC-Firmware über die Webschnittstelle aktualisieren

ANMERKUNG: Bevor Sie die CMC-Firmware aktualisieren, achten Sie darauf, dass das Gehäuse eingeschaltet ist, aber alle Server im Gehäuse ausgeschaltet sind.

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. Im Feld **Firmware-Image** geben Sie den Pfad zur Firmware-Image-Datei auf der Management Station oder dem gemeinsam genutzten Netzwerk ein oder klicken Sie auf **Durchsuchen**, um zum Dateispeicherort zu navigieren. Der Standardname des CMC-Firmware-Image ist `vrtx_cmc.bin`.
4. Klicken Sie auf **Firmware-Aktualisierung beginnen** und klicken Sie auf **Ja**. 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 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 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 der 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.

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 ist und die Server ausgeschaltet sind.

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 Firmware für iDRAC7 oder höher aktualisieren. Um diese Funktione zu nutzen, müssen Sie über eine Enterprise-Linzenz verfügen

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 eine iDRAC-Firmware zu aktualisieren, muss der CMC eine SD-Karte haben.

Server-iDRAC-Firmware mittels RACADM aktualisieren

Sie können die iDRAC7-Firmware durch Ausführen des Befehls `fwupdate` aktualisieren. Sie müssen dafür eine Enterprise-Lizenz aufweisen. Die iDRAC7-Version muss 1.40.40 oder später sein. 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).

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**.
   - **Gehäuseübersicht** → **Gehäuse-Controller** → **Aktualisieren.**
   - **Gehäuseübersicht** → **E/A-Modulübersicht** → **Aktualisieren.**

   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. Um iDRAC7 Firmware zu aktualisieren, klicken Sie im Abschnitt **iDRAC7 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 **firmimg.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

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.

Dell Update Packages (DUPs) werden zur Durchführung der Firmware-Aktualisierungen mit dem Lifecycle-Controller verwendet. Die DUP-Komponente für das Betriebssystem-Treiberpaket überschreitet diesen Grenzwert und muss separat über die Funktion „Erweiterter Speicher“ aktualisiert werden.

Der Lifecycle Controller bietet eine Modulaktualisierungsunterstützung für iDRAC6 und Server mit neueren Versionen. Die iDRAC-Firmware muss in einer Version ab Version 2.3 vorliegen, um die Firmware mithilfe von Lifecycle Controller aktualisieren zu können.

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

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

- BIOS
- Lifecycle-Controller
- iDRAC

Um die Serverkomponenten-Firmware mithilfe der CMC-Webschnittstelle zu aktualisieren, klicken Sie auf **Gehäuseübersicht → Server-Übersicht → Aktualisierung → Server-Komponentenaktualisierung** .

Wenn der Server den Lifecycle-Controller-Dienst nicht unterstützt, wird im Abschnitt **Komponente/Gerät-Firmware-Bestandsaufnahme 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 möglich.

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 einer Dateinamenerweiterung **.usc** verfügbar. Diese Datei ermöglicht es 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 *Lifecycle-Controller Benutzerhandbuch*.

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

```
Lifecycle-Controller kann ggf. nicht aktiviert werden an.
```

Aktivierung des Lifecycle Controllers

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

- Drücken Sie auf der Startkonsole des iDRAC6-Servers auf <Strg><R>, wenn die folgende Meldung angezeigt wird.

  ```
  Drücken Sie innerhalb von 5 Sekunden für die Einrichtung des Remote-
  Zugriffs die Tastenkombination <Strg-E>.
  ```

  . Aktivieren Sie anschließend auf dem Setup-Bildschirm die Option **Systemdienste**. Gehen Sie auf die Seite **System-Setup-Hauptmenü** und klicken Sie auf **Fertig stellen**, um die Einstellungen zu speichern.
- Klicken Sie für iDRAC7-Server auf der Startkonsole für das **System Setup**-Programm auf 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.

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 zu nutzen, benötigen Sie eine Enterprise-Lizenz.

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 **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 Aktualiserung 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 es darauf hin, dass sich der iDRAC auf dem Server zum Zeitpunkt des Abrufens der Firmware-Bestandsaufnahme noch in der Initialisierungsphase befand. Warten Sie etwas, 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, dann müssen Sie während des Server-Startvorgangs Lifecycle-Controller aufrufen. Dies ist beim Aktualisieren der internen Komponenten- und Geräteinformationen hilfreich und stellt eine Möglichkeit zur Prüfung der derzeit installierten Komponenten und Geräte dar. Dieses Verhalten tritt auf, 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-Einstellungsdienstprogramm (für iDRAC7) eine Option bereit, auf die über die Startkonsole zugegriffen werden kann:

     1. Um auf **System Setup** zuzugreifen, drücken Sie für iDRAC7-Server auf der Startkonsole auf <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 4. 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.

Feld	Beschreibung
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**.

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. Filtern Sie auf der Seite **Serverkomponenten-Aktualisierung** die Komponente oder das Gerät (optional).
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** – 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. Filtern Sie auf der Seite **Serverkomponentenaktualisierung** die Komponente oder das Gerät (optional).
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 Speicher**funktion 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 über die CMC-Webschnittstelle

So aktualisieren Sie Firmware zu der nächsten Version:

1. Klicken Sie im linken Fensterbereich auf **Serverübersicht**, und klicken Sie dann auf **Aktualisierung**.
2. Filtern Sie auf der Seite **Serverkomponenten-Aktualisierung** die Komponente oder das Gerät (optional).
3. Wählen Sie in der Spalte **Aktualisierung** die Optionen der Komponente oder des Geräts, für das Sie die Firmware auf die nächste Version aktualisieren möchten.

   ANMERKUNG: Wählen Sie mithilfe des <Strg>-Tastenkurzbefehls einen Komponenten- oder Gerätetyp für die Aktualisierung auf allen anwendbaren Servern aus. Durch das gedrückt Halten der <Strg>-Taste werden alle Komponenten gelb markiert. Während die <Strg>-Taste gedrückt wird, wählen Sie die gewünschte Komponente oder das Gerät aus, indem Sie die zugehörigen Optionen in der Spalte **Aktualisierung** aktivieren.

   Eine andere 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.

4. Geben Sie die Firmware-Image-Datei für die ausgewählten Komponenten bzw. die ausgewählten Geräte an. Dies ist eine Microsoft Windows Dell Update Package (DUP)-Datei für Microsoft Windows.
5. Wählen Sie eine der folgenden Optionen:
   - **Jetzt neustarten** – Den Server sofort neu starten..
   - **Bei nächstem Neustart** – Manuell zu einem späteren Zeitpunkt neu starten.

   ANMERKUNG: Dieser Schritt ist für Lifecycle-Controller- und 32-Bit-Diagnose-Firmwareaktualisierung nicht gültig. Ein Server-Neustart wird für diese Geräte sofort ausgeführt.
6. Klicken Sie auf **Aktualisieren**. Die Firmware-Version für die ausgewählten Komponenten oder Geräte wird aktualisiert.

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 **Aktualisierung von Speicherkomponenten** auf **Durchsuchen**, wählen Sie das DUP, das vorher heruntergeladen wurde, aus und klicken Sie dann auf **Hochladen**.

   Das DUP wird auf den CMC hochgeladen und die Seite **Firmware-Aktualisierungstatus** wird mit den folgenden Informationen angezeigt:
   - Verstrichene Zeit
   - Zielkomponenten

- Aktuelle Firmware-Version
- Aktualisierungsstatus

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 *iDRAC7User's Guide* (iDRAC7-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

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 Gehäusefunktionszustand 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, Servermodule, E/A-Module (EAMs), Lüfter, Netzteileinheiten (PSUs), LCD-Einheit, Speicher-Controller und 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*.

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 Rückansichten dargestellt (jeweils die oberen und unteren Bilder). Server, DVDs, HDDs, KVMs, und LCD werden in der Vorderansicht gezeigt und die restlichen Komponenten werden in der Rückansicht gezeigt. Die Komponentenauswahl wird durch eine blaue Einfärbung angezeigt und wird durch Anklicken des Bildes der erforderlichen Komponente gesteuert. Wenn eine Komponente im Gehäuse vorhanden ist, dann 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 Komponenten 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 5. Serversymbolzustände

Symbol	Beschreibung
	Ein Server ist vorhanden, eingeschaltet, und funktioniert 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.

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.
- Quicklinks – Ermöglicht den Wechsel zu häufig besuchten Seiten und zu den am häufigsten durchgeführten Maßnahmen. Nur Links, die für die ausgewählte Komponente gelten, werden in diesem Bereich angezeigt.

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. Klicken Sie im linken Fensterbereich auf **Server-Übersicht**. Alle Server (STECKPLATZ-01 bis STECKPLATZ-04) werden in der Liste der Server angezeigt. Ist ein Server im Steckplatz nicht vorhanden, wird das entsprechende Abbild in der Grafik grau unterlegt.
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 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. Wählen Sie **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*.

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>]
```

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.

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), verfügbar unter dell.com/support/manuals.

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:

   ```
   Lüfter <Nummer> ist niedriger als der kritische Warnungsschwellenwert.
   ```

   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.

Um die Offset-Funktion einzustellen, gehen Sie zu **Gehäuseübersicht → Lüfter → Setup**. Wählen Sie auf der Seite **Erweiterte Lüfterkonfiguration** entsprechend im Drop-Down-Menü **Wert** das dem **Lüfter-Offset** entspricht aus.

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 Serversteckplätzen 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.

Um den ECM-Modus einzustellen, gehen Sie zu **Gehäuseübersicht** → **Lüfter** → **Setup**. Wählen Sie auf der Seite **Erweiterte Lüfterkonfiguration** aus dem Drop-Down-Menü **Wert** das **Erweiterter Kühlmodus** entspricht, entsprechend aus.

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.

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.
- Einrichten der Gehäusegruppe 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)

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

Verwenden Sie zum Anzeigen von IPv4-Einstellungen die folgenden Unterbefehle und Objekte:

- `getniccfg`
- `getconfig`
- cfgCurrentLanNetworking

Verwenden Sie zum Anzeigen von IPv6-Einstellungen die folgenden Unterbefehle und Objekte:

- `getconfig`
- cfgIPv6LanNetworking

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).

Aktivieren der CMC-Netzwerkschnittstelle

Um die CMC-Netzwerkschnittstelle für IPv4 bzw. IPv6 zu aktivieren oder 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 4cfgNicIPv4Enable 0
```

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

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

```
racadm conf4ig -g cfgIpv6LanNetworking -o cfgIPv6Enable 1 racadm config -g
cfgIpv6LanNetworking -o cfgIPv6Enable 0
```

ANMERKUNG: 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 <statische IP-Adresse> racadm config -g
cfgLanNetworking -o cfgNicGateway <statisches Gateway> racadm config -g racadm
config -g cfgLanNetworking -o cfgNicNetmask <statische Subnetzmaske>
```

Standardmäßig fordert der CMC für IPv6 automatisch eine CMC-IP-Adresse vom IPv6-AutoConfiguration-Mechanismus 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-Adresse> racadm config -g
cfgIPv6LanNetworking -o cfgIPv6PrefixLength 64 racadm config -g
cfgIPv6LanNetworking -o cfgIPv6Gateway <IPv6-Adresse>
```

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-Server-Adressfunktionen zu aktivieren und bevorzugte statische und alternative DNS-Server-Adressen anzugeben, geben Sie Folgendes ein:

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

Um die Funktion DHCP für DNS-Server-Adressfunktionen für IPv6 zu aktivieren 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 der DNS-Einstellungen (IPv4 und IPv6)

- **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 vorgegebene Standardname des CMC-Moduls am DNS-Server ist 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.
- **DNS-Domänenname** – Der Standard-DNS-Domänenname ist ein einziges 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“ (IPv4 und IPv6)

Wenn aktiviert, bestimmt die automatische Verhandlungsfunktion, 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 <Duplexmodus>
```

wobei:

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

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

wobei:

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

Einstellen der maximalen Übertragungseinheit (MTU) (IPv4 und IPv6)

Über die MTU-Eigenschaft können Sie die maximale Größe von Paketen festlegen, die über die Schnittstelle übertragen werden können. Um die maximale Paketgröße festzulegen, geben Sie Folgendes ein:

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

wobei <*mtu*> ein Wert zwischen 576-1500 ist (einschließlich; Standardeinstellung ist 1500).

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

Netzwerksicherheitseinstellungen konfigurieren

Sie können die Netzwerksicherheitseinstellungen nur für IPv4 konfigurieren.

Netzwerksicherheitseinstellungen über die CMC-Webschnittstelle konfigurieren

ANMERKUNG: Um die folgenden Tasks auszuführen, müssen Sie die Berechtigung als **Gehäusekonfiguration-Administrator** besitzen.

So konfigurieren Sie die Netzwerksicherheitseinstellungen über die CMC-Webschnittstelle:

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** und klicken Sie dann auf **Netzwerk**. Die Seite **Netzwerkkonfiguration** wird angezeigt.
2. Im Abschnitt **IPv4-Einstellungen**, klicken Sie auf **Erweiterte Einstellungen**. Die Seite **Netzwerksicherheit** wird angezeigt.
3. Geben Sie den IP-Bereich und die IP-Blockierungswerte ein. Weitere Informationen finden Sie in der *Online-Hilfe*.
4. Klicken Sie auf **Anwenden**, um diese Einstellungen zu speichern.

CMC-Netzwerksicherheitseinstellungen über RACADM konfigurieren

Die IP-Filterung vergleicht die IP-Adresse einer eingehenden Anmeldung mit dem IP-Adressenbereich, der in den folgenden **cfgRacTuning**-Eigenschaften angegeben ist:

- **cfgRacTuneIpRangeAddr**
- **cfgRacTuneIpRangeMask**

Eine Anmeldung von der eingehenden IP-Adresse ist nur erlaubt, wenn Folgendes identisch ist:

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

Konfigurieren der virtuellen LAN-Tag-Einstellungen für CMC

VLANs werden verwendet, um zu ermöglichen, dass mehrere virtuelle LANs auf dem gleichen physischen Netzwerkkabel existieren, und um den Netzwerkverkehr für Sicherheits- und Lastverteilungszwecke abzusondern. Wenn die VLAN-Funktionalität aktiviert wird, wird jedem Netzwerkpaket ein VLAN-Tag zugewiesen.

Konfiguration der LAN-Tag-Eigenschaften für CMC unter Verwendung von RACADM

1. Aktivieren Sie die VLAN-Funktionen 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-Priorität>
   ```
   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-Priorität>
   ```
   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 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.

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

Nach dem Einrichten der Gehäusegruppe fügen Sie Mitglieder zur Gruppe hinzu, indem Sie wie folgt vorgehen:

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 die Option **Eigenschaften des neuen Mitglieds mit den Eigenschaften des Führungsgehäuses synchronisieren** aus, um die Eigenschaften des Führungsgehäuses auf das Mitglied zu übertragen. Weitere Informationen über das Hinzufügen von Mitglieder zu einer Gehäusegruppe finden Sie unter Synchronisieren eines neuen Mitglieds mit den Eigenschaften des Führungsgehäuses.
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**.

Starten der Webseite eines Mitgliedsgehäuses oder Servers

Sie können auf die Webseite des Mitgliedsgeräts, der Remote-Konsole des Servers oder der Webseite des iDRAC-Servers über die Gruppenseite des Führungsgehäuses zugreifen. Wenn das Mitgliedsgerät die gleichen Anmeldeinformationen als das Führungsgehäuse hat, können Sie dieselben Anmeldeinformationen für den Zugriff auf das Mitgliedsgerät anwenden.

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 Gehäuseabbild, das im Abschnitt **Funktionszustand** erscheint, den Server.
   c) Wählen Sie im mit **Quicklinks** bezeichneten Kästchen das Zielgerät aus. Es wird ein neues Fenster mit der Zielseite oder dem Anmeldebildschirm angezeigt.

Synchronisieren eines neuen Mitglieds mit den Eigenschaften des Führungsgehäuses

Sie können die Eigenschaften des Führungsgehäuses auf ein neu hinzugefügtes Mitgliedsgehäuse in einer Gruppe anwenden. So synchronisieren Sie ein neues Mitglied mit den Eigenschaften des Führungsgehäuses:

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, während Sie ein neues Mitglied zur Gruppe hinzufügen, auf der Seite **Gehäusegruppe** die Option **Neues Mitglied mit Eigenschaften des Führungsgehäuses synchronisieren** aus.
5. Klicken Sie auf **Anwenden**. Das Mitglied übernimmt die Eigenschaften des Führungsgehäuses.

Die folgenden Konfigurationsdiensteigenschaften für verschiedene Systeme innerhalb des Gehäuses sind von der Synchronisation betroffen:

Tabelle 6. Konfigurationsdiensteigenschaften

Eigenschaft	Navigation
SNMP-Konfiguration	Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** → **Netzwerk** → **Dienste** → **SNMP**.
Remote-Gehäuseprotokollierung	Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** → **Netzwerk** → **Dienste** → **Remote-Syslog**.
Benutzerauthentifizierung mithilfe der Dienste „LDAP“ und „Active Directory“	Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** → **Benutzerauthentifizierung** → **Verzeichnisdienst** .
Gehäusewarnungen	Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** und dann auf **Warnungen**.

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 7. Servermodul Bestandsaufnahme-Feldbeschreibungen

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

Datenfeld	Beispiel
	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.

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. Öffnen Sie eine Telnet/SSH-Textkonsole für den CMC, melden Sie sich an und geben Sie Folgendes 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, **<filename>.cfg**, wird mit dem Befehl `racadm config -f <filename>.cfg` verwendet, um eine einfache Textdatei zu erstellen. Mit dem Befehl können Sie eine Konfigurationsdatei erstellen (ähnlich einer **.ini**-Datei) und den CMC von dieser Datei aus 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 über den 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 Datei **.cfg**, wenn Sie zum ersten Mal auf den CMC geladen wird, um zu überprüfen, dass gültige Gruppen- und Objektnamen vorhanden sind und einfache Syntaxregeln eingehalten werden. Fehler werden mit der Zeilennummer markiert, in der der Fehler ermittelt wurde. Eine Meldung beschreibt das Problem. Die gesamte Datei wird auf Richtigkeit geparst und alle Fehler werden angezeigt. Wenn ein Fehler in der **.cfg**-Datei festgestellt wird, werden Schreibbefehle nicht zum CMC übertragen. Sie müssen alle Fehler korrigieren, bevor eine Konfiguration erfolgen kann.

Um auf Fehler zu prüfen, bevor Sie die Konfigurationsdatei erstellen, verwenden Sie die Option `-c` mit dem Unterbefehl `config`. Mit der Option `-c` prüft `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 aus. Alle Objekte innerhalb dieser Gruppe sind Modifizierungen, wenn der CMC konfiguriert wird. Wenn ein modifiziertes Objekt einen neuen Index darstellt, 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. Mit 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 ermöglicht Flexibilität beim Hinzufügen indizierter Einträge, wobei der Benutzer keine genauen Index-Übereinstimmungen zwischen allen verwalteten CMCs erstellen muss. Neue Benutzer werden dem ersten verfügbaren Index hinzugefügt. Dadurch kann eine **.cfg**-Datei, die auf einem CMC richtig geparst und ausgeführt wird, auf einem anderen möglicherweise nicht richtig ausgeführt werden, 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`, um den CMC auf die ursprünglichen Standardeinstellungen zurückzusetzen, und führen Sie dann den Befehl `racadm config -f <filename>.cfg` aus. Stellen Sie sicher, dass die **.cfg**-Datei alle gewünschten Objekte, Benutzer, Indizes und anderen Parameter enthält. Eine vollständige Liste der Objekte 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. Während der Stammbenutzer 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 eindeutige **.cfg**-Datei verwendet werden.

Parsing-Regeln

- Zeilen, die mit dem Raute-Zeichen (#) beginnen, werden als Anmerkungen behandelt.

  Eine Kommentarzeile muss in Spalte 1 beginnen. Ein „#"-Zeichen in jeder anderen Spalte wird als das Zeichen # behandelt.

  Einige Modemparameter können #-Zeichen in den Zeichenketten enthalten. Ein Escape-Zeichen ist nicht erforderlich. Sie können einen **.cfg**-Befehl von einem `racadm getconfig -f <filename> .cfg`-Befehl erstellen und dann einen `racadm config -f <filename> .cfg`-Befehl auf einem anderen CMC ausführen, ohne dass Sie Escape-Zeichen hinzufügen müssen.

  Beispiel:

  ```
  # # Dies ist ein Kommentar [cfgUserAdmin]
  cfgUserAdminPageModemInitString=<Modem init # Dies ist kein Kommentar>
  ```

- Alle Gruppeneinträge müssen in Klammern stehen ([und]).

  Das Anfangszeichen [, das einen Gruppennamen anzeigt, muss in Spalte Eins stehen. 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 zusammengefasst, wie im Kapitel Datenbankeigenschaften des *RACADM-Befehlszeilen-Referenzhandbuchs für iDRAC6 und CMC* definiert. Das folgende Beispiel zeigt einen Gruppennamen, ein Objekt und den Eigenschaftswert des Objekts an.

  ```
  [cfgLanNetworking] -{Gruppenname} cfgNicIpAddress=143.154.133.121
  {Objektname} {Objektwert}
  ```

- 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 Modemchat-Skriptzeichen.

  ```
  [cfgLanNetworking] -{Gruppenname} cfgNicIpAddress=143.154.133.121
  {Objektwert}
  ```

- 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, so dass Sie die enthaltenen Anmerkungen sehen können.

  ANMERKUNG: Sie können eine indizierte Gruppe manuell mit folgendem Befehl erstellen:

  ```
  racadm config-g <Gruppenname>-o <verankertes Objekt>-i <Index 1-16>
  <eindeutiger Ankername>
  ```

- 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 <Gruppenname> -o <Objektname> -i <Index 1-16> ""
  ```

  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 <Gruppenname> -i <Index 1-16>
  ```

- Für indizierte Gruppen muss es sich bei dem Objektanker um das erste Objekt nach dem "[ ]"-Paar handeln. Im Folgenden finden Sie Beispiele für aktuelle indizierte Gruppen:

  `[cfgUserAdmin] cfgUserAdminUserName= <BENUTZERNAME>`
- Wenn bei Verwendung von Remote-RACADM zur Erfassung der Konfigurationsgruppen in eine 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 vor Ausführung des Befehls `getconfig -f` festgelegt werden. Oder Sie können die fehlenden Eigenschaften nach Ausführung des Befehls `getconfig -f` manuell in die Konfigurationsdatei eingeben. 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:

```
# # Objektgruppe "cfgLanNetworking" # [cfgLanNetworking]
cfgNicIpAddress=10.35.10.110 cfgNicGateway=10.35.10.1
```

Die Datei wird aktualisiert wie folgt:

```
# # Object Gruppe "cfgLanNetworking" # [cfgLanNetworking]
cfgNicIpAddress=10.35.9.143 # Kommentar, der Rest dieser Zeile wird ignoriert
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.

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

Steckplatznamen konfigurieren

Steckplatznamen werden zur Identifizierung einzelner Server verwendet. Bei der Auswahl von Steckplatznamen gelten folgende Regeln:

- Namen dürfen maximal 15 nicht erweiterte ASCII-Zeichen (ASCII-Codes 32 bis 126) enthalten.
- Steckplatznamen müssen innerhalb des Gehäuses eindeutig sein. Derselbe Name darf nicht für einen zweiten Steckplatz verwendet werden.
- Für Zeichenketten wird nicht zwischen Groß- und Kleinschreibung unterschieden. `Server-1, server-1, und SERVER-1` gelten als gleiche Namen.
- Steckplatznamen dürfen nicht mit einer der folgenden Zeichenketten beginnen:
  - Switch-
  - Lüfter-
  - PS-
  - DRAC-
  - MC-
  - Gehäuse
  - Housing-Left
  - Housing-Right
  - Housing-Center
- Die Zeichenketten `Server-1` bis `Server-4` können verwendet werden, allerdings nur für den entsprechenden Steckplatz. Z. B. ist `Server-3` ein gültiger Name für Steckplatz 3, aber nicht für Steckplatz 4. `Server-3` ist jedoch 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 ein 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 Fensterbereich auf **Gehäuseübersicht** → **Serverübersicht** → **Setup** → **Steckplatznamen**.
2. Bearbeiten Sie auf der Seite **Steckplatznamen** im Feld **Steckplatznamen** den Steckplatzname.
3. Um einen Serverhostnamen als Steckplatznamen zu verwenden, wählen Sie **Hostname verwenden für den Steckplatzname** aus. Dadurch werden die statischen Steckplatznamen mit dem Host-Namen des Servers (oder dem Systemnamen) überschrieben, falls verfügbar. Dazu muss der OMSA-Agent auf dem Server installiert sein. Weitere Informationen zu dem OMSA-Agent finden Sie im *Dell OpenManage Server Administrator User's Guide* (Dell OpenManage Server Administrator-Benutzerhandbuch) unter dell.com/support/manuals.
4. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

Um den Standardsteckplatznamen (STECKPLATZ-01 bis STECKPLATZ-4) 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 *iDRAC7 User's Guide* (iDRAC7-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 Fensterbereich auf **Gehäuseübersicht** → **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 8. QuickDeploy-Einstellungen

Einstellung	Beschreibung
QuickDeploy aktiviert	Wählen Sie die Option zur Aktivierung der Funktion **QuickDeploy** (Schnelle Bereitstellung), welche die iDRAC-Einstellungen, die auf dieser Seite konfiguriert sind, automatisch auf neu eingefügte Server anwendet; die automatische Konfiguration muss lokal auf dem LCD-Bedienfeld bestätigt werden.
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-

Einstellung	Beschreibung
	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.
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, 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.

Einstellung	Beschreibung
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.

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.

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 Eigenschaften der Standardwerte finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC), verfügbar unter dell.com/support/manuals.

Konfigurieren der iDRAC-VLAN-Einstellungen

VLANs werden verwendet, um zu ermöglichen, dass mehrere virtuelle LANs auf dem gleichen physischen Netzwerkkabel existieren, und um den Netzwerkverkehr für Sicherheits- und Lastverteilungszwecke abzusondern. Wenn die VLAN-Funktionalität aktiviert wird, wird jedem Netzwerkpaket ein VLAN-Tag zugewiesen. VLAN-Tags sind Gehäuseeigenschaften. Sie bleiben mit dem Gehäuse verbunden, selbst wenn eine Komponente entfernt wird.

iDRAC-VLAN-Tag-Einstellungen über RACADM einstellen

- Geben Sie die VLAN-Kennung und Priorität eines bestimmten Servers mit dem folgenden Befehl ein:
  `racadm setniccfg -m server-<n> -v <VLAN-ID> <VLAN-Priorität>`

  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 – 16.

  Beispiel:

  ```
  racadm setniccfg -m server- 1 -v
  ```

iDRAC-VLAN-Tag-Einstellungen mittels der Webschnittstelle konfigurieren

So konfigurieren Sie VLAN für 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 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 9. Startlaufwerke

Startlaufwerk	Beschreibung
PXE	Start von einem PXE (Preboot Execution Environment)-Protokoll über die Netzwerkschnittstellenkarte.
Festplattenlaufwerk	Start von der Festplatte auf dem Server.

Startlaufwerk	Beschreibung
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.
iSCSI	Start von einem iSCSI-Gerät (Internetschnittstelle für kleine Computer).
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-Anmelde**berechtigungen 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 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 das Laufwerk angeschlossen ist, kann auf die Remote-Datei zugegriffen werden, wie wenn sie sich auf dem lokalen System befinden würde. Es werden zwei Arten von Datenträgern 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 zu verwenden, müssen Sie eine Enterprise-Lizenz aufweisen.

So konfigurieren Sie die Remote-Dateifreigabe:

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

BIOS-Einstellungen mithilfe der Funktion zum Klonen von Servern konfigurieren

Mit der Funktion zum Erstellen von Server-Klonen können Sie alle BIOS-Einstellungen von einem bestimmten Server auf einen oder mehrere Server anwenden. Klonbare BIOS-Einstellungen sind nur solche BIOS-Einstellungen, die geändert

werden können und dazu dienen, auf verschiedenen Servern repliziert zu werden. Um diese Funktion zu verwenden, müssen Sie eine Enterprise-Lizenz aufweisen.

Die Funktion zum Klonen von Servern unterstützt iDRAC7-Server. 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 Klonen von Servern:

- iDRAC muss in der erforderlichen Mindestversion vorliegen. iDRAC7-Server müssen mindestens in Version 1.40.40 vorliegen.
- Auf dem Server muss die unterstützte iDRAC-Generation vorliegen.
- Der Server muss eingeschaltet sein.

Die Quell- und Zielserver müssen nicht zur gleichen Generation gehören. Es werden nur verfügbare klonbare Einstellungen von einem Server-Profil auf andere Server angewendet.

Sie können Folgendes durchführen:

- Kopieren der BIOS-Einstellungen von einem Server auf einen anderen.
- Speichern eines Profils eines Servers.
- Anwenden eines Profils auf andere Server.
- Anzeigen der BIOS-Einstellungen eines Servers oder eines gespeicherten Profils.
- Anzeigen der Protokollaktivität für letzte BIOS-Profil-Tasks.

Zugreifen auf die Seite Bios-Profil

Sie können BIOS-Profile einem oder mehreren Servern mithilfe der Seite **BIOS-Profil** hinzufügen, sie verwalten und sie anwenden.

Um auf die Seite **BIOS-Profil** über die CMC-Webschnittstelle zuzugreifen, klicken Sie im linken Fensterbereich auf **Geräuse-Übersicht** → **Server-Übersicht** → **Setup** → **Profile**. Die Seite **BIOS-Profile** wird angezeigt.

Profil hinzufügen

Vor dem Root-Klonen der BIOS-Eigenschaften auf einen Server müssen Sie zunächst die Eigenschaften in ein gespeichertes Profil erfassen.

Wenn Sie ein gespeichertes Profil erstellen, müssen Sie einen Namen und eine optionale Beschreibung für jedes Profil bereitstellen. Sie können maximal 16 gespeicherte Profile auf einem nichtflüchtigen, erweiterten CMC-Speichermedium speichern.

Das Entfernen oder Deaktivieren eines nichtflüchtigen, erweiterten Speichermediums verhindert den Zugriff auf gespeicherte Profile und deaktiviert die Funktion „Erstellen von Server-Klonen“.

So fügen Sie ein Profil hinzu:

1. Auf der Seite **BIOS-Profil** klicken Sie auf **Profil hinzufügen**.
2. Geben Sie auf der Seite **BIOS-Profil hinzufügen** den Profilnamen und eine Beschreibung (optional) ein, wählen Sie den Server, von dem das Profil erfasst werden soll, aus und klicken Sie abschließend auf **Speichern**. Der CMC kommuniziert mit dem Lifecycle-Controller, um die verfügbaren BIOS-Einstellungen zu erhalten und sie als bezeichnetes Profil zu speichern.

Verwalten von gespeicherten Profilen

Sie können BIOS-Profile bearbeiten, anzeigen oder löschen. Gehen Sie so vor, um die gespeicherten Profile auf einem CMC zu verwalten:

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht → Serverübersicht → Setup → Profile**.
2. Klicken Sie auf der Seite **BIOS-Profile** im Abschnitt **Profil anwenden** auf **Profile verwalten**. Die Seite **BIOS-Profile verwalten** wird angezeigt.

- Um ein Profil zu bearbeiten, klicken Sie auf **Bearbeiten**.
- Um BIOS-Einstellungen anzuzeigen, klicken Sie auf **Anzeigen**.
- Klicken Sie auf **Löschen**, um ein Profil zu löschen. Weitere Informationen über Feldbeschreibungen finden Sie in der *Online-Hilfe*.

Profil anwenden

Wenn gespeicherte Profile auf dem nichtflüchtigen CMC-Medium verfügbar sind, um das Klonen eines Servers zu initiieren, können Sie ein Speicherprofil auf einem oder mehreren Servern anwenden.

Der Vorgangsstatus, die Einschubnummer, der Einschubname und der Modellname werden für jeden Server in der Tabelle **Profil anwenden** angezeigt.

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 einem oder mehreren Servern an:

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht → Serverübersicht → Setup → Profile**.
2. Wählen Sie auf der Seite **BIOS-Profile** im Abschnitt **Profil anwenden** im Dropdown-Menü **Ein Profil auswählen** das Profil aus, das Sie anwenden möchten.
3. Wählen Sie im Abschnitt **Ziel-Server auswählen** die Server aus, für die Sie ein Profil anwenden möchten. Weitere Informationen über die Feldbeschreibungen auf dieser Seite finden Sie in der *Online-Hilfe*.
4. Klicken Sie auf **Anwenden**. Das ausgewählte Profil wird auf den/die Server angewendet und der Server wird automatisch neu gestartet.

BIOS-Einstellungen anzeigen

Klicken Sie zum Anzeigen der BIOS-Einstellungen für einen ausgewählten Server auf der Seite **BIOS Profile** im Abschnitt **Profil anwenden** auf **Anzeigen** in der Spalte der BIOS-Einstellungen. Die Seite **Einstellungen anzeigen** wird angezeigt.

Es werden nur BIOS-Einstellungen auf dem Server angezeigt, die durch das Anwenden eines Profils (klonbare Einstellungen) geändert werden können. Die Einstellungen werden auf dieselbe Weise in Gruppen partitioniert, wie sie auf der Seite **iDRAC BIOS-Setup** angezeigt werden.

ANMERKUNG: Mit der CMC Server-Klonen-Anwendung werden die korrekten BIOS- und Starteinstellungen für einen bestimmten Server nur dann abgerufen und angezeigt, wenn die Option Control System Inventory on Restart (CSIOR) aktiviert ist.

So aktivieren Sie CSIOR auf:

- Server der 12. Generation – Drücken Sie nach dem Neustart des Servers auf **F2**, wählen Sie **iDRAC-Einstellungen → Lifecycle-Controller** aus, aktivieren Sie **CSIOR** und speichern Sie die Änderungen.

Profilprotokoll anzeigen

Um das Profilprotokoll auf der Seite **BIOS-Profile** anzuzeigen, siehe den Abschnitt **Neu erstelltes Profilprotokoll**, der die letzten 10 Profilprotokolleinträge direkt aus Server-Klonvorgängen aufführt. Jedes neu erstellte Profilprotokoll zeigt den Schweregrad sowie Uhrzeit und Datum der Bestätigung des Server-Klonvorgangs sowie die Beschreibung der Klonprotokollmeldung an. Die Protokolleinträge stehen auch im RAC-Protokoll zur Verfügung. Klicken Sie zum Anzeigen weiterer verfügbarer Einträge auf **Gehe zu Profilprotokoll**. Die Seite **Profilprotokoll** wird angezeigt.

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 **BIOS-Profile** die Job ID (JID) des übermittelten Jobs aus dem Abschnitt **Neu erstelltes Profilprotokoll**.
3. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** → **Fehlerbehebung** → **Lifecycle-Controller-Aufträge**. Suchen Sie die gleiche JID in der Tabelle **Aufträge.** Weitere Informationen über die Ausführung von Lifecycle-Controller-Aufträgen finden Sie in Lifecycle-Controller-Auftragsvorgänge.

iDRAC mit einfacher Anmeldung starten

Der CMC bietet eine eingeschränkte Verwaltung individueller Gehäusekomponenten, wie z. B. Server. Zur kompletten Verwaltung dieser individuellen Komponenten bietet der CMC einen Startpunkt für die webbasierte Schnittstelle des Verwaltungs-Controllers des Servers (iDRAC).

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 unten beschrieben.

- Ein CMC-Benutzer, der Serveradministratorberechtigungen hat, wird automatisch mit einfacher Anmeldung bei iDRAC angemeldet. Sobald er sich auf der iDRAC-Site befindet, erhält dieser Benutzer automatisch Administratorrechte. Dies gilt sogar dann, wenn derselbe Benutzer kein Konto auf iDRAC besitzt oder wenn das Konto keine Administratorrechte aufweist.
- Ein CMC-Benutzer, der **KEINE** Serveradministratorrechte aufweist, aber dasselbe Konto auf iDRAC besitzt, wird automatisch mit einfacher Anmeldung bei iDRAC angemeldet. Sobald er sich auf der iDRAC-Site befindet, erhält dieser Benutzer die Berechtigungen, die für das iDRAC-Konto erstellt wurden.
- Ein CMC-Benutzer, der keine Serveradministratorrechte hat oder nicht dasselbe Konto auf iDRAC besitzt, wird **NICHT** automatisch mit einfacher Anmeldung bei iDRAC angemeldet. Dieser Benutzer wird zur iDRAC-Anmeldungsseite umgeleitet, wenn auf **iDRAC-GUI starten** geklickt wird.

  ANMERKUNG: Die Bezeichnung „dasselbe Konto“ bedeutet in diesem Zusammenhang, dass der Benutzer denselben Anmeldenamen mit einem übereinstimmenden Kennwort für CMC und für iDRAC besitzt. Der Benutzer, der denselben Anmeldenamen ohne ein übereinstimmendes Kennwort hat, hat nicht dasselbe Konto.

  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 der Server vom Gehäuse entfernt wird, die iDRAC-IP-Adresse geändert wird oder die iDRAC-Netzwerkverbindung ein Problem aufweist, kann das Klicken auf „iDRAC-GUI starten“ zur Anzeige einer Fehlerseite führen.

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-GUI 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 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 Maßnahmen für bestimmte Ereignisse einstellen, die auf dem Gehäuse eintreten. Dieser Fall tritt ein, wenn der Status einer Systemkomponente den vordefinierten Zustand überschreitet. Wenn ein Ereignis mit dem entsprechenden Filter übereinstimmt und Sie diesen für die Erzeugung einer Warnungsmeldung (E-Mail-Warnung oder SNMP-Trap) konfiguriert haben, wird eine Warnung an ein oder mehrere konfigurierte Ziele, wie E-Mail-Adresse, IP-Adresse, oder an einen externen Server gesendet.

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 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.

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 über RACADM aktivieren oder deaktivieren

Um die Erstellung von Warnungen zu aktivieren oder zu deaktivieren, verwenden Sie das **cfgIpmiLanAlertEnable** RACADM-Objekt. 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).

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**
4. Klicken Sie auf **Anwenden**.

   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*.

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, Standard-IPv6-Adressnotation oder FQDN. Zum 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>
   ```

Einstellungen für E-Mail-Warnungen konfigurieren

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.

Sie müssen den SMTP-E-Mail-Server so konfigurieren, 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. Wie Sie dies auf sichere Art und Weise einrichten können, können Sie in der mit dem SMTP-Server mitgelieferten Dokumentation nachlesen.

ANMERKUNG: Wenn Ihr Mail-Server Microsoft Exchange Server 2007 ist, ist sicherzustellen, dass der iDRAC7-Domänenname so konfiguriert ist, dass der Mail-Server die E-Mail-Warnungen des iDRAC7 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 <Maskenwert>
   ```
   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. 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 an, um E-Mail-Warnungen zu erhalten:
   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertAddress <E-Mail-Adresse> -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 der Person an, die E-Mail-Warnungen empfangen soll:
   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertAddress <E-Mail-Name> -i
   <Index>
   ```
   wobei `<email 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 Berechtigungen (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.

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 die Berechtigung als **Server-Administrator** besitzt, werden die einem CMC-Benutzer gewährten Berechtigungen nicht automatisch auf denselben Benutzer auf einem Server übertragen, da Serverbenutzer unabhängig von CMC-Benutzern erstellt werden. Mit anderen Worten, CMC Active Directory-Benutzer und iDRAC Active Directory-Benutzer befinden sich 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 Benutzerkonfiguration-Administrator kann keinen Serverbenutzer aus einem CMC-Benutzer erstellen oder umgekehrt. Diese Regel schützt die Sicherheit und Integrität der Server.

Tabelle 10. 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. Es ist möglich, dass ein Benutzer andere Berechtigungen ohne CMC-Anmeldebenutzerberechtigung besitzt. Diese Funktion ist sinnvoll, wenn sich ein Benutzer vorübergehend nicht anmelden darf. Wenn die CMC-Anmeldeberechtigung 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.

Berechtigung	Beschreibung
	• 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, wie z. B. der Name des Steckplatzes und die Steckplatzpriorität. Obwohl sich diese Eigenschaften auf die Server beziehen, 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, ungeachtet, ob sich Server in den Steckplätzen befinden oder nicht. Wenn ein Server auf ein anderes Gehäuse verschoben wird, werden der Steckplatzname und die Priorität, die dem im neuen Gehäuse belegten Steckplatz zugewiesen werden, übertragen. Der vorherige Steckplatzname und die vorherige Priorität verbleiben beim vorherigen Gehäuse. **ANMERKUNG:** CMC-Benutzer mit einer Berechtigung als **Administrator für die Gehäusekonfiguration** können die Energieversorgungseinstellungen konfigurieren. Es sind jedoch Benutzer mit einer Berechtigung als **Administrator für die Gehäusesteuerung** erforderlich, um Energieversorgungsvorgänge auf dem Gehäuse auszuführen, darunter Strom einschalten und Strom ausschalten sowie Strom ein- und ausschalten.
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 einer Berechtigung als Administrator für die **Gehäusestromversorgung** können alle Vorgänge im Zusammenhang mit der Stromversorgung ausführen. Sie können Gehäusestromvorgänge steuern, einschließlich Strom einschalten, Strom ausschalten und Strom aus- und einschalten. **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 eine **Server Administrator**-Berechtigung eine Maßnahme zum Ausführen auf einem Server ausgibt, sendet die CMC-Firmware den Befehl zum Zielserver, ohne die Berechtigungen des Benutzers auf dem Server zu überprüfen. Mit anderen Worten: die **Server Administrator**-Berechtigung setzt alle fehlenden Administratorrechte auf dem Server außer Kraft.

Berechtigung	Beschreibung
	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 **Server Administrator**-Berechtigung verfügt, eine Maßnahme ausgibt, die auf einem Server ausgeführt werden soll, sendet der CMC mit dem Benutzernamen und dem Kennwort des Benutzers einen Befehl an den Zielserver. Wenn der Benutzer auf dem Server nicht vorhanden ist oder das Kennwort nicht übereinstimmt, wird dem Benutzer das Ausführen der Maßnahme verweigert. Wenn der Benutzer auf dem Zielserver vorhanden ist und das Kennwort übereinstimmt, reagiert der Server mit den Berechtigungen, die dem Benutzer auf dem Server gewährt wurden. Basierend auf den Berechtigungen, mit denen der Server reagiert, wird über die CMC-Firmware entschieden, ob dem Benutzer das Recht zum Ausführen der Maßnahme zusteht. Im Folgenden werden die Berechtigungen und Maßnahmen auf dem Server aufgeführt, auf die der Server Administrator Anspruch hat. Diese Rechte werden nur dann angewendet, wenn der Gehäusebenutzer nicht über die Server Administrator-Berechtigung auf dem Gehäuse verfügt. 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.

Berechtigung	Beschreibung
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 11. CMC-Gruppenberechtigungen

Benutzergruppe	Gewährte Berechtigungen
Administrator	• CMC-Anmeldung, Benutzer • Gehäusekonfiguration-Administrator • Benutzerkonfigurations-Administrator • Administrator zum Löschen von Protokollen • 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
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

Benutzergruppe	Gewährte Berechtigungen
Keine	Keine zugewiesenen Berechtigungen

Tabelle 12. 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.

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.

```
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
```

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 13. Standardeinstellungsberechtigungen der Rollengruppe

Rollengruppe	Standard-Berechtigungsebene	Gewährte Berechtigungen	Bitmaske
1	Keine	• CMC-Anmeldung, Benutzer • Gehäusekonfiguration-Administrator • Benutzerkonfigurations-Administrator	0x00000fff

Rollengruppe	Standard-Berechtigungsebene	Gewährte Berechtigungen	Bitmaske
		• Administrator zum Löschen von Protokollen • Gehäusesteuerungs-Administrator (Strombefehle) • Server Administrator • Warnungstests für Benutzer • Administrator für Debug-Befehle • Struktur A-Administrator	
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. Geben Sie folgendes an:
   - Aktivieren Sie Active Directory, geben Sie den Root-Domänennamen und den Zeitüberschreitungswert ein.
   - Wenn der gezielte Aufruf den Domänen-Controller und den globalen Katalog durchsuchen soll, wählen Sie **AD-Server für Suche durchsuchen (optional)** aus.
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 **Standardschemaeinstellungen** 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** ab 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-Befehszeileneingabe 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 <allgemeiner Name der Rollengruppe>
racadm config -g cfgStandardSchema -i <Index> -o
cfgSSADRoleGroupDomain <vollqualifizierter Domänenname> racadm config -
g cfgStandardSchema -i <Index> -o cfgSSADRoleGroupPrivilege
<Bitmaskenwert für bestimmte Rollengruppenberechtigungen>
```

```
racadm config -g cfgActiveDirectory -o cfgADDomainController1
<vollqualifizierter Domänenname oder IP-Adresse des Domänen-
Controllers> racadm config -g cfgActiveDirectory -o
cfgADDomainController2 <vollqualifizierter Domänenname oder IP-Adresse
des Domänen-Controllers> racadm config -g cfgActiveDirectory -o
cfgADDomainController3 <vollqualifizierter Domänenname oder IP-Adresse
des Domänen-Controllers>
```

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
<vollqualifizierter Domänenname oder IP-Adresse des Domänen-
Controllers> racadm config -g cfgActiveDirectory -o
cfgADGlobalCatalog2 <vollqualifizierter Domänenname oder IP-Adresse
des Domänen-Controllers> racadm config -g cfgActiveDirectory -o
cfgADGlobalCatalog3 <vollqualifizierter Domänenname oder IP-Adresse
des Domänen-Controllers>
```

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-Zertifikat>
```

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 14. 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

Klassenname	Zugewiesene Objekt-Identifikationsnummer (OID)
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Tabelle 15. 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 16. 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 17. 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 18. 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
SuperClasses	Benutzer
Attribute	dellRAC4Privileges

Tabelle 19. 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 20. 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	TRUE

Zugewiesener OID/Syntax-Objektkennzeichner	Einzelbewertung
Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
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
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

Zugewiesener OID/Syntax-Objektkennzeichner	Einzelbewertung
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)	
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 konfiguriert werden sollen, werden auf derselben Seite angezeigt.
3. Geben Sie folgendes an:
   - Aktivieren Sie Active Directory, geben Sie den Root-Domänennamen und den Zeitüberschreitungswert ein.
   - Wenn der gezielte Aufruf den Domänen-Controller und den globalen Katalog durchsuchen soll, wählen Sie **AD-Server für Suche durchsuchen (optional)** aus.

     ANMERKUNG: Das Einstellen der IP-Adresse auf 0.0.0.0 deaktiviert die Suche des CMC nach einem Server.

     ANMERKUNG: Sie können eine kommagetrennte Liste von Domänen-Controllern oder Servern des globalen Katalogs angeben. Der CMC ermöglicht es Ihnen, bis zu drei IP-Adressen oder Host-Namen festzulegen.

     ANMERKUNG: Domänen-Controller und Server des globalen Katalogs, die nicht korrekt für alle Domänen und Anwendungen konfiguriert sind, können zu unerwarteten Ergebnissen bei der Funktionsweise der vorhandenen Anwendungen/Domänen führen.
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 `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 **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 das Register **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 von DNS-Serveradressen verwenden** aus, um die DNS-Server-Adressen zu aktivieren, die automatisch vom DHCP-Server abgerufen werden sollen.

    – 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 „Erweitertes Schema“ werden 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 <allgemeiner RAC-Name> racadm config -g cfgActiveDirectory -o
cfgADRacDomain < vollständig qualifizierter Domänenname > racadm config -g
cfgActiveDirectory -o cfgADDomainController1 < vollständig qualifizierter
Domänenname oder IP-Adresse des Domänen-Controllers > racadm config -g
cfgActiveDirectory -o cfgADDomainController2 < vollständig qualifizierter
Domänenname oder IP-Adresse des Domänen-Controllers > racadm config -g
cfgActiveDirectory -o cfgADDomainController3 < vollständig qualifizierter
Domänenname oder IP-Adresse des Domänen-Controllers >
```

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-Zertifikat >
```

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-Zertifikat >
```

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. Optionale Bindung zum Verzeichnisdienst. Standard ist die anonyme Bindung.
2. Suche nach dem Benutzer auf Basis von dessen Benutzeranmeldung. Das Standardattribut ist `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 nicht binden kann, wird die Anmeldung nicht erfolgreich sein.
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.

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:

   ```
   C:\>ktpass -princ HTTP/cmcname.domain_name.com@REALM_NAME.COM - mapuser
   dracname -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 den DES-CBC-MD5-Typ 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 <Benutzer>@<Domäne>
   ```

   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.

Konfiguration 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 -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).

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 21. 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-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.

Befehl	Beschreibung
`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 gleichzeiting 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 Kennwort-Eingabeaufforderung eingeblendet wird.

Um dieses Problem zu beheben, laden Sie Hotfix 824810 von **support.microsoft.com** herunter. Weitere Informationen finden Sie im Microsoft Knowledge Base-Artikel 824810.

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: 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. Lesen Sie für weitere Informationen über die RACADM-Befehle das *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 22. 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 Typ Benutzer IP-Adresse Anmeldung Datum/Zeit SSH PC1 x.x.x.x
16.06.09 09:00:00 SSH PC2 x.x.x.x 16.06.09 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 Bits für den Schlüssel ein. Der Wert sollte im Bereich von 768 bis 4096 liegen.

   ANMERKUNG: CMC blendet möglicherweise keine Meldung ein, wenn Sie Schlüssel mit einem Wert kleiner als 768 oder größer als 4096 hinzufügen, doch wenn Sie versuchen, sich anzumelden, werden diese Schlüssel fehlschlagen.
3. Klicken Sie auf **Generieren** und bewegen Sie die Maus gemäß Anleitung im Fenster.

   Nachdem der Schlüssel erstellt wurde, können Sie das Schlüsselanmerkungsfeld ändern.

   Sie können auch einen Kennsatz 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 23. 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

Verbindung zu Servern oder E/A-Modulen mit dem connect-Befehl herstellen

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:

- CMC Befehlszeilenschnittstelle (CLI) oder der Befehl RACADM `connect`. Weitere Informationen über die Ausführung 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.

Bei einer seriellen, Telnet- oder SSH-Konsole unterstützt der CMC den Befehl `connect`, um eine serielle Verbindung zu einem Server oder E/A-Modul herzustellen. Die serielle Serverkonsole umfasst sowohl die BIOS-Boot- und Setup-Bildschirme als auch die serielle Betriebssystemkonsole. Für E/A-Module ist die serielle Switch-Konsole verfügbar. Es gibt ein einziges EAM auf dem Gehäuse.

VORSICHT: Bei Ausführung von der seriellen CMC-Konsole aus bleibt die Option `connect -b` verbunden, bis der CMC zurückgesetzt wird. Diese Verbindung stellt ein potenzielles Sicherheitsrisiko dar.

ANMERKUNG: Der Befehl `connect` stellt die Option `-b` (binär) bereit. Bei der Option `-b` werden reine Binärdaten übergegeben und `cfgSerialConsoleQuitKey` wird nicht verwendet. Zudem verursachen Übergänge beim DTR-Signal (z. B. wenn das serielle Kabel entfernt wird, um eine Verbindung eines Debuggers herzustellen) keine Beendung der Anwendung, wenn eine Verbindung zu einem Server über die serielle CMC-Konsole hergestellt wird.

ANMERKUNG: Wird die EAM-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 standardmäßige Konsolen-Escape-Sequenz ist <Strg><\>.

Um eine Verbindung zu einem EAM herzustellen, geben Sie Folgendes ein:

`connect switch-`*`n`*

wobei `n` eine EAM-Kennungszeichnung A1 ist.

Wenn Sie sich beim connect-Befehl auf die EAMs beziehen, werden den EAMs-Switches zugeordnet, wie in der folgenden Tabelle dargestellt.

Tabelle 24. 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 verwalteten seriellen Serverkonsole herzustellen, verwenden Sie den Befehl `connect server-`*`n`*, wobei *`n`* 1–4 ist. Sie können auch den Befehl `racadm connect server-n` verwenden. Wenn Sie mit der Option `-b` eine Verbindung zu einem Server herstellen, wird eine binäre Datenübertragung vorausgesetzt und das Escape-Zeichen wird deaktiviert. Wenn der iDRAC nicht verfügbar ist, sehen Sie die Fehlermeldung `No route to host`.

Der Befehl `connect server-n` ermöglicht dem Benutzer 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 anzeigen, die sowohl die serielle BIOS-Boot-Konsole als auch die serielle Betriebssystemkonsole umfasst.

ANMERKUNG: Um die BIOS-Boot-Bildschirme anzuzeigen, muss die serielle Umleitung im BIOS-Setup des Servers aktiviert werden. Zudem müssen Sie das Terminalemulationsfenster auf 80 x 25 einstellen. Ansonsten werden die Zeichen auf der Seite fehlerhaft dargestellt.

ANMERKUNG: Nicht alle Tasten auf den BIOS-Setup-Bildschirmen funktionieren; Sie sollten daher entsprechende Tastaturkürzel für <Strg> <Alt> <Löschen> und andere eingeben. Der anfängliche Umleitungsbildschirm zeigt die benötigten Tastaturkürzel an.

BIOS des verwalteten Servers für die serielle Konsolenumleitung konfigurieren

Sie können eine Remote-Konsolensitzung verwenden, um sich mit dem verwalteten System unter Verwendung der iDRAC7-Webschnittstelle zu verbinden. Weitere Informationen finden Sie im *iDRAC7 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:
   - **Aus**
   - **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. Speichern Sie die Änderungen und beenden Sie.

   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/sda1 # 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

FlexAddress- und FlexAdress Plus-Karten verwenden

Dieser Abschnitt enthält Informationen über FlexAddress- und FlexAddress Plus-Karten und das Konfigurieren und Verwenden dieser Karten.

ANMERKUNG: Die FlexAddress-Funktion ist lizenziert und Sie müssen zu ihrer Verwendung eine Enterprise-Lizenz aufweisen.

Über FlexAddress

Die FlexAddress-Funktion ist eine optionale Erweiterung, die es Servermodulen ermöglicht, die werkseitig zugewiesenen WWN- und MAC-Netzwerkkennungen (World Wide Name, Media Access Control) durch vom Gehäuse bereitgestellte WWN/MAC-Kennungen zu ersetzen.

Jedem Servermodul wird als Teil des Herstellungsprozesses eine eindeutige WWN- und/oder MAC-Kennung (WWN/MAC-ID) zugewiesen. Wenn Sie früher ein Servermodul durch ein anderes ersetzen mussten, hätten sich die WWN/MAC-IDs vor der Einführung von FlexAddress geändert und die Ethernet-Netzwerkverwaltungsinstrumente und SAN-Ressourcen (Storage Area Network) hätten neu konfiguriert werden müssen, um das neue Servermodul erkennen zu können.

FlexAddress ermöglicht es dem CMC, WWN/MAC-IDs einem bestimmten Steckplatz zuzuweisen und die werkseitigen IDs außer Kraft zu setzen. Wird das Servermodul ausgetauscht, bleiben die steckplatzbasierten WWN/MAC-IDs 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-IDs verwendet.

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> + 0xCF (208 – 1) = mac_end
```

wobei 208 *mac_count* ist und die Formel lautet:

```
<mac_start> + <mac_start> – 1 = <mac_end>
```

Beispiel:

```
(starting_mac)00188BFFDCFA + 0xCF = (ending_mac)00188BFFDDC9
```

.

ANMERKUNG: Sperren Sie die SD-Karte vor dem Einsetzen in den USB-Speicherkartenleser, um versehentliches Ändern des Inhalts zu verhindern. Die SD-Karte *muss entsperrt* werden, 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.

Aktivierung von FlexAddress

FlexAddress wird auf einer SD-Karte (Secure Digital) geliefert, die in den CMC eingesetzt werden muss, um die Funktion zu aktivieren. Um eine FlexAddress-Funktion zu aktivieren, sind u. U. Softwareaktualisierungen erforderlich; wenn Sie FlexAddress nicht aktivieren, sind diese Aktualisierungen nicht erforderlich. Die Aktualisierungen, die in der untenstehenden Tabelle aufgeführt sind, umfassen Servermodul-BIOS und CMC-Firmware. Diese Aktualisierungen müssen angewendet werden, bevor FlexAddress aktiviert wird. Wenn diese Aktualisierungen nicht angewendet werden, funktioniert FlexAddress nicht wie vorgesehen.

ANMERKUNG: FlexAddress kann auf den monolithischen Servern von Dell nicht aktiviert werden.

Tabelle 25. Voraussetzungen für Aktivierung von FlexAddress

Komponente	Erforderliche Mindestversion
Servermodul-BIOS	• M620 • M520 **ANMERKUNG:** Die BIOS-Version für M520 und M620 muss 1.7.6 oder höher sein.
PowerEdgeM600/M605 LAN auf der Hauptplatine (LOM)	• Bootcode-Firmware 4.4.1 oder höher • iSCSI-Bootfirmware 2.7.11 oder höher
iDRAC7	Version 1.40.40 und höher
LC–USC	Version 1.1.5 und höher
CMC	Version 1.10 oder höher

Um die korrekte Bereitstellung der FlexAddress-Funktion sicherzustellen, aktualisieren Sie das BIOS und die Firmware in der folgenden Reihenfolge:

1. Aktualisieren Sie das Servermodul-BIOS.
2. Aktualisieren Sie die iDRAC-Firmware auf dem Servermodul.
3. Aktualisieren Sie die gesamte CMC-Firmware im Gehäuse; falls redundante CMCs vorhanden sind, stellen Sie sicher, dass beide aktualisiert sind.
4. Legen Sie die SD-Karte in das passive Modul ein für ein redundantes CMC-Modulsystem oder in das einzige CMC-Modul für ein nicht-redundantes System.

ANMERKUNG: Wenn keine CMC-Firmware installiert ist, die FlexAddress (Version 1.10 oder höher) unterstützt, wird die Funktion nicht aktiviert.

Installationsanleitungen für SD-Karten finden Sie im Dokument *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification* (Chassis Management Controller (CMC) technische Spezifikationen der gesicherten digitalen (SD)-Karte).

ANMERKUNG: Die SD-Karte enthält eine FlexAddress-Funktion. 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 führen könnte.

ANMERKUNG: Die SD-Karte kann nur für ein einzelnes Gehäuse verwendet werden. Bei mehreren Gehäusen müssen Sie weitere SD-Karten erwerben.

Die Aktivierung der FlexAddress-Funktion findet automatisch bei Neustart des CMC mit der installierten SD-Funktionskarte statt. Diese Aktivierung bindet diese Funktion an das Gehäuse. Wenn Sie eine SD-Karte auf einem redundanten CMC installiert haben, wird die Aktivierung der FlexAddress-Funktion erst stattfinden, nachdem Sie den redundanten CMC zum aktiven gemacht haben. Beachten Sie auch das Dokument *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification* (Chassis Management Controller (CMC) technische Spezifikationen der gesicherten digitalen (SD)-Karte) für Informationen zur Aktivierung eines redundanten CMC.

Wenn der CMC neu startet, bestätigen Sie den Aktivierungsprozess. Weitere Informationen zur Aktivierung von FlexAddress finden Sie under Bestätigung von FlexAddress Aktivierung.

Aktivieren von FlexAddress Plus

FlexAddress Plus wird auf der FlexAddress Plus-SD-Karte (Secure Digital) zusammen mit der FlexAddress-Funktion geliefert.

ANMERKUNG: Die SD-Karte mit der Bezeichnung FlexAddress enthält nur die FlexAddressen, und die Karte mit der Bezeichnung FlexAddress Plus enthält FlexAddress und FlexAddress Plus. Die Karte muss in den CMC eingelegt werden, um die Funktion zu aktivieren.

Einige Server benötigen möglicherweise, je nach Konfiguration, mehr MAC-Adressen als FA für den CMC bereitstellen kann. Für diese Server ermöglicht die Erweiterung auf FlexAddress Plus die vollständige Optimierung der WWN/MACs-Konfiguration. Wenden Sie sich bitte an Dell, um Unterstützung für die FlexAddress Plus-Funktion zu erhalten.

Zur Aktivierung der FlexAddress Plus-Funktion sind die folgenden Softwareaktualisierungen erforderlich: Server-BIOS, Server-iDRAC und CMC-Firmware. Wenn diese Aktualisierungen nicht angewendet werden, steht nur die FlexAddress-Funktion zur Verfügung. Weitere Informationen zu den erforderlichen Mindestversionen dieser Komponenten finden Sie in *Dell Chassis Management Controller (CMC) for Dell PowerEdge VRTX Version 1.00 Release Notes* (Versionshinweise zum Dell Chassis Management Controller (CMC) für Dell PowerEdge VRTX Version 1.00) unter **dell.com/support/manuals**.

Bestätigung FlexAddress-Aktivierung

Eine Funktionskarte enthält eine oder mehrere der folgenden Funktionen: FlexAddress, FlexAddress Plus, und/oder erweiterte Speicher. Führen Sie den folgenden RACADM-Befehl aus, um die SD-Funktionskarte und ihren Status zu bestätigen:

```
racadm featurecard -s
```

Tabelle 26. Statusmeldungen, zurückgegeben vom Befehl featurecard -s

Statusmeldung	Maßnahmen
`Keine Funktionskarte eingesetzt.`	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.
`Die eingesetzte Funktionskarte ist gültig und enthält die folgenden Funktion(en) FlexAddress: gebunden.`	Keine Maßnahme erforderlich.
`Die Funktionskarte ist gültig und enthält die folgenden Funktion(en) FlexAddress: an ein anderes Gehäuse gebunden, svctag = ABC1234, SD-Karte SN = 01122334455.`	Entfernen Sie die SD-Karte; bestimmen und installieren Sie die SD-Karte für das aktuelle Gehäuse.
`Die Funktionskarte ist gültig und enthält die folgenden Funktion(en) FlexAddress: nicht gebunden.`	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:

```
Funktion = FlexAddress Aktivierungsdatum = 8. April 2008 - 10:39:40 Funktion
installiert von SD-Karte SN = 01122334455
```

Wenn es keine aktiven Funktionen auf dem Gehäuse gibt, gibt der Befehl eine Meldung zurück:

```
racadm feature -s Keine Funktionen auf dem Gehäuse aktiviert
```

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:

```
FEHLER: Eine oder mehrere Funktionen auf der SD-Karte sind auf einem anderen
Gehäuse aktiv
```

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).

Deaktivierung von FlexAddress

Die Funktion FlexAddress kann deaktiviert werden und die SD-Karte kann mittels eines RACADM-Befehls auf einen Vorinstallationszustand zurückgesetzt werden. Es gibt keine Deaktivierungsfunktion in der Webschnittstelle. Die Deaktivierung versetzt die SD-Karte in ihren Originalzustand zurück, in dem sie für ein anderes Gehäuse installiert und aktiviert werden kann. Der Begriff FlexAddress bedeutet in diesem Kontext sowohl FlexAddress als auch FlexAddressPlus.

ANMERKUNG: Die SD-Karte muss physisch im CMC installiert sein und das Gehäuse muss ausgeschaltet sein, bevor Sie den Deaktivierungsbefehl ausführen.

Wenn Sie den Deaktivierungsbefehl ausführen, ohne eine SD Karte zu installieren oder mit einer Karte aus einem anderen Gehäuse installiert, wird die Funktion deaktiviert und es werden keine Änderungen auf der Karte vorgenommen.

Deaktivierung der FlexAddress-Funktion und Wiederherstellung der SD-Karte:

```
racadm feature -d -c flexaddress
```

Der Befehl gibt die folgende Statusmeldung bei erfolgreicher Ausführung zurück:

```
Die Funktion FlexAddress wurde erfolgreich für das Gehäuse deaktiviert.
```

Wurde das Gehäuse vor der Ausführung nicht ausgeschaltet, schlägt der Befehl mit der folgenden Fehlermeldung fehl:

```
FEHLER: Die Funktion kann nicht deaktiviert werden, da das Gehäuse
eingeschaltet ist
```

Lesen Sie für weitere Informationen zu diesem Befehl den Abschnitt zum **feature**-Befehl im *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX).

Anzeige von FlexAddress-Informationen

Sie können die Statusinformationen für das gesamte Gehäuse oder für einen einzelnen Server anzeigen lassen. Die angezeigten Informationen beinhalten:

- Strukturkonfiguration.
- FlexAddress ist aktiv oder nicht aktiv.
- Steckplatznummer und -name.
- Gehäusezugewiesene und serverzugewiesene Adressen.
- Verwendete Adressen.

Anzeigen der FlexAddress-Gehäuseinformationen

Die FlexAddress-Statusinformationen können für das gesamte Gehäuse angezeigt werden. Die Statusinformationen beinhalten, ob die Funktion aktiv ist, und einen Überblick über den FlexAddress-Status für jeden Server.

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 Eintrag **Aktiv** bedeutet, dass die Funktion für das Gehäuse installiert wurde und **Nicht aktiv** bedeutet, dass die Funktion nicht für das Gehäuse installiert wurde und nicht verfügbar ist.

Führen Sie den folgenden RACADM-Befehl aus, um den FlexAddress-Status für das gesamte Gehäuse anzuzeigen:

```
racadm getflexaddr
```

Um den FlexAddress-Status für einen bestimmten Steckplatz anzuzeigen:

```
racadm getflexaddr [-i <Steckplatz-Nr.>]
```

wobei *<Steckplatz-Nr>* ein Wert von 1– 4 ist.

Weitere Informationen über den **getflexaddr**-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).

Anzeigen von FlexAddress-Informationen für alle Server

Um FlexAddress-Status für alle Server mit der CMC-Webschnittstelle anzuzeigen, klicken Sie auf **Server-Übersicht** → **Eigenschaften** → **WWN/MAC**.

Die Seite **WWN/MAC-Systemzusammenfassung** enthält Informationen über Folgendes:

- WWN-Konfiguration
- MAC-Adressen für alle Steckplätze im Gehäuse

Strukturkonfiguration	Struktur A zeigt den Typ der installierten Eingabe/Ausgabe-Struktur an. iDRAC zeigt die Server Management-MAC-Adresse an. **ANMERKUNG:** Wenn Struktur A aktiviert ist, werden die nicht bestückten Steckplätze gehäusezugewiesene MAC-Adressen für Struktur A anzeigen.
WWN/MAC-Adressen	Zeigt die FlexAddress-Konfiguration für jeden Steckplatz im Gehäuse an. Die angezeigten Informationen beinhalten: • Steckplatznummer und -position. • FlexAddress ist aktiv oder nicht aktiv. • Strukturtyp. • Serverzugewiesene und gehäusezugewiesene verwendete WWN/MAC-Adressen. Ein grünes Häkchen zeigt den aktiven Adresstyp, entweder serverzugewiesen oder gehäusezugewiesen. **ANMERKUNG:** Der iDRAC-Management-Controller ist keine Struktur, doch wird seine FlexAddress als Struktur betrachtet.

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

Anzeige der FlexAddress Informationen für einzelne Server

So werden FlexAddress-Informationen für einen bestimmten Server unter Verwendung der CMC-Webschnittstelle angezeigt:

1. Erweitern Sie im linken Fensterbereich **Server-Übersicht**.
   Alle Server, die sich im Gehäuse befinden sind aufgelistet.
2. Klicken Sie auf den Server, den Sie anzeigen möchten.
   Die Seite **Serverstatus** wird angezeigt.
3. Klicken Sie auf das Register **Setup** und dann auf **FlexAddress**.
   Die Seite **FlexAddress**, die WWN-Konfiguration und die MAC-Adressen für ausgewählten Server bietet, wird angezeigt. Weitere Informationen finden Sie in der *Online-Hilfe.*

FlexAddress konfigurieren

FlexAddress ist eine optionale Erweiterung, die es ermöglicht, die werkseitig zugewiesenen WWN/MAC-IDs der Servermodule mit einer WWN/MAC-ID 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 zur Standardwerkseinstellung „Deaktiviert" zurücksetzen. Die RACADM-Syntax ist:

```
racadm racresetcfg -c flex
```

Weitere Informationen über RACADM-Befehle, die sich auf die FlexAddress beziehen, und Daten über andere Werkseinstellungseigenschaften finden Sie unter *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge VRTX) erhältlich unter **dell.com/support/manuals**.

Sie müssen die FlexAddress-Erweiterung kaufen und installieren, um die FlexAddress zu Konfigurieren. Wenn die Erweiterung nicht gekauft und installiert wurde, wird der folgende Text in der Webschnittstelle angezeigt:

```
Optionale Funktion nicht installiert. Nutzen Sie das Dell Benutzerhandbuch zur
Gehäuseverwaltung für Informationen bezüglich der Administratorfunktion der
gehäusebasierten WWN und MAC-Adresse. Um diese Funktion zu erstehen,
kontaktieren Sie Dell bitte unter www.dell.com.
```

Wenn Sie FlexAddress mit dem Gehäuse bestellt haben, ist es beim Einschalten des Systems installiert und aktiviert. Wenn Sie FlexAddress zu einem späteren Zeitpunkt erwerben, müssen Sie die SD-Funktionskarte gemäß den Anweisungen im Dokument *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification* (Chassis Management Controller (CMC) technische Spezifikationen der gesicherten digitalen (SD)-Karte) unter **dell.com/support/manuals** installieren.

Der Server muss ausgeschaltet sein, bevor Sie mit der Konfiguration beginnen. Sie können FlexAddress auf Basis der jeweiligen Struktur aktivieren oder deaktivieren. Zusätzlich können Sie die Funktion steckplatzbasiert aktivieren oder deaktivieren. Nachdem Sie die Funktion auf Strukturbasis aktiviert haben, können Sie die zu aktivierenden Steckplätze auswählen. Ist zum Beispiel Struktur-A aktiviert, werden alle aktivierten Steckplätze FlexAddress nur für die Struktur-A aktiviert haben. In allen anderen Strukturen werden die werkseitigen WWN/MAC-IDs des Servers verwendet.

Wake-On-LAN mit FlexAddress

Wenn die FlexAddress-Funktion zum ersten Mal auf einem Servermodul bereitgestellt wird, erfordert dies ein Herunterfahren und erneutes Hochfahren, 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, was erfordert, dass das Servermodul eingeschaltet ist. Ist das Herunter-/Hochfahren abgeschlossen, sind die gehäusezugewiesenen MAC-IDs für die Wake-On-LAN (WOL)-Funktion verfügbar.

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.

ANMERKUNG: Wenn keine Struktur ausgewählt wurde, wird die folgende Meldung angezeigt.

```
FlexAddress ist für die ausgewählten Steckplätze nicht aktiviert.
```

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: Wirk kein Steckplatz ausgewählt, wird FlexAddress für die ausgewählten Strukturen nicht aktiviert.

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 <Strukturname> <Status>]
```

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 <Steckplatz-Nr.> <Status>
```

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, kommt sie vorinstalliert und aktiviert für alle Steckplätze und Strukturen. 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, und Daten über andere Werkseinstellungseigenschaften finden Sie unter *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Gehäuseverwaltungs-Controller für PowerEdge VRTX RACADM Befehlszeilenreferenzhandbuch) erhältlich unter **dell.com/support/manuals**.

Anzeigen von World Wide Name/Media Access Control (WWN/MAC)-IDs

Die Seite **WWN/MAC-Zusammenfassung** ermöglicht Ihnen, die WWN-Konfiguration und die MAC-Adresse eines Steckplatzes im Gehäuse einzusehen.

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.

Befehlsmeldungen

In der folgenden Tabelle werden RACADM-Befehle und -Ausgaben für häufig auftretende FlexAddress-Situationen aufgelistet.

Tabelle 27. FlexAddress-Befehle und -Ausgaben

Situation	Befehl	Output (Ausgabe)
SD-Karte im aktiven CMC-Modul ist an eine andere Service-Tag-Nummer gebunden.	`$racadm featurecard -s`	`Die eingesetzte Funktionskarte ist ungültig und enthält die folgenden Funktionen` `FlexAddress: Die Funktionskarte ist an ein anderes Gehäuse gebunden, svctag = <Service-Tag-Nummer> SD-Karte SN =<Gültige Seriennummer für die Flex-Adresse>`
SD-Karte im aktiven CMC-Modul ist an die gleiche Service-Tag-Nummer gebunden.	`$racadm featurecard -s`	`Die eingesetzte Funktionskarte ist ungültig und enthält die folgenden Funktionen` `FlexAddress: gebunden`
Die SD-Karte im aktiven CMC-Modul ist an keine Service-Tag-Nummer gebunden.	`$racadm featurecard -s`	`Die eingesetzte Funktionskarte ist ungültig und enthält die folgenden Funktionen` `FlexAddress:nicht gebunden`
Die Funktion FlexAddress ist auf dem Gehäuse aus irgendeinem Grunde (keine SD-Karte eingesetzt / beschädigte SD-Karte / Funktion deaktiviert / SD-Karte an anderes Gehäuse gebunden) nicht aktiv.	`$racadm setflexaddr [-f <Strukturname> <Steckplatzstatus>]` `$racadm setflexaddr [-i <Steckplatz-Nr> <Steckplatzstatus>]`	`FEHLER: Die Funktion FlexAddress ist nicht auf dem Gehäuse aktiviert`
Gastbenutzer versucht FlexAddress für Steckplätze/Strukturen festzulegen	`$racadm setflexaddr [-f <Strukturname> <Steckplatzstatus>]` `$racadm setflexaddr [-i <Steckplatz-Nr> <Steckplatzstatus>]`	`FEHLER: Unzureichende Benutzerrechte, zur Ausführung der Operation`
Die Funktion FlexAddress bei eingeschaltetem Gehäuse deaktivieren.	`racadm feature -d -c flexaddress`	`FEHLER: Die Funktion kann nicht deaktiviert werden, da das Gehäuse eingeschaltet ist`
Gastbenutzer versucht die Funktion auf dem Gehäuse zu deaktivieren.	`racadm feature -d -c flexaddress`	`FEHLER: Unzureichende Benutzerrechte, zur Ausführung der Operation`
Ändern der FlexAddress-Einstellungen für einen Steckplatz/ eine Struktur, während die Servermodule eingeschaltet sind.	`$racadm setflexaddr -i 1 1`	`FEHLER: Die Einstell-Operation kann nicht vorgenommen werden, da sie einen eingeschalteten Server betrifft`

Situation	Befehl	Output (Ausgabe)
Flexaddress-Einstellungen auf Steckplatz oder Struktur ändern, wenn die CMC Enterprise-Lizenz nicht installiert ist.	`$racadm setflexaddr -i<Steckplatz-Nr> <Status>` `$racadm setflexaddr [-f <Strukturname> <Steckplatzstatus>]`	`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.

Ungültige Konfigurationen

Es gibt drei Typen ungültiger Konfigurationen:

- Eine ungültige MC- oder LOM-Konfiguration liegt vor, wenn sich eine neu installierte Serverstruktur von der vorhandenen EAM-Struktur unterscheidet, d. h. dass das LOM oder die MC eines einzelnen Servers vom entsprechenden EAM nicht unterstützt wird. In diesem Fall werden alle anderen Server im Gehäuse ausgeführt, aber der Server mit der nicht übereinstimmenden MC-Karte kann nicht eingeschaltet werden. Der Netzschalter am Server blinkt gelb und warnt über eine Nichtübereinstimmung der Struktur.
- Eine ungültige EAM-MC-Konfiguration liegt vor, wenn ein neu installierter Strukturtyp des E/A-Moduls und die vorhandenen MC-Strukturen nicht übereinstimmen oder nicht kompatibel sind. Das nicht übereinstimmende EAM wird im ausgeschalteten Zustand belassen. Der CMC fügt den CMC- und Hardwareprotokollen einen Eintrag mit der ungültigen Konfiguration hinzu und gibt den EAM-Namen an. Der CMC lässt die Fehler-LED des fehlerhaften EAMs blinken. Wenn der CMC zum Versenden von Warnungen konfiguriert ist, wird für dieses Ereignis eine E-Mail- und/oder SNMP-Warnung gesendet.
- Eine ungültige EAM-EAM-Konfiguration liegt vor, wenn ein neu installiertes EAM einen anderen oder inkompatiblen Strukturtyp aufweist als ein EAM, das bereits in der Gruppe installiert ist. Der CMC sorgt dafür, dass das neu installierte EAM im ausgeschalteten Zustand bleibt, bewirkt, dass die Fehler-LED des EAMs blinkt und erstellt in den CMC- und Hardwareprotokollen Einträge zur festgestellten Nichtübereinstimmung.

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** 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.

3. Klicken Sie auf **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>
```

14

Energieverwaltung und -überwachung

Das Dell PowerEdge VRTX-Gehäuse ist der energieeffizienteste modulare Server auf dem Markt. Er 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 internen Netzteileinheiten. Das System kann bis zu 5000 Watt Wechselstrom übertragen, der Servermodulen und der damit verbundenen Gehäuseinfrastruktur zugeteilt wird. Diese Kapazität variiert jedoch auf Basis der eingestellten Stromredundanzregel, die Sie auswählen.

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.

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:

- Wechselstromredundanz
- Netzteilredundanz

Wechselstrom-Redundanzregel

Die Wechselstrom-Redundanzregel 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 Wechselstromredundanz 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 Wechselstromredundanz toleriert auch den Ausfall einzelner Netzteileinheiten.

ANMERKUNG: Eine der Aufgaben der Wechselstromredundanz ist es, für nahtlosen Serverbetrieb zu sorgen, selbst bei Ausfall eines ganzen Stromnetzes, aber der meiste Strom ist für die Aufrechterhaltung der Wechselstromredundanz verfügbar, wenn die Kapazitäten der beiden Netze etwa gleich sind.

ANMERKUNG: Wechselstromredundanz besteht nur dann, wenn die Ladungsanforderungen nicht die Kapazität des schwächeren Stromnetzes übersteigen.

Wechselstromredundanzstufen

Eine Netzteileinheit in jedem Netz ist die Minimalkonfiguration, die für die Verwendung als Wechselstromredundanz 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 Wechselstromredundanz nicht aufrechterhalten kann, dann werden E-Mail- bzw. SNMP-Warnungen an die Administratoren gesendet, wenn das Ereignis „Redundanz verloren“ für Warnungen konfiguriert ist.

Wenn eine einzelne Netzteileinheit in dieser Konfiguration ausfällt, werden die verbleibenden Netzteileinheiten des ausgefallenen Netzes als „Online“ markiert. In diesem Zustand kann jede der verbleibenden Netzteileinheiten ausfallen, ohne dass der Betrieb des Systems unterbrochen wird. Wenn eine Netzteileinheit 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 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. Die Abbildung unten zeigt den Netzteilredundanz-Modus.

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 Wechselstromredundanz ist es so, dass wenn Netzteilredundanz ausgewählt ist, der CMC nicht verlangt, dass die Netzteileinheiten an bestimmten Netzteileinheit-Steckplatzpositionen vorhanden sein müssen.

ANMERKUNG: Dynamische Netzteilzuschaltung (DPSE) ermöglicht, dass Netzteileinheiten als Standby eingesetzt werden. Der Standby-Zustand zeigt einen physischen Zustand der Netzteile 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.

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 **Wechselstromredundanzmodus** mit dynamischer Zuschaltung von Netzteileinheiten (DPSE) sind mindestens zwei Netzteileinheiten aktiv, eine in jedem Stromnetz. Bei Wechselstromredundanz 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 sechs 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 **Wechselstromredundanz**.

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 **Wechselstromredundanz** 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.

Eine höherer Strombedarf in der **Wechselstromredundanz**-Konfiguration 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 28. Standard-Redundanzkonfiguration

Konfiguration der Netzteileinheiten	Standard-Redundanzregel	Standardeinstellung für die dynamische Zuschaltung von Netzteileinheiten
Zwei Netzteile	Gleichstromredundanz	Deaktiviert
Vier Netzteile	Gleichstromredundanz	Deaktiviert

Wechselstromredundanz

Im Wechselstromredundanzmodus 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 Wechselstromredundanz 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 Wechselstromredundanzmodus muss ein ausgeglichener Satz von Netzteileinheiten (mindestens eine Netzteileinheit pro Stromnetz) vorhanden sein. Wenn diese Bedingung nicht erfüllt wird, ist keine Wechselstromredundanz 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 *iDRAC7 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
```

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 bei Bestimmen des allgemeinen Stromzustands. Wenn die Stromredundanzregel festgelegt ist, zum Beispiel „Wechselstromredundanz“, und der Redundanzstatus zeigt an, dass das System mit Redundanz betrieben wird, ist der allgemeine Stromzustand typischerweise **OK**. Wenn jedoch die Bedingungen für Betrieb mit Wechselstromredundanz nicht erfüllt werden können, ist der Redundanzstatus **Keine** und der allgemeine Stromzustand **Kritisch**. Der Grund dafür ist, dass das System nicht in Übereinstimmung mit der konfigurierten Stromredundanzregel funktionieren kann.

ANMERKUNG: Der CMC führt keine Vorabprüfung dieser Bedingungen durch, wenn Sie die Redundanzregel auf oder von „Wechselstromredundanz“ 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 29. 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: • Für neuen Server benötigter Strom ist verfügbar • Für neuen Server benötigter Strom ist nicht verfügbar	Zugelassen 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 30. Auswirkung auf das Gehäuse bei Ausfall oder Entfernung einer Netzteileinheit

Konfiguration der Netzteileinheiten	Dynamische Zuschaltung von Netzteileinheiten	Firmware-Reaktion
Wechselstromredundanz	Deaktiviert	Der CMC alarmiert Sie über den Verlust der Wechselstromredundanz.
Netzteil-Redundanz	Deaktiviert	Der CMC alarmiert Sie über den Verlust der Netzteilredundanz.
Wechselstromredundanz	Aktiviert	Der CMC alarmiert Sie über den Verlust der Wechselstromredundanz. Netzteile im Standby-Modus (wenn vorhanden) werden eingeschaltet, um den Stromverlust in Folge eines Netzteileinheitfehlers oder -ausfalls zu kompensieren.
Netzteil-Redundanz	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 31. SEL-Ereignisse für Netzteiländerungen

Netzteilereignis	Systemereignisprotokoll (SEL)-Eintrag
Einfügen	Netzteil ist vorhanden.
Entfernung	Netzteil ist nicht vorhanden.
Wechselstromeingang	Verlust der Stromzufuhr vom Netzteil.
Wechselstrom-Eingangsverlust	Die Stromzufuhr vom Netzteil wurde wiederhergestellt.
Gleichstromausgabe hergestellt	Netzteil funktioniert normal.
Gleichstromausgabeverlust	Netzteil fehlerhaft.

Ereignisse, die mit Änderungen der Stromredundanzregeln zusammenhängen, die Einträge im SEL verursachen, sind Redundanzverlust und Redundanzwiederherstellung für das modulare Gehäuse, das entweder für eine **Wechselstromredundanz**regel oder eine **Netzteilredundanz**regel konfiguriert ist. Die folgende Tabelle listet die SEL-Einträge auf, die mit Änderungen der Stromredundanzregeln zusammenhängen.

Stromregelereignis	Systemereignisprotokoll (SEL)-Eintrag
Redundanzverlust	Verlust der Netzteilredundanz.
Redundanz wiederhergestellt	Die Netzteile sind redundant.

Strombudget und Redundanz konfigurieren

Sie können das Energiebudget, die Redundanz und die dynamische Energie des gesamten Gehäuses (Gehäuse, Server, E/A- Module, KVM, CMC und Netzteile) konfigurieren, für welches vier Netzteile zur Verfügung stehen. Der Energieverwaltungsdienst optimiert die Leistungsaufnahme und weist den verschiedenen Modulen, basierend auf dem gegenwärtigen Bedarf, Energie zu.

Sie können Folgendes konfigurieren:

- Systemeingangsstrom-Obergrenze
- Redundanzregel
- Dynamische Netzteil-Einsatzfähigkeit aktivieren
- Netzschalter des Gehäuses deaktivieren
- Max. Stromkonservierungsmodus
- Remote-Stromprotokollierung
- Remote-Stromverbrauchsprotokollierungszeitraum
- Serverbasierte Stromverwaltung

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 5000 W begrenzt.

Maximaler Stromsparmodus

Dies ist nur aktiv, wenn Wechselstromredundanz ausgewählt ist. 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.

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 Server der 12. Generation
- Server-Priorität für Server der 12. Generation
- Eingangsstromkapazität des Systems
- Maximaler Stromsparmodus

CMC setzt die Aufrechterhaltung oder Verwaltung der folgenden Aktivitäten fort:

- Redundanzregel
- Remote-Stromprotokollierung
- Serverleistung über Stromredundanz
- Dynamische Netzteil-Einsatzfähigkeit
- Stromversorgung für Server bis einschließlich zur 11. Generation

OPMC verwaltet daraufhin die Priorisierung und die Stromversorgung für Server-Knoten der 12. Generation 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 Server der zwölften Generation 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 <Wert>
     ```
     wobei *Wert*> 0 (Wechselstromredundanz) und 1 (Netzteilredundanz) ist. Die Standardeinstellung ist 0.

     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 <Wert>
     ```
     wobei <*Wert*> eine Zahl zwischen der aktuellen Gehäusebelastungslaufzeit und 5000 ist und die maximale Stromgrenze in Watt angibt. Die Standardeinstellung ist 5000.

     Der folgende Befehl setzt zum Beispiel das maximale Strombudget mit 5000 Watt fest:
     ```
     racadm config -g cfgChassisPower -o cfgChassisPowerCap 5000
     ```
   - Um die dynamische Zuschaltung von Netzteileinheiten zu aktivieren oder deaktivieren, geben Sie Folgendes ein:
     ```
     racadm config -g cfgChassisPower -o
     cfgChassisDynamicPSUEngagementEnable <Wert>
     ```
     wobei <*Wert*> 0 (deaktivieren) oder 1 (aktivieren) bedeutet.

     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.

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.
   - 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.
3. Klicken Sie unter jedem installieren Controller die Links **Virtuelle Festplatten anzeigen**, **<Gehäusename>** und **Physische Festplatten anzeigen**, um die entsprechenden Seiten zu öffnen.

Virtuelle Adapter den Slots zuweisen

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 zu einem Serversteckplatz sicher, dass:

  - der Serversteckplatz leer ist, oder dass der Server im Steckplatz ausgeschaltet ist.
  - Heben Sie die Zuweisung zwischen dem VA und einem Server auf.
- Virtuelle Festplatten werden erstellt und als **Virtueller Adapter 1**, **Virtueller Adapter 2**, **Virtueller Adapter 3** oder **Virtueller Adapter 4** zugewiesen. Weitere Informationen finden Sie unter Zugangsrichtlinien für virtuelle Adapter auf virtuelle Festplatten anwenden.

ANMERKUNG: Sie können nur einen virtuellen Adapter auf einmal einem Server zuordnen. Sie können ohne eine entsprechende Lizenz den VA einem Standardserver zuordnen oder eine VA–Server-Zuordnung aufheben. Die Standardzuordnung ist: VA1–Serversteckplatz 1, VA2–Serversteckplatz 2, VA3–Serversteckplatz 3 und VA4–Serversteckplatz 4.

Unter Verwendung der virtuellen Adapter-Funktion können Sie den installierten Speicher mit den vier Servern freigeben. So heben Sie die Zuordnung eines virtuellen Adapters auf einem Serversteckplatz auf:

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** → **Speicher** → **Setup** → **Virtualization**.
2. Wählen Sie auf der Seite **Speicher-Virtualization** vom Drop-Down-Menü **Maßnahme Zuordnung aufheben** aus und klicken Sie dann auf **Anwenden**.

   Die Zuordnung des VA zu dem ausgewählten Serversteckplatz wird aufgehoben.

   ANMERKUNG: Sie können virtuelle Festplatten durch die Auswahl von entweder dem Modus **Einzelzuweisung** oder **Mehrfache Zuweisung** virtuellen Adaptern zuweisen. Weitere Informationen über diese Modi finden Sie unter *Online Help*.

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 . 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 von Fremdkonfigurationen

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. Auf der Seite **Controller-Setup,** im Abschnitt **Fremdkonfiguration** für den entsprechenden Controller, klicken Sie auf:
   - **Fremdkonfiguration löschen**, um die bestehende Konfiguration der Festplatte zu löschen.

– **Import-/Wiederherstellung**, um die Festplatte mit der Fremdkonfiguration zu importieren.

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 . Sie können auch die folgenden Filter verwenden, um spezifische Eigenschaften physischer 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

Globalen Hotspare unter Verwendung der CMC Web-Schnittstelle zuweisen

Zuweisen und Aufheben der Zuordnung von globalen Hot-Spares:

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** → **Speicher** → **Physische Festplatten** → **Setup**.
   Die Seite **Setup von physischen Festplatten** wird angezeigt.
2. Wählen Sie im Abschnitt **Zuweisung von globalen Hotspares** aus dem Drop-Down-Menü **Hotspare-Maßnahme** **Nicht zugewiesen** oder **Globaler Hotspare** für jede der physischen Festplatten aus und klicken Sie dann auf **Anwenden**. Als Alternative wählen Sie aus dem Drop-Down-Menü **Hotspare-Maßnahme - Allen zuweisen** aus, wählen Sie **Nicht zugewiesen** oder **Globaler Hotspare** aus und klicken Sie dann auf **Anwenden**.

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).

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

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. Geben Sie auf der Seite **Virtuelle Festplatte erstellen**, im Abschnitt **Einstellungen** die entsprechenden Daten ein und wählen Sie aus dem Abschnitt **Physische Festplatten auswählen** die Anzahl der physischen Festplatten basierend auf dem vorher ausgewählen RAID-Stufen aus, und klicken Sie dann auf **Virtuelle Festplatte erstellen**.

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 das Löschen einer virtuellen Festplatte die Daten, die auf dieser virtuellen Festplatte verfügbar sind, permanent löscht.

   ```
   Das Löschen der virtuellen Festplatte entfernt die virtuelle Festplatte
   aus der Konfiguration des Controllers. Durch das Initialisieren einer
   virtuellen Festplatte werden alle Daten von der virtuellen Festplatte
   permanent gelöscht.
   ```

   ANMERKUNG: Wenn Sie „Löschen“ auswählen, wird die folgende Meldung angezeigt, die angibt, dass das Löschen einer virtuellen Festplatte die Daten, die auf dieser virtuellen Festplatte verfügbar sind, permanent löscht.

   ```
   Das Löschen der virtuellen Festplatte entfernt die virtuelle Festplatte
   aus der Konfiguration des Controllers. Durch das Initialisieren einer
   virtuellen Festplatte werden alle Daten von der virtuellen Festplatte
   permanent gelöscht.
   ```

   - **Richtlinie bearbeiten: Lese-Cache**
   - **Richtlinie bearbeiten: Schreib-Cache**
   - **Richtlinie bearbeiten: Festplatten-Cache**
   - **Initialisieren: Schnell**
   - **Initialisieren: Voll**

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.
- Sie können den Servern PCIe-Steckplätze zuweisen oder die Zuweisung rückgängig machen

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 Faktoren, bevor Sie die Zuweisung zwischen einem Server und einem PCIe-Steckplatz aufheben:

- 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.

Weitere Informationen über das Zuweisen und das Aufheben der Zuweisung von PCIe-Steckplätzen finden Sie in der *Online-Hilfe*.

ANMERKUNG: Ohne eine Lizenz könne Sie einem Server maximal zwei PCIe-Geräte zuweisen.

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** .

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-Menu **Maßnahme** den entsprechenden Servernamen aus, und klicken Sie dann auf **Anwenden**.

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.

- Um die aktuelle Zuweisung von PCIe-Geräten auf Servern anzuzeigen, führen Sie den folgenden Befehl aus:
  `racadm getpiecfg -a`
- Um die Eigenschaften von PCIe-Geräten unter Verwendung von FQDD anzuzeigen, führen Sie 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 Serversteckplatz zuzuweisen, führen Sie den folgenden Befehl aus:
  `racadm setpciecfg assign [-c <FQDD>] [i <Serversteckplatz>]`
- Um zum Beispiel PCIe-Steckplatz 5 dem Serversteckplatz 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`

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 sammeln, Fehlerstatus und Fehlerprotokolle.
- Diagnosekonsole verwenden.
- Strom auf einem Remote-System verwalten.
- Lifecycle Controller-Aufträge 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.

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).

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`
NIC-Informationen (CMC-Modul)	`getniccfg`
Redundanzinformationen	`getredundancymode`
Ablaufverfolgungsprotokollinformationen	`gettracelog`
RAC-Ereignisprotokoll	`getraclog`
System-Ereignisprotokoll	`getsel`

Herunterladen der SNMP-MIB-Datei Verwaltungsinformationsbasis

Die CMC-SNMP-MIB-Datei definiert die Gehäusetypen, Ereignisse und Anzeigen. Mit CMC können Sie die MIB-Datei über die Web-Schnittstelle herunterladen.

So laden Sie die CMC-SNMP-MIB-Datei Verwaltungsinformationsbasis über die Web-Schnittstelle 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 **Wechselstromredundanz** eingestellt und es wurde ein Ereignis „Stromversorgungsredundanz verloren“ gemeldet.

- **Lösung A**: Diese Konfiguration erfordert mindestens ein Netzteil in Seite 1 (die linken zwei Steckplätze) und ein Netzteil in 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 um die **Wechselstromredundanz** zu erhalten. (Bei vollständigem Wechselstromredundanz-Betrieb 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 in Seite 1 müssen mit dem einen Wechselstromnetz verbunden sein und die Netzteile in Seite 2 müssen mit dem anderen Wechselstromnetz verbunden sein. Beide Wechselstromnetze müssen funktionieren. **Wechselstromredundanz** 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 Strompriorität des Serversteckplatzes, die dem neu eingesetzten Server zugewiesen ist, und stellen Sie sicher, dass die Priorität nicht niedriger ist als die Strompriorität 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, sodass 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 **Wechselstromredundanz**-Konfiguration mit vier Netzteilen betrieben wurde.

- **Lösung:** Dies kann auftreten, wenn die Netzteile zum Zeitpunkt, an den das Wechselstromnetz ausfällt, nicht korrekt an die redundanten Wechselstromnetze angeschlossen sind. Die **Wechselstromredundanz**-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 ein 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

```
Kritisches Systemsoftwareereignis: Redundanz verloren Mittwoch, 09. Mai
15:26:28 2007 normales Systemsoftwareereignis: Löschen des Protokolls wurde
bestätigt Mittwoch, 09. Mai 16:06:00 2007 Systemsoftwareereignis Warnmeldung:
vorhergesagter Fehler wurde bestätigt vorhergesagter Fehler wurde bestätigt
Mittwoch, 09. Mai 15:26:31 2007 kritisches Systemsoftwareereignis: Protokoll
voll wurde bestätigt Mittwoch, 09. Mai 15:47:23 2007 unbekanntes
Systemsoftwareereignis: unbekanntes Ereignis
```

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

Der CMC erstellt ein Protokoll von Ereignissen, die sich auf das Gehäuse beziehen.

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 sie 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 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.

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 dieser Zeit nach wie vor keine Änderung auftritt, handelt es sich möglicherweise um ein Problem, das untersucht werden muss. Der CMC kann seine Uhr möglicherweise aus diesen Gründen nicht synchronisieren:

- Es könnte ein Problem mit den 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 NTP-bezogene Ausfälle. Falls der CMC sich nicht mit einem konfigurierten NTP-Server synchronisieren kann, dann ist 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
```

Wenn '*' für einen der konfigurierten Servernicht angezeigt wird, könnten die Einstellungen nicht korrect konfiguriert sein. Die Ausgabe dieses Befehls enthält detaillierte NTP-Statistikdaten, die bei der Analyse, warum der Server nicht synchronisiert, nützlich sein können.

Wenn Sie versuchen, einen NTP-Server zu konfigurieren, der Windows-basiert ist, wird empfohlen, dass Sie den `MaxDist`-Parameter für `ntpd` erhöhen. Bevor Sie diesen Parameter ändern, sollten Sie alle möglichen Auswirkungen einer solchen Änderung verstehen, insbesondere weil die Standardeinstellung ausreichend hoch sein sollte, um mit den meisten NTP-Servern zu funktionieren.

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 unter Verwendung der CMC-Schnittstelle 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, jedoch routinemäßiges Ereignis hin, wie z. B. das Hochladen von Firmware, währenddessen die Einheit nicht betriebsbereit ist. Dies zeigt keinen Fehler an.
- Eine blinkende gelbe LED an einem Modul weist auf einen Fehler in diesem Modul hin.
- Blaue, blinkende LEDs können vom Benutzer konfiguriert und zur Identifikation genutzt werden. Weitere Informationen über Konfigurationen finden Sie unter Herunterladen der SNMP-MIB-Datei Verwaltungsinformationsbasis.

Tabelle 32. 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	Bereitschaftsmodus
Server	Grün, beständig leuchtend	Eingeschaltet
	Grün, blinkend	Firmware wird hochgeladen

Komponente	LED-Farbe, Blinkmuster	Status
	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
	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

Komponente	LED-Farbe, Blinkmuster	Status
	Gelb blinkend	Fehler
	Gelb, dunkel	Kein Fehler
	(Kreis) Grün, beständig leuchtend	Gleichstrom OK
	(Kreis) Grün, dunkel	Gleichstrom nicht OK

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.

   Bei einem Kernspeicherfehler wird alle 5 Sekunden eine Fehlermeldung angezeigt.
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 Selbsttestfehler

recover2[Bad FW images] CMC2-Images beschädigt
```

- 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 **firmimg.cmc** 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 internen CMC-Ablaufverfolgungsprotokoll können Sie CMC-Warnmeldungen und den CMC-Netzwerkbetrieb debuggen. Sie können auf das Verlaufsprotokoll mittels CMC-Webschnittstelle oder RACADM zugreifen. Weitere Informationen zum gettracelog-Befehl finden Sie im Abschnitt zum `gettracelog`-Befehl im *RACADM-Befehlszeilenreferenzhandbuch für iDRAC7 und CMC*.

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 interne 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** → **Gehäuse** → **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.
   – **TTY-Protokoll exportieren** – Das TTY-Debug-Protokoll vom Speichercontroller wird auf Ihr lokales System exportiert.

   ANMERKUNG: Wenn ein gepinnter Cache vorhanden ist, ist die Option zum Löschen auch vorhanden. Wenn kein gepinnter Cache vorhanden ist, wird diese Option nicht angezeigt.

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.

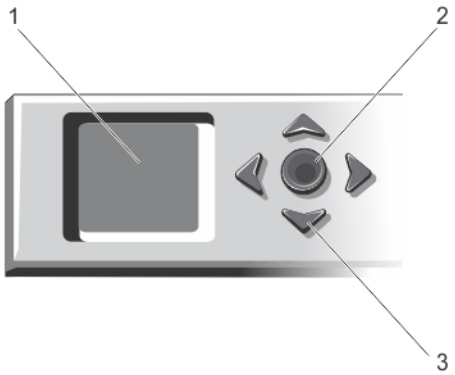


Abbildung 2. LCD-Anzeige

1. LCD-Bildschirm
2. Auswahlschaltfläche zum Markieren
3. Scrolltasten (4)

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 33. 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**
- **Rückseite**
- **Seitenansicht**
- **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.

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 - Server oder Gehäuse - angezeigt, das zum fehlerhaften Server bzw. Modul 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 34. CMC-Status

Element	Beschreibung
Beispiel: CMC1, CMC2	Name/Standort.
Keine Fehler	Wenn kein Fehler auftritt, wird „Keine Fehler“ angezeigt, ansonsten werden Fehlermeldungen aufgeführt.
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.
Globale IP6-Adresse: <Adresse>	Wird nur dann angezeigt, wenn IPv6 nur auf einem aktiven CMC aktiviert wurde.

Tabelle 35. Gehäusestatus

Element	Beschreibung
Benutzerdefinierter Name	Beispiel: „Dell-Rack-System“. Dies ist über die CMC-CLI oder die Web-GUI einstellbar.
Fehlermeldungen	Bei keinem Fehler wird Keine Fehler angezeigt; ansonsten werden Fehlermeldungen aufgelistet - zuerst schwerwiegende Fehler und danach Warnungen.
Modellnummer	Beispiel „PowerEdgeM1000“.
Stromverbrauch	Aktueller Stromverbrauch in Watt.
Spitzenleistung	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, wechselstromredundant oder gleichstromredundant.

Tabelle 36. Lüfterstatus

Element	Beschreibung
Name/Standort.	Beispiel: Lüfter1, Lüfter2 und so weiter.
Fehlermeldungen	Bei keinem Fehler wird „Keine Fehler“ angezeigt; ansonsten werden Fehlermeldungen aufgelistet - zuerst schwerwiegende Fehler und danach Warnungen.
RPM	Aktuelle Lüftergeschwindigkeit in U/Min.

Tabelle 37. Netzteileinheitstatus

Element	Beschreibung
Name/Standort.	Beispiel: Netzteil1, Netzteil2 und so weiter.
Fehlermeldungen	Bei keinem Fehler wird „Keine Fehler“ angezeigt; ansonsten werden Fehlermeldungen aufgelistet - zuerst schwerwiegende Fehler und danach Warnungen.
Status	Offline, Online oder Standby.
Maximale Wattzahl	Maximale Wattzahl, welche die Netzteileinheit dem System zuführen kann.

Tabelle 38. EAM-Status

Element	Beschreibung
Name/Standort.	EAM A
Fehlermeldungen	Bei keinem Fehler wird „Keine Fehler“ angezeigt; ansonsten werden Fehlermeldungen aufgelistet - zuerst schwerwiegende Fehler und danach Warnungen.
Status	Aus oder Ein.
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 39. Serverstatus

Element	Beschreibung
Beispiel: Server 1, Server 2, etc.	Name/Standort.
Keine Fehler	Bei keinem Fehler wird Keine Fehler angezeigt; ansonsten werden Fehlermeldungen aufgelistet. Die schwerwiegenden Fehler werden zuerst aufgelistet und danach die Warnungen. Weitere Informationen finden Sie unter „LCD-Fehlermeldungen.“

Element	Beschreibung
Steckplatzname	Gehäuse-Steckplatzname. Zum Beispiel SLOT-01. **ANMERKUNG:** Sie können diese Tabelle über die CMC CLI oder Web GUI 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.
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, dann werden die folgenden Informationen nicht angezeigt, anderenfalls 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
- iKVM

RACADM

Nach dem Ausführen eines CMC-Resets (mithilfe des RACADM-Unterbefehls racreset), wenn ein Befehl eingegeben wird, wird die folgende Meldung angezeigt:

```
racadm <Unterbefehl> 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 (racadm-Befehl fehlerhaft).
```

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 nicht übereinstimmendes doppeltes Anführungszeichen (") oder ein nicht übereinstimmendes einfaches Anführungszeichen (’) 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

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, weil das Standardzertifikat als CMC-Standardzertifikat ausgegeben wird, was 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**.

   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-Zugriff: SNMP-Authentifizierungsfehler

   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.

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 Webschnitstelle zeigt die folgende Fehlmeldung an:

```
Diese Funktionskarte wurde auf einem anderen Gehäuse aktiviert. Sie muss vor
einem Zugriff auf die Funktion FlexAddress entfernt werden.
Aktuelle Gehäuse-Service-Tag-Nummer = XXXXXXXX
Gehäuse-Service-Tag-Nummer der Funktionskarte = YYYYYYYY
Der folgende Eintrag wird dem CMC-Protokoll hinzugefügt:
cmc <Datum Zeitstempel> : feature 'FlexAddress@XXXXXXX' not activated; chassis
ID='YYYYYYY'
```

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:

```
Keine Funktionskarte eingesetzt.
FEHLER: Datei kann nicht geöffnet werden
```

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 Webschnittstelle 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 Deaktivierung auf diesem oder einem beliebigen anderen Gehäuse berechtigt, es sei denn Dell-Service programmiert das Original-Gehäuse-Service-Tag wieder in ein Gehäuse zurück, und der CMC, der die Original-Funktionskarte besitzt, wird auf diesem Gehäuse aktiviert

  .
- 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:

```
Keine Funktionen auf dem Gehäuse aktiviert. FEHLER: schreibgeschütztes
Dateisystem
```

Was passiert, wenn sich keine SD-Karte im aktiven CMC-Modul befindet?

Der Befehl **$racadm featurecard -s** wird folgende Meldung zurückgeben:

```
Keine Funktionskarte eingesetzt.
```

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.