Dell Chassis Management Controller Firmware Version 4.0

Benutzerhandbuch

Anmerkungen und Vorsichtshinweise

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

VORSICHTSHINWEIS: Durch VORSICHT werden Sie auf Gefahrenquellen hingewiesen, die Hardwareschäden oder Datenverlust zur Folge haben könnten, wenn die Anweisungen nicht befolgt werden.

2012 - 03

Inhalt

1

Übersicht

Der Dell Chassis Management Controller (CMC) ist eine hotplug-fähige Hardware- und Softwarelösung zur Systemverwaltung für die folgenden Funktionen für Dell PowerEdge M1000e-Gehäusesysteme.

- Remote-Verwaltungsfunktionen
- Energiesteuerung
- Kühlsteuerung

Der CMC, der über einen eigenen Mikroprozessor und Speicher verfügt, wird vom modularen Gehäuse, an das er angeschlossen ist, mit Strom versorgt. Eine Einführung zum CMC zu finden Sie unter „Installation und Setup des CMC“ auf Seite 33.

Der CMC ist mit verschiedenen Systemverwaltungsfunktionen für Blade-Server ausgestattet. Die Energie- und Temperaturverwaltung stellen die Hauptfunk-tionen des CMC dar.

- Automatische Energie- und Temperaturüberwachung in Echtzeit für das gesamte Gehäuse.
  - CMC überwacht die Systemenergieanforderungen und unterstützt den optionalen Modus für die dynamische Netzteilzuschaltung. Auf diese Weise kann CMC zur Verbesserung der Energieeffizienz die Netzteile dynamisch in den Standby-Modus versetzen, und zwar unabhängig von den Last-Redundanzanforderungen.
  - CMC meldet den Leistungsbedarf in Echtzeit und zeichnet Hoch- und Tiefpunkte mit Zeitstempel auf.
  - CMC ermöglicht das Einrichten eines optionalen maximalen Energieverbrauchswerts für das Gehäuse. Beim Erreichen des Grenzwerts wird entweder eine Warnmeldung ausgegeben oder es werden Maßnahmen ergriffen, um den Energieverbrauch des Gehäuses unter den festgelegten Wert abzusenken – beispielsweise, indem Servermodule gedrosselt werden oder das Hochfahren neuer Blades verhindert wird.

  - CMC überwacht und steuert automatisch die Lüfter 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 des M1000e-Gehäuses
  - Einstellungen für die Stromversorgungsredundanz und eine Obergrenzendefinition für den Stromverbrauch
  - E/A-Switches und iDRAC-Netzwerkeinstellungen
  - Erstes Startgerät auf den Serverblades
  - CMC überprüft die Konsistenz der E/A-Struktur zwischen den E/A-Modulen und Blades. Gegebenenfalls werden Komponenten deaktiviert, um die Systemhardware zu schützen.
  - Sicherheitsmerkmale für den Benutzerzugriff

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

Sie können das M1000e-Gehäuse entweder mit einem einzelnen CMC oder mit redundanten CMCs konfigurieren. Bei redundanten CMC-Konfigurationen und wenn der primäre CMC die Verbindung mit dem M1000e-Gehäuse oder dem Verwaltungsnetzwerk verliert, übernimmt der Standby-CMC die Gehäuseverwaltung.

Was ist neu in dieser Version?

Diese Version von CMC unterstützt die folgenden Funktionen:

- Speichern und Wiederherstellen der Gehäusekonfiguration.
- Verbessertes SEL-Protokoll.
- Broadcom 57810-k Dual Port 10-GB-Blade-Netzwerk-Tochterkarte.
- Broadcom 57810-k Dual Port 10-GB-Blade-Mezzanine-Karte.
- Intel I350 Quad Port 1-GB-Blade-Mezzanine-Karte.

- Intel x520-k Dual Port 10-GB-Blade-Netzwerk-Tochterkarte.
- Intel x520-k Dual Port 10-GB-Blade-Netzwerk-Mezzanine-Karte.
- Qlogic QMD8262-k Dual Port 10-GB-Blade-Netzwerk-Tochterkarte.
- Mellanox M4001Q QDR/DDR InfiniBand-Switch.
- Mellanox M4001F FDR InfiniBand-Switch.
- Mellanox ConnectX-3 QDR/DDR InfiniBand-Blade-Mezzanine-Karte.
- Mellanox ConnectX-3 FDR InfiniBand-Blade-Mezzanine-Karte.
- Erweiterte CMC-MIB für die Speicherung von OIDs für den physischen Gehäusestandort.
- Erweiterte CMC-MIB für die Speicherung von OIDs für die Blade-Service-Tag-Nummer und den Einschubnamen.
- Deckt die externe Energieverwaltung über **Open Manage Power Connect** (OMPC) ab.
- Replikation von einem bis zu vielen BIOS-Server-Einstellungen für iDRAC6- und iDRAC7-Server (Klonen von Servern).
- Erweiterung der Mehrgehäuseverwaltungsfunktion für die Synchronisation der Eigenschaften neuer Mitgliedern mit denen des Führungsgehäuses.
- Unterstützung des Erst-iDRAC7 PowerEdge M620-Servers.
- CPU- und Speicherinformationen über die GUI für Server, die den **Lifecycle Controller** (LC) unterstützen.
- Unterstützung von Bestandslisten für Server und EAMs und Melden der Generierung einer MCM-Gruppe (Gruppe für die Mehrgehäuseverwaltung).

CMC-Verwaltungsfunktionen

Der CMC enthält die folgenden Verwaltungsfunktionen:

- Redundante CMC-Umgebung.
- Registrierung des dynamischen Domänennamensystems (DDNS) für IPv4 und IPv6.
- Remote-Systemverwaltung und -überwachung über SNMP, eine Webschnittstelle, ein iKVM oder eine Telnet-/SSH-Verbindung.

- Überwachung - Zugriff auf Systeminformationen und Komponentenstatus.
- Zugriff auf Systemereignisprotokolle - Bietet Zugriff auf das Hardwareprotokoll und das CMC-Protokoll.
- Firmware-Aktualisierungen für verschiedene Gehäusekomponenten – Damit können Sie die Firmware für CMC, Server, iKVM und EAM-Infrastrukturgeräte 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 **IT Assistent** zu starten.
- CMC-Warnung - Warnt Sie anhand einer E-Mail-Benachrichtigung oder eines SNMP-Traps über potenzielle Probleme mit verwalteten Knoten.
- Remote-Stromverwaltung - Bietet Remote-Stromverwaltungsfunktionen wie z. B. Herunterfahren 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). Weitere Informationen finden Sie unter „FlexAddress verwenden“ auf Seite 281.
- 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 8 weitere Gehäuse vom Hauptgehäuse aus sichtbar sind.

Sicherheitsfunktionen

Der CMC bietet die folgenden Sicherheitsfunktionen:

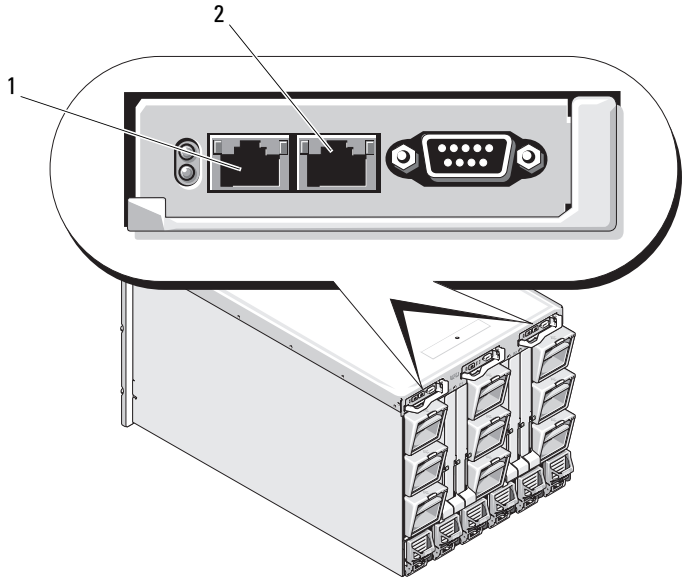
- Sicherheitsverwaltung auf Kennwortebene – Verhindert den unberechtigten Zugriff auf ein Remote-System.
- Benutzerauthentifizierung über Active Directory (optional) oder hardware-gespeicherte Benutzer-IDs und Kennwörter.
- Rollenbasierte Autorität – Ermöglicht es einem Administrator, spezifische Berechtigungen 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

Abbildung 1-1 zeigt die Vorderansicht des CMC (Blende) und die CMC-Steckplätze im Gehäuse.

Abbildung 1-1. Dell M1000e-Gehäuse und CMC



1 GB-Schnittstelle 2 STK-Schnittstelle

Hardwarespezifikationen

Der folgende Abschnitt enthält Informationen zur den technischen Hardware-Daten für CMC.

TCP/IP-Schnittstellen

Beim Öffnen von Firewalls für Remote-Zugriff auf einen CMC sind Schnittstelleninformationen erforderlich.

Tabelle 1-1. Abhörschnittstellen des CMC-Servers

Schnittstellennummer	Funktion
22*	SSH
23*	Telnet
80*	HTTP
161	SNMP-Agent
443*	HTTPS

* Konfigurierbare Schnittstelle

Tabelle 1-2. CMC-Client-Schnittstelle

Schnittstellennummer	Funktion
25	SMTP
53	DNS
68	DHCP-zugewiesene IP-Adresse
69	TFTP
162	SNMP-Trap
514*	Remote-Syslog
636	LDAPS
3269	LDAPS für globalen Katalog (GC)

* Konfigurierbare Schnittstelle

Unterstützte Remote-Zugriffsverbindungen

Tabelle 1-3 listet die unterstützten Remote Access Controller auf.

Tabelle 1-3. Unterstützte Remote-Zugriffsverbindungen

Verbindung	Funktionen
CMC-Netzwerkschnittstellen	• GB-Schnittstelle: Dedizierte Netzwerkschnittstelle für die CMC-Web-Schnittstelle. Zwei 10/100/1000-GB-Schnittstellen; eine für die Verwaltung und die andere für die Gehäuse-Gehäuse-Kabelkonsolidierung • STK: Uplink-Schnittstelle für die Gehäuse-Gehäuse-Netzwerkkabelkonsolidierung • 10 MBit/s/100 MBit/s/1 GBit/s Ethernet über CMC-GbE-Schnittstelle • 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 • Die serielle Schnittstelle kann mit dem Befehl `connect` (oder `racadm connect`) intern an die serielle Konsole eines Servers oder E/A-Moduls angeschlossen werden.
Weitere Verbindungen	• Zugriff auf die Dell-CMC-Konsole über das Avocent Integrated KVM Switch-Modul (iKVM)

Unterstützte Plattformen

Der CMC unterstützt modulare Systeme, die für die M1000e-Plattform vorgesehen sind. Informationen über die Kompatibilität des CMC finden Sie in der Dokumentation Ihres Geräts.

Eine Liste der aktuell unterstützten Betriebssysteme finden Sie in der *Dell Systems Software Support Matrix* unter **support.dell.com/manuals**.

Unterstützte Web-Browser

Die folgenden Web-Browser werden für CMC 4.0 unterstützt:

- Microsoft Internet Explorer 8.0 für Windows 7, Windows Vista, Windows XP und Windows Server 2003-Familie.
- Microsoft Internet Explorer 7.0 für Windows 7, Windows Vista, Windows XP und Windows Server 2003-Familie.
- Mozilla Firefox 1.5 (32-Bit) – beschränkte Funktionalität.

Die neuesten Informationen über unterstützte Web-Browser für CMC 4.0 finden Sie in der *Dell Systems Software Support Matrix* unter **support.dell.com/manuals**.

Lokalisierte Versionen der CMC-Webschnittstelle können folgendermaßen angezeigt werden:

1. Öffnen Sie die Windows-**Systemsteuerung**.
2. Doppelklicken Sie auf das Symbol **Regionale Einstellungen**.
3. Wählen Sie das erforderliche Gebietsschema aus dem Drop-Down-Menü **Ihr Gebietsschema (Standort)**.

Unterstützte Verwaltungskonsolenanwendungen

Der CMC unterstützt die Integration mit Dell OpenManage IT Assistant. Weitere Informationen finden Sie in der IT Assistant-Dokumentation auf der Dell Support-Website unter **support.dell.com/manuals**.

Unterstützung für das WS-Management

Web Services für Management (WS-MAN) ist ein SOAP-basiertes (Simple Object Access Protocol) Protokoll, das für Systemverwaltung verwendet wird. WS-MAN biete ein interoperables Protokoll für Geräte, um Daten über Netzwerke freizugeben und auszutauschen. CMC verwendet WS-MAN zur Übertragung von Distributed Management Task Force (DMTF) Common Information Model (CIM)-basierten Verwaltungsinformationen. Die CIM-Informationen definieren die Semantik und die Informationstypen, die in einem verwalteten System manipuliert werden können. Die Dell-embedded Schnittstellen zur Verwaltung der Serverplattform sind in Profile gegliedert, wobei jedes Profil die spezifischen Schnittstellen für eine bestimmte Management-Domäne oder einen Funktionalitätsbereich definiert. Darüber hinaus hat Dell eine Reihe von Modell- und Profilerweiterungen definiert, die Schnittstellen für weitere Funktionen bieten.

Der Zugriff auf WS-Management erfordert Anmeldung mit lokalen Benutzer-berechtigungen und Standardauthentifizierung über das SSL-Protokoll (Secured Socket Layer) auf Schnittstelle 443. Lesen Sie für Informationen zum Einrichten von Benutzerkonten den Abschnitt über die Datenbankeigenschaften der Sitzungsverwaltung (Session Management) im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*.

Die über das WS-Management verfügbaren Daten sind eine Teilmenge der Daten, die von der CMC-Instrumentationsschnittstelle geliefert werden und den folgenden DMTF-Profilen der Version 1.0.0 zugewiesen sind:

- Profil zu Zuweisungsfunktionen
- Profil zur Basismetrik
- Profil zum Basisserver
- Profil zum Computersystem
- Profil zum modularen System
- Profil zum physischen Bestand
- Profil zur Dell-Stromzuweisung
- Profil zur Dell-Stromversorgung
- Profil zur Dell-Stromtopologie
- Profil zur Stromzustandsverwaltung

- Profil zur Profilregistrierung
- Profil zum Datensatzprotokoll
- Profil zur Ressourcenzuweisung
- Profil zur rollenbasierten Autorisierung
- Profil zu Sensoren
- Profil zum Serviceprozessor
- Profil zur einfachen Identitätsverwaltung
- Profil zu Dell Active Directory Client
- Profil zur Boot-Steuerung
- Profil zu Dell Simple NIC

Die CMC WS-MAN-Implementierung verwendet SSL auf Schnittstelle 443 für Transportsicherheit und unterstützt Standardauthentifizierung. Lesen Sie für Informationen zum Einrichten von Benutzerkonten den Abschnitt über die cfgSessionManagement-Datenbankeigenschaften im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*. 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.

Für Client-Verbindungen mithilfe von Microsoft WinRM ist mindestens die Version 2.0 erforderlich. Weitere Informationen dazu finden Sie im Microsoft-Artikel, **<http://support.microsoft.com/kb/968929>**.

Zusätzliche Implementierungsrichtlinien, Weißbücher, Profil- und Codebeispiele finden Sie im Dell Tech Center unter **www.delltechcenter.com**. Weitere Informationen finden Sie unter:

- DTMF-Website: **www.dmtf.org/standards/profiles/**
- WS-MAN-Versionshinweise oder Read-Me-Datei.
- **www.wbemsolutions.com/ws_management.html**
- DMTF WS-Management-Spezifikationen: **www.dmtf.org/standards/wbem/wsman**

Weitere nützliche Dokumente

Zusätzlich zu dieser Anleitung, können Sie auf die folgenden Anleitungen zugreifen, die unter **support.dell.com/manuals** zur Verfügung stehen. Auf der Seite „Handbücher“ klicken Sie auf **Software→ Systemverwaltung**. Klicken Sie auf den entsprechenden Produktlink auf der rechten Seite, um auf die Dokumente zuzugreifen:

- Die *CMC-Online-Hilfe* enthält Informationen zur Verwendung der Webschnittstelle.
- Die *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification* enthält Informationen über Minimal-BIOS und Firmwareversion, Installation und Verwendung.
- Das Benutzerhandbuch *Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server* enthält Informationen über Installation, Konfiguration und Wartung des iDRAC auf verwalteten Systemen.
- Das *Dell OpenManage IT Assistant-Benutzerhandbuch* enthält Informationen über IT Assistant.
- Die Dokumentation zu Ihrer Verwaltungskonsolenanwendung eines Drittanbieters.
- 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.

Die folgenden Systemdokumente enthalten weitere Informationen über das System, auf dem 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**. Garantiebestimmungen können als separates Dokument beigelegt sein.

- Das zum Lieferumfang der Rack-Lösung gehörende *Rack-Installationshandbuch* und die *Rack-Installationsanweisungen* beschrieben, wie das System in einem Rack installiert wird.
- Im *Hardware-Benutzerhandbuch* finden Sie Informationen über Systemfunktionen, Fehlerbehebung im System und zum Installieren oder Austauschen von Systemkomponenten.
- 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.
- Versionsinformationen oder Infodateien können vorhanden sein. Diese geben den letzten Stand der Änderungen am System oder an der Dokumentation wieder und enthalten erweitertes technisches Referenzmaterial für erfahrene Benutzer oder Techniker.
- Weitere Informationen zu EAM-Netzwerkeinstellungen finden Sie in den Dokumenten *Dell PowerConnect M6220 Switch - Wichtige Informationen* und *White Paper zum Dell PowerConnect 6220 Series Port Aggregator.*

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.

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 weiteren Schritte zum Konfigurieren des CMC:

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

Weitere Informationen zur Installation und Einrichtung redundanter CMC-Umgebungen finden Sie unter „Die redundante CMC-Umgebung verstehen“ auf Seite 60.

Bevor Sie beginnen

Laden Sie die neueste Version der CMC-Firmware von Dells Support-Website unter **support.dell.com** 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.

CMC-Hardware installieren

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. Weitere Informationen zum Standby-CMC finden Sie unter „Die redundante CMC-Umgebung verstehen“ auf Seite 60.

Checkliste für die Integration eines Gehäuses

Mit den folgenden Schritten 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 vom CMC-Port mit der Bezeichnung **GB** mit dem Verwaltungsnetzwerk.

   ANMERKUNG: Legen Sie kein Kabel an die CMC-Ethernet-Schnittstelle mit der Bezeichnung **STK** an. Weitere Informationen zur Verkabelung der STK-Schnittstelle finden Sie unter „Die redundante CMC-Umgebung verstehen" auf Seite 60.

2. Installieren Sie die E/A-Module im Gehäuse, und verkabeln Sie diese.
3. Schieben Sie die Server in das Gehäuse ein.
4. Schließen Sie das Gehäuse an der Stromquelle an.
5. Betätigen Sie den Netzschalter an der linken unteren Ecke des Gehäuses, oder schalten Sie das Gehäuse über die CMC-GUI ein, nachdem Sie Schritt 7 abgeschlossen haben.

   ANMERKUNG: Schalten Sie die Server nicht ein.

6. Über das LCD-Bedienfeld an der Systemvorderseite können Sie den CMC mit einer statischen IP-Adresse versorgen oder ihn für DHCP konfigurieren.
7. Stellen Sie über den Webbrowser 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 im CMC-GUI und aktivieren Sie die LAN- und IPMI-Schnittstelle.

   ANMERKUNG: Auf manchen Servern ist die iDRAC-LAN-Schnittstelle standardmäßig deaktiviert.

9. Geben Sie jedem E/A-Modul im CMC-GUI eine IP-Adresse.
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 „calvin".
11. Stellen Sie über den Webbrowser 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.

Jeder CMC hat zwei RJ-45 Ethernet-Schnittstellen mit der Bezeichnung **GB** (*Uplink*-Schnittstelle) und **STK** (*Stacking*- oder Kabelkonsolidierungs-Schnittstelle). Bei einer Basisverkabelung verbinden Sie die GB-Schnittstelle mit dem Verwaltungsnetzwerk und belassen die STK-Schnittstelle unbenutzt.

VORSICHTSHINWEIS: Anschließen der STK-Schnittstelle an das Verwaltungsnetzwerk kann unvorhersehbare Ergebnisse bewirken. Wenn GB und STK mit demselben Netzwerk verkabelt werden (Broadcast-Domäne), kann dies zu einer Broadcastüberlastung führen.

Verkettete CMC-Netzwerkverbindung

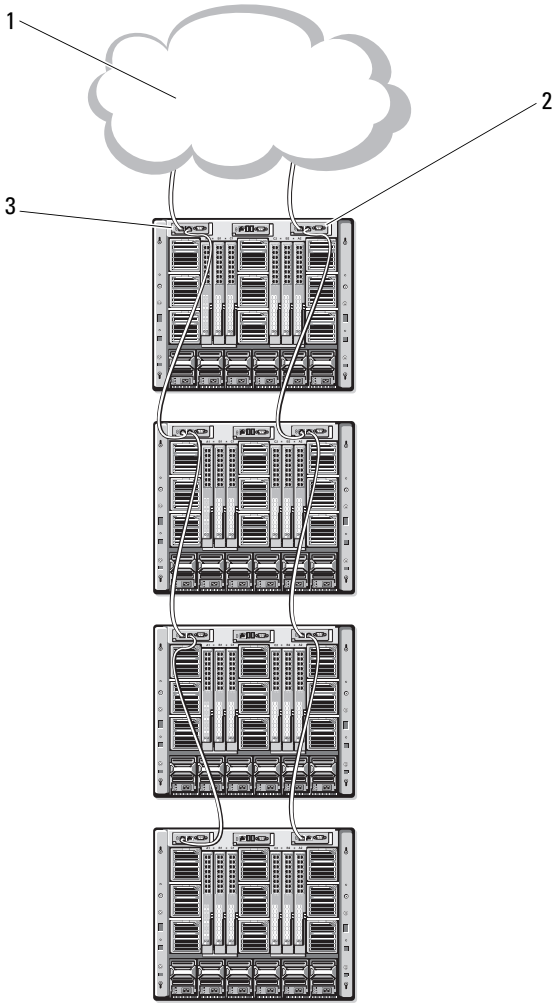
Wenn in einem Rack mehrere Gehäuse vorhanden sind, können Sie die Anzahl an Verbindungen mit dem Verwaltungsnetzwerk verringern, indem Sie bis zu vier Gehäuse miteinander verketten. Wenn jedes der vier Gehäuse einen redundanten CMC enthält, können Sie durch eine Verkettung die Anzahl an erforderlichen Verwaltungsnetzwerkverbindungen von acht auf zwei reduzieren. Wenn jedes Gehäuse nur über einen CMC verfügt, können Sie die Anzahl an erforderlichen Anschlüsse von vier auf einen reduzieren.

Wenn Sie Gehäuse miteinander verketten, ist GB die „Uplink"-Schnittstelle und STK die Stacking-Schnittstelle (Kabelkonsolidierung). Verbinden Sie die GB-Schnittstellen mit dem Verwaltungsnetzwerk oder der STK-Schnittstelle des CMC in einem Gehäuse, das sich näher am Netzwerk befindet. Sie sollten die STK-Schnittstelle nur mit einer GB-Schnittstelle verbinden, die weiter von der Verkettung bzw. vom Netzwerk entfernt ist.

Bilden Sie separate Verkettungen für die CMCs im aktiven CMC-Steckplatz und im sekundären CMC-Steckplatz.

Abbildung 2-1 zeigt die Anordnung der Kabel für vier verkettete Gehäuse, jeweils mit einem aktiven und einem Standby-CMC.

Abbildung 2-1. Verkettete CMC-Netzwerkverbindung



1 Verwaltungsnetzwerk 2 Standby-CMC

3 Aktiver CMC

Abbildung 2-2, Abbildung 2-3 und Abbildung 2-4 zeigen Beispiele für die inkorrekte Verkabelung des CMC.

Abbildung 2-2. Inkorrekte Verkabelung für CMC-Netzwerkverbindung - 2 CMCs

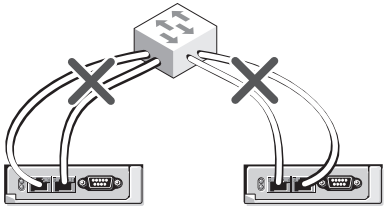


Abbildung 2-3. Inkorrekte Verkabelung für CMC-Netzwerkverbindung - 1 CMC

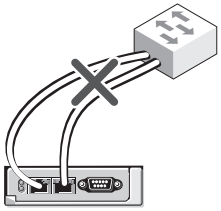
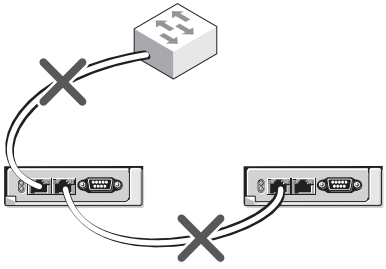


Abbildung 2-4. Inkorrekte Verkabelung für CMC-Netzwerkverbindung - 2 CMCs



So verketten Sie bis zu vier Gehäuse:

1. Verbinden Sie die GB-Schnittstelle des aktiven CMC im ersten Gehäuse mit dem Verwaltungsnetzwerk.
2. Verbinden Sie die GB-Schnittstelle des aktiven CMC im zweiten Gehäuse mit der STK-Schnittstelle des aktiven CMC im ersten Gehäuse.
3. Wenn ein drittes Gehäuse vorhanden ist, verbinden Sie dessen GB-Schnittstelle vom aktiven CMC mit der STK-Schnittstelle des aktiven CMC im zweiten Gehäuse.
4. Wenn ein viertes Gehäuse vorhanden ist, verbinden Sie dessen GB-Schnittstelle vom aktiven CMC mit der STK-Schnittstelle des dritten Gehäuses.
5. Wenn redundante CMCs im Gehäuse vorhanden sind, verbinden Sie diese nach demselben Muster.

VORSICHTSHINWEIS: Die STK-Schnittstelle von CMCs darf niemals mit dem Verwaltungsnetzwerk verbunden werden. Sie kann nur mit der GB-Schnittstelle an einem anderen Gehäuse verbunden werden. Einen STK-Anschluss mit dem Verwaltungsnetzwerk zu verbinden, kann das Netzwerk stören und Datenverlust zur Folge haben. Wenn GB und STK mit demselben Netzwerk verkabelt werden (Broadcast-Domäne), kann dies zu einer Broadcastüberlastung führen.

ANMERKUNG: Verbinden Sie nie einen aktiven CMC mit einem Standby-CMC.

ANMERKUNG: Wird ein CMC zurückgesetzt, dessen STK-Schnittstelle mit einem anderen CMC verkettet ist, kann das Netzwerk für CMCs, die nachfolgend in der Verkettung auftreten, gestört werden. Die untergeordneten CMCs geben eventuell Meldungen aus, die darauf hinweisen, dass keine Netzwerkverbindung mehr besteht und dass möglicherweise auf die redundanten CMCs umgeschaltet wird.

Eine Einführung zum CMC zu finden Sie unter „Remote-Zugriffssoftware auf einer Management Station installieren“ auf Seite 38.

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 und Sicherheit-Benutzerhandbuch* oder unter **support.dell.com/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 ausführbaren Dateien ausführen.

4 Wechseln 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 zu RACADM finden Sie unter „RACADM-Befehlszeilenschnittstelle verwenden“ auf Seite 81.

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>
```

Weitere Informationen zu Remote-racadm finden Sie unter „RACADM im Remote-Zugriff aufrufen“ auf Seite 88 und den folgenden Abschnitten.

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 Verwenden Sie den `rpm`-Abfragebefehl, 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* der *Dell Systems Software Support Matrix* unter **support.dell.com/manuals**.

Der für den CMC und die Management Station verwendete Browser muss sich in demselben Netzwerk befinden, das als das *Verwaltungsnetzwerk* bezeichnet wird. Je nach 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 den 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.

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 **Extras→ Internetoptionen→ Sicherheit**.
3. Klicken Sie im Abschnitt **LAN-Einstellungen** auf **LAN-Einstellungen**.
4. Klicken Sie im Abschnitt **Proxy-Server** 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 3.0:

1. Mozilla Firefox starten.
2. Klicken Sie auf **Extras→ Optionen** (für Windows) oder klicken Sie auf **Bearbeiten→ Einstellungen** (für Linux).
3. Klicken Sie auf **Erweitert** und dann auf das Register **Netzwerk**.
4. Klicken Sie auf **Einstellungen**.
5. Wählen Sie die **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 7 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. Folgen Sie diesen Schritten, um den Phishing-Filter zu deaktivieren:

1. Starten Sie den Internet Explorer.
2. Klicken Sie auf **Extras→ Phishing-Filter** und dann auf **Phishing-Filter-Einstellungen**.
3. Wählen Sie das Kontrollkästchen **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 Web Server ein Zertifikat verwendet, das sich auf einer Liste widerrufener Zertifikate befindet, die aus dem Internet abgerufen wurde. Wenn kein Zugriff auf das Internet möglich ist, kann diese Funktion zu Verzögerungen von mehreren Sekunden führen, wenn Sie mit dem Browser oder einer Befehlszeilenschnittstelle, 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 **Extras→ Internetoptionen** und klicken Sie dann auf **Erweitert**.
3. Gehen Sie mit der Bildlaufleiste zum Abschnitt „Sicherheit“, deaktivieren Sie das Kontrollkästchen **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 **Extras→ Internetoptionen** und klicken Sie dann auf **Erweitert**.
3. Scrollen Sie zum Abschnitt „Sicherheit“ und wählen Sie **Verschlüsselte Seiten nicht auf der Festplatte speichern** aus.

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. Für den Internet Explorer muss der Browser so konfiguriert sein, dass Animationen wiedergegeben werden können, was der Standardeinstellung entspricht.

So konfigurieren Sie Internet Explorer zum Abspielen von Animationen:

1. Starten Sie den Internet Explorer.
2. Klicken Sie auf **Extras→ Internetoptionen** und klicken Sie dann auf **Erweitert**.
3. Gehen Sie mit der Bildlaufleiste zum Abschnitt „Multimedia“ und aktivieren Sie **Animationen auf Webseiten wiedergeben**.

Ursprünglichen Zugriff auf den CMC einrichten

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 M1000e-Lösung zu verwalten, muss sie mit Ihrem Verwaltungsnetzwerk verbunden sein.

Weitere Informationen über die Konfiguration der CMC-Netzwerkeinstellungen finden Sie unter „CMC-Netzwerk konfigurieren“ auf Seite 45. Diese anfängliche Konfiguration 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 M1000e-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 erfolgen über den CMC. Umgekehrt erfolgt der Zugriff auf die verwalteten Server über Netzwerkverbindungen zu E/A-Modulen (EAMs). Dies ermöglicht, dass Anwendungsnetzwerk und Verwaltungsnetzwerk voneinander getrennt sind.

ANMERKUNG: Es wird empfohlen, die Gehäuseverwaltung vom Datennetzwerk zu trennen. Dell kann die Betriebszeit eines Gehäuses, das nicht ordnungsgemäß in Ihre Umgebung integriert ist, nicht unterstützen oder garantieren. Aufgrund des potenziellen Verkehrs im Datennetzwerk können die Verwaltungsschnittstellen im internen Verwaltungsnetzwerk mit Datenverkehr für die Server ausgelastet sein. Dies führt zu Kommunikationsverzögerungen beim CMC und iDRAC. Diese Verzögerungen können unvorhersehbares Gehäuseverhalten verursachen, zum Beispiel: CMC zeigt iDRAC als offline an, obwohl iDRAC läuft, was wiederum weiteres unerwünschtes Verhalten hervorrufen kann. Falls physische Trennung des Verwaltungsnetzwerks nicht praktikabel ist, besteht die Option, CMC- und iDRAC-Verkehr in einem getrennten VLAN zu isolieren. Die CMC- und die einzelnen iDRAC-Netzwerkschnittstellen können mit dem Befehl `racadm setniccfg` für die Verwendung eines VLAN konfiguriert werden. Weitere Informationen finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*.

Wenn Sie ein Gehäuse haben, verbinden Sie den CMC und, falls vorhanden, den Standby-CMC mit dem Verwaltungsnetzwerk. Wenn Sie einen redundanten CMC haben, verwenden Sie ein anderes Netzwerkkabel und verbinden die CMC-Schnittstelle **GB** mit einer zweiten Schnittstelle des Verwaltungsnetz-werkes.

Wenn Sie mehr als ein Gehäuse haben, können Sie zwischen einer Basisverbindung, bei der jeder CMC mit dem Verwaltungsnetzwerk verbunden ist, oder verketteten Gehäuseverbindung wählen, bei der die Gehäuse verkettet sind und nur ein CMC direkt mit dem Verwaltungsnetzwerk verbunden ist. Der Basisverbindungstyp verwendet mehrere Schnittstellen im Verwaltungsnetz-werk und bietet höhere Redundanz. Der verkettet Verbindungstyp verwendet weniger Schnittstellen im Verwaltungsnetzwerk, schafft jedoch Abhängigkeiten zwischen den CMCs, wodurch sich die Redundanz des Systems verringert.

Weitere Informationen zu Verkettung finden Sie unter „Verkettete CMC-Netzwerkverbindung“ auf Seite 35.

ANMERKUNG: Wenn der CMC in einer redundanten Konfiguration nicht ordnungsgemäß verkabelt ist, kann dies zu Verwaltungsausfällen führen und Broadcast-Überlastungen bewirken.

CMC-Netzwerk 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 über eine IP-Adresse zugeteilt 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 anfänglichen Netzwerkeinstellungen, *nachdem* der CMC über eine IP-Adresse verfügt, kann über eine der folgenden Optionen erfolgen:

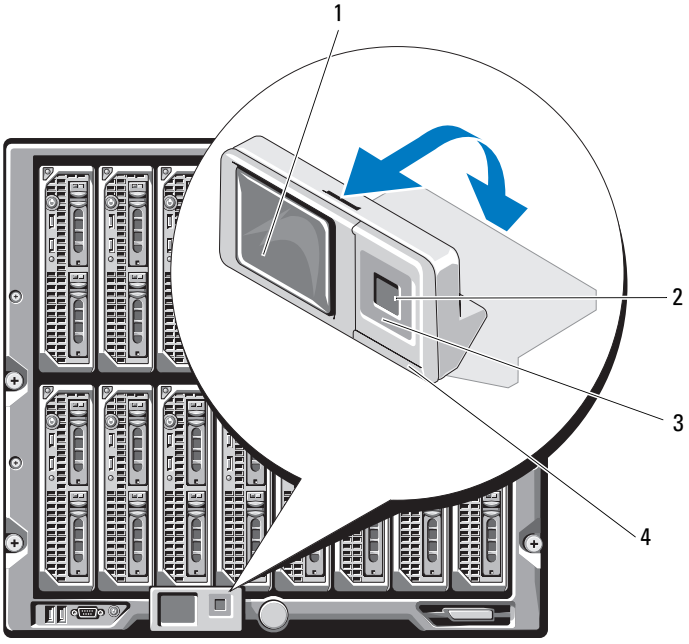
- Befehlszeilenschnittstellen (CLIs), wie z. B. eine serielle Konsole, Telnet, SSH oder die Dell-CMC-Konsole über iKVM
- Remote-RACADM
- Die CMC-Webschnittstelle

Netzwerkbetrieb mit dem LCD-Konfigurationsassistent konfigurieren

ANMERKUNG: Die CMC-Konfiguration über den LCD-Konfigurationsassistenten ist nur so lange möglich, bis das CMC-Modul installiert oder das Standardkennwort geändert wird. Wurde das Kennwort nicht geändert, kann die LCD weiterhin zur Neukonfiguration des CMC genutzt werden, was ein mögliches Sicherheitsrisiko darstellt.

Die LCD-Anzeige befindet sich unten links an der Gehäusevorderseite. Abbildung 2-5 veranschaulicht das LCD-Bedienfeld.

Abbildung 2-5. LCD-Anzeige



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

Auf dem LCD-Bildschirm werden Menüs, Symbole, Bilder und Meldungen angezeigt.

Eine LED-Statusanzeige auf dem LCD-Bedienfeld zeigt den Gesamtfunktions-zustand 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.

Auf dem LCD-Bildschirm navigieren

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 den Konfigurationsassistent verwenden, können Sie jederzeit zum vorhergehenden Bildschirm zurückkehren.
- *Um auf einem Bildschirm über die Bildlaufleiste 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.

Lesen Sie für weitere Informationen über die Verwendung des LCD-Bedienfelds den Abschnitt zum LCD-Bedienfeld im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*.

LCD-Konfigurationsassistent verwenden

So richten Sie ein Netzwerk unter Verwendung des LCD-Konfigurationsassistenten ein:

1. Falls Sie den Netzschalter des Gehäuses noch nicht eingeschaltet haben, drücken Sie ihn, um das Gehäuse einzuschalten.

   Der LCD-Bildschirm zeigt während des Einschaltens eine Reihe von Initialisierungsbildschirmen an. Wenn das Gerät bereit ist, wird der Bildschirm **Spracheinstellungen** angezeigt.

2 Wählen Sie Ihre Sprache mit den Pfeilschaltflächen aus und drücken Sie dann die Schaltfläche in der Mitte, um **Annehmen/Ja** auszuwählen, und drücken Sie die mittlere Schaltfläche erneut.

3 Der Bildschirm **Gehäuse** zeigt die folgende Frage an: **Gehäuse konfigurieren?**

   a Klicken Sie auf die mittlere Schaltfläche, um mit dem Bildschirm **CMC-Netzwerkeinstellungen** fortzufahren. Siehe Schritt 4.

   b Um das Menü **Gehäuse konfigurieren** zu beenden, wählen Sie das Symbol NEIN aus und drücken Sie die mittlere Schaltfläche. Siehe Schritt 9.

4 Klicken Sie auf die mittlere Schaltfläche, um mit dem Bildschirm **CMC-Netzwerkeinstellungen** fortzufahren.

5 Wählen Sie mit der Pfeilschaltfläche nach unten die Netzwerkgeschwindigkeit aus (10 MBit/s, 100 MBit/s, Automatisch (1 GBit/s)).

   ANMERKUNG: Die Einstellung der Netzwerkgeschwindigkeit muss mit Ihrer Netzwerkkonfiguration übereinstimmen, um einen effektiven Netzwerkdurchsatz zu gewährleisten. Wenn die Netzwerkgeschwindigkeit geringer eingestellt wird als die Geschwindigkeit Ihrer Netzwerkkonfiguration, steigt der Verbrauch der Bandbreite und die Netzwerkkommunikation wird verlangsamt. **Stellen Sie fest, ob Ihr Netzwerk höhere Netzwerkgeschwindigkeiten unterstützt, und stellen Sie sie entsprechend ein.** Wenn Ihre Netzwerkkonfiguration mit keinem dieser Werte übereinstimmt, wird empfohlen, die automatische Verhandlung (Option „**Automatisch**“) zu verwenden oder sich mit dem Hersteller Ihrer Netzwerkausrüstung in Verbindung zu setzen.

   Drücken Sie die Schaltfläche in der Mitte, um mit den **CMC-Netzwerkeinstellungen** auf dem nächsten Bildschirm fortzufahren.

6 Wählen Sie den Duplexmodus (halb oder voll), der der Netzwerkumgebung entspricht.

ANMERKUNG: Die Netzwerkgeschwindigkeits- und Duplexmodus-Einstellungen sind nicht verfügbar, wenn die automatische Verhandlung auf „Ein" eingestellt oder 1000 MB (1 GBit/s) ausgewählt ist.

ANMERKUNG: Wenn die automatische Verhandlung für ein Gerät eingeschaltet ist, jedoch nicht für ein anderes, kann das Gerät, das die automatische Verhandlung verwendet, die Netzwerkgeschwindigkeit des anderen Geräts, jedoch nicht den Duplexmodus, bestimmen; in diesem Fall schaltet der Duplexmodus während der automatischen Verhandlung in die Halbduplex-Einstellung zurück. Ein derartiger Duplex-Übereinstimmungsfehler resultiert in einer langsamen Netzwerkverbindung.

Drücken Sie die Schaltfläche in der Mitte, um mit den **CMC-Netzwerkeinstellungen** auf dem nächsten Bildschirm fortzufahren.

7 Wählen Sie das Internet-Protokoll (IPv4, IPv6 oder beide) aus, das Sie für den CMC verwenden möchten.

Drücken Sie die Schaltfläche in der Mitte, um mit den **CMC-Netzwerkein-stellungen** auf dem nächsten Bildschirm fortzufahren.

8 Wählen Sie den Modus aus, in dem der CMC die NIC-IP-Adressen abrufen soll:

Dynamisches Host-Konfigurationsprotokoll (DHCP)	Der CMC ruft 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. Klicken Sie auf die mittlere Schaltfläche, wenn Sie die DHCP-Option ausgewählt haben. Der Bildschirm **iDRAC konfigurieren?** wird angezeigt; gehen Sie zu Schritt 10.

Statisch

Sie geben die IP-Adresse, das Gateway und die Subnetzmaske auf den nachfolgend eingeblendeten Bildschirmen ein.

Wenn Sie die Option **Statisch** ausgewählt haben, drücken Sie die Schaltfläche in der Mitte, um mit dem nächsten Bildschirm **CMC-Netzwerkeinstellungen** fortzufahren. Dann:

a Bestimmen Sie die **Statische IP-Adresse**, indem Sie mit den Pfeilschaltflächen nach rechts und nach links zwischen den Positionen wechseln und mit den Pfeilschaltflächen nach oben und nach unten eine Nummer für jede Position auswählen. Wenn die Festlegung der **statischen IP-Adresse** abgeschlossen ist, drücken Sie die Schaltfläche in der Mitte, um fortzufahren.

b Bestimmen Sie die Subnetzmaske und drücken Sie dann die Schaltfläche in der Mitte.

c Bestimmen Sie den Gateway und drücken Sie dann die Schaltfläche in der Mitte. Der Bildschirm **Netzwerk-Zusammenfassung** wird angezeigt.

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, navigieren Sie zur Pfeilschaltfläche nach links und drücken Sie dann die Schaltfläche in der Mitte, um zum Bildschirm für diese Einstellung zurückzukehren. Nachdem Sie eine Korrektur vorgenommen haben, drücken Sie die Schaltfläche in der Mitte.

d Wenn Sie die Richtigkeit der von Ihnen eingegebenen Einstellungen bestätigt haben, drücken Sie die Schaltfläche in der Mitte. Der Bildschirm **DNS registrieren?** wird angezeigt.

ANMERKUNG: Falls der Modus „Dynamisches Host-Konfigurationsprotokoll (DHCP)“ für die CMC-IP-Konfiguration ausgewählt ist, dann ist auch DNS-Registrierung standardmäßig aktiviert.

9 Wenn Sie im vorhergehenden Schritt **DHCP** ausgewählt haben, fahren Sie mit Schritt 10 fort.

Um die IP-Adresse des DNS-Servers zu registrieren, drücken Sie die Schaltfläche in der Mitte, um fortzufahren. Wenn Sie über keinen DNS-Server verfügen, drücken Sie die Pfeilschaltfläche nach rechts. Der Bildschirm **DNS registrieren?** wird eingeblendet; fahren Sie mit Schritt 10 fort.

Bestimmen Sie die **IP-Adresse des DNS-Servers**, indem Sie mit den Pfeilschaltflächen nach rechts und nach links zwischen den Positionen wechseln und mit den Pfeilschaltflächen nach oben und nach unten eine Nummer für jede Position wählen. Wenn die Festlegung der IP-Adresse des DNS-Servers abgeschlossen ist, drücken Sie die Schaltfläche in der Mitte, um fortzufahren.

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

- **Nein:** Fahren Sie mit Schritt 13 fort.
- **Ja:** Drücken Sie die Schaltfläche in der Mitte.

Sie können iDRAC auch über die CMC-GUI konfigurieren.

11 Wählen Sie das Internet-Protokoll (IPv4, IPv6 oder beide) aus, das Sie für die Server verwenden möchten.

Dynamisches Host-Konfigurationsprotokoll (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 die mittlere Schaltfläche.

Statisch

Sie geben die IP-Adresse, das Gateway und die Subnetzmaske auf den nachfolgend eingeblendeten Bildschirmen ein.

Wenn Sie die Option **Statisch** ausgewählt haben, drücken Sie die Schaltfläche in der Mitte, um mit dem nächsten Bildschirm **iDRAC-Netzwerkeinstellungen** fortzufahren, Dann:

a Bestimmen Sie die **Statische IP-Adresse**, indem Sie mit den Pfeilschaltflächen nach rechts und nach links zwischen den Positionen wechseln und mit den Pfeilschaltflächen nach oben und nach unten eine Nummer für jede Position auswählen. Diese Adresse ist die statische IP des iDRAC, der sich im ersten Steckplatz befindet. Die statische IP-Adresse jedes nachfolgenden iDRAC wird als Steckplatznummer-Inkrement dieser IP-Adresse berechnet. Wenn die Festlegung der **statischen IP-Adresse** abgeschlossen ist, drücken Sie auf die Schaltfläche in der Mitte, um fortzufahren.

b Bestimmen Sie die Subnetzmaske und drücken Sie dann die Schaltfläche in der Mitte.

c Bestimmen Sie den Gateway und drücken Sie dann die Schaltfläche in der Mitte.

a Wählen Sie, ob der IPMI-LAN-Kanal **Aktiviert** oder **Deaktiviert** werden soll. Drücken Sie die mittlere Schaltfläche, um fortzufahren.

b Heben Sie auf dem Bildschirm **iDRAC-Konfiguration** das Symbol **Annehmen/Ja** hervor und drücken Sie die mittlere Schaltfläche, um alle iDRAC-Netzwerkeinstellungen auf die installierten Server anzuwenden. Um die iDRAC-Netzwerkeinstellungen nicht auf die installierten Server anzuwenden, heben Sie das Symbol **Nein** hervor, drücken Sie die mittlere Schaltfläche und fahren Sie mit Schritt c fort.

c Heben Sie auf dem nächsten Bildschirm **iDRAC-Konfiguration** das Symbol **Annehmen/Ja** hervor und drücken Sie auf die mittlere Schaltfläche, um alle iDRAC-Netzwerkeinstellungen auf neu installierte Server anzuwenden; wenn ein neuer Server in das Gehäuse eingesetzt wird, wird der Benutzer auf der LCD gefragt, ob der Server unter Verwendung der zuvor konfigurierten Einstellungen/Richtlinien automatisch bereitgestellt werden soll. Um die iDRAC-Netzwerkeinstellungen nicht auf neu installierte Server anzuwenden, heben Sie das Symbol **Nein** hervor und drücken Sie die mittlere Schaltfläche; wenn ein neuer Server in das Gehäuse eingesetzt wird, werden die iDRAC-Netzwerkeinstellungen nicht konfiguriert.

12 Heben Sie auf dem Bildschirm **Gehäuse** das Symbol **Annehmen/Ja** hervor und drücken Sie die mittlere Schaltfläche, um alle Gehäuseeinstellungen anzuwenden. Um die Gehäuseeinstellungen nicht anzuwenden, heben Sie das Symbol **Nein** hervor und drücken Sie die mittlere Schaltfläche.

13 Überprüfen Sie die von Ihnen bereitgestellten IP-Adressen auf dem Bildschirm **IP-Zusammenfassung**, um sicherzustellen, dass die Adressen korrekt sind. Für eine korrekte Einstellung, navigieren Sie zur linken Pfeilschaltfläche und drücken Sie dann die Schaltfläche in der Mitte, um zum Bildschirm für diese Einstellung zurückzukehren. Nachdem Sie eine Korrektur vorgenommen haben, drücken Sie die Schaltfläche in der Mitte. Wenn nötig, navigieren Sie zur rechten Pfeilschaltfläche und drücken Sie dann die Schaltfläche in der Mitte, um zum Bildschirm **IP-Zusammenfassung** zurückzukehren.

Wenn Sie die von Ihnen eingegebenen Einstellungen als korrekt bestätigt haben, klicken auf die mittlere Schaltfläche. Der Konfigurationsassistent wird geschlossen und kehrt zurück zum Bildschirm **Hauptmenü**.

ANMERKUNG: Falls Sie **Ja/Annehmen** ausgewählt haben, wird **Bitte warten** eingeblendet, bevor der Bildschirm **IP-Zusammenfassung** angezeigt wird.

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.

ANMERKUNG: Nachdem Sie das Netzwerk-Setup mit dem LCD-Konfigurationsassistent abgeschlossen haben, steht der Assistent nicht mehr zur Verfügung.

Über ein Netzwerk auf den CMC zugreifen

Nachdem Sie die CMC-Netzwerkeinstellungen konfiguriert haben, können Sie über verschiedene Schnittstellen im Remote-Zugriff auf den CMC zugreifen: Tabelle 2-1 listet die Schnittstellen auf, die Sie für den Remote-Zugriff auf CMC verwenden können.

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

Tabelle 2-1. CMC-Schnittstellen

Schnittstelle	Beschreibung
Webschnittstelle	Ermöglicht Remote-Zugriff auf den CMC über eine grafische Benutzeroberfläche. Die Webschnittstelle ist in die CMC-Firmware integriert und der Zugriff erfolgt von einem unterstützten Webbrowser auf der Management Station über die NIC-Schnittstelle. Eine Liste der unterstützten Webbrowser finden Sie im Abschnitt „Unterstützte Webbrowser“in der *Dell Systems Software Support Matrix* unter **support.dell.com/manuals**.
Remote-RACADM-Befehlszeilenschnittstelle	Ermöglicht den Remote-Zugriff auf den CMC von einer Management Station über eine Befehlszeilenschnittstelle (CLI). Remote-RACADM verwendet die Option **racadm -r** mit der IP-Adresse des CMC, um Befehle auf dem CMC auszuführen. Weitere Informationen zum Remote-racadm finden Sie unter „RACADM im Remote-Zugriff aufrufen“ auf Seite 88 und den folgenden Abschnitten.
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 ein unsicheres Protokoll, das alle Daten, einschließlich Kennwörtern, als Klartext überträgt. Verwenden Sie bei Übertragung vertraulicher Informationen die SSH-Schnittstelle.

Tabelle 2-1. CMC-Schnittstellen *(fortgesetzt)*

Schnittstelle	Beschreibung
SSH	Bietet dieselben Fähigkeiten wie Telnet unter Verwendung einer verschlüsselten Transportschicht für höhere Sicherheit.

ANMERKUNG: Der Standard-Benutzername lautet **root** und das Standardkennwort **calvin**.

Sie können über die CMC-Netzwerkschnittstelle mit einem unterstützten Webbrowser auf die CMC- und iDRAC-Webschnittstellen zugreifen; Sie können sie auch vom Dell Server Administrator oder Dell OpenManage IT Assistant starten.

Eine Liste der unterstützten Webbrowser finden Sie im Abschnitt „Unterstützte Webbrowser“in der *Dell Systems Software Support Matrix* unter **support.dell.com/manuals**. Um auf den CMC zuzugreifen, verwenden Sie einen unterstützten Webbrowser, siehe „Auf die CMC-Webschnittstelle zugreifen“ auf Seite 121.

Um mit dem Dell Server Administrator auf die CMC-Schnittstelle zuzugreifen, starten Sie Server Administrator auf der Management Station. Von der Systemstruktur im linken Fensterbereich der Server Administrator-Startseite klicken Sie auf **System→ Hauptsystemgehäuse→ Remote-Access-Controller**. Weitere Informationen finden Sie im *Dell Server Administrator-Benutzerhandbuch*.

Um auf die CMC Befehlszeile mit Telnet oder SSH zuzugreifen, lesen Sie bitte „CMC zur Verwendung von Befehlszeilenkonsolen konfigurieren“ auf Seite 65.

Weitere Informationen über die Verwendung von RACADM finden Sie unter „RACADM-Befehlszeilenschnittstelle verwenden“ auf Seite 81.

Weitere Informationen zur Verwendung der Befehle **connect** oder **racadm connect** für Verbindungen zu den Servern und E/A-Modulen finden Sie unter „Verbindung zu Servern oder Modulen mit dem connect-Befehl herstellen“ auf Seite 72.

Installieren oder Aktualisieren der CMC-Firmware

Der folgende Abschnitt beschreibt die Installation oder Aktualisierung der CMC-Firmware.

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.

Die folgenden Softwarekomponenten sind im CMC-Firmwarepaket enthalten:

- Kompilierter CMC-Firmware-Code und -Daten
- Webschnittstelle JPEG und weitere Dateien mit Benutzerschnittstellendaten
- Standard-Konfigurationsdateien

ANMERKUNG: Während der Aktualisierung von CMC-Firmware laufen einige oder alle Lüftereinheiten im Gehäuse mit 100 % Leistung.

ANMERKUNG: Die Firmware-Aktualisierung behält standardmäßig die aktuellen CMC-Einstellungen bei. Während des Aktualisierungsvorgangs haben Sie die Möglichkeit, die CMC-Konfigurationseinstellungen auf die werkseitigen Voreinstellungen zurückzusetzen.

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

Sie können den RACADM-Befehl **getsysinfo** (siehe Abschnitt **getsysinfo**-Befehl im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*) oder die Seite **Gehäusezusammenfassung** (siehe „Aktuelle Firmware-Versionen anzeigen“ auf Seite 232) verwenden, um die aktuellen Firmwareversionen der CMCs in Ihrem Gehäuse anzuzeigen.

Wenn Sie über einen Standby-CMC verfügen, sollten Sie beide CMCs gleichzeitig in einem Vorgang aktualisieren. 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. (Hilfe zum Rollentausch finden Sie im Abschnitt zum **cmcchangeover**-Befehl im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*.) Damit können Sie überprüfen, ob die Aktualisierung erfolgreich war und die neue Firmware einwandfrei funktioniert, bevor Sie die Firmware für den zweiten CMC aktualisieren. Nachdem beide CMCs aktualisiert wurden, können Sie den Befehl **cmcchangeover** verwenden, um die vorhergehenden Rollen der CMCs wiederherzustellen. Die CMC Firmwareversion 2.x aktualisiert sowohl den primären CMC wie auch den redundanten CMC ohne Verwendung des **cmcchangeover**-Befehls.

CMC-Firmware über die Webschnittstelle aktualisieren

Anleitungen zur Verwendung der Webschnittstelle, um die CMC-Firmware zu aktualisieren, finden Sie unter „CMC-Firmware aktualisieren“ auf Seite 234.

Aktualisieren der CMC-Firmware über RACADM

Anweisungen zur Verwendung des RACADM-Unterbefehls **fwupdate** zur Aktualisierung der CMC-Firmware finden Sie im Abschnitt **fwupdate**-Befehl im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*.

CMC-Eigenschaften konfigurieren

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

Weitere Informationen zur Verwendung der Internetschnittstelle finden Sie unter „Auf die CMC-Webschnittstelle zugreifen“ auf Seite 121. Weitere Informationen über die Verwendung von RACADM finden Sie unter „RACADM-Befehlszeilenschnittstelle verwenden“ auf Seite 81.

VORSICHTSHINWEIS: Die Verwendung von mehr als einem CMC-Konfigurationshilfsprogramm zur gleichen Zeit kann zu unerwarteten Ergebnissen führen.

Strombudget konfigurieren

Der CMC bietet einen Strombudgetdienst, mit dem Sie Strombudget, Redun-danz 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.

Weitere Informationen über die Stromverwaltung des CMC finden Sie unter „Stromverwaltung“ auf Seite 363.

Anleitungen zum Konfigurieren des Strombudgets und anderer Energieeinstel-lungen über die Webschnittstelle finden Sie unter „Strombudget konfigurieren“ auf Seite 231.

CMC-Netzwerkeinstellungen konfigurieren

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

Sie können die CMC-Netzwerkeinstellungen mit einem der folgenden Konfigu-rationshilfsprogramme konfigurieren:

- RACADM – Weitere Informationen dazu finden Sie unter „Mehrere CMCs in mehreren Gehäusen konfigurieren“ auf Seite 110.

ANMERKUNG: Wird der CMC in einer Linux-Umgebung bereitgestellt, finden Sie entsprechende Informationen unter „RACADM auf einer Linux-Management Station installieren“ auf Seite 39.

- Webschnittstelle – Weitere Informationen dazu finden Sie unter „CMC-Netzwerkeigenschaften konfigurieren“ auf Seite 174.

Benutzer hinzufügen und konfigurieren

Sie können CMC-Benutzer entweder über RACADM oder die CMC-Webschnittstelle hinzufügen und konfigurieren. Sie können auch Microsoft Active Directory zum Verwalten von Benutzern verwenden.

Anweisungen zum Hinzufügen und Konfigurieren von Benutzern mit öffentlichen Schlüsseln für den CMC mithilfe von RACADM finden Sie unter „Verwendung von RACADM zum Konfigurieren der Authentifizierung mit öffentlichem Schlüssel über SSH“ auf Seite 104. Anleitungen zum Hinzufügen und Konfigurieren von Benutzern mittels Webschnittstelle finden Sie unter „CMC-Benutzer hinzufügen und konfigurieren“ auf Seite 188.

Für Anleitungen zur Verwendung von Active Directory mit dem CMC finden Sie unter „CMC-Verzeichnisdienst verwenden“ auf Seite 309.

Hinzufügen von SNMP- und E-Mail-Warnungen

Sie können den CMC so konfigurieren, dass bei bestimmten Gehäuseereignissen SNMP- oder E-Mail-Warnungen erzeugt werden. Weitere Informationen finden Sie unter „Konfiguration von SNMP-Alarmen“ auf Seite 474 und „Konfiguration von E-Mail-Benachrichtigungen“ auf Seite 481.

Remote-Syslog konfigurieren

Die Funktion *Remote-Syslog* wird entweder über die CMC-GUI oder über den **racadm**-Befehl aktiviert oder konfiguriert. Zu den Konfigurationsoptionen gehören der Syslog-Servername (bzw. die IP-Adresse) und die UDP-Schnitt-stelle, die vom CMC verwendet wird, um die Protokolleinträge weiterzuleiten. Sie können in der Konfiguration bis zu 3 verschiedene Syslog-Serverziele angeben. 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: Da das Netzwerkübertragungsprotokoll für die weitergeleiteten Protokolleinträge UDP ist, gibt es weder eine Garantie, dass Protokolleinträge zugestellt werden, noch gibt es Feedback an den CMC darüber, ob die Protokolleinträge erfolgreich empfangen wurden.

So konfigurieren Sie die CMC-Dienste:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie auf das Register **Netzwerk**.
3. Klicken Sie auf das Unterregister **Dienste**. Die Seite **Dienste** wird angezeigt.

Weitere Informationen über das Konfigurieren des Remote-Syslog finden Sie unter Tabelle 5-58.

Die redundante CMC-Umgebung verstehen

Sie können einen Standby-CMC installieren, der aktiviert wird, wenn der aktive CMC ausfällt. Ihr redundanter CMC kann vorinstalliert sein oder zu einem späteren Zeitpunkt hinzugefügt werden. Es ist wichtig, dass das CMC-Netzwerk korrekt verkabelt ist, um volle Redundanz bzw. optimale Leistung zu gewährleisten.

Failover-Ereignisse können auftreten, wenn:

- Der RACADM-Befehl **cmcchangeover** ausgeführt wird. (Lesen Sie den Abschnitt zum **cmcchangeover**-Befehl im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC.)*
- Der RACADM-Befehl **racreset** auf dem aktiven CMC ausgeführt wird. (Lesen Sie den Abschnitt zum **racreset**-Befehl im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC.)*
- Setzen Sie den aktiven CMC über die Webschnittstelle zurück. (Siehe Option **Reset CMC** für **Stromsteuerungsvorgänge**, Beschreibung unter „Durchführen von Energieverwaltungsmaßnahmen am Gehäuse“ auf Seite 409.)
- 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 funktioniert nicht mehr.

ANMERKUNG: Im Falle eines CMC-Failovers gehen alle iDRAC-Verbindungen und alle aktiven CMC-Sitzungen verloren. Benutzer mit verlorenen 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 herabgesetzte Redundanz.

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 Standby-CMC finden Sie im *Hardware-Benutzerhandbuch*. Für Anleitungen zur Installation der CMC-Firmware auf Ihrem Standby-CMC, folgenden Sie den Anweisungen unter „Installieren oder Aktualisieren der CMC-Firmware“ auf Seite 56.

CMC-Failsafe-Modus

Ähnlich wie beim Failover-Schutz, der durch den redundanten CMC angeboten wird, aktiviert das M1000e-Gehäuse im Failsafe-Modus den Failsafe-Modus, um die Blades und die E/A-Module vor Ausfällen und Fehlern zu schützen. Der Failsafe-Modus wird aktiviert, wenn kein CMC durch das Gehäuse gesteuert wird. Während des CMC-Failover-Zeitraums oder während des Verlusts einer einzelnen CMC-Verwaltung:

- können Sie neu installierte Blades nicht einschalten.
- können Sie nicht per Remote auf vorhandene Blades zugreifen.
- laufen die Gehäusekühllüfter bei 100 %, um die Komponenten vor Überhitzung zu schützen.
- wird die Blade-Leistung reduziert, um den Stromverbrauch zu reduzieren, bis die Verwaltung des CMC wiederhergestellt ist.

Im Folgenden finden Sie einige der Bedingungen, die aus dem Verlust der CMC-Verwaltung resultieren können:

- Entfernen des CMC – Die Gehäuseverwaltung wird wieder aufgenommen, nachdem der CMC ausgetauscht wurde oder nachdem ein Failover auf dem Standby-CMC aufgetreten ist.
- Entfernen des CMC-Netzwerkkabels oder Verlust der Netzwerkverbindung – Die Gehäuseverwaltung wird wieder aufgenommen, nachdem das Gehäuse auf den Standby-CMC umgeschaltet wurde. Der Netzwerk-Failover wird nur im redundanten CMC-Modus aktiviert.
- Zurücksetzen des CMC – Die Gehäuseverwaltung wird wiederaufgenommen, nachdem der CMC neu gestartet oder das Gehäuse auf den Standby-CMC umgeschaltet wurde.
- Befehl für CMC-Failover ausgegeben – Die Gehäuseverwaltung wird nach dem Umschalten des Gehäuses auf den Standby-CMC wieder aufgenommen.
- 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 das 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. Bei redundanten CMC-Konfigurationen und wenn der primäre CMC die Verbindung mit dem Gehäuse oder dem Verwaltungsnetzwerk verliert, übernimmt der Standby-CMC die Gehäuseverwaltung.

Aktiver CMC – Auswahlprozess

Die beiden CMC-Steckplätze unterscheiden sich nicht; das bedeutet, dass der Steckplatz alleine nicht eine 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 (links) 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/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 „Gehäuse- und Komponenten-Zusammenfassungen anzeigen“ auf Seite 146.

3

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. Informationen zur Verwendung der RACADM-Befehle im CMC über die Befehlszeilenkonsole finden Sie unter „RACADM-Befehlszeilenschnittstelle verwenden“ auf Seite 81.

Funktionen der Befehlszeilenkonsole auf dem CMC

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 Protokoll.
- Steuerung der Sitzungszeitüberschreitung auf allen Konsolen-Schnittstellen.

Verwendung einer seriellen, Telnet- oder SSH-Konsole

Wenn Sie zur CMC-Befehlszeile verbinden, können Sie folgende Befehle eingeben:

Tabelle 3-1. CMC-Befehlszeilenbefehle

Befehl	Beschreibung
racadm	RACADM-Befehle beginnen mit dem Stichwort **racadm** und werden von einem Unterbefehl wie **getconfig**, **serveraction** oder **getsensorinfo** gefolgt. Beachten Sie „RACADM-Befehlszeilenschnittstelle verwenden“ auf Seite 81 für Details zur Verwendung von RACADM-Befehlen.
connect	Verbindet sich mit der seriellen Konsole eines Servers oder eines E/A-Moduls. „Verbindung zu Servern oder Modulen mit dem connect-Befehl herstellen“ auf Seite 72 enthält Hilfe bei der Verwendung des **connect**-Befehls. **ANMERKUNG:** Es kann auch der **racadm connect**-Befehl verwendet werden.
exit, logout und quit	Alle diese Befehle führen die gleiche Maßnahme aus: sie beenden die aktuelle Sitzung und kehren zu einer Anmeldungseingabeaufforderung zurück.

Telnet-Konsole mit dem CMC verwenden

Bis zu vier Telnet-Client-Systeme und vier SSH-Clients können zu jederzeit angeschlossen werden.

Wenn auf Ihrer Verwaltungsstation Windows XP oder Windows 2003 ausgeführt wird, tritt möglicherweise ein Problem mit den Zeichen in einer CMC-Telnet-Sitzung auf. Dieses Problem kann in der Form einer eingefrorenen Anmeldung auftreten, bei der die Eingabetaste nicht reagiert und die Eingabeaufforderung für das Kennwort nicht angezeigt wird.

Um dieses Problem zu beheben, laden Sie Hotfix 824810 von der Microsoft Support-Website unter **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. Der CMC unterstützt SSH Version 2 mit Kennwortauthentifizierung. SSH ist beim CMC standardmäßig aktiviert.

ANMERKUNG: Der CMC unterstützt die SSH-Version 1 nicht.

Wenn während des Anmeldeverfahrens ein Fehler auftritt, gibt der SSH-Client eine Fehlermeldung aus. Der Meldungstext ist vom Client abhängig und wird nicht vom CMC gesteuert. Überprüfen Sie die RACLog-Meldungen, um die Ursache für den Fehler zu bestimmen.

ANMERKUNG: `OpenSSH` sollte 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 für Linux SSH-Client-Dienste aus, um über beliebige Shells eine Verbindung zum CMC herzustellen.

Vier gleichzeitige SSH-Sitzungen werden jeweils zu einem gegebenen Zeit unterstützt. Die Sitzungszeitüberschreitung wird durch die Eigenschaft `cfgSsnMgtSshIdleTimeout` gesteuert. Lesen Sie für weitere Informationen das Kapitel Datenbankeigenschaften des *RACADM Befehlszeilen-Referenzhandbuchs für iDRAC6 und CMC*, die Seite **Diensteverwaltung** in der Webschnittstelle, oder lesen Sie „Dienste konfigurieren“ auf Seite 221.

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 „Verwendung von RACADM zum Konfigurieren der Authentifizierung mit öffentlichem Schlüssel über SSH“ auf Seite 104.

SSH auf dem CMC aktivieren

SSH ist standardmäßig aktiviert. Falls SSH deaktiviert ist, können Sie die Option mit jeder anderen unterstützten Schnittstelle aktivieren.

Anleitungen zum Aktivieren von SSH-Verbindungen auf dem CMC unter Verwendung von RACADM sind im Abschnitt **config**-Befehl und im Abschnitt **cfgSerial**-Datenbankeigenschaft im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC* zu finden. Eine Anleitung zum Aktivieren von SSH-Verbindungen auf dem CMC unter Verwendung der Webschnittstelle finden Sie unter „Dienste konfigurieren“ auf Seite 221.

SSH-Schnittstelle ändern

Verwenden Sie den folgenden Befehl, um die SSH-Schnittstelle zu ändern:

```
racadm config -g cfgRacTuning -o cfgRacTuneSshPort
<port mumber>
```

Weitere Informationen über die Eigenschaften von `cfgSerialSshEnable` und `cfgRacTuneSshPort` finden Sie im Kapitel zu den Datenbankeigenschaften des *RACADM-Befehlszeilen-Referenzhandbuchs für iDRAC6 und CMC*.

Die CMC-SSH-Umsetzung unterstützt mehrfache Verschlüsselungsschemata gemäß Tabelle 3-2.

Tabelle 3-2. 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

Frontblende für iKVM-Verbindung aktivieren

Informationen und Anleitungen zur Verwendung der iKVM-Fronblenden-Schnittstellen finden Sie unter „Frontblende aktivieren oder deaktivieren“ auf Seite 440.

Terminalemulationssoftware konfigurieren

Ihr 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 Ihre Art der Terminalsoftware zu konfigurieren, führen Sie die in den folgenden Abschnitten aufgeführten Schritte aus.

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. Verwenden Sie die Informationen in „Erforderliche Minicom-Einstellungen“ auf Seite 71 zur Konfiguration anderer Minicom-Versionen.

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 13 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 **Setup als config_name speichern** aus und drücken Sie die Taste <Eingabe>.

11 Wählen Sie **Minicom beenden** aus und drücken Sie die Taste <Eingabe>.

12 An der Befehls-Shell-Eingabeaufforderung geben Sie `minicom <Minicom config file name>` ein

13 Drücken Sie <Strg+a>, <x>, <Eingabe>, um Minicom zu beenden.

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 Tabelle 3-3 zum Konfigurieren einer beliebigen Minicom-Version.

Tabelle 3-3. 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 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 Umleitung der seriellen Konsole auf verschiedene Arten erzielt werden:

- über die CMC-Befehlszeile mit dem **connect**- oder **racadm connect**-Befehl. Lesen Sie für weitere Informationen über **connect** unter dem **racadm connect**-Befehl im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC* nach.
- Verwendung der seriellen Konsolenumleitungsfunktion der iDRAC-Webschnittstelle.
- Verwendung der 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 EAMs 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.

VORSICHTSHINWEIS: 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 Abmeldung, wenn eine Verbindung zu einem Server über die serielle CMC-Konsole hergestellt wird.

ANMERKUNG: Wenn ein 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>\.

Es gibt bis zu sechs EAMs im verwalteten System. Um eine Verbindung zu einem EAM herzustellen geben Sie folgendes ein:

`connect switch-`*n*

wobei *n* eine EAM-Kennung A1, A2, B1, B2, C1 und C2 ist.

(Beachten Sie Abbildung 11-1 für eine Veranschaulichung der Positionierung der EAMs im Gehäuse.) Wenn Sie sich beim **connect**-Befehl auf die EAMs beziehen, werden die EAMs Switches zugewiesen (siehe Tabelle 3-4).

Tabelle 3-4. E/A-Module zu Switches zuweisen

Bezeichnung des E/A-Moduls	Switch
A1	switch-a1 oder switch-1
A2	switch-a2 oder switch-2
B1	switch-b1 oder switch-3
B2	switch-b2 oder switch-4
C1	switch-c1 oder switch-5
C2	switch-c2 oder switch-6

ANMERKUNG: Es kann jeweils nur eine EAM-Verbindung pro Gehäuse aktiv sein.

ANMERKUNG: Von der seriellen Konsole aus kann keine Verbindung zu Passthroughs hergestellt werden.

Um eine Verbindung zu einer seriellen Konsole eines verwalteten Servers herzustellen, verwenden Sie den Befehl **connect server-n**, wobei *-n* die Steckplatznummer des Servers 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 `Keine Route zum Host`.

Der Befehl **connect server-n** ermöglicht dem Benutzer Zugriff auf die serielle Schnittstelle Server. Sobald diese Verbindung hergestellt ist, kann der Benutzer die Konsolenumleitung des Servers über die serielle Schnittstelle des CMC sehen, die sowohl die serielle BIOS-Boot-Konsole als auch die serielle Betriebssystemkonsole umfasst.

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

ANMERKUNG: Nicht alle Tasten auf den BIOS-Setup-Bildschirmen funktionieren; Sie sollten daher entsprechende Escape-Sequenzen für **STRG+ALT+ENTF** und andere Escape-Sequenzen angeben. Der anfängliche Umleitungsbildschirm zeigt die benötigten Escape-Sequenzen an.

BIOS des verwalteten Servers für die serielle Konsolenumleitung konfigurieren

Es ist erforderlich, mit dem iKVM eine Verbindung zum verwalteten Server herzustellen (siehe „Server mit iKVM verwalten“ auf Seite 427) oder über die iDRAC-Web-GUI eine Remote-Konsolen-Sitzung aufzubauen (siehe *iDRAC-Benutzerhandbuch* unter **support.dell.com/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. Starten Sie den verwalteten Server.
2. Drücken Sie <F2>, um das BIOS-Setup-Dienstprogramm während POST aufzurufen.
3. Scrollen Sie zu **Serielle Kommunikation** herunter und drücken Sie die Taste <Eingabe>. Im Popup-Dialogfeld wird die Liste der seriellen Kommunikation mit den folgenden Optionen angezeigt:
   - „Off“ (Aus)
   - Ein ohne Konsolenumleitung
   - Ein mit Konsolenumleitung über COM1

   Verwenden Sie die Pfeiltasten, um zwischen diesen Optionen hin und her zu schalten.
4. Stellen Sie sicher, dass **Ein mit Konsolenumleitung über COM1** aktiviert ist.
5. Aktivieren Sie **Umleitung nach Start** (Standardwert ist **deaktiviert**). Durch diese Option wird die BIOS-Konsolenumleitung für nachfolgende Neustarts aktiviert.
6. Speichern Sie die Änderungen und beenden Sie.
7. Der verwaltete Server startet neu.

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 wären erforderlich, um einen anderen Bootloader zu verwenden.

ANMERKUNG: Beim Konfigurieren des Client-VT100-Emulationsfensters stellen Sie das Fenster bzw. die Anwendung, die die umgeleitete Konsole anzeigt, auf 25 Reihen x 80 Spalten ein, um eine korrekte Textanzeige sicherzustellen; andernfalls werden einige Textanzeigen möglicherweise unleserlich dargestellt.

Bearbeiten Sie die Datei **/etc/grub.conf** wie folgt:

1. Suchen Sie die allgemeinen Einstellungsabschnitte in der Datei und fügen Sie die folgenden zwei Zeilen hinzu:

   ```
   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 generated by anaconda
#
# Note that you do not have to rerun grub after making
changes
# to this file
# NOTICE: You do not have a /boot partition. This
means that
#          all kernel and initrd paths are relative to
/, e.g.
```

```
#          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=
ttyS1,57600
   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
   initrd /boot/initrd-2,4.9-e.3.img
```

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
```

Bearbeiten Sie die Datei **/etc/securetty** wie folgt:

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
```

4

RACADM-Befehlszeilenschnittstelle verwenden

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 iKVM oder im Remote-Zugriff unter Verwendung der auf einer Management Station installierten RACADM-Befehlszeilenschnittstelle.

Die RACADM-Schnittstelle wird wie folgt klassifiziert:

ANMERKUNG: Remote-RACADM ist Teil der *Dell Systems Management Tools and Documentation DVD* und wird auf einer Management Station installiert.

- 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.
- Firmware-RACADM – damit können Sie sich über Telnet, SSH, eine serielle Verbindung oder das iKVM 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. Der CMC unterstützt kein Scripting, was bedeutet, dass Sie keine Skripts direkt auf dem CMC ausführen können. Weitere Informationen zur gleichzeitigen Konfiguration mehrerer CMCs finden Sie unter „Mehrere CMCs in mehreren Gehäusen konfigurieren“ auf Seite 110.

Verwendung einer seriellen, Telnet- oder SSH-Konsole

Sie können sich am CMC entweder mit einer seriellen oder einer Telnet-/SSH-Verbindung anmelden oder über die Dell-CMC-Konsole auf dem iKVM. Informationen, um den CMC für seriellen oder Remote-Zugriff zu konfigurieren, finden Sie unter „CMC zur Verwendung von Befehlszeilenkonsolen konfigurieren“ auf Seite 65. Die gebräuchlichen Unterbefehlsoptionen sind in Tabelle 4-2 aufgelistet. Eine vollständige Liste der RACADM-Unterbefehle finden Sie im Kapitel „RACADM-Unterbefehle“ des *RACADM-Befehlszeilen-Referenzhandbuchs für iDRAC6 und CMC*.

Am CMC anmelden

Nachdem Sie die Terminalemulationssoftware Ihrer Management Station und den verwalteten Knoten im BIOS konfiguriert haben, führen Sie die folgenden Schritte aus, um sich am 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.

Textkonsole starten

Sie können sich über eine Telnet- oder SSH-Verbindung über ein Netzwerk, eine serielle Schnittstelle oder eine Dell CMC-Konsole über das iKVM am CMC anmelden. Öffnen Sie eine Telnet- oder SSH-Sitzung, stellen Sie eine Verbindung zum CMC her und melden Sie sich am CMC an.

Weitere Informationen über die CMC-Verbindung über das iKVM finden Sie unter „iKVM-Modul verwenden“ auf Seite 419.

RACADM verwenden

RACADM-Unterbefehle können im Remote-Zugriff von der Eingabeaufforderung der seriellen, Telnet- oder SSH-Konsole aus oder über eine normale Befehlseingabeaufforderung ausgeführt werden.

Verwenden Sie RACADM-Unterbefehle zum Konfigurieren von CMC-Eigenschaften und zum Ausführen von Remote-Verwaltungs-Tasks. Um eine Liste mit RACADM-Unterbefehlen anzuzeigen, geben Sie Folgendes ein:

```
racadm help
```

Bei Ausführung ohne Optionen oder Unterbefehle zeigt RACADM Syntax-Informationen und Anleitungen dazu an, wie Sie auf die Unterbefehle und die Hilfe zugreifen können. Um eine Liste mit Syntax- und Befehlszeilenoptionen zu einzelnen Unterbefehlen anzuzeigen, geben Sie Folgendes ein:

```
racadm help <subcommand>
```

RACADM-Unterbefehle

Tabelle 4-1 enthält eine kurze Liste mit allgemeinen in RACADM verwendeten Unterbefehlen. Eine vollständige Liste der RACADM-Unterbefehle, einschließlich Syntax und gültigen Einträgen, finden Sie im Kapitel „RACADM-Unterbefehle“ des *RACADM-Befehlszeilen-Referenzhandbuchs für iDRAC6 und CMC*.

ANMERKUNG: Der Befehl **connect** ist sowohl als RACADM-Befehl als auch als integrierter CMC-Befehl verfügbar. Die Befehle **exit, quit** und **logout** sind integrierte CMC-Befehle und nicht RACADM-Befehle. Keiner dieser Befehle kann mit Remote-RACADM verwendet werden. Informationen zur Verwendung dieser Befehle finden Sie unter „Verbindung zu Servern oder Modulen mit dem connect-Befehl herstellen“ auf Seite 72.

Tabelle 4-1. RACADM-Unterbefehle

Befehl	Beschreibung
Hilfe	Zeigt eine Liste mit Beschreibungen von CMC-Unterbefehlen an.
help <-*Unterbefehl*>	Zeigt eine Übersicht zur Verwendung des angegebenen Unterbefehls an.
?	Zeigt eine Liste mit Beschreibungen von CMC-Unterbefehlen an.
? <*Unterbefehl*>	Zeigt eine Übersicht zur Verwendung des angegebenen Unterbefehls an.
arp	Zeigt den Inhalt der ARP-Tabelle an. Es dürfen keine ARP-Tabelleneinträge hinzugefügt oder gelöscht werden.
chassisaction	Führt die Maßnahmen Einschalten, Ausschalten, Zurücksetzen sowie Aus- und Einschalten für Gehäuse, Switch und KVM aus.
closessn	Schließt eine Sitzung.
clrraclog	Löscht das CMC-Protokoll und erstellt einen einzelnen Eintrag, der angibt, von welchem Benutzer und zu welcher Uhrzeit das Protokoll gelöscht wurde.
clrsel	Löscht die Einträge des Systemereignisprotokolls.
cmcchangeover	Wechselt in redundanten CMC-Umgebungen den Status des CMC von „Aktiv“ zu „Standby“ oder umgekehrt.
config	Konfiguriert den CMC.
connect	Verbindet sich mit der seriellen Konsole eines Servers oder eines E/A-Moduls. Siehe „Verbindung zu Servern oder Modulen mit dem connect-Befehl herstellen“ auf Seite 72 für Hilfe bei der Verwendung des **connect-**Unterbefehls.
deploy	Stellt einen Server durch Angabe erforderlicher Eigenschaften bereit.
feature	Zeigt aktive Funktionen und Funktionsdeaktivierung an.
featurecard	Zeigt Statusinformationen der Funktionskarte an.
fwupdate	Führt Aktualisierungen der Firmware der Systemkomponenten durch und zeigt den Status der Firmwareaktualisierung an.
getassettag	Zeigt die Systemkennnummer für das Gehäuse an.
getchassisname	Zeigt den Namen des Gehäuses an.

Tabelle 4-1. RACADM-Unterbefehle *(fortgesetzt)*

Befehl	Beschreibung
getconfig	Zeigt die aktuellen CMC-Konfigurationseigenschaften an.
getdcinfo	Zeigt allgemeine Fehlkonfigurationsinformationen von E/A-Modulen und Tochterkarten an.
getfanreqinfo	Zeigt Lüfteranforderung für Server und Switches in % an.
getflexaddr	Zeigt den Status aktiviert/deaktiviert von FlexAddress auf Basis der einzelnen Steckplätze/Strukturen an. Bei Verwendung mit der Option `-i` zeigt der Befehl die WWN- und MAC-Adresse für einen bestimmten Steckplatz an.
getioinfo	Zeigt allgemeine E/A-Modulinformationen an.
getkvminfo	Zeigt Informationen über das iKVM an.
getled	Zeigt die LED-Einstellungen auf einem Modul an.
getmacaddress	Zeigt die MAC-Adresse eines Servers an.
getmodinfo	Zeigt die Konfigurations- und Statusinformationen eines Moduls an.
getniccfg	Zeigt die derzeitige IP-Konfiguration für den Controller an.
getpbinfo	Zeigt Strombudget-Statusinformationen an.
getpminfo	Zeigt Energieverwaltungs-Statusinformationen an.
getraclog	Zeigt das CMC-Protokoll an.
getractime	Zeigt die CMC-Uhrzeit an.
getredundancymode	Zeigt den Redundanzmodus des CMC an.
getsel	Zeigt das Systemereignisprotokoll (Hardwareprotokoll) an.
getsensorinfo	Zeigt Informationen zu Systemsensoren an.
getslotname	Zeigt den Namen eines Steckplatzes im Gehäuse an.
getssninfo	Zeigt Informationen über aktive Sitzungen an.
getsvctag	Zeigt Service-Tag-Nummern an.
getsysinfo	Zeigt allgemeine Informationen zum CMC und zum System an.
gettracelog	Zeigt das CMC-Ablaufprotokoll an. Bei Verwendung mit der Option `-i` zeigt der Befehl eine Anzahl von Einträgen im CMC-Ablaufprotokoll an.

Tabelle 4-1. RACADM-Unterbefehle *(fortgesetzt)*

Befehl	Beschreibung
getversion	Zeigt die aktuelle Software-Version und Modellinformationen an und gibt Auskunft darüber, ob das Gerät aktualisiert werden kann.
ifconfig	Zeigt die aktuelle CMC-IP-Konfiguration an.
krbkeytabupload	Lädt ein Kerberos-Keytab auf den CMC.
netstat	Zeigt die Routingtabelle und die aktuellen Verbindungen an.
ping	Überprüft, ob die Ziel-IPv4-Adresse vom CMC mit den Inhalten der aktuellen Routing-Tabelle aus erreichbar ist.
ping6	Überprüft, ob die Ziel-IPv4-Adresse vom CMC mit den Inhalten der aktuellen Routing-Tabelle aus erreichbar ist.
racdump	Zeigt die umfassenden Gehäuse- und Konfigurationsstatusinformationen sowie alle historischen Ereignisprotokolle an. Wird zur Überprüfung der Konfiguration nach der Zuweisung und während Debugging-Sitzungen verwendet.
racreset	Setzt den CMC zurück.
racresetcfg	Setzt den CMC auf die Standardkonfiguration zurück.
remoteimage	Verbinden, Trennen oder Bereitstellen einer Datenträgerdatei auf einem Remote-Server.
serveraction	Führt Energieverwaltungsvorgänge auf dem verwalteten System aus.
setassettag	Legt die Systemkennnummer für das Gehäuse fest.
setchassisname	Legt den Namen des Gehäuses fest.
setflexaddr	Aktiviert/deaktiviert FlexAddress auf einem bestimmten Steckplatz/Struktur, wenn die Funktion FlexAddress für das Gehäuse aktiviert ist.
setled	Legt die LED-Einstellungen auf einem Modul fest.
setniccfg	Stellt die IP-Konfiguration für den Controller ein.
setractime	Legt die CMC-Uhrzeit fest.
setslotname	Legt den Namen eines Steckplatzes im Gehäuse fest.
setsysinfo	Legt den Namen und den Standort des Gehäuses fest.

Tabelle 4-1. RACADM-Unterbefehle *(fortgesetzt)*

Befehl	Beschreibung
sshpkauth	Lädt bis zu 6 verschiedene öffentliche SSSH-Schlüssel hoch, löschte vorhandene Schlüssel und zeigt die Schlüssel an, die bereits im CMC vorhanden sind.
sslcertdownload	Lädt ein von einer Zertifizierungsstelle unterzeichnetes Zertifikat herunter.
sslcertupload	Lädt ein von einer Zertifizierungsstelle unterzeichnetes Zertifikat oder Serverzertifikat auf den CMC hoch.
sslcertview	Zeigt ein von Zertifizierungsstelle unterzeichnetes Zertifikat oder Serverzertifikat auf dem CMC an.
sslcsrgen	Erstellt die SSL-CSR und lädt sie herunter.
sslresetcfg	Regeneriert das selbstsignierte Zertifikat, das vom der grafischen CMC-Web-GUI verwendet wird.
testemail	Zwingt den CMC, eine E-Mail über den CMC NIC zu senden.
testfeature	Erlaubt Ihnen die Prüfung der Konfigurationsparameter einer bestimmten Funktion. Zum Beispiel wird das Testen der Active Directory-Konfiguration unter Verwendung einfacher Authentifizierung (Benutzername und Kennwort) oder unter Verwendung von Kerberos-Authentifizierung (einfache Anmeldung oder Smart Card-Anmeldung) unterstützt.
testtrap	Zwingt den CMC, ein SNMP über die CMC-Netzwerkschnittstelle zu senden.
traceroute	Druckt die Route der IPv4-Pakete zu einem Netzwerkknoten.
traceroute6	Druckt die Route der IPv6-Pakete zu einem Netzwerkknoten.

RACADM im Remote-Zugriff aufrufen

Tabelle 4-2. Optionen für die Remote-RACADM-Unterbefehle

Option	Beschreibung
`-r <racIpAddr>`	Bestimmt die Remote-IP-Adresse des Controllers.
`-r <racIpAddr>:<port>`	Verwenden Sie *<Schnittstellennummer>*, wenn die CMC-Schnittstellennummer nicht der Standardschnittstelle (443) entspricht.
`-i`	Weist RACADM an, den Benutzer interaktiv nach dem Benutzernamen und dem Kennwort zu fragen.
`-u <userName>`	Gibt den Benutzernamen an, der verwendet wird, um die Befehlstransaktion zu authentifizieren. Wenn die Option **-u** verwendet wird, muss die Option **-p** verwendet werden und die Option **-i** (interaktiv) darf nicht verwendet werden.
`-p <password>`	Gibt das Kennwort an, das zur Authentifizierung der Befehlstransaktion verwendet wird. Wenn die Option **-p** verwendet wird, ist die Option **-i** nicht zulässig.

Um RACADM im Remote-Zugriff aufzurufen, geben Sie die folgenden Befehle ein:

`racadm -r <CMC-IP-Adresse> -u <userName> -p <password> <subcommand> <subcommand options>`
`racadm -i -r <CMC-IP-Adress> <subcommand> <subcommand options>`

ANMERKUNG: Die Option **-i** weist RACADM an, die Eingabe des Benutzernamens und des Kennworts interaktiv anzufordern. Ohne die Option **-i** müssen der Benutzername und das Kennwort mit dem Befehl unter Verwendung der Optionen **-u** und **-p** angegeben werden.

Beispiel:

```
racadm -r 192.168.0.120 -u root -p calvin getsysinfo
racadm -i -r 192.168.0.120 getsysinfo
```

Wenn die HTTPS-Schnittstellennummer des CMC auf eine von der Standardschnittstelle (443) abweichende benutzerdefinierten Schnittstelle geändert wurde, muss die folgende Syntax verwendet werden:

```
racadm -r <CMC-IP-Adress>:<port> -u <userName> -p
<password> <subcommand> <subcommand options>
```

```
racadm -i -r <CMC-IP-Adress>:<port> <subcommand>
<subcommand options>
```

RACADM-Remote-Fähigkeit aktivieren und deaktivieren

ANMERKUNG: Dell empfiehlt, dass diese Befehle am Gehäuse ausgeführt werden.

Die RACADM-Remote-Fähigkeit ist standardmäßig auf dem CMC aktiviert. In den folgenden Befehlen gibt **-g** die Konfigurationsgruppe an, zu der das Objekt gehört, und **-o** das Konfigurationsobjekt, das konfiguriert werden soll. Zum Deaktivieren der RACADM-Remote-Fähigkeit geben Sie Folgendes ein:

```
racadm config -g cfgRacTuning -o
cfgRacTuneRemoteRacadmEnable 0
```

Um die RACADM-Remote-Fähigkeit wieder zu aktivieren, geben Sie Folgendes ein:

```
racadm config -g cfgRacTuning -o
cfgRacTuneRemoteRacadmEnable 1
```

RACADM im Remote-Zugriff verwenden

ANMERKUNG: Konfigurieren Sie die IP-Adresse auf dem CMC, bevor Sie die RACADM-Remote-Fähigkeit verwenden. Weitere Informationen zum Einstellen Ihres CMC finden Sie unter „Installation und Setup des CMC“ auf Seite 33.

Mit der Remote-Option (`-r`) der RACADM-Konsole können Sie eine Verbindung zum verwalteten System herstellen und RACADM-Unterbefehle von einer Remote-Konsole oder einer Management Station ausführen. Um die Remote-Fähigkeit zu verwenden, sind ein gültiger Benutzername (Option **`-u`**) und Kennwort (Option **`-p`**) sowie die CMC-IP-Adresse erforderlich.Prüfen Sie, ob Sie über die entsprechenden Berechtigungen verfügen, bevor Sie versuchen, RACADM im Remote-Zugriff aufzurufen. Um Ihre Benutzerberechtigungen anzuzeigen, geben Sie Folgendes ein:

`racadm getconfig -g cfguseradmin -i` *n*
wobei *n* Ihre Benutzer-ID (1-16) ist.
Wenn Sie Ihre Benutzer-ID nicht kennen, versuchen Sie verschiedene Werte für *n*.

ANMERKUNG: Die RACADM-Remote-Fähigkeit wird nur auf Management Stationen über einen unterstützten Browser unterstützt. Weitere Informationen finden Sie im Abschnitt „Unterstützte Internet-Browser“ in der *Dell Systems Software Support Matrix* unter **support.dell.com/manuals**.

ANMERKUNG: Wenn Sie die RACADM-Remote-Fähigkeit verwenden, müssen Sie über Schreibberechtigungen für die Ordner verfügen, für die Sie die RACADM-Unterbefehle, die Dateivorgänge einbeziehen, verwenden. Beispiel:

`racadm getconfig -f <Dateiname> -r <IP-Adress>`
oder
`racadm sslcertupload -t 1 -f c:\cert\cert.txt`

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
```

RACADM-Fehlermeldungen

Informationen zu RACADM-CLI-Fehlermeldungen finden Sie unter „Fehlerbehebung“ auf Seite 118.

RACADM zum Konfigurieren des CMC verwenden

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.

Am schnellsten lässt sich der CMC über die CMC-Webschnittstelle konfigurieren (siehe „CMC-Webschnittstelle verwenden“ auf Seite 121). Wenn Sie CLI- oder Skript-Konfigurationen bevorzugen oder mehrere CMCs konfigurieren müssen, verwenden Sie Remote-RACADM, das mit den CMC-Agenten auf der Management Station installiert wird.

CMC-Netzwerkeigenschaften konfigurieren

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

Ursprünglichen Zugriff auf den CMC einrichten

Dieser Abschnitt erklärt, wie die anfängliche CMC-Netzwerkkonfiguration mit RACADM-Befehlen ausgeführt wird. Alle in diesem Abschnitt beschriebenen Konfigurationsschritte können über die Frontblenden-LCD ausgeführt werden. Siehe „Netzwerkbetrieb mit dem LCD-Konfigurationsassistent konfigurieren“ auf Seite 46.

VORSICHTSHINWEIS: Die Änderung von Einstellungen über den Bildschirm „CMC-Netzwerkeinstellungen" kann Ihre aktuelle Netzwerkverbindung unterbrechen.

Weitere Informationen über Netzwerkunterbefehle finden Sie in den Kapiteln zu den RACADM-Unterbefehlen und Gruppen- und Objektdefinitionen der Eigenschaftendatenbank des *RACADM-Befehlszeilen-Referenzhandbuchs für iDRAC6 und CMC*.

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

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

Aktuelle IPv4-Netzwerkeinstellungen anzeigen

Um eine Zusammenfassung der NIC-, DHCP-, Netzwerkgeschwindigkeits- und Duplex-Einstellungen anzuzeigen, geben Sie Folgendes ein:

```
racadm getniccfg
```

oder

```
racadm getconfig -g cfgCurrentLanNetworking
```

Aktuelle IPv6-Netzwerkeinstellungen anzeigen

Um eine Zusammenfassung der Netzwerkeinstellungen anzuzeigen, geben Sie Folgendes ein:

```
racadm getconfig -g cfgIpv6LanNetworking
```

Um IPv4- und IPv6-Adressierungsinformationen anzuzeigen, geben Sie Folgendes ein:

```
racadm getsysinfo
```

Standardmäßig fordert der CMC automatisch eine CMC-IP-Adresse vom DHCP-Server (Dynamisches Host-Konfigurationsprotokoll) an und empfängt diese.

Sie können diese Funktion deaktivieren und eine statische CMC-IP-Adresse, ein statisches Gateway und eine statische Subnetzmaske bestimmen.

Um DHCP zu deaktivieren und eine statische CMC-IP-Adresse, ein Gateway und eine Subnetzmaske anzugeben, geben Sie Folgendes ein:

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

racadm config -g cfgLanNetworking -o cfgNicIpAddress
<static IP address>

racadm config -g cfgLanNetworking -o cfgNicGateway
<static gateway>

racadm config -g cfgLanNetworking -o cfgNicNetmask
<static subnet mask>
```

Aktuelle Netzwerkeinstellungen anzeigen

Um eine Zusammenfassung der NIC-, DHCP-, Netzwerkgeschwindigkeits- und Duplex-Einstellungen anzuzeigen, geben Sie Folgendes ein:

```
racadm getniccfg
```

oder

```
racadm getconfig -g cfgCurrentLanNetworking
```

Um Informationen zu IP-Adresse und DHCP, MAC-Adresse und DNS-Server-Informationen für das Gehäuse anzuzeigen, geben Sie Folgendes ein:

```
racadm getsysinfo
```

Konfigurieren der Netzwerk-LAN-Einstellungen

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

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

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

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

Aktivieren der CMC-Netzwerkschnittstelle

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

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

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

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

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

```
racadm config -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
<static IP address>

racadm config -g cfgLanNetworking -o cfgNicGateway
<static gateway>

racadm config -g cfgLanNetworking -o cfgNicNetmask
<static subnet mask>
```

Standardmäßig fordert der CMC für IPv6 automatisch eine CMC-IP-Adresse vom IPv6-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 address>

racadm config -g cfgIPv6LanNetworking -o
cfgIPv6PrefixLength 64

racadm config -g cfgIPv6LanNetworking -o
cfgIPv6Gateway <IPv6 address>
```

Aktivieren oder Deaktivieren von DHCP für die CMC-Netzwerkschnittstellenadresse

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

Sie können die Funktion „DHCP für NIC-Adresse“ deaktivieren und eine statische IP-Adresse, eine statische Subnetzmaske und ein statisches Gateway angeben. Weitere Informationen finden Sie unter „Ursprünglichen Zugriff auf den CMC einrichten“ auf Seite 91.

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-Adressen zu deaktivieren 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-Adressen“ für IPv6 zu deaktivieren und bevorzugte statische und alternative DNS-Server-Adressen festzulegen, 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- address>
racadm config -g cfgLanNetworking -o cfgDNSServer2
<IPv4-address>
```

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

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

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: Einige DNS-Server registrieren nur Namen mit höchstens 31 Zeichen. Stellen Sie sicher, dass sich der bestimmte Name im vom DNS verlangten Bereich befindet.

  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 –** Standardmäßig lautet der CMC-Name auf dem DNS-Server wie folgt: „cmc-<*service tag*>“. 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 Verhandlung ist standardmäßig aktiviert.

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

```
racadm config -g cfgNetTuning -o cfgNetTuningNicAutoneg 0
```

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

wobei

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

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

wobei

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

Einrichten von CMC-VLAN (IPv4 und IPv6)

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 priority>
   ```

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

Beispiel:

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

Sie können auch beides, VLAN-Kennung und VLAN-Priorität, in einem einzigen Befehl eingeben:

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

Beispiel:

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

Entfernen des CMC-VLAN

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
```

Einrichten eines Server-VLAN

Geben Sie die VLAN-Kennung und Priorität eines bestimmten Servers mit dem folgenden Befehl ein:

```
racadm setniccfg -m server-<n> -v <VLAN-ID>
<VLAN-Priority>
```

Gültige Werte für <*n*> sind 1 – 16.

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

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

Beispiel:

```
racadm setniccfg -m server-1 -v 1 7
```

Entfernen von Server-VLAN

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-<n> -v
```

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.

Einstellen der SMTP-Server-IP-Adresse (IPv4 und IPv6)

Sie können für den CMC die Funktion aktivieren, dass E-Mail-Warnungen mit dem einfachen Mail-Übertragungsprotokoll (SMTP) an eine angegebene IP-Adresse gesendet werden. Um diese Funktion zu aktivieren, geben Sie Folgendes ein:

```
racadm config -g cfgRemoteHosts -o
cfgRhostsSmtpServerIpAddr <SMTP IP address>
```

wobei die <*SMTP IP address*> die IP-Adresse des Netzwerk-SMTP-Servers ist.

ANMERKUNG: Wenn Ihr Netzwerk über einen SMTP-Server verfügt, der periodisch IP-Adressen vergibt und erneuert, und die Adressen unterschiedlich sind, funktioniert diese Einstellung der Eigenschaften während eines gewissen Zeitraums aufgrund einer Änderung in der festgelegten SMTP-Server-IP-Adresse nicht. Verwenden Sie in solchen Fällen den DNS-Namen.

Konfigurieren der Netzwerksicherheitseinstellungen (nur IPv4)

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

Aktivieren der IP-Bereichsüberprüfung (nur IPv4)

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**

RACADM zum Konfigurieren von Benutzern verwenden

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 RACADM-Befehl `racresetcfg` ausgeführt haben, ist der einzige aktuelle Benutzer `root` mit dem Kennwort `calvin`. Der Unterbefehl `racresetcfg` setzt den CMC auf die ursprünglichen Standardeinstellungen zurück.

VORSICHTSHINWEIS: Verwenden Sie den Befehl `racresetcfg` mit Vorsicht, da *alle* Konfigurationsparameter auf die ursprünglichen Standardeinstellungen zurückgesetzt werden. 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 den folgenden Befehl einmal für jeden Index von 1–16 ein:

```
racadm getconfig -g cfgUserAdmin -i <Index>
```

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.

ANMERKUNG: Wenn Sie einen Benutzer mit dem Unterbefehl racadm **`config`** manuell aktivieren oder deaktivieren, *muss* der Index mit der Option **`-i`** angegeben werden. Beobachten Sie, ob das im vorausgehenden Beispiel angezeigte Objekt **`cfgUserAdminIndex`** das Zeichen **#** enthält. 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 mehr Flexibilität beim Konfigurieren eines zweiten CMC mit denselben Einstellungen wie der Haupt-CMC.

CMC-Benutzer hinzufügen

Um einen neuen Benutzer zur CMC-Konfiguration hinzuzufügen, können Sie einige grundlegende Befehle verwenden. Führen Sie folgende Maßnahmen durch:

1. Legen Sie den Benutzernamen fest.
2. Legen Sie das Kennwort fest.
3. Legen Sie Benutzerberechtigungen fest. Weitere Informationen zu Benutzerberechtigungen finden Sie unter Tabelle 5-42 und Tabelle 5-43.
4. Aktivieren Sie den Benutzer.

Beispiel

Das folgende Beispiel erläutert, wie man einen neuen Benutzer mit dem Namen „John“ und dem Kennwort „123456“ mit ANMELDUNGS-Berechtigung zum CMC hinzufügt.

ANMERKUNG: In Tabelle 3-1 des Kapitels Datenbankeigenschaften im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC* finden Sie eine Liste der gültigen Bitmaskenwerte für bestimmte Benutzerberechtigungen. 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, verwenden Sie einen der folgenden Befehle:

```
racadm getconfig –g cfgUserAdmin –i 2
```

Verwendung von RACADM zum Konfigurieren der Authentifizierung mit öffentlichem Schlüssel über SSH

Sie können bis zu 6 öffentliche Schlüssel konfigurieren, die mit dem Dienst-Benutzernamen über die SSH-Schnittstelle verwendet werden können. Verwenden Sie vor dem Hinzufügen oder Löschen öffentlicher Schlüssel unbedingt den Anzeigebefehl, 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.

Beachten Sie vor dem Einrichten dieser Funktionen Folgendes:

- 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, da alle PKA-Benutzer den Dienst-Benutzernamen zur Anmeldung verwenden.

Beispiel: zwei öffentliche Schlüssel, einer mit Anmerkung PC1 und einer mit Anmerkung PC2:

```
racadm getssninfo

Type      User          IP Address        Login
Date/Time
SSH       PC1           x.x.x.x           06/16/2009
09:00:00
SSH       PC2           x.x.x.x           06/16/2009
09:00:00
```

Lesen Sie für weitere Informationen zu `sshpkauth` das *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*.

Generieren öffentlicher Schlüssel für Windows

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 Windows-Clients zum Erstellen des 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: Der 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-Option „dsa“ oder „rsa“ sein muss.

die Option **-b** gibt die Bit-Verschlüsselungsgröße zwischen 768 und 4096 an.

-C Option ermöglicht das Ändern der Anmerkung des öffentlichen Schlüssels und ist optional.

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 einen öffentlichen Schlüssel mit der Datei-Hochladen-Option (**-f**) zum CMC hinzuzufügen, geben Sie Folgendes ein:

```
racadm sshpkauth –I svcacct –k 1 –p 0xfff –f
<public key file>
```

ANMERKUNG: Sie können die Datei-Hochladen-Option nur mit Remote-RACADM verwenden. Weitere Informationen finden Sie unter „RACADM im Remote-Zugriff aufrufen“ auf Seite 88 und den folgenden Abschnitten.

Lesen Sie für weitere Informationen zu den Berechtigungen für öffentliche Schlüssel in Tabelle 3-1das Kapitel Datenbankeigenschaften im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*.

Um einen öffentlichen Schlüssel mit der Text-Hochladen-Option hinzuzufügen, geben Sie Folgendes ein:

```
racadm sshpkauth –I svcacct –k 1 –p 0xfff –t "<public key
text>"
```

Öffentliche Schlüssel löschen

Um einen öffentlichen Schlüssel zu löschen, geben Sie Folgendes ein:

```
racadm sshpkauth –i svcacct –k 1 –d
```

Um alle öffentlichen Schlüssel zu löschen, geben Sie Folgendes ein:

```
racadm sshpkauth –i svcacct –k all –d
```

Anmeldung mit Authentifizierung mit öffentlichem Schlüssel

Nachdem die öffentlichen Schlüssel hochgeladen wurden, sollten Sie sich über SSH beim CMC anmelden können, ohne ein Kennwort eingeben zu müssen. Sie können auch einen einzelnen RACADM-Befehl als Befehlszeilenargument an die SSH-Anwendung senden. Die Befehlszeilenoptionen verhalten sich wie Remote-RACADM, da die Sitzung endet, wenn der Befehl abgeschlossen ist. Beispiel:

Anmeldung:

```
ssh service@<domain>
```

Oder

```
ssh service@<IP_address>
```

wobei <*IP-Adress*> die IP-Adresse des CMC ist.

Senden von racadm-Befehlen:

```
ssh service@<Domain> racadm getversion
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 sowohl Windows- als auch Linux-Clients Methoden zur Automatisierung. Für Windows-Clients können Sie die Anwendung „Pageant“ verwenden. Sie läuft im Hintergrund und macht die Eingabe des Kennsatzes transparent. Für Linux-Clients können Sie die Anwendung „ssh-agent“ verwenden. Informationen über Einrichtung und Verwendung dieser Anwendungen finden Sie in der zur Anwendung gehörenden Dokumentation.

CMC-Benutzer mit Berechtigungen aktivieren

Um einen Benutzer mit spezifischen administrativen Berechtigungen (rollenbasierte Autorität) zu aktivieren, machen Sie zuerst einen verfügbaren Benutzer-Index ausfindig, indem Sie die Schritte unter „Bevor Sie beginnen“ auf Seite 33 ausführen. Geben Sie dann die folgenden Befehlszeilen mit dem neuen Benutzernamen und dem neuen Kennwort ein.

```
racadm config -g cfgUserAdmin -o
cfgUserAdminPrivilege -i <Index> <user privilege bitmask value>
```

ANMERKUNG: In Tabelle 3-1 des Kapitels Datenbankeigenschaften im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC* finden Sie eine Liste der gültigen Bitmaskenwerte für bestimmte Benutzerberechtigungen. Der Standard-Berechtigungswert ist 0, was darauf hinweist, dass der Benutzer über keine aktivierten Berechtigungen verfügt.

Einen CMC-Benutzer deaktivieren

Mit RACADM können Sie CMC-Benutzer nur manuell und einzeln deaktivieren. Sie können Benutzer nicht mit einer Konfigurationsdatei löschen.

Im folgenden Beispiel wird die Befehls-Syntax gezeigt, die zum Löschen eines CMC-Benutzers verwendet werden kann:

```
racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminPrivilege 0x0
```

Konfiguration von SNMP- und E-Mail-Warnmeldungen

Sie können den CMC so konfigurieren, dass bei bestimmten Gehäuseereignissen SNMP-Ereignis-Traps und/oder E-Mail-Warnungen gesendet werden. Weitere Informationen und Anweisungen finden Sie unter „Konfiguration von SNMP-Alarmen“ auf Seite 474 und „Konfiguration von E-Mail-Benachrichtigungen“ auf Seite 481.

Sie können die Trap-Ziele als korrekt formatierte numerische Adressen (IPv6 oder IPv4) oder vollqualifizierte Domänennamen (FQDNs) angeben. Wählen Sie ein Format, das mit Ihrer Netzwerk-Technologie/Infrastruktur in Einklang steht.

ANMERKUNG: Die Test-TRAP-Funktionalität erkennt keine inkorrekten Einstellungen aufgrund der aktuellen Netzwerkkonfiguration. Zum Beispiel die Verwendung eines IPv6-Ziels in einer reinen IPv4-Umgebung.

Mehrere CMCs in mehreren Gehäusen 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.

   ANMERKUNG: 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. Weitere Informationen finden Sie unter „RACADM im Remote-Zugriff aufrufen“ auf Seite 88.

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 Folgendes in die Befehlszeile ein:

   ```
   racadm config -f myfile.cfg
   ```

5 Setzen Sie den konfigurierten Ziel-CMC zurück. Geben Sie Folgendes in die Befehlszeile ein:

   ```
   racadm reset
   ```

Der Unterbefehl **getconfig -f myfile.cfg** (Schritt 1) 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 verwenden, 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 *Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*.

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 einige 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. Schreibbefehle werden nicht zum CMC übertragen, wenn ein Fehler in der **.cfg**-Datei festgestellt wird. 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 <Dateiname>.cfg` aus. Stellen Sie sicher, dass die **.cfg**-Datei alle gewünschten Objekte, Benutzer, Indizes und anderen Parameter enthält. Lesen Sie das Kapitel Datenbankeigenschaften des *RACADM-Befehlszeilen-Referenzhandbuchs für iDRAC6 und CMC*, um eine vollständige Liste mit Objekten und Gruppen zu erhalten.

VORSICHTSHINWEIS: 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.

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:

```
#
# This is a comment
[cfgUserAdmin]
cfgUserAdminPageModemInitString=<Modem init # not
a comment>
```

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

  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] -{Group name}
  ```

  ```
  cfgNicIpAddress=143.154.133.121 {Object name}
  {Object value}
  ```

- Alle Parameter werden als „Objekt=Wert“-Paare ohne Leerzeichen zwischen „Objekt“, „=“ und „Wert“ angegeben. Leerzeichen nach dem Wert werden ignoriert. Ein Leerzeichen innerhalb einer Wertezeichenkette bleibt unverändert. Jedes Zeichen rechts neben dem = (z. B. ein zweites =, ein #, [,] usw.) wird wie eingegeben übernommen. Bei diesen Zeichen handelt es sich um gültige Modemchat-Skriptzeichen.

  ```
  [cfgLanNetworking] -{Group name}
  cfgNicIpAddress=143.154.133.121 {Object value}
  ```

- Der **.cfg**-Parser ignoriert einen Index-Objekt-Eintrag.

  Benutzer können nicht angeben, welcher Index verwendet werden soll. Wenn der Index bereits vorhanden ist, wird dieser entweder verwendet oder ein neuer Eintrag wird im ersten verfügbaren Index für diese Gruppe erstellt.

  Der Befehl `racadm getconfig -f <filename>.cfg` setzt eine Anmerkung vor die Index-Objekte, so dass Sie die enthaltenen Anmerkungen sehen können.

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

  ```
  racadm config -g <Group name> -o <anchored
  object> -i <Index 1-16> <unique anchor name>
  ```

- Die Zeile für eine indizierte Gruppe kann nicht aus einer **.cfg-**Datei gelöscht werden. Wenn Sie die Zeile mit einem Texteditor löschen, hält RACADM beim Parsen der Konfigurationsdatei an und gibt eine Warnung zum Fehler aus.

  Benutzer müssen ein indiziertes Objekt manuell mit folgendem Befehl entfernen:

  ```
  racadm config -g <groupName> -o <objectName> -i
  <Index 1-16> ""
  ```

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

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

  ```
  [cfgUserAdmin]

  cfgUserAdminUserName=<USER_NAME>
  ```

Wenn Sie `racadm getconfig -f <MeinBeispiel>.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.

CMC-IP-Adresse modifizieren

Wenn Sie die CMC-IP-Adresse in der Konfigurationsdatei modifizieren, entfernen Sie alle unnötigen Einträge von *<variable>=<value>*. Es verbleibt nur die tatsächliche Bezeichnung der variablen Gruppe mit [und], einschließlich der beiden *<Variable>=<Wert>*-Einträge, die sich auf die Änderung der IP-Adresse beziehen.

Beispiel:

```
#
# Object group "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.10.110
cfgNicGateway=10.35.10.1
```

Die Datei wird aktualisiert wie folgt:

```
#
# Object group "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.9.143
# comment, the rest of this line is ignored
cfgNicGateway=10.35.9.1
```

Mit dem Befehl `racadm config -f <meineDatei>.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 <meineDatei>.cfg` über das Netzwerk zu konfigurieren.

ANMERKUNG: *Anchor* ist ein reserviertes Wort und sollte nicht in der **.cfg**-Datei verwendet werden.

RACADM zum Konfigurieren von Eigenschaften auf iDRAC verwenden

RACADM config/getconfig-Befehle unterstützen die Option `-m <Modul>` für die folgenden Konfigurationsgruppen:

- cfgLanNetworking
- cfgIPv6LanNetworking
- cfgRacTuning
- cfgRemoteHosts
- cfgSerial
- cfgSessionManagement

ANMERKUNG: Weitere Informationen über die Standardwerte und Bereiche der einzelnen Eigenschaften finden Sie im Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server-Benutzerhandbuch.

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
```

Fehlerbehebung

Tabelle 4-3listet bekannte Probleme bezüglich des Remote-Zugriffs RACADM auf.

Tabelle 4-3. Verwenden von seriellen/RACADM-Befehlen: Häufig gestellte Fragen

Frage	Antwort
Nach Durchführung eines CMC-Reset (mit Hilfe des RACADM-Unterbefehls **racreset**) gebe ich einen Befehl ein, woraufhin folgende Meldung angezeigt wird: `racadm <Unterbefehl> Transport: ERROR: (RC=-1)` Was bedeutet diese Meldung?	Sie müssen warten, bis der CMC-Reset abgeschlossen ist, bevor Sie einen anderen Befehl absetzen.
Wenn ich die RACADM-Unterbefehle verwende, erhalte ich Fehler, die ich nicht verstehe.	Es können ein oder mehrere der folgenden Fehler bei der Verwendung von RACADM auftreten: • Lokale Fehlermeldungen – Probleme, wie z B. Syntax, typografische Fehler und falsche Namen. Beispiel: `ERROR: <Meldung>` Verwenden Sie den RACADM-Unterbefehl **help**, um richtige Syntax- und Anwendungsinformationen anzuzeigen. • Fehlermeldungen, die sich auf den CMC beziehen - Probleme, bei denen der CMC keine Maßnahme durchführen kann. Dies kann auch „racadm command failed“ (racadm-Befehl fehlerhaft) sein. Geben Sie für Informationen zum Debuggen **racadm gettracelog** ein.

Tabelle 4-3. Verwenden von seriellen/RACADM-Befehlen: Häufig gestellte Fragen

Frage	Antwort
Während ich Remote-RACADM verwendet habe, ist die Eingabeaufforderung zu „>“ gewechselt, und ich kann nicht zur Eingabeaufforderung „$“ zurückkehren.	Wenn Sie ein nicht übereinstimmendes doppeltes Anführungszeichen (") oder ein nicht übereinstimmendes einfaches Anführungszeichen (’) als Teil des Befehls eingeben, dann wechselt die Befehlszeile zur Aufforderung „>“ und stellt alle Befehle in die Warteschlange. Um zur Eingabeaufforderung „$“ zurückzukehren, geben Sie <Strg>–d ein.

Ich habe versucht, die folgenden Befehle zu verwenden und erhielt eine Fehlermeldung „Not Found“ (Nicht gefunden):
`$ logout`
`$ quit`
	Die Abmelden- und Beenden-Befehle sind in der CMC-Befehlszeilenschnittstelle nicht unterstützt.

5

CMC-Webschnittstelle verwenden

Der CMC beinhaltet eine Webschnittstelle, über die Sie die CMC-Eigenschaften und Benutzer konfigurieren, Remote-Verwaltungs-Tasks ausführen und Fehler und Probleme auf einem (verwalteten) Remote-System feststellen und beheben können. Verwenden Sie zur täglichen Gehäuseverwaltung die CMC-Web-schnittstelle. Dieses Kapitel beschreibt, wie allgemeine Gehäuseverwaltungs-Tasks über die CMC-Webschnittstelle ausgeführt werden.

Sie können auch alle Konfigurations-Tasks mit lokalen RACADM-Befehlen oder Befehlszeilenkonsolen (serielle Konsole, Telnet oder SSH) ausführen. Weitere Informationen zur Verwendung der RACADM finden Sie unter „RACADM-Befehlszeilenschnittstelle verwenden“ auf Seite 81. Weitere Informationen zur Verwendung der Befehlszeilenkonsolen finden Sie unter „CMC zur Verwendung von Befehlszeilenkonsolen konfigurieren“ auf Seite 65.

ANMERKUNG: Wenn Sie Microsoft Internet Explorer verwenden, die Verbindung über einen Proxy herstellen und der Fehler „Die XML-Seite kann nicht angezeigt werden“ angezeigt wird, müssen Sie den Proxy deaktivieren, um fortzufahren.

Auf die CMC-Webschnittstelle zugreifen

So greifen Sie über IPv4 auf die CMC-Webschnittstelle zu:

1. Öffnen Sie einen unterstützten Webbrowser.

   Die neuesten Informationen über unterstützte Webbrowser finden Sie in der *Dell Systems Software Support Matrix* unter **support.dell.com/manuals**.

2. Geben Sie die folgende URL in das Feld „Adresse“ ein und drücken Sie <Eingabe>:

   `https://<CMC IP address>`

Wenn die Standard-HTTPS-Anschlussnummer (Anschluss 443) geändert wurde, geben Sie folgendes ein:

`https: //<CMC IP address>:<port number>`

wobei <*CMC-IP-Adresse*> die IP-Adresse für den CMC ist und <*Schnittstellennummer*> die HTTPS-Schnittstellennummer.

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

So greifen Sie über IPv6 auf die CMC-Webschnittstelle zu:

1. Öffnen Sie einen unterstützten Webbrowser.

   Die neuesten Informationen über unterstützte Webbrowser finden Sie in der *Dell Systems Software Support Matrix* unter **support.dell.com/manuals**.

2. Geben Sie die folgende URL in das Feld **Adresse** ein und drücken Sie <Eingabe>:

   `https://[<CMC IP address>]`

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

   Die Angabe der HTTPS-Schnittstellennummer in der URL ist optional, solange unverändert der Standardwert (443) verwendet wird. Andernfalls muss die Schnittstellennummer angegeben werden. Die Syntax für die IPv6 CMC-URL mit angegebener Schnittstellennummer lautet:

   `https://[<CMC IP address]:<port number>`

   wobei <`CMC IP address`> die IP-Adresse für den CMC ist und <`Schnittstellennummer`> die HTTPS-Schnittstellennummer.

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

Anmeldung

ANMERKUNG: Um sich am CMC anzumelden, müssen Sie ein CMC-Konto mit der Berechtigung zum **Anmelden am CMC** besitzen.

ANMERKUNG: Der Standardbenutzername für das CMC-Modul ist **root** und das Standardkennwort lautet **calvin**. Das Konto „root" ist das werkseitig voreingestellte Verwaltungskonto des CMC. Um die Sicherheit zu erhöhen, empfiehlt Dell dringend, das Standardkennwort des root-Kontos bei der Ersteinrichtung zu ändern.

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

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

Sie können sich entweder als CMC-Benutzer oder als Directory-Benutzer anmelden.

So melden Sie sich an:

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

   ANMERKUNG: Dieses Feld unterscheidet Groß- und Kleinschreibung.
2. Geben Sie im Feld **Kennwort** Ihr CMC-Benutzerkennwort oder das Active Directory-Benutzerkennwort ein.

   ANMERKUNG: Dieses Feld ist von Groß-/Kleinschreibung anhängig.
3. Optional können Sie eine Sitzungszeitüberschreitung wählen. Dies ist die Zeit, die Sie ohne Aktivität angemeldet bleiben können, bevor Sie automatisch abgemeldet werden. Der Standardwert ist die Web Service-Inaktivitätszeitüberschreitung. Weitere Einzelheiten finden Sie unter „Dienste konfigurieren“.
4. Klicken Sie auf **OK** oder drücken Sie die Taste <Eingabe>.

Abmeldung

Wenn Sie an der Webschnittstelle angemeldet sind, können Sie sich jederzeit abmelden, indem Sie auf einer beliebigen Seite oben rechts auf **Abmeldung** klicken.

ANMERKUNG: Achten Sie darauf, dass Sie alle von Ihnen auf einer Seite eingegebenen Einstellungen oder Informationen anwenden (speichern). Wenn Sie sich abmelden oder zu einer anderen Seite wechseln, ohne dass Sie Ihre Änderungen angewendet haben, gehen die Änderungen verloren.

CMC-Basiseinstellungen konfigurieren

In den folgenden Abschnitten erhalten Sie Informationen zur Konfiguration der CMC-Basiseinstellungen.

Einrichten des physischen Standorts und des Namens für das Gehäuse

Sie können den Gehäusestandort in einem Rechenzentrum und den Gehäuse-namen 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.

So richten Sie den Standort und den Namen für ein Gehäuse ein:

1. Melden Sie sich bei der CMC-Webschnittstelle an.

   Die Seite **Gehäusefunktionszustand** wird angezeigt.

2. Klicken Sie auf die Registerkarte **Setup**.

   Die Seite **Allgemeine Gehäuseeinstellungen** wird angezeigt.

3. Geben Sie die Standorteigenschaften in die Felder **Rechenzentrum**, **Gang**, **Rack** und **Rack-Einschub** ein.

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

4. Geben Sie den neuen Namen in das Feld **Gehäusename** ein, und klicken Sie dann auf **Anwenden**.

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

1. Melden Sie sich bei der CMC-Webschnittstelle an.

   Die Seite **Gehäusefunktionszustand** wird angezeigt.

2. Klicken Sie auf die Registerkarte **Setup**.

   Die Seite **Allgemeine Gehäuseeinstellungen** wird angezeigt.

3 Klicken Sie auf das Unterregister **Datum/Uhrzeit**.

Die Seite **Datum/Uhrzeit** wird angezeigt.

4 Um das Datum und die Uhrzeit mit einem Network Time Protocol (NTP)-Server zu synchronisieren, markieren Sie **NTP aktivieren** und geben Sie bis zu drei NTP-Server an.

5 Um das Datum und die Uhrzeit manuell einzustellen, heben Sie die Markierung von **NTP aktivieren** auf und bearbeiten Sie die Felder **Datum** und **Uhrzeit**, wählen Sie die **Zeitzone** aus dem Drop-Down-Menü aus und klicken Sie auf **Anwenden**.

Anleitungen zum Einstellen von Datum und Uhrzeit mit der Befehlszeilenschnittstelle finden Sie in den Abschnitten für den `config`-Befehl und die Datenbankeigenschaftsgruppen `cfgRemoteHosts` im *RACADM Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC*.

Aktivieren von wechselbaren Flash-Datenträgern

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:

1 Melden Sie sich bei der CMC-Webschnittstelle an.

Die Seite **Gehäusefunktionszustand** wird angezeigt.

2 Klicken Sie in der Strukturliste auf **Gehäuse-Controller**.

Die Seite **Gehäuse-Controllerstatus** wird angezeigt.

3 Klicken Sie auf das Register **Flash-Datenträger**.

Die Seite **Wechselbarer Flash-Datenträger** wird angezeigt.

4 Wählen Sie in der Dropdown-Liste **Flash-Datenträger zum Speichern von Gehäusedaten verwenden** aus, um mit der Verwendung des Datenträgers zu beginnen.

5 Wenn es den Anschein hat, dass der Datenträger auf einem CMC ein Problem hat, dann machen Sie diesen CMC aktiv und wählen Sie in der Dropdown-Liste **Aktiven Controller-Datenträger vorbereiten oder reparieren** aus.

Wenn im Gehäuse zwei CMC vorhanden sind, müssen beide CMCs Flash-Datenträger enthalten. CMC-Funktionen, die abhängig von Flash-Datenträgern sind (mit Ausnahme von Flexaddress) arbeiten so lange nicht ordnungsgemäß, bis der durch Dell authorisierte Datenträger installiert und auf dieser Seite aktiviert wurde.

Seite „Gehäusefunktionszustand"

Wenn Sie sich am CMC anmelden, wird die Seite **Gehäusefunktionszustand** (**Gehäuse-Übersicht→ Eigenschaften→ Funktionszustand**) angezeigt. Auf dieser Seite stehen die am häufigsten benötigten Informationen und Maßnahmen zur Verfügung. Wenn Ihr Gehäuse als Gruppenführung konfiguriert wurde, wird nach der Anmeldung die Seite **Gruppenfunktionszustand** angezeigt. Weitere Informationen finden Sie unter„Verwendung von Gehäusegruppen" auf Seite 127.

Die Seite **Gehäusefunktionszustand** zeigt eine Live-Grafikansicht des Gehäuses und seiner Komponenten an, sowie auch Details zu den Komponenten. Je nach ausgewählter Komponente stehen verschiedene Maßnahmen oder Links auf andere Seiten zur Verfügung. Außerdem werden die neuesten Ereignisse im CMC-Hardwareprotokoll angezeigt.

Alle Informationen auf der Seite **Gehäusefunktionszustand** werden dynamisch aktualisiert. Die Seite enthält zwei Hauptbereiche: die **Gehäusekomponenten-Zusammenfassung** oben und die Liste der **Neuesten CMC-Hardwareprotokoll-Ereignisse** darunter.

Der Abschnitt **Gehäusekomponenten-Zusammenfassung** (auch „Gehäusefunktionszustand" genannt, wenn die Gesamt-Gehäuseinformationen angezeigt werden) zeigt die Grafik und die dazugehörigen Informationen. Sie können diesen gesamten Bereich ausblenden, indem Sie auf das Symbol **Schließen** klicken.

Die linke Hälfte des Bereichs **Gehäusekomponenten-Zusammenfassung** zeigt die Grafik und die Gehäuse-Quicklinks. Die rechte Hälfte des Bereichs zeigt Informationen, Links und Maßnahmen, die mit der ausgewählten Komponente zusammenhängen. Klicken Sie auf die grafische Darstellung einer Komponente, um die Komponente auszuwählen. Die Grafik wird nach Auswahl blau überschattet.

Die Liste der **Letzten CMC-Hardwareprotokoll-Ereignisse** zeigt die neuesten 10 Ereignisse aus diesem Protokoll an. Der Inhalt dieses Abschnittes wird dynamisch aktualisiert und zeigt die neuesten Ereignisse immer ganz oben in der Liste an. Weitere Informationen zu CMC-Hardwareprotokoll-Einträgen finden Sie unter „Ereignisprotokolle anzeigen“ auf Seite 497.

Verwendung von Gehäusegruppen

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.

Gehäusegruppenfunktionen

Im Folgenden werden die Gehäusegruppenfunktionen dargestellt:

- Die Gehäusegruppen-GUI-Seite 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 die Schaltfläche **Details** klicken.
- Es sind Schnellstart-Links zum Öffnen der Webseiten von Mitgliedsgehäusen oder Servern vorhanden.
- Für eine Gruppe sind ein Blade 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.

Einrichten einer Gehäusegruppe

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 richten Sie die Gehäusegruppe über die GUI ein:

1. Melden Sie sich an dem als Führungsserver eingeplanten Gehäuse mit Administratorrechten an.
2. Klicken Sie auf **Setup→ Gruppenverwaltung**.

   Die Seite **Gehäusegruppe** wird angezeigt.
3. Wählen Sie auf der **Gehäusegruppenseite** 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 GUI wechselt beim Erstellen der Gehäusegruppe automatisch zur Gehäusegruppen-GUI-Seite. Die Systemstruktur zeigt die Gruppe über den Gruppennamen an und das Führungsgehäuse sowie die nicht bestückten Mitgliedergehäuse werden in der Systemstruktur angezeigt.

Nach dem Einrichten der Gehäusegruppe können Sie Mitglieder zur Gruppe hinzufügen:

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 auf dem Mitgliedsgehäuse im Feld **Benutzernamen** einen Benutzernamen mit Gehäuseadministratorrechten 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 Inforationen finden Sie im Unterabschnitt „Synchronisieren eines neuen Mitglieds mit den Eigenschaften des Führungsgehäuses“ auf Seite 132.

8 Wählen Sie die Schaltfläche **Anwenden**.

9 Wiederholen Sie Schritt 4 bis Schritt 8, um maximal acht Mitglieder hinzuzufügen.

Der Gehäusename des neuen Mitglieds wird im mit **Mitglieder** bezeichneten Dialogfeld angezeigt.

Der Status des neuen Mitglieds wird angezeigt, indem die Gruppe in der Struktur ausgewählt wird. Details werden durch Anklicken des Gehäusebildes oder der Schaltfläche „Details“ zur Verfügung gestellt.

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 in der Struktur das Führungsgehäuse aus.

3 Klicken Sie auf **Setup→ Gruppenverwaltung**.

4 Wählen Sie aus der Liste **Mitglieder entfernen** den bzw. die 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. Weitere Informationen finden Sie im Unterabschnitt „Deaktivieren eines einzelnen Mitglieds am Mitgliedsgehäuse“ auf Seite 131.

Auflösen einer Gehäusgruppe

So lösen Sie eine Gehäusegruppe vom Führungsgehäuse aus auf:

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 auf der **Gehäusegruppenseite** unter **Rolle**, **Keine** aus und klicken Sie anschließend auf **Anwenden**.

Das Führungsgehäuse benachrichtigt anschließend alle Mitglieder, dass sie aus der Gruppe entfernt wurden. Schließlich setzt das Führungsgehäuse seine Rolle nicht weiter fort. Es kann nun einer anderen Gruppe als Mitglied oder Führung zugewiesen werden.

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. Weitere Informationen finden Sie im Unterabschnitt „Deaktivieren eines einzelnen Mitglieds am Mitgliedsgehäuse“ auf Seite 131.

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 auf **Setup→ Gruppenverwaltung**.
3. Wählen Sie **Keine** und klicken Sie anschließend auf **Anwenden**.

Starten der Webseite eines Mitgliedsgehäuses oder Servers

Links auf die Webseite eines Mitgliedsgehäuses, die Remote-Konsole eines Servers oder die Webseite des Server-iDRACs innerhalb der Gruppe stehen über die Gruppenseite des Führungsgehäuses zur Verfügung. Sie können zum Anmelden am Mitgliedsgerät den gleichen Benutzernamen und das gleiche Kennwort verwenden, die Sie zum Anmelden am Führungsgehäuse verwendet haben. Wenn das Mitgliedsgerät die gleichen Anmeldeinformationen hat, ist keine weitere Anmeldung erforderlich. Anderenfalls wird der Benutzer auf die Anmeldeseite des Mitgliedsgerätes geleitet. 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 unterhalb des gewünschten Gehäuses **CMC starten** aus.

   Wenn ein Server in einem Gehäuse das benötigte Ziel ist, dann verfahren Sie folgendermaßen:

   a. Wählen Sie das Bild des Zielgehäuses aus.
   b. Wählen Sie im unterhalb des Bereichs **Zustand und Warnmeldungen** angezeigten Bild des Gehäuses den Server aus.
   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 5-1. Konfigurationsdiensteigenschaften

Eigenschaft	Navigation
SNMP-Konfiguration	Klicken Sie für weitere Details auf **Gehäuse-Übersicht→ Netzwerk→ Dienste→ SNMP**.
Remote-Gehäuseprotokollierung	Klicken Sie für weitere Details auf **Gehäuse-Übersicht→ Netzwerk→ Dienste→ Remote-Syslog**.
Benutzerauthentifizierung mithilfe der Dienste „LDAP“ und „Active Directory“	Klicken Sie für weitere Details auf **Gehäuse-Übersicht→ Benutzerauthentifizierung→ Verzeichnisdienste**.
Gehäusewarnungen	Klicken Sie für weitere Details auf **Gehäuse-Übersicht→ Warnungen**.

Blade-Bestandsliste für MCM-Gruppe

Auf der Seite **Zustand der Gehäusegruppe** werden alle Mitgliedsgehäuse angezeigt. Hier können Sie den Bericht zur Blade-Bestandsliste über die Download-Funktion eines Standard-Internet-Browsers in eine Datei speichern. Der Bericht enthält Daten zu:

- allen Blades, die sich derzeit in der Gehäusegruppe befinden (einschließlich Führungsgehäuse)
- leeren Einschüben und Erweiterungseinschüben (einschließlich Blades mit voller Höhe und doppelter Breite)

Speichern des Berichts zur Blade-Bestandsliste

So speichern Sie den Bericht zur Blade-Bestandsliste:

1. Melden Sie sich an der CMC-Web-Schnittstelle an, und wählen Sie die Option **Gruppe** aus der Strukturansicht aus.

   Die Seite **Zustand der Gehäusegruppe** wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Bericht zur Bestandsliste speichern**.

   Im Dialogfeld **Datei-Download** werden Sie 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 Blade-Bestandsliste ein.

   ANMERKUNG: Das Führungsgehäuse für die Gehäusegruppe und das Mitgliedsgehäuse für die Gehäusegruppe sowie alle Blades im verknüpften Gehäuse müssen sich für einen präzisen Bericht zur Blade-Bestandsliste in der Position **Ein** befinden.

Exportierte Daten

Der Bericht zur Blade-Bestandsliste enthält Daten, die kürzlich im Rahmen der normalen Abfrage durch das Führungsgehäuse der Gehäusegruppe (alle 30 Sek.) von jedem Mitglied in der Gehäusegruppe gemeldet wurden.

So erstellen Sie einen präzisen Bericht zur Blade-Bestandsliste:

- Das Führungsgehäuse der Gehäusegruppe sowie alle Mitgliedsgehäuse der Gehäusegruppe müssen **eingeschaltet** sein.
- Alle Blades im verknüpften Gehäuse müssen eingeschaltet sein.

Die Bestandslistendaten für das verknüpfte Gehäuse und die verknüpften Blades sind möglicherweise nicht im Bericht enthalten, falls sich ein Teilbereich der Mitgliedsgehäuse der Gehäusegruppe im folgenden Zustand befinden:

- **Gehäusegruppe ist ausgeschaltet**
- Ausgeschaltet

Tabelle 5-2 listet die spezifischen Datenfelder und Anforderungen für Felder auf, die für jedes Blade gemeldet werden müssen:

Tabelle 5-2. Blade-Bestandsliste – 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-Nummer	1PB8VF1
Gesamtsystemspeicher	4 GB **ANMERKUNG:** Es wird ein CMC ab Version 4.0 auf dem Mitglied benötigt. Ansonsten wird er leer angezeigt.

Tabelle 5-2. Blade-Bestandsliste – Feldbeschreibungen

Datenfeld	Beispiel
Anzahl der CPUs	2 **ANMERKUNG:** Es wird ein CMC ab Version 4.0 auf dem Mitglied benötigt. Ansonsten wird er leer angezeigt.
CPU-Info	Intel (R) Xeon (R) CPU E5502 @1,87 GHzn **ANMERKUNG:** Es wird ein CMC ab Version 4.0 auf dem Mitglied benötigt. Ansonsten wird er leer angezeigt.

Datenformat

Der Bestandslistenbericht wird in einem **CSV**-Dateiformat generiert, damit er in verschiedene Tools importiert werden kann, z. B. Microsoft Excel. Die **CSV**-Datei für den Bestandslistenbericht kann in die Vorlage importiert werden, indem Sie in MS Excel auf **Daten→ Aus Text** auswählen. Nachdem der Bestandslistenbericht 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.

Gehäusekomponenten-Zusammenfassung

Die folgenden Abschnitte enthalten Informationen zur Übersicht über die Gehäusekomponenten.

Gehäuse-Grafiken

Das Gehäuse wird in Vorder- und Rückansichten dargestellt (jeweils die oberen und unteren Bilder). Die Server 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 Komponente an. Das Serversymbol wird in Tabelle 5-1 als Beispiel verwendet. Andere Komponenten zeigen Symbole an, die die physische Komponente visuell darstellen. Symbole für Server und EAMs überspannen mehrere Steckplätze, wenn eine Komponente doppelter Größe installiert ist. Wenn der Cursor auf einer Komponente positioniert wird, wird eine Quickinfo mit zusätzlichen Informationen über diese Komponente angezeigt.

Tabelle 5-3. Serversymbolzustände

Symbol	Beschreibung
	Der Server ist eingeschaltet und arbeitet normal.
	Der Server ist ausgeschaltet.

Tabelle 5-3. Serversymbolzustände *(fortgesetzt)*

Symbol	Beschreibung
	Der Server meldet einen nicht-kritischen Fehler.
	Der Server meldet einen kritischen Fehler.
	Es ist kein Server vorhanden.

Tabelle 5-4 zeigt die Gehäuse-Quicklinks an.

Tabelle 5-4. Gehäuse-Quicklinks

Feld	Beschreibung
Benutzer konfigurieren	Wechseln Sie zu **Gehäuse-Übersicht→ Benutzer-Authentifizierung→ Lokale Benutzer**
Netzwerkkonfiguration	Wechseln Sie zu **Gehäuse-Übersicht→ Netzwerk → Netzwerk**
Stromkonfiguration	Wechseln Sie zu **Gehäuse-Übersicht→ Strom→ Konfiguration**
Firmware-Aktualisierung	Wechseln Sie zu **Gehäuse-Übersicht → Aktualisierung→ Firmware-Aktualisierung**

Gehäusefunktionszustand

Wenn die Seite erstmalig angezeigt wird, dann enthält die rechte Seite der Seite die Informationen und Warnungen auf Gehäuseebene. Es werden alle aktiven kritischen und nicht-kritischen Warnungen angezeigt.

Wenn eine Komponente angeklickt wird, werden die Informationen der Gehäuseebene mit den Informationen für die ausgewählte Komponente ersetzt. Um zu den Informationen der Gehäuseebene zurückzukehren, klicken Sie oben rechts auf **Zurück zum Gehäusefunktionszustand**.

Tabelle 5-5. Informationen der Gehäuseseite

Feld	Beschreibung
Modell	Zeigt das Modell des Gehäuse-LCD-Bedienfelds an.
Firmware	Zeigt die Firmware-Version des aktiven CMC an.
Service-Tag-Nummer	Zeigt die Service-Tag-Nummer des Gehäuses an. Die Service-Tag-Nummer ist eine vom Hersteller eindeutig identifizierbare Nummer für Support- und Wartungsbelange.
Systemkennnummer	Zeigt die Systemkennnummer für das Gehäuse an.
Eingangsstrom	Strommenge, die das Gehäuse derzeit verbraucht.
Stromobergrenze	Vom Benutzer zugewiesener maximaler Eingangsstrom, der verbraucht werden kann. Wenn das Gehäuse die Grenze erreicht, beginnt der Server zu drosseln, um einen weiteren Anstieg beim erforderlichen Eingangsstrom zu vermeiden.
Stromregel	Vom Benutzer festgelegte Präferenzen für die Koordination mehrerer Netzteileinheiten.
Seite „Funktionszustand“	Zeigt den gesamten Funktionszustand des Gehäusestrom-Untersystems an.

Ausgewählte Komponenteninformationen

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

- Funktionszustand, Leistung und Eigenschaften

  Die aktiven, kritischen und nicht-kritischen Ereignisse gemäß der Anzeige im Hardwareprotokoll werden gegebenenfalls hier angezeigt. Die mit der Zeit variierenden Leistungsdaten werden ebenfalls hier angezeigt.

- Eigenschaften

  Komponenteneigenschaften, die sich nicht mit der Zeit ändern oder sich nur selten ändern, werden hier angezeigt.

- Quicklinks

  Der Bereich „Quicklinks“ ermöglicht den bequemen 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.

Tabelle 5-6. Funktions- und Leistungsinformationen - Server

Element	Beschreibung
Stromzustand	Ein/Aus-Zustand des Servers. Einzelheiten zu den verschiedenen Arten von Stromzuständen finden Sie unter Tabelle 5-25.
Seite „Funktionszustand“	Zeigt die Textentsprechung zum Symbol des Funktionszustandes an.
Leistungsbedarf	Strommenge, die der Server derzeit verbraucht.
Zugeteilter Strom	Für den Server im Budget zugeteilter Strom.
Temperatur	Vom Server-Temperatursensor abgelesene Temperatur.

Tabelle 5-7. Servereigenschaften

Element	Beschreibung
Name	Vom Benutzer vergebener Steckplatzname.
Modell	Servermodell, zum Beispiel „PowerEdge M600“ oder „PowerEdge M605“.
Service-Tag-Nummer	Die Service-Tag-Nummer des Servers. Die Service-Tag-Nummer ist eine vom Hersteller eindeutig identifizierbare Nummer für Support- und Wartungsbelange. Wenn kein Server vorhanden ist, ist dieses Feld leer.
Betriebssystem	Betriebssystem des Servers.
Host-Name	Name des Servers, der vom Betriebssystem festgelegt wird.
iDRAC	Version der iDRAC-Firmware auf dem Server.
BIOS	Server-BIOS-Version.
CPLD	Zeigt die CPLD-Versionsnummer (Complex Programmable Logic Device) des Servers an.
CPU Information	Zeigt die Anzahl der auf dem Server installierten CPUs mit dem jeweiligen Typ an.
Gesamtsystem speicher	Zeigt den gesamten auf dem Server installierten Systemspeicher (in GB) an.

Tabelle 5-8. Quicklinks - Server

Element	Beschreibung
Serverstatus	Wechseln Sie zu **Server-Übersicht→** *<Ausgewählter Server>* **→ Eigenschaften→ Status**
Remote-Konsole starten	Startet eine Keyboard-Video-Mouse (KVM)-Sitzung auf dem Server, wenn der Server diesen Vorgang unterstützt.
iDRAC-GUI starten	Startet eine iDRAC-Verwaltungskonsole für den Server.
Server einschalten	Strom an einen Server anlegen, der sich im Zustand „Aus“ befindet.
Server ausschalten	Strom vom Server trennen, der sich im Zustand „Ein“ befindet.
Remote-Dateifreigabe	Wechseln Sie zu **Server-Übersicht→ Setup→ Remote-Dateifreigabe**
iDRAC-Netzwerk bereitstellen	Wechselns Sie zu **Server-Übersicht→ Setup→ iDRAC** (iDRAC bereitstellen)
Lifecycle Controller	Wechseln Sie zu **Server-Übersicht→ Aktualisierung→ Firmware-Aktualisierung**

Tabelle 5-9. EAM-Funktionszustand und Leistung

Element	Beschreibung
Stromzustand	Zeigt den Stromstatus des E/A-Moduls an: Ein, Aus oder Unbekannt (nicht vorhanden).
Rolle	Zeigt die E/A-Modul-Stack-Zugehörigkeit beim Verknüpfen der E/A-Module an. Member (Stack-Zugehörigkeit) bedeutet, dass das Modul Teil eines Stack-Satzes ist. Master bedeutet, dass das Modul ein primärer Zugangspunkt ist.

Tabelle 5-10. EAM-Eigenschaften

Element	Beschreibung
Modell	Zeigt den E/A-Modul-Produktnamen an.
Service-Tag-Nummer	Zeigt die Service-Tag-Nummer des E/A-Moduls an. Die Service-Tag-Nummer ist eine eindeutige Kennung von Dell für Support- und Wartungsbelange.

Tabelle 5-11. Quicklinks - E/A-Module

Element	Beschreibung
EAM-Status	Wechseln Sie zu **E/A-Module**→ <*Ausgewähltes EAM*>→ **Eigenschaften**→ **Status**
EAM-GUI starten	Wenn der Link *EAM-GUI starten* für ein bestimmtes E/A-Modul vorhanden ist, bewirkt Klicken darauf, dass die EAM-Verwaltungskonsole für dieses E/A Modul in einem neuen Fenster oder Register des Browsers gestartet wird.

Tabelle 5-12. Funktionszustand und Leistung des aktiven CMC

Element	Beschreibung
Redundanzmodus	Zeigt die Failover-Bereitschaft des Standby-CMC an. Wenn die CMC-Firmware nicht passt oder das CMC nicht ordnungsgemäß mit dem Verwaltungsnetzwerk verkabelt ist, dann wird die Redundanz als nicht verfügbar angezeigt.
MAC-Adresse	Zeigt die MAC-Adresse für die CMC-Netzwerkschnittstellenkarte (NIC) an. Die MAC-Adresse ist eine eindeutig identifizierte Adresse für den CMC über das Netzwerk.
IPv4	Zeigt die aktuelle IPv4-Adresse für die CMC-Netzwerkschnittstelle an.
IPv6	Zeigt die erste IPv6-Adresse für die CMC-Netzwerkschnittstelle an.

Tabelle 5-13. CMC-Eigenschaften

Element	Beschreibung
Firmware	Zeigt die Firmware-Version des aktiven CMC an.
Standby-Firmware	Zeigt die auf dem Standby-CMC installierte Firmware-Version an. Wenn Sie keinen zweiten CMC installiert haben, dann zeigt dieses Feld „-“ an.
Letzte Aktualisierung	Zeigt an, wann die Firmware das letzte Mal aktualisiert wurde. Wenn keine Aktualisierungen stattgefunden haben, zeigt dieses Feld „-“ an.
Hardware	Zeigt die Hardwareversion des aktiven CMC an.

Tabelle 5-14. Quicklinks - CMC

Element	Beschreibung
CMC-Status	Wechseln Sie zu **Gehäuse-Controller→ Eigenschaften→ Status**
Networrking (Netzwerk)	Wechseln Sie zu **Gehäuse-Übersicht→ Netzwerk→ Netzwerk**
Firmware-Aktualisierung	Wechseln Sie zu **Gehäuse-Übersicht→ Aktualisierung→ Firmware-Aktualisierung**

Tabelle 5-15. iKVM-Funktionszustand und Leistung

Element	Beschreibung
OSCAR-Konsole	Zeigt an, ob der VGA-Konnektor am rückseitigen Bedienfeld für den Zugriff auf den CMC aktiviert ist (Ja oder Nein).

Tabelle 5-16. iKVM-Eigenschaften

Element	Beschreibung
Name	Zeigt den Namen des iKVM-Moduls an.
Part Number (Teilenummer)	Zeigt die Teilenummer des iKVM an. Die Teilenummer ist eine vom Hersteller eindeutig identifizierbare Nummer. Die Namenskonventionen von Teilenummern sind von Hersteller zu Hersteller unterschiedlich.
Firmware	Zeigt die iKVM-Firmware-Version an.
Hardware	Zeigt die iKVM-Hardwareversion an.

Tabelle 5-17. Quicklinks - iKVM

Element	Beschreibung
iKVM Status	Wechseln Sie zu **iKVM→ Eigenschaften→ Status**
Firmware-Aktualisierung	Wechseln Sie zu **Gehäuse-Übersicht→ Aktualisierung→ Firmware-Aktualisierung**

Tabelle 5-18. Lüfter-Funktionszustand und Leistung

Element	Beschreibung
Speed (Taktrate)	Gibt die Lüftergeschwindigkeit in Umdrehungen pro Minute (U/Min.) an.

Tabelle 5-19. Lüftereigenschaften

Element	Beschreibung
Unterer kritischer Schwellenwert	Wenn diese Geschwindigkeit unterschritten wird, gilt der Lüfter als fehlerhaft.
Oberer kritischer Schwellenwert	Wenn diese Geschwindigkeit überschritten wird, gilt der Lüfter als fehlerhaft.

Tabelle 5-20. Quicklinks - Lüfter

Element	Beschreibung
Fan Status (Lüfterstatus)	Wechseln Sie zu **Lüfter→ Eigenschaften→ Status**

Tabelle 5-21. Netzteileinheitsfunktionszustand und Leistung

Element	Beschreibung
Power Status (Stromstatus)	Zeigt den Stromzustand der Netzteile an: Initialisierung, Online, Standby, Diagnosemodus, Fehler, Aktualisierung, Offline oder Unbekannt.

Tabelle 5-22. Netzteileinheitseigenschaften

Element	Beschreibung
Capacity (Kapazität)	Zeigt die Kapazität des Netzteils in Watt an.

Tabelle 5-23. Quicklinks - Netzteileinheit

Element	Beschreibung
Netzteilstatus	Wechseln Sie zu **Netzteile → Eigenschaften→ Status**
Leistungsbedarf	Wechseln Sie zu **Gehäuse-Übersicht→ Strom→ Stromverbrauch**
Systembudget	Wechseln Sie zu **Gehäuse-Übersicht→ Strom→ Budgetstatus**

Tabelle 5-24. LCD-Funktionszustand und Leistung

Element	Beschreibung
LCD-Funktionszustand	Zeigt das Vorhandensein und den Funktionszustand des LCD-Bedienfeldes an.
Gehäusefunktionszusta nd	Zeigt die Textbeschreibung zum Gehäusefunktionszustand an.

Es gibt keine Quicklinks für die LCD.

Systemfunktionszustand überwachen

Gehäuse- und Komponenten-Zusammenfassungen anzeigen

Der CMC zeigt eine grafische Darstellung des Gehäuses auf der Seite **Gehäusefunktionszustand** an und bietet damit einen visuellen Überblick über den Status der installierten Komponenten. Die Seite **Gehäusefunktionszustand** wird dynamisch aktualisiert und die Farben der Komponenten-Untergrafiken und Texthinweise werden automatisch geändert, um den derzeitigen Zustand widerzuspiegeln.

Abbildung 5-1. Beispiel für die Gehäuse-Grafiken in der Webschnittstelle

Die Seite **Gehäusefunktionszustand** enthält den Gesamtfunktionszustand für: Gehäuse, aktive und Standby-CMCs, Servermodule, E/A-Module (EAMs), Lüfter, iKVM, Netzteile und LCD-Einheit. Detaillierte Informationen zu den einzelnen Komponenten erhalten Sie, wenn Sie auf die jeweilige Komponente klicken. Anleitungen zum Betrachten der Gehäuse- und der Komponentenzusammenfassung finden Sie unter „Gehäusezusammenfassungen anzeigen“ auf Seite 492.

Strombudgetstatus anzeigen

Die Seite **Strombudgetstatus** zeigt den Strombudgetstatus für das Gehäuse, die Server und die Gehäuse-Netzteileinheiten an.

Anleitungen zum Anzeigen des Strombudgetstatus finden Sie unter „Anzeige des Stromverbrauchsstatus“ auf Seite 389. Weitere Informationen über die Stromverwaltung des CMC finden Sie unter „Stromverwaltung“ auf Seite 363.

Servermodellnamen und Service-Tag-Nummer anzeigen

Der Modellname und die Service-Tag-Nummer der einzelnen Server können momentan ermittelt werden durch Ausführung der folgenden Schritte:

- Erweitern Sie die Server in der Systemstruktur. Es werden alle Server (1 - 16) in der erweiterten Liste der Server angezeigt. Namen von Steckplätzen ohne Server sind grau unterlegt.
- 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.

Funktionszustand von allen Servern anzeigen

Sie können den Funktionszustand für alle Server im Abschnitt **Gehäuse-Grafiken** auf der Seite **Gehäusefunktionszustand** oder der Seite **Status der Server** anzeigen.

Gehäuse-Grafiken bietet einen grafischen Überblick über alle im Gehäuse installierten Server.

Um den Funktionszustand aller Server mittels Gehäuse-Grafiken einzusehen:

1. Melden Sie sich bei der CMC-Webschnittstelle an.

   Die Seite **Gehäusefunktionszustand** wird angezeigt. Der mittlere Abschnitt der **Gehäuse-Grafiken** stellt die Vorderansicht des Gehäuses dar und enthält den Funktionszustand aller Server. Der Serverfunktionszustand wird durch die Farbe der Server-Untergrafik angegeben:

   - Keine Unterlegung - Server ist vorhanden, wird mit Strom versorgt und kommuniziert mit dem CMC; es gibt keine Anzeichen eines ungünstigen Zustands.

- Gelbes Vorsichtzeichen - Zeigt an, dass nur Warnungen ausgegeben wurden und dass Korrekturmaßnahmen getroffen werden müssen.
- Rotes X - Zeigt an, dass mindestens ein Fehlerzustand vorliegt. Dies bedeutet, dass der CMC weiterhin mit der Komponente kommunizieren kann und der angegebene Funktionszustand kritisch ist.
- Grau unterlegt - Zeigt an, dass die Komponente vorhanden ist, aber nicht eingeschaltet. Sie kommuniziert nicht mit dem CMC und es gibt keine Anzeichen eines ungünstigen Zustands.

Die Seite **Status der Server** enthält Übersichten zu den Servern im Gehäuse. So zeigen Sie den Funktionszustand aller Server unter Verwendung der Seite „Status der Server“ an:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur **Server-Übersicht** aus.

   Die Seite **Serverstatus** wird angezeigt.

Tabelle 5-25. Informationen zum Status aller Server

Element	Beschreibung
Slot (Steckplatz)	Zeigt die Position des Servers an. Die Steckplatznummer ist eine sequenzielle Nummer, die das Servermodul anhand seiner Position im Gehäuse identifiziert.
Name	Zeigt den Namen des Servers an, der standardmäßig mit dem **Steckplatznamen** (STECKPLATZ-01 bis STECKPLATZ-16) identifiziert wird. **ANMERKUNG:** Sie können den Standardservernamen ändern. Anleitungen hierzu finden Sie unter „Steckplatznamen bearbeiten“ auf Seite 151.
Model (Modell)	Zeigt den Namen des Servermodells an. Wenn dieses Feld leer ist, ist der Server nicht vorhanden. Wenn dieses Feld die Erweiterung von # (wobei das Zeichen # für 1 - 8 steht) anzeigt, dann bezeichnet die Nummer (#) den Hauptsteckplatz eines Mehrfach-Steckplatz-Servers.

Tabelle 5-25. Informationen zum Status aller Server *(fortgesetzt)*

Element	Beschreibung		
Seite „Funk„Funktionszustand“tions-zustand“		OK	Zeigt an, dass der Server vorhanden ist und mit dem CMC kommuniziert. Im Falle eines Fehlers bei der Datenübertragung zwischen dem CMC und dem Server kann der CMC den Funktionszustand des Servers weder abrufen noch anzeigen.
		Informativ	Zeigt Informationen über den Server an, wenn beim Funktionsstatus (OK, Warnung, Schwerwiegend) keine Änderung aufgetreten ist.
		Warnung	Zeigt an, dass Warnungen ausgegeben wurden und *Korrekturmaßnahmen ergriffen werden müssen*. Falls keine Korrekturmaßnahmen ergriffen werden, können kritische Fehler die Integrität des Servers beinträchtigen.
		Kritisch	Zeigt an, dass mindestens eine Fehlerwarnung ausgegeben wurde. Ein kritischer Status stellt einen Systemfehler auf dem Server dar. *Es müssen umgehend Korrekturmaßnahmen getroffen werden*.
		Kein Wert	Wenn sich kein Server im Steckplatz befindet, werden keine Informationen zum Funktionszustand angezeigt.

Tabelle 5-25. Informationen zum Status aller Server *(fortgesetzt)*

Element	Beschreibung
Launch Remote Console (Remote-Konsole starten)	Klicken Sie darauf, um eine Keyboard-Video-Mouse (KVM)-Sitzung auf dem Server in einem neuen Browserfenster oder -register zu starten. Dieses Symbol wird nur für einen Server angezeigt, auf den alle folgenden Bedingungen zutreffen: • Server, die iDRAC6 und iDRAC7 unterstützen. • Das Gehäuse ist eingeschaltet. • Die LAN-Schnittstelle auf dem Server ist aktiviert. • Die iDRAC-Version ist 2.20 oder höher. Diese Funktion arbeitet nur dann korrekt, wenn die folgenden Bedingungen erfüllt sind: • Auf dem Host-System ist JRE 6 Aktualisierung 16 (Java Runtime Environment) oder höher installiert. • Der Browser auf dem Host-System erlaubt Popup-Fenster (Popup-Blockierung ist deaktiviert).
Launch iDRAC-GUI (iDRAC-GUI starten)	Klicken Sie mit der linken Maustaste auf die Schaltfläche, um die iDRAC-Verwaltungskonsole für einen Server in einem neuen Fenster oder Register des Browsers zu starten. Dieses Symbol wird nur für einen Server angezeigt, auf den alle folgenden Bedingungen zutreffen: • Der Server ist vorhanden. • Das Gehäuse ist eingeschaltet. • Die LAN-Schnittstelle auf dem Server ist aktiviert. Diese Funktion arbeitet nur dann korrekt, wenn die folgende Bedingung erfüllt ist: • Der Browser auf dem Host-System erlaubt Popup-Fenster (Popup-Blockierung ist deaktiviert). **ANMERKUNG:** Wenn der Server vom Gehäuse entfernt wird, die IP-Adresse des iDRAC geändert wird oder die Netzwerkverbindung beim iDRAC Probleme aufweist, wird durch Klicken auf das Symbol **iDRAC GUI starten** eventuell eine Fehlerseite auf der iDRAC LAN-Schnittstelle angezeigt.

Tabelle 5-25. Informationen zum Status aller Server *(fortgesetzt)*

Element	Beschreibung
Power State (Stromzustand)	Zeigt den Stromzustand des Servers: • **k.A.** - Der CMC hat den Stromzustand des Servers noch nicht bestimmt. • **Aus** - Entweder der Server oder das Gehäuse sind ausgeschaltet. • **Ein** - Sowohl Gehäuse, als auch Server sind eingeschaltet. • **Einschalten** - vorübergehender Zustand zwischen Aus und Ein. Ist der Vorgang erfolgreich abgeschlossen, wird der **Stromzustand** auf **Ein** stehen. • **Ausschalten** - vorübergehender Zustand zwischen Ein und Aus. Ist der Vorgang erfolgreich abgeschlossen, wird der **Stromzustand** auf **Aus** stehen.
Service Tag (Service-Tag-Nummer)	Zeigt die Service-Tag-Nummer des Servers an. Die Service-Tag-Nummer ist eine vom Hersteller eindeutig identifizierbare Nummer für Support- und Wartungsbelange. Wenn kein Server vorhanden ist, ist dieses Feld leer.

Informationen zum Starten der iDRAC-Verwaltungskonsole und Richtlinien über Verfahren zur einfachen Anmeldung finden Sie unter „iDRAC mit einfacher Anmeldung starten“ auf Seite 262.

Steckplatznamen bearbeiten

Über die Seite **Steckplatznamen** können Sie Steckplatznamen im Gehäuse aktualisieren. Steckplatznamen werden zur Identifizierung einzelner Server verwendet. Bei der Auswahl von Steckplatznamen gelten folgende Regeln:

- Namen dürfen **maximal 15** nichterweiterte 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-`
  - `Fan-`
  - `PS-`
  - `KVM`
  - `DRAC-`
  - `MC-`
  - `Gehäuse`
  - `Housing-Left`
  - `Housing-Right`
  - `Housing-Center`
- Die Zeichenketten `Server-1` bis `Server-16` 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. Beachten Sie, dass `Server-03` ein gültiger Namen für einen beliebigen Steckplatz ist.

ANMERKUNG: Um einen Steckplatznamen zu ändern, müssen Sie die Berechtigung als **Gehäusekonfigurations-Administrator** besitzen.

ANMERKUNG: 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.

ANMERKUNG: Die Einstellung des Steckplatznamens kann nicht auf das optionale iKVM erweitert werden. Steckplatznameninformationen sind über iKVM-FRU erhältlich.

ANMERKUNG: 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:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur **Server-Übersicht** im Menü **Gehäuse** aus.

3 Klicken Sie auf **Setup→ Steckplatznamen**.

Die Seite **Steckplatznamen** wird angezeigt.

4 Geben Sie den aktualisierten oder neuen Namen eines Steckplatzes in das Feld **Steckplatzname** ein. Wiederholen Sie diese Maßnahme für jeden Steckplatz, den Sie umbenennen möchten und klicken Sie auf **Anwenden**.

5 Um den Standardsteckplatznamen (**STECKPLATZ-01** bis **STECKPLATZ-16**, basierend auf der Position des Serversteckplatzes) zum Server wiederherzustellen, verwenden Sie **Standardwert wiederherstellen**.

Host-Name des Servers als Steckplatzname verwenden

Auf der Seite **Steckplatznamen** können die statischen Steckplatznamen mit dem Host-Namen des Servers (oder dem Systemnamen) überschrieben werden, falls verfügbar. Dazu muss der OMSA-Agent auf dem Server installiert sein. Näheres zum OMSA-Agenten finden Sie im *Dell OpenManage Server Administrator-Benutzerhandbuch*.

So verwenden Sie den Host-Namen des Servers als Steckplatznamen:

1 Melden Sie sich bei der CMC-Webschnittstelle an.

2 Wählen Sie in der Systemstruktur **Server-Übersicht** im Menü **Gehäuse** aus.

3 Klicken Sie auf **Setup→ Steckplatznamen**.

Die Seite **Steckplatznamen** wird angezeigt.

4 Wählen Sie **Host-Name als Steckplatznamen verwenden** und klicken Sie auf **Anwenden**.

Festlegen des ersten Startlaufwerks für Server

Über die Seite **Erstes Startlaufwerk** können Sie das Startlaufwerk für jeden Server festlegen. Dieses muss nicht unbedingt das erste Startlaufwerk für den Server sein und nicht unbedingt ein Gerät in diesem Server repräsentieren; stattdessen stellt es ein Gerät dar, das vom CMC als erstes Startlaufwerk mit Bezug zu diesem Server verwendet wird.

Neben dem Standard-Startlaufwerk können Sie auch ein Laufwerk für einen einmaligen Start definieren. So können Sie ein spezielles Image starten, um beispielsweise Diagnoseaufgaben durchzuführen oder ein Betriebssystem neu zu installieren.

Das von Ihnen angegebene Startlaufwerk muss vorhanden sein und einen startfähigen Datenträger enthalten.

Tabelle 5-26. Startlaufwerke

Startlaufwerke	Beschreibung
PXE	Start von einem PXE (Preboot Execution Environment)-Protokoll über die Netzwerkschnittstellenkarte.
Festplatte	Start von der Festplatte auf dem Server.
Lokale CD/DVD	Start von einem CD-/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-/DVD-Laufwerk oder CD/-DVD-ISO-Image. Das optische Laufwerk oder die ISO-Image-Datei befindet sich auf einem anderen Computer oder auf einer anderen Festplatte 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 iDRAC6- und iDRAC7-Systeme unterstützen.
Diskette	Start von einer Diskette im lokalen Diskettenlaufwerk.
RFS	Start von einem RFS (Remote File Share)-Abbild. Die Abbilddatei wird über den iDRAC-GUI-Konsolen-Viewer angehängt.

ANMERKUNG: Um das erste Startgerät für Server festzulegen, müssen Sie **Server Administrator**-Berechtigungen oder **Gehäusekonfiguration-Administrator**-Berechtigungen und **iDRAC-Anmeldeberechtigungen** haben.

So legen Sie das erste Startlaufwerk für einige oder alle Server im Gehäuse fest:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf **Server-Übersicht** und dann auf **Setup→ Erstes Startgerät**.

   Eine Serverliste wird angezeigt.
3. Wählen Sie im Listenfeld das Startgerät für die einzelnen Server aus.
4. Wenn der Server bei jedem Hochfahren von dem ausgewählten Gerät starten soll, deaktivieren Sie das Kontrollkästchen **Einmaliger Start** für den betreffenden Server.

   Wenn der Server beim nächsten Hochfahren einmalig von dem ausgewählten Gerät starten soll, aktivieren Sie das Kontrollkästchen **Boot Once** (Einmalig starten) für den betreffenden Server und klicken Sie auf **Anwenden**.

Funktionszustand eines einzelnen Servers anzeigen

Der Funktionszustand für einen einzelnen Server kann auf zwei Arten eingesehen werden – im Abschnitt **Gehäuse-Grafiken** auf der Seite **Gehäusefunktionszustand** oder auf der Seite **Serverstatus**.

Die Seite **Gehäusefunktionszustand** bietet einen grafischen Überblick über einen einzelnen Server, der im Gehäuse installiert ist.

Um den Funktionszustand aller Server mittels Gehäuse-Grafiken einzusehen:

1. Melden Sie sich bei der CMC-Webschnittstelle an.

   Die Seite **Gehäusefunktionszustand** wird angezeigt. Der mittlere Bereich der **Gehäuse-Grafiken** stellt die Vorderansicht des Gehäuses dar und zeigt den Funktionszustand für einzelne Server an. Der Serverfunktionszustand wird durch die Farbe der Server-Untergrafik angegeben:

   - Keine Unterlegung – Zeigt an, dass der Server vorhanden und eingeschaltet ist und mit dem CMC kommuniziert; es gibt keine Anzeichen eines ungünstigen Zustands.
   - Gelbes Vorsichtzeichen – Zeigt an, dass nur Warnungen ausgegeben wurden und dass Korrekturmaßnahmen getroffen werden müssen.

- Rotes X – Zeigt an, dass mindestens ein Fehlerzustand vorliegt. Dies bedeutet, dass der CMC weiterhin mit der Komponente kommunizieren kann und der Funktionszustand als kritisch angegeben ist.
- Grau unterlegt – Zeigt an, dass die Komponente vorhanden ist, aber nicht eingeschaltet. Sie kommuniziert nicht mit dem CMC und es gibt keine Anzeichen eines ungünstigen Zustands.

2 Positionieren Sie den Cursor auf einer einzelnen Server-Untergrafik.

Ein entsprechender Texthinweis oder Bildschirmtipp wird angezeigt. Der Texthinweis liefert zusätzliche Informationen zum Server.

3 Klicken Sie auf die Server-Untergrafik, um die Informationen zu diesem Server auszuwählen und Quicklinks rechts neben der Gehäuse-Grafik anzuzeigen.

Die Seite **Serverstatus** (nicht zu verwechseln mit der Seite *Status der Server*) enthält eine Übersicht des Servers und eine Start-URL zur Webschnittstelle für den Integrated Dell Remote Access Controller (iDRAC), der Firmware, die zur Verwaltung des Servers verwendet wird.

ANMERKUNG: Um die iDRAC-Benutzeroberfläche zu verwenden, müssen Sie für iDRAC einen Benutzernamen und ein Kennwort besitzen. Weitere Informationen zum iDRAC und zur Verwendung der iDRAC-Webschnittstelle finden Sie im *Benutzerhandbuch zur integrierten Firmware des Dell Remote Access Controllers*.

So zeigen Sie den Funktionszustand eines einzelnen Servers an:

1 Melden Sie sich bei der CMC-Webschnittstelle an.

2 Erweitern Sie in der Systemstruktur **Server-Übersicht**.

Es werden alle Server (1–16) in der erweiterten Liste der **Server** angezeigt.

3 Klicken Sie auf den Server (Steckplatz), den Sie anzeigen möchten.

Die Seite **Serverstatus** wird angezeigt.

Sie können die Serverstatusseite auch anzeigen, indem Sie auf den Status-Link bei den Server-Quicklinks rechts auf der Seite klicken.

Tabelle 5-27. Individueller Serverstatus - Eigenschaften

Element	Beschreibung		
Slot (Steckplatz)	Zeigt den vom Server auf dem Gehäuse belegten Steckplatz an. Steckplatznummern sind sequenzielle IDs von 1 bis 16 (im Gehäuse befinden sich 16 verfügbare Steckplätze), die bei der Identifizierung der Position des Servers im Gehäuse hilfreich sind.		
Slot Name (Steckplatzname)	Zeigt den Namen des Steckplatzes an, in dem sich der Server befindet.		
Präsentation	Zeigt an, ob der Server im Steckplatz vorhanden ist (Ja oder Nein). Wenn der Server nicht vorhanden ist, sind die Serverinformationen über Funktionszustand, Stromzustand und Service-Tag-Nummer unbekannt (nicht angezeigt).		
Seite „Funktionszustand“		OK	Zeigt an, dass der Server vorhanden ist und mit dem CMC kommuniziert. Im Falle eines Fehlers bei der Datenübertragung zwischen dem CMC und dem Server kann der CMC den Funktionszustand des Servers weder abrufen noch anzeigen.
		Informativ	Zeigt Informationen über den Server an, wenn beim Funktionsstatus (OK, Warnung, Schwerwiegend) keine Änderung aufgetreten ist.
		Warnung	Zeigt an, dass Warnungen ausgegeben wurden und *Korrekturmaßnahmen ergriffen werden müssen*. Falls keine Korrekturmaßnahmen ergriffen werden, können kritische Fehler die Integrität des Servers beinträchtigen.
		Kritisch	Zeigt an, dass mindestens eine Fehlerwarnung ausgegeben wurde. Ein kritischer Status stellt einen Systemfehler auf dem Server dar. *Es müssen umgehend Korrekturmaßnahmen getroffen werden.*
		Kein Wert	Wenn sich kein Server im Steckplatz befindet, werden keine Informationen zum Funktionszustand angezeigt.

Tabelle 5-27. Individueller Serverstatus - Eigenschaften *(fortgesetzt)*

Element	Beschreibung
Server Model (Servermodell)	Zeigt das Modell des Servers im Gehäuse an. Beispiele: **PowerEdge M600**, **PowerEdge M605**.
Service-Tag-Nummer	Zeigt die Service-Tag-Nummer des Servers an. Die Service-Tag-Nummer ist eine vom Hersteller eindeutig identifizierbare Nummer für Support- und Wartungsbelange. Wenn kein Server vorhanden ist, ist dieses Feld leer.
iDRAC Firmware	Zeigt die derzeit auf dem Server installierte iDRAC-Version an.
CPLD-Version	Zeigt die CPLD-Versionsnummer (Complex Programmable Logic Device) des Servers an.
BIOS-Version	Zeigt die BIOS-Version auf dem Server an.
„Operating System“ (Betriebssystem)	Zeigt das Betriebssystem auf dem Server an.
CPU Information	Zeigt den Typ und die Anzahl der auf dem Server installierten CPUs an.
Gesamtsystem speicher	Zeigt den gesamten auf dem Server installierten Systemspeicher (in GB) an.

Tabelle 5-28. Individueller Serverstatus - iDRAC-Systemereignisprotokoll

Element	Beschreibung		
Severity (Schweregrad)		OK	Zeigt ein normales Ereignis an, das keine Korrekturmaßnahmen erfordert.
		Informativ	Zeigt einen Informationseintrag über ein Ereignis an, in dem der Schweregradstatus nicht verändert wurde.
		Unbekannt	Zeigt ein unbekanntes/nicht-kategorisiertes Ereignis an.
		Warnung	Zeigt ein nicht-kritisches Ereignis an, bei dem möglichst bald Korrekturmaßnahmen getroffen werden müssen, um Systemfehler zu vermeiden.
		Kritisch	Zeigt ein kritisches Ereignis an, das umgehend Korrekturmaßnahmen erfordert, um Systemfehler zu vermeiden.
Date/Time (Uhrzeit/Datum)	Gibt das genaue Datum und die genaue Uhrzeit an, als das Ereignis eingetreten ist (z. B. Wed May 02 16:26:55 2007).		
Description (Beschreibung)	Enthält eine kurze Beschreibung des Ereignisses.		

Tabelle 5-29. Individueller Serverstatus - iDRAC-Netzwerkeinstellungen

Element	Beschreibung
LAN aktiviert	Zeigt an ob der LAN-Kanal aktiviert (**Ja**) oder deaktiviert (**Nein**) ist.

Tabelle 5-30. Individueller Serverstatus - IPv4 iDRAC-Netzwerkeinstellungen

Element	Beschreibung
Enabled (Aktiviert)	Zeigt an, ob das IPv4-Protokoll beim LAN verwendet wird (Ja). Wenn der Server IPv6 nicht unterstützt, ist das IPv4-Protokoll stets aktiviert und diese Einstellung wird nicht angezeigt.
DHCP aktiviert	Zeigt an ob das dynamische Host-Konfigurationsprotokoll (DHCP) aktiviert (**Ja**) oder deaktiviert (**Nein**) ist. Wenn diese Option aktiviert (**Ja**) ist, ruft der Server die IP-Konfiguration (IP-Adresse, Subnetzmaske und Gateway) automatisch von einem DHCP-Server in Ihrem Netzwerk ab. Dem Server in Ihrem Netzwerk ist immer eine eindeutige IP-Adresse zugewiesen.
IPMI-über-LAN aktiviert	Zeigt an, ob der IPMI-LAN-Kanal aktiviert (**Ja**) oder deaktiviert (**Nein**) ist.
IP-Adresse	Gibt die IP-Adresse für die iDRAC-Netzwerkschnittstelle an.
Subnetzmaske	Gibt die Subnetzmaske für die iDRAC-Netzwerkschnittstelle an.
Gateway	Gibt das Gateway für die iDRAC-Netzwerkschnittstelle an.

Tabelle 5-31. Individueller Serverstatus - IPv6 iDRAC-Netzwerkeinstellungen

Element	Beschreibung
Aktiviert	Zeigt an, ob das IPv6-Protokoll beim LAN verwendet wird (Ja).
AutoConfiguration aktiviert	Zeigt an, ob AutoConfiguration für IPv6 aktiviert ist (Ja). Wenn AutoConfiguration aktiviert ist, ruft der Server die IPv6-Konfiguration (**IPv6-Adresse, Präfixlänge** und **IPv6-Gateway**) automatisch von einem IPv6-Router in Ihrem Netzwerk ab. Der Server verfügt immer über eine eindeutige IPv6-Adresse über Ihr Netzwerk und kann bis zu 16 IPv6-Adressen erhalten.
Lokale Adresse verbinden	Dem CMC zugewiesene IPv6-Adresse, basierend auf der MAC-Adresse des CMC.

Tabelle 5-31. Individueller Serverstatus - IPv6 iDRAC-Netzwerkeinstellungen

Element	Beschreibung
Gateway	Zeigt das IPv6-Gateway für die iDRAC-Netzwerkschnittstelle an.
IPv6-Adresse	Zeigt eine IPv6-Adresse für die iDRAC-Netzwerkschnittstelle an. Es können bis zu 16 dieser Adressen bestehen. Die Präfixlänge, falls nicht Null, wird nach dem Schrägstrich („/“) angegeben.

Tabelle 5-32. Status eines einzelnen Servers - WWN/MAC-Adresse

Element	Beschreibung
Slot (Steckplatz)	Zeigt den vom Server auf dem Gehäuse besetzten Steckplatz an.
Location (Standort)	Zeigt den von den E/A-Modulen besetzen Standort an. Die sechs Standorte werden mit einer Kombination von Gruppenname (A, B oder C) und Steckplatznummer (1 oder 2) identifiziert. Steckplatznamen: A1, A2, B1, B2, C1 oder C2.
Fabric	Zeigt den Typ der E/A-Struktur an.
Server-Assigned (Serverzugewiesen)	Zeigt die serverzugewiesenen WWN/MAC-Adressen an, die in die Hardware der Steuerung eingebettet sind. WWN/MAC-Adressen, die „-“ anzeigen, weisen darauf hin, dass keine Schnittstelle für die angegebene Struktur installiert ist.

Tabelle 5-32. Status eines einzelnen Servers - WWN/MAC-Adresse *(fortgesetzt)*

Element	Beschreibung
Chassis-Assigned (Gehäusezugewiesen)	Zeigt die gehäusezugewiesenen WWN/MAC-Adressen an, die für einen bestimmten Steckplatz verwendet werden. WWN/MAC-Adressen, die „-“anzeigen, weisen darauf hin, dass die FlexAddress-Funktion nicht installiert ist. **ANMERKUNG:** Ein grünes Häkchen in der Spalte **Server zugewiesen** oder **Gehäuse zugewiesen** zeigt den Typ der aktiven Adressen an. **ANMERKUNG:** Wenn FlexAddress aktiviert ist, zeigen Steckplätze ohne installierte Server die gehäusezugewiesene MAC/WWN-Zuweisung für die eingebetteten Ethernet-Controller (Struktur A) an. Die gehäusezugewiesenen Adressen für die Strukturen B und C zeigen „-“ an, außer wenn diese Strukturen auf Servern mit belegten Steckplätzen verwendet werden; es wird angenommen, dass dieselben Strukturtypen in den nicht belegten Steckplätzen bereitgestellt werden.

Informationen zum Starten der iDRAC-Verwaltungskonsole und Richtlinien über Verfahren zur einfachen Anmeldung finden Sie unter „iDRAC mit einfacher Anmeldung starten“ auf Seite 262.

Funktionszustand der E/A-Module anzeigen

Der Funktionszustand der EAMs kann auf zwei Arten eingesehen werden: im Abschnitt **Gehäusekomponenten-Zusammenfassung** auf der Seite **Gehäusefunktionszustand** oder auf der Seite **E/A-Modulstatus**. Die Seite **Gehäusefunktionszustand** bietet einen grafischen Überblick über die im Gehäuse installierten EAMs.

Um den Funktionszustand der EAMs mittels Gehäuse-Grafiken anzuzeigen:

1. Melden Sie sich bei der CMC-Webschnittstelle an.

   Die Seite **Gehäusefunktionszustand** wird angezeigt. Der untere Bereich der **Gehäuse-Grafiken** stellt die Rückansicht des Gehäuses dar und enthält den Funktionszustand für die EAMs. Der EAM-Funktionszustand wird durch die Farbe der EAM-Untergrafik angegeben:

   - Keine Unterlegung - IOM ist vorhanden, wird mit Strom versorgt und kommuniziert mit dem CMC; es gibt keine Anzeichen eines ungünstigen Zustands.
   - Gelbes Vorsichtzeichen - Zeigt an, dass nur Warnungen ausgegeben wurden und dass Korrekturmaßnahmen getroffen werden müssen.
   - Rotes X - Zeigt an, dass mindestens ein Fehlerzustand vorliegt. Dies bedeutet, dass der CMC weiterhin mit der Komponente kommunizieren kann und der angegebene Funktionszustand kritisch ist.
   - Grau unterlegt - Zeigt an, dass das EAM vorhanden ist, aber nicht eingeschaltet. Sie kommuniziert nicht mit dem CMC und es gibt keine Anzeichen eines ungünstigen Zustands.

2. Bewegen Sie den Cursor über eine einzelne EAM-Untergrafik.

   Ein Texthinweis oder Bildschirmtipp wird angezeigt. Der Texthinweis liefert zusätzliche Informationen zu diesem EAM.

3. Klicken auf die EAM-Untergrafik, wählt die Informationen zu diesem EAM und die Quicklinks zur Anzeige rechts neben den Gehäuse-Grafiken aus.

Die Seite **Status der E/A-Module** enthält Übersichten zu allen mit dem Gehäuse verbundenen E/A-Modulen. Wie Sie den Funktionszustand der E/A-Module über die Webschnittstelle oder RACADM anzeigen, erfahren Sie unter „EAM-Funktionszustand überwachen“ auf Seite 458.

Funktionszustand der Lüfter anzeigen

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.

Der Funktionszustand der Lüfter kann auf zwei Arten eingesehen werden: im Abschnitt **Gehäusekomponenten-Zusammenfassung** auf der Seite **Gehäusefunktionszustand** oder auf der Seite **Lüfterstatus**. Die Seite **Gehäusefunktionszustand** bietet einen grafischen Überblick über alle Lüfter, die im Gehäuse installiert sind.

Um den Funktionszustand aller Lüfter mittels **Gehäuse-Grafiken** einzusehen:

1. Melden Sie sich bei der CMC-Webschnittstelle an.

   Die Seite **Gehäusefunktionszustand** wird angezeigt. Der untere Abschnitt der **Gehäuse-Grafiken** stellt die Rückansicht des Gehäuses dar und enthält den Funktionszustand aller Lüfter. Der Lüfter-Funktionszustand wird durch die Farbe der Lüfter-Untergrafik angegeben:

   - Keine Unterlegung - Der Lüfter ist vorhanden und läuft; es gibt keine Anzeichen eines ungünstigen Zustands.
   - Gelbes Vorsichtzeichen - Zeigt an, dass nur Warnungen ausgegeben wurden und dass Korrekturmaßnahmen getroffen werden müssen.
   - Rotes X - Zeigt an, dass mindestens ein Fehlerzustand vorliegt. Dies bedeutet, dass der Funktionszustand als kritisch angegeben wird.
   - Grau unterlegt - Zeigt an, dass der Lüfter vorhanden ist, aber nicht eingeschaltet. Es gibt kein Anzeichen für einen ungünstigen Zustand.

2. Positionieren Sie den Cursor auf einer einzelnen Lüfter-Untergrafik.

   Ein Texthinweis oder Bildschirmtipp wird angezeigt. Der Texthinweis liefert zusätzliche Informationen zu diesem Lüfter.

3. Klicken auf die Lüfter-Untergrafik wählt die Informationen zu diesem Lüfter und die Quicklinks zur Anzeige rechts neben den Gehäuse-Grafiken aus.

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

Der CMC, der die Lüftergeschwindigkeit steuert, erhöht oder verringert die Lüftergeschwindigkeit automatisch anhand systemweiter Ereignisse.
Der CMC erstellt eine Warnung und erhöht die Lüftergeschwindigkeiten, wenn die folgenden Ereignisse auftreten:

- Der Schwellenwert der CMC-Umgebungstemperatur wird überschritten.
- Ein Lüfter fällt aus.
- Ein Lüfter wird aus dem Gehäuse entfernt.

So zeigen Sie den Funktionszustand der Lüftereinheiten an:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur **Lüfter** aus.

   Die Seite **Lüfterstatus** wird angezeigt.

Sie können die Seite **Lüfterstatus** auch anzeigen, indem Sie auf den Status-Link bei den Lüfter-Quicklinks rechts auf der Seite klicken.

Tabelle 5-33. Informationen zum Funktionsstatus der Lüfter

Element	Beschreibung	
Name	Zeigt den Lüfternamen im folgenden Format an: **FAN**-*n*, wobei *n* die Nummer des Lüfters darstellt.	
Präsentation	Zeigt an, ob der Lüfter vorhanden ist (**Ja** oder **Nein**).	
Seite „Funktionszustand“	 OK	Zeigt an, dass die Lüftereinheit vorhanden ist und mit dem CMC kommuniziert. Im Falle eines Fehlers bei der Datenübertragung zwischen dem CMC und der Lüftereinheit kann der CMC den Funktionsstatus der Lüftereinheit weder abrufen noch anzeigen.
	 Kritisch	Zeigt an, dass mindestens eine Fehlerwarnung ausgegeben wurde. Ein kritischer Status weist auf einen Systemfehler in der Lüftereinheit hin, und es müssen sofort Korrekturmaßnahmen ergriffen werden, um ein Überhitzen und Herunterfahren des Systems zu verhindern.

Tabelle 5-33. Informationen zum Funktionsstatus der Lüfter *(fortgesetzt)*

Element	Beschreibung	
	Unbekannt	Wird angezeigt, wenn das Gehäuse zuerst eingeschaltet wird. Im Falle eines Fehlers bei der Datenübertragung zwischen dem CMC und der Lüftereinheit kann der CMC den Funktionsstatus der Lüftereinheit weder abrufen noch anzeigen.
Taktrate		Zeigt die Geschwindigkeit des Lüfters in U/Min. an.

iKVM-Status anzeigen

Das Lokalzugriffs-KVM-Modul für das Dell M1000e-Servergehäuse lautet Avocent Integrated KVM Switch Modul (iKVM). Der Funktionszustand des mit dem Gehäuse verbundenen iKVM kann auf der Seite **Gehäusefunktionszustand** eingesehen werden.

So zeigen Sie den Funktionszustand des iKVM über **Gehäuse-Grafiken** an:

1 Melden Sie sich bei der CMC-Webschnittstelle an.

Die Seite **Gehäusefunktionszustand** wird angezeigt. Der untere Abschnitt der **Gehäuse-Grafiken** zeigt die Rückansicht des Gehäuses und enthält den Funktionszustand des iKVM. Der iKVM-Funktionszustand wird durch die Farbe der iKVM-Untergrafik angezeigt:

- Keine Unterlegung - iKVM ist vorhanden, wird mit Strom versorgt und kommuniziert mit dem CMC; es gibt keine Anzeichen eines ungünstigen Zustands.
- Gelbes Vorsichtzeichen - Zeigt an, dass nur Warnungen ausgegeben wurden und dass Korrekturmaßnahmen getroffen werden müssen.
- Rotes X - Zeigt an, dass mindestens ein Fehlerzustand vorliegt. Dies bedeutet, dass das iKVM weiterhin mit der Komponente kommunizieren kann und der angegebene Funktionszustand kritisch ist.
- Grau unterlegt - Zeigt an, dass das iKVM vorhanden ist, aber nicht eingeschaltet. Sie kommuniziert nicht mit dem CMC und es gibt keine Anzeichen eines ungünstigen Zustands.

2 Fahren Sie mit dem Cursor über die iKVM-Untergrafik.

Ein Texthinweis oder Bildschirmtipp wird angezeigt. Der Texthinweis liefert zusätzliche Informationen zu diesem iKVM.

3 Klicken auf die iKVM-Untergrafik wählt die Informationen zu diesem iKVM und die Quicklinks zur Anzeige rechts neben den Gehäuse-Grafiken aus.

Sie können die Seite **iKVM-Status** auch anzeigen, indem Sie auf den Status-Link bei den iKVM-Quicklinks rechts neben dem Gehäuse-Grafiken klicken.

Wie Sie den iKVM-Status anzeigen und die Eigenschaften für das iKVM einrichten, erfahren Sie unter:

- „iKVM-Status und -Eigenschaften anzeigen“ auf Seite 442
- „Frontblende aktivieren oder deaktivieren“ auf Seite 440
- „Dell CMC-Konsole über iKVM aktivieren.“ auf Seite 441
- „Aktualisieren der iKVM-Firmware“ auf Seite 444

Weitere Informationen zum iKVM finden Sie unter „iKVM-Modul verwenden“ auf Seite 419.

Funktionszustand der Netzteileinheiten anzeigen

Der Funktionszustand der Netzteileinheiten innerhalb des Gehäuses kann auf zwei Arten eingesehen werden: im Abschnitt **Gehäusekomponenten-Zusammenfassung** auf der Seite **Gehäusefunktionszustand** oder auf der Seite **Netzteilstatus**. Die Seite **Gehäusefunktionszustand** bietet einen grafischen Überblick über alle Netzteileinheiten, die im Gehäuse installiert sind.

Um den Funktionszustand aller Netzteileinheiten mittels **Gehäuse-Grafiken** einzusehen:

1 Melden Sie sich bei der CMC-Webschnittstelle an.

Die Seite **Gehäusefunktionszustand** wird angezeigt. Der untere Abschnitt der **Gehäuse-Grafiken** stellt die Rückansicht des Gehäuses dar und enthält den Funktionszustand aller Netzteileinheiten. Der Netzteileinheit-Funktionszustand wird durch die Farbe der Netzteileinheit-Untergrafik angegeben:

- Keine Unterlegung - PSU ist vorhanden, wird mit Strom versorgt und kommuniziert mit dem CMC; es gibt keine Anzeichen eines ungünstigen Zustands.

- Gelbes Vorsichtzeichen - Zeigt an, dass nur Warnungen ausgegeben wurden und dass Korrekturmaßnahmen getroffen werden müssen.
- Rotes X - Zeigt an, dass mindestens ein Fehlerzustand vorliegt. Dies bedeutet, dass der CMC weiterhin mit der Netzteileinheit kommunizieren kann und der Funktionszustand als kritisch angegeben ist.
- Grau unterlegt - Zeigt an, dass die Netzteileinheit vorhanden ist, aber nicht eingeschaltet. Sie kommuniziert nicht mit dem CMC und es gibt keine Anzeichen eines ungünstigen Zustands.

2 Bewegen Sie den Cursor über eine einzelne Netzteileinheit-Untergrafik und ein entsprechender Texthinweis oder Bildschirmtipp wird angezeigt. Der Texthinweis liefert zusätzliche Informationen zu diesem Netzteil.

3 Klicken auf die Netzteileinheit-Untergrafik wählt die Informationen zu diese Netzteileinheit und die Quicklinks zur Anzeige rechts neben den Gehäuse-Grafiken aus.

Die Seite **Netzteilstatus** zeigt den Status und die Messwerte der Netzteileinheiten an, die dem Gehäuse zugeordnet sind. Weitere Informationen über die Stromverwaltung des CMC finden Sie unter „Stromverwaltung“ auf Seite 363.

So zeigen Sie den Funktionszustand der Netzteileinheiten an:

1 Melden Sie sich bei der CMC-Webschnittstelle an.

2 Wählen Sie in der Systemstruktur **Netzteile** aus.

Die Seite **Netzteilstatus** wird angezeigt.

Sie können die Seite **Netzteilstatus** auch anzeigen, indem Sie auf den Status-Link bei den Netzteil-Quicklinks rechts neben dem Gehäuse-Grafiken klicken.

Tabelle 5-34. Informationen zum Funktionszustand von Netzteilen

Element	Beschreibung	
Name		Zeigt den Namen der Netzteileinheit an: *PS-n*, wobei *n* die Nummer des Netzteils ist.
Präsentation		Zeigt an, ob das Netzteil vorhanden ist (**Ja** oder **Nein**).
Seite „Funktionszustand“	 OK	Zeigt an, dass die Netzteileinheit vorhanden ist und mit dem CMC kommuniziert. Zeigt an, dass der Funktionszustand der Netzteileinheit in Ordnung ist. Im Falle eines Fehlers bei der Datenübertragung zwischen dem CMC und der Lüftereinheit kann der CMC den Funktionsstatus der Lüftereinheit weder abrufen noch anzeigen.
	 Kritisch	Zeigt an, dass die Netzteileinheit einen Fehler aufweist und der Funktionszustand kritisch ist. **Es müssen sofort Korrekturmaßnahmen ergriffen werden.** Wird dies nicht getan, wird die Komponente auf Grund von Stromverlust möglicherweise heruntergefahren.
	 Unbekannt	Wird angezeigt, wenn das Gehäuse anfänglich eingeschaltet wird. Im Falle eines Fehlers bei der Datenübertragung zwischen dem CMC und der Lüftereinheit kann der CMC den Funktionsstatus der Lüftereinheit weder abrufen noch anzeigen.
Stromstatus		Zeigt den Stromzustand der Netzteileinheit an: **Online**, **Aus**, **Steckplatz unbelegt**.
Kapazität		Zeigt die Stromkapazität in Watt an.

Tabelle 5-35. Systemstromstatus

Element	Beschreibung
Gesamt-Stromfunktions-zustand	Zeigt den Funktionszustand (**OK**, **Nicht-kritisch**, **Kritisch**, **Nicht behebbar**, **Andere**, **Unbekannt**) für die Energieverwaltung im gesamten Gehäuse an.
Systemstromstatus	Zeigt den Stromstatus (**Ein**, **Aus**, **Einschalten**, **Ausschalten**) für das Gehäuse an.
Redundanz	Zeigt den Netzteilredundanzstatus an. Zu den Werten gehören: **Nein**: Netzteile sind nicht redundant. **Ja**: Volle Redundanz wirksam.

Status der Temperatursensoren anzeigen

Die Seite **Temperatursensorstatus** zeigt den Status und die Messergebnisse der Temperatursonden des gesamten Gehäuses an (Gehäuse und Server).

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.

So zeigen Sie den Funktionszustand der Temperatursonden an.

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur **Temperatursensoren** aus.

   Die Seite **Temperatursensorenstatus** wird angezeigt.

Tabelle 5-36. Informationen zum Funktionszustand der Temperatursensoren

Element	Beschreibung	
ID	Zeigt den Standort der Temperatursonde an.	
Name	Zeigt den Namen jeder Temperatursonde für das Gehäuse und die Server an.	
Präsentation	Zeigt an, ob das Modul im Gehäuse vorhanden (Ja) oder nicht vorhanden (Nein) ist.	
Seite „Funktionszustand“	OK	Zeigt an, dass das Modul vorhanden ist und mit dem CMC kommuniziert. Im Falle eines Fehlers bei der Datenübertragung zwischen dem CMC und dem Server kann der CMC den Funktionszustand des Servers weder abrufen noch anzeigen.
	Warnung	Zeigt an, dass Warnungen ausgegeben wurden und Korrekturmaßnahmen getroffen werden müssen. Falls keine Korrekturmaßnahmen getroffen werden, können kritische oder schwerwiegende Fehler die Integrität des Moduls beinträchtigen.
	Kritisch	Zeigt an, dass eine Fehlerwarnung ausgegeben wurde. Ein schwerwiegender Status zeigt einen Systemfehler auf dem Server. Es müssen umgehend Korrekturmaßnahmen getroffen werden.
	Unbekannt	Zeigt, dass keine Kommunikation mit dem Modul aufgebaut wurde. Dies liegt gewöhnlich daran, dass das Gehäuse ausgeschaltet ist oder die Gehäuseinitialisierung noch nicht abgeschlossen ist.
Messwert	Zeigt die aktuelle Temperatur in Grad Celsius und Grad Fahrenheit an.	
Maximaler Schwellenwert	Zeigt die höchste Temperatur in Grad Celsius und Grad Fahrenheit an, bei der eine Fehlerwarnung ausgegeben wird.	

LCD-Status anzeigen

Sie können den Funktionsstatus der LCD mithilfe der Gehäuse-Grafiken anzeigen, die auf der Seite **Gehäusefunktionszustand** mit dem Gehäuse verknüpft sind.

So zeigen Sie den Funktionszustand der LCD an:

1. Melden Sie sich bei der CMC-Webschnittstelle an.

   Die Seite **Gehäusefunktionszustand** wird angezeigt. Der obere Abschnitt der Gehäuse-Grafiken erläutert die Vorderansicht des Gehäuses. Der LCD-Funktionszustand wird durch die Farbe der LCD-Untergrafik angegeben:

   - Keine Unterlegung - LCD ist vorhanden, eingeschaltet und kommuniziert mit dem CMC. Es liegt kein ungünstiger Zustand vor.
   - Gelbes Vorsichtzeichen - Warnungen wurden ausgegeben und Korrekturmaßnahmen müssen getroffen werden.
   - Rotes X - mindestens ein Fehlerzustand liegt vor. Der Funktionszustand ist kritisch.
   - Grau unterlegt - die LCD ist vorhanden und nicht eingeschaltet. Es kommuniziert nicht mit dem CMC und es gibt keine Anzeichen eines ungünstigen Zustands.

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 auszuwählen und rechts neben dem Gehäuse-Grafiken anzuzeigen.

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, Struktur B und Struktur C 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 Funktion FlexAddress finden Sie unter „FlexAddress verwenden“ auf Seite 281.

WWN/MAC-Adressen

Der Abschnitt **WWN/MAC-Adresse** zeigt die WWN/MAC-Informationen an, die allen Servern zugewiesen sind, selbst wenn diese Serversteckplätze zurzeit unbelegt sind. **Position** zeigt die Position des von den Eingabe/Ausgabe-Modulen belegten Steckplatzes an. Die sechs Steckplätze werden durch eine Kombination des Gruppennamen (A, B oder C) und der Steckplatznummer (1 oder 2) identifiziert: Steckplatznamen A1, A2, B1, B2, C1 oder C2. Der iDRAC ist der integrierte Management-Controller des Servers. **Struktur** zeigt den Typ der E/A-Struktur an. **Serverzugewiesen** zeigt die serverzugewiesenen WWN/MAC-Adressen an, die in die Hardware der Steuerung eingebettet sind. **Gehäusezugewiesen** zeigt die gehäusezugewiesenen WWN/MAC-Adressen an, die für einen bestimmten Steckplatz verwendet werden. Ein grünes Häkchen in der Spalte **Serverzugewiesen** oder **Gehäusezugewiesen** zeigt den Typ der aktiven Adressen an. Gehäusezugewiesene Adressen werden zugewiesen, wenn FlexAddress auf dem Gehäuse aktiviert ist, und stellen die steckplatzgebundenen Adressen dar. Wenn die gehäusezugewiesenen Adressen markiert sind, werden diese Adressen selbst dann verwendet, wenn ein Server mit einem anderen ausgetauscht wird.

CMC-Netzwerkeigenschaften konfigurieren

ANMERKUNG: Netzwerkkonfigurationsänderungen können zu Verbindungsverlust der aktuellen Netzwerkanmeldung führen.

Einrichtung des Erstzugriffs auf den CMC

Bevor Sie mit der Konfiguration des CMC beginnen, müssen Sie zuerst die CMC-Netzwerkeinstellungen konfigurieren, sodass Sie den CMC im Remote-Zugriff verwalten können. Diese Erstkonfiguration weist die TCP/IP-Netzwerkbetriebsparameter zu, die den Zugriff auf den CMC aktivieren.

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

1. Melden Sie sich bei der Webschnittstelle an.
2. Wählen Sie in der Systemstruktur **Gehäuse-Übersicht** aus.
3. Klicken Sie auf das Register **Netzwerk**.

   Die Seite **Netzwerkkonfiguration** wird angezeigt.
4. Aktivieren oder deaktivieren Sie DHCP für den CMC, indem Sie das Kontrollkästchen **DHCP verwenden (für CMC-Netzwerkschnittstellen-IP-Adresse)** auswählen oder abwählen.
5. Wenn Sie DHCP deaktiviert haben, geben Sie die IP-Adresse, das Gateway und die Subnetzmaske ein.
6. Klicken Sie unten auf der Seite auf **Änderungen anwenden**.

Konfigurieren der Netzwerk-LAN-Einstellungen

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

ANMERKUNG: Die Einstellungen auf der Seite **Netzwerkkonfiguration**, z. B. Community-Zeichenkette und SMTP-Server-IP-Adresse, betreffen die CMC-Einstellungen sowie die externen Einstellungen des Gehäuses.

ANMERKUNG: Wenn Sie über zwei CMCs (Aktiv und Standby) im Gehäuse verfügen und beide mit dem Netzwerk verbunden sind, übernimmt der Standby-CMC automatisch die Netzwerkeinstellungen für den Fall, dass ein Fehlerereignis auf dem aktiven CMC eintritt.

Konfiguration der LAN-Netzwerkeinstellungen:

1. Melden Sie sich bei der Webschnittstelle an.
2. Klicken Sie auf das Register **Netzwerk**.
3. Konfigurieren Sie die in Tabelle 5-37 beschriebenen CMC-Netzwerkeinstellungen über Tabelle 5-39 und klicken Sie auf **Änderungen anwenden**.

Um den IP-Bereich und die Einstellungen für die Blockierung von IP-Adressen zu konfigurieren, klicken Sie auf die Schaltfläche **Erweiterte Einstellungen** (siehe „CMC-Netzwerksicherheitseinstellungen konfigurieren“ auf Seite 185).

Um den Inhalt der Seite **Netzwerkkonfiguration** zu aktualisieren, klicken Sie auf **Aktualisieren**.

Um den Inhalt der Seite **Netzwerkkonfiguration** zu drucken, klicken Sie a uf **Drucken**.

Tabelle 5-37. Netzwerkeinstellungen

Einstellung	Beschreibung
CMC-MAC-Adresse	Zeigt die MAC-Adresse des Gehäuses an, die eine eindeutig identifizierbare Adresse für das Gehäuse im Netzwerk ist.
CMC-Netzwerkschnittstelle aktivieren	Aktiviert die Netzwerkschnittstelle des CMC. **Standardeinstellung:** Aktiviert. Wenn diese Option ausgewählt ist: • Kommuniziert der CMC mit dem Computernetzwerk und ist über dieses zugänglich. • Mit dem CMC verbundene Webschnittstelle, CLI (Remote-RACADM), WSMAN, Telnet und SSH sind verfügbar. Wenn diese Option nicht ausgewählt ist: • Die Netzwerkschnittstelle kann nicht über das Netzwerk kommunizieren. • Die Kommunikation über den CMC zum Gehäuse steht nicht zur Verfügung. • Mit dem CMC verbundene Webschnittstelle, CLI (Remote-RACADM), WSMAN, Telnet und SSH sind nicht verfügbar. • Auf die iDRAC-Webschnittstelle des Servers, die lokale CLI, E/A-Module und das iKVM kann noch zugegriffen werden. • Netzwerkadressen für den iDRAC und CMC können in diesem Fall von der Gehäuse-LCD abgelesen werden. **ANMERKUNG:** Der Zugriff auf die anderen Gehäusekomponenten im Netzwerk ist nicht betroffen, wenn das Netzwerk im Gehäuse deaktiviert wird (oder verloren geht).
CMC auf DNS registrieren	Diese Eigenschaft registriert den CMC-Namen auf dem DNS-Server. **Standard:** standardmäßig nicht markiert (deaktiviert). **ANMERKUNG:** Einige DNS-Server registrieren nur Namen mit maximal 31 Zeichen. Stellen Sie sicher, dass sich der jeweilige Name innerhalb des DNS-erforderlichen Limits befindet.

Tabelle 5-37. Netzwerkeinstellungen *(fortgesetzt)*

Einstellung	Beschreibung
DNS-CMC-Name	Zeigt den CMC-Namen nur an, wenn **CMC auf DNS registrieren** ausgewählt ist. Der Standard-CMC-Name ist *CMC_service_tag*, wobei *service tag* die Service-Tag-Nummer des Gehäuses ist, z. B. CMC-00002. Die maximale Anzahl von Zeichen beträgt 63. Das erste Zeichen muss ein Buchstabe (a-z, A-Z) sein, gefolgt von einem alphanumerischen Zeichen (a-z, A-Z, 0-9) oder einem Bindestrich (-).
DHCP für den DNS-Domänennamen verwenden	Verwendet den Standard-DNS-Domänennamen. Dieses Kontrollkästchen ist nur dann aktiv, wenn **DHCP verwenden (für CMC-Netzwerkschnittstellen-IP-Adresse)** ausgewählt ist. **Standardeinstellung:** Aktiviert.
DNS-Domänenname	Der Standard-DNS-Domänenname ist ein Leerzeichen. Dieses Feld kann nur bearbeitet werden, wenn das Kontrollkästchen **DHCP für den DNS-Domänennamen verwenden** ausgewählt ist.
Automatische Verhandlung (1 Gb)	Legt fest, ob der CMC automatisch den Duplexmodus und die Netzwerkgeschwindigkeit festlegt, indem er mit dem nächstgelegenen Router oder Switch kommuniziert (**Ein**), oder ob Sie den Duplexmodus und die Netzwerkgeschwindigkeit manuell festlegen können (**Aus**). **Standardeinstellung**: Ein. **Wenn Automatische Verhandlung eingeschaltet ist**, kommuniziert der CMC automatisch mit dem nächsten Router oder Switch und arbeitet mit einer Geschwindigkeit von 1 Gb. **Wenn Automatische Verhandlung ausgeschaltet ist**, müssen Sie den Duplexmodus und die Netzwerkgeschwindigkeit manuell festlegen.

Tabelle 5-37. Netzwerkeinstellungen *(fortgesetzt)*

Einstellung	Beschreibung
Netzwerk-geschwindigkeit	Legen Sie die Netzwerkgeschwindigkeit in Übereinstimmung mit der Netzwerkumgebung auf 1 GBit/s, 100 MBit/s oder 10 MBit/s fest. **ANMERKUNG:** Die Einstellung der Netzwerkgeschwindigkeit muss mit Ihrer Netzwerkkonfiguration übereinstimmen, um einen effektiven Netzwerkdurchsatz zu gewährleisten. Wenn die Netzwerkgeschwindigkeit geringer eingestellt wird als die Geschwindigkeit Ihrer Netzwerkkonfiguration, steigt der Verbrauch der Bandbreite und die Netzwerkkommunikation wird verlangsamt. **Stellen Sie fest, ob Ihr Netzwerk höhere Netzwerkgeschwindigkeiten unterstützt, und stellen Sie sie entsprechend ein.** Wenn Ihre Netzwerkkonfiguration mit keinem dieser Werte übereinstimmt, empfiehlt Dell, die **Automatische Verhandlung** zu verwenden oder sich mit dem Hersteller Ihrer Netzwerkausstattung in Verbindung zu setzen. **ANMERKUNG:** Um eine Geschwindigkeit von 1000 Mb oder 1 Gb zu verwenden, wählen Sie **Automatische Verhandlung**.
Duplexmodus	Legen Sie den Duplexmodus in Übereinstimmung mit der Netzwerkumgebung auf „Voll“ oder „Halb“ fest. **Auswirkungen:** 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 Verhandlung automatisch auf Standard (Halbduplex). Ein derartiger Duplex-Übereinstimmungsfehler resultiert in einer langsamen Netzwerkverbindung. **ANMERKUNG:** Die Einstellungen der Netzwerkgeschwindigkeit und des Duplexmodus sind nicht verfügbar, wenn die automatische Verhandlung auf „Ein“ eingestellt ist.

Tabelle 5-37. Netzwerkeinstellungen *(fortgesetzt)*

Einstellung	Beschreibung
MTU	Legt den Wert für die maximale Größe der Übertragungseinheit (MTU) fest bzw. das größte Paket, das über die Schnittstelle übertragen werden kann. **Konfigurationsbereich:** 576 - 1500. **Standardeinstellung:** 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.

Tabelle 5-38. IPv4-Einstellungen

Einstellung	Beschreibung
IPv4 aktivieren	Der CMC kann das IPv4-Protokoll verwenden, um im Netzwerk zu kommunizieren. Wenn dieses Feld deaktiviert wird, wird dadurch IPv6-Netzwerkverkehr nicht verhindert. Standardeinstellung: Markiert (aktiviert).
DHCP aktivieren	Hierdurch kann der CMC automatisch vom Server des IPv4-DHCP (dynamisches Host-Konfigurationsprotokoll) eine IP-Adresse anfordern und abrufen. Standardeinstellung: Markiert (aktiviert). Wenn diese Option ausgewählt ist, ruft der CMC die IPv4-Konfiguration (IP-Adresse, Subnetzmaske und Gateway) automatisch von einem DHCP-Server in Ihrem Netzwerk ab. Dem Server in Ihrem Netzwerk ist immer eine eindeutige IP-Adresse zugewiesen. **ANMERKUNG:** Wenn diese Funktion aktiviert ist, werden die Eigenschaftsfelder **Statische IP-Adresse**, **Statische Subnetzmaske** und **Statisches Gateway** (auf der Seite **Netzwerkkonfiguration** unmittelbar neben dieser Option) deaktiviert. Hierbei werden alle zu einem früheren Zeitpunkt eingegebenen Werte für diese Eigenschaften ignoriert. Falls diese Option nicht aktiviert ist, müssen die **statische IP-Adresse**, die **statische Subnetzmaske** und das **statische Gateway** unmittelbar im Anschluss an diese Option auf der Seite **Netzwerkkonfiguration** manuell eingegeben werden.
Statische IP-Adresse	Gibt die IPv4-Adresse für die CMC Netzwerkschnittstelle an.
Statische Subnetzmaske	Gibt die statische IPv4-Subnetzmaske für die CMC-Netzwerkschnittstelle an.

Tabelle 5-38. IPv4-Einstellungen *(fortgesetzt)*

Einstellung	Beschreibung
Statisches Gateway	Gibt das IPv4-Gateway für die CMC Netzwerkschnittstelle an. **ANMERKUNG:** Die Felder **Statische IP-Adresse**, **Statische Subnetzmaske** und **Statisches Gateway** sind nur aktiviert, wenn **DHCP aktivieren** (das Eigenschaftsfeld, das diesen Feldern vorangeht) deaktiviert (nicht markiert) ist. In diesem Fall müssen die **statische IP-Adresse**, die **statische Subnetzmaske** und das **statische Gateway** für den Gebrauch durch den CMC über das Netzwerk manuell eingegeben werden. **ANMERKUNG:** Die Felder **Statische IP-Adresse**, **Statische Subnetzmaske** und **Statisches Gateway** gelten nur für das Gehäusegerät. Sie haben keine Auswirkung auf die anderen über das Netzwerk zugänglichen Komponenten der Gehäuselösung, zum Beispiel Servernetzwerk, lokaler Zugriff, E/A-Module und iKVM.

Tabelle 5-38. IPv4-Einstellungen *(fortgesetzt)*

Einstellung	Beschreibung
DHCP zum Abrufen von DNS-Serveradressen verwenden	Ruft die primären und sekundären DNS-Serveradressen vom DHCP-Server anstatt von den statischen Einstellungen ab. **Standardeinstellung:** Standardmäßig markiert (aktiviert) **ANMERKUNG:** Wenn **DHCP verwenden (für CMC-Netzwerkschnittstellen-IP-Adresse)** aktiviert ist, aktivieren Sie die Eigenschaft **DHCP zum Abrufen von DNS-Serveradressen verwenden**. Wenn diese Option aktiviert ist, ruft der CMC seine DNS-IP-Adresse automatisch von einem DHCP-Server im Netzwerk ab. **ANMERKUNG:** Wenn diese Eigenschaft aktiviert ist, sind die Eigenschaftsfelder des statischen bevorzugten DNS-Servers und des statisch alternativen DNS-Servers (unmittelbar nach dieser Option auf der Seite „Netzwerkkonfiguration") deaktiviert, und alle zu einem früheren Zeitpunkt eingegebenen Werte für diese Eigenschaften werden ignoriert. Wenn diese Option **nicht** ausgewählt ist, ruft der CMC die DNS-Server-IP-Adresse vom statischen bevorzugten DNS-Server und statischen alternativen DNS-Server ab. Die Adressen dieser Server werden in den Textfeldern festgelegt, die dieser Option auf der Seite **Netzwerkkonfiguration** unmittelbar folgen.
Statischer bevorzugter DNS-Server	Legt die statische IP-Adresse für den bevorzugten DNS-Server fest. Der statische bevorzugte DNS-Server wird nur implementiert, wenn **DHCP zum Abrufen von DNS-Serveradressen verwenden** deaktiviert ist.
Statischer alternativer DNS-Server	Legt die statische IP -Adresse für den alternierenden DNS -Server fest. Der statische alternative DNS-Server wird nur implementiert, wenn **DHCP zum Abrufen von DNS-Serveradressen verwenden** deaktiviert ist. Wenn Sie über keinen alternativen DNS-Server verfügen, geben Sie eine IP-Adresse mit 0.0.0.0 ein.

Tabelle 5-39. IPv6-Einstellungen:

Einstellung	Beschreibung
IPv6 aktivieren	Der CMC kann das IPv6-Protokoll verwenden, um im Netzwerk zu kommunizieren. Wenn dieses Feld deaktiviert wird, wird dadurch IPv4-Netzwerkverkehr nicht verhindert. Standardeinstellung: Markiert (aktiviert).
AutoConfiguration aktivieren	Der CMC kann das IPv6-Protokoll verwenden, um IPv6-Adress- und -Gateway-Einstellungen von einem IPv6-Router zu erhalten, der zur Bereitstellung dieser Informationen konfiguriert ist. Der CMC verfügt dann in Ihrem Netzwerk über eine eindeutige IPv6-Adresse. **Standardeinstellung:** Markiert (aktiviert). **ANMERKUNG:** Wenn diese Funktion aktiviert ist, werden die Eigenschaftsfelder **Statische IPv6-Adresse, Statische Präfixlänge** und **Statisches Gateway** (auf der Seite **Netzwerkkonfiguration** unmittelbar neben dieser Option) deaktiviert. Hierbei werden alle zu einem früheren Zeitpunkt eingegebenen Werte für diese Eigenschaften ignoriert. Falls diese Option nicht aktiviert ist, müssen die statische IPv6-Adresse, die statische Präfixlänge und das statische Gateway unmittelbar im Anschluss an diese Option auf der Seite **Netzwerkkonfiguration** manuell eingegeben werden.
Statische IPv6-Adresse	Gibt die IPv6-Adresse für die CMC-Netzwerkschnittstelle an, wenn Autokonfiguration nicht aktiviert ist.
Statische Präfixlänge	Gibt die IPv6-Präfixlänge für die CMC-Netzwerkschnittstelle an, wenn Autokonfiguration nicht aktiviert ist.

Tabelle 5-39. IPv6-Einstellungen: *(fortgesetzt)*

Einstellung	Beschreibung
Statisches Gateway	Gibt das statische IPv6-Gateway für die CMC-Netzwerkschnittstelle an, wenn Autokonfiguration nicht aktiviert ist. **ANMERKUNG:** Die Felder **Statische IPv6-Adresse**, **Statische Präfixlänge** und **Statisches Gateway** sind nur aktiviert, wenn **AutoConfiguration aktivieren** (das Eigenschaftsfeld, das diesen Feldern vorangeht) deaktiviert (nicht markiert) ist. In diesem Fall müssen die **statische IPv6-Adresse**, die **statische Präfixlänge** und das **statische Gateway** für Gebrauch durch den CMC über das IPv6-Netzwerk manuell eingegeben werden. **ANMERKUNG:** Die Felder **Statische IPv6-Adresse**, **Statische Präfixlänge** und **Statisches Gateway** gelten nur für das Gehäusegerät. Sie haben keine Auswirkung auf die anderen über das Netzwerk zugänglichen Komponenten der Gehäuselösung, zum Beispiel Servernetzwerk, lokaler Zugriff, E/A-Module und iKVM.
Statischer bevorzugter DNS-Server	Gibt die statische IPv6-Adresse für den bevorzugten DNS-Server an. Der Eintrag für den statischen bevorzugten DNS-Server wird nur berücksichtigt, wenn **DHCP zum Abrufen von DNS-Serveradressen verwenden** deaktiviert/nicht markiert ist. Es gibt in beiden Konfigurationsbereichen, IPv4 und IPv6, einen Eintrag für diesen Server.
Statischer alternativer DNS-Server	Legt die statische IPv6-Adresse für den alternativen DNS-Server fest. Wenn Sie über keinen alternativen DNS-Server verfügen, geben Sie eine IPv6-Adresse von „::“ ein. Der Eintrag für den statischen alternativen DNS-Server wird nur berücksichtigt, wenn **DHCP zum Abrufen von DNS-Serveradressen verwenden** deaktiviert/nicht markiert ist. Es gibt in beiden Konfigurationsbereichen, IPv4 und IPv6, einen Eintrag für diesen Server.

CMC-Netzwerksicherheitseinstellungen konfigurieren

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

So konfigurieren Sie die CMC-Netzwerksicherheitseinstellungen:

1. Melden Sie sich bei der Webschnittstelle an.
2. Klicken Sie auf das Register **Netzwerk**.

   Die Seite **Netzwerkkonfiguration** wird angezeigt.
3. Klicken Sie auf die Schaltfläche **Erweiterte Einstellungen**.

   Die Seite **Netzwerksicherheit** wird angezeigt.
4. Konfigurieren Sie die CMC-Netzwerksicherheitseinstellungen.

   Tabelle 5-40 beschreibt die **Einstellungen** auf der Seite **Netzwerksicherheit**.

   ANMERKUNG: Die Einstellungen „IP-Bereich“ und „IP-Blockierung“ gelten nur für IPv4.

Tabelle 5-40. Einstellungen der Seite „Netzwerksicherheit“

Einstellungen	Beschreibung
IP-Bereich aktiviert	Aktiviert die Funktion zum Prüfen des IP-Bereichs, mit der ein bestimmter Bereich an IP-Adressen definiert wird, die auf den CMC zugreifen können.
IP-Bereichs-Adresse	Bestimmt die Haupt-IP-Adresse für die Bereichsüberprüfung.

Tabelle 5-40. Einstellungen der Seite „Netzwerksicherheit" *(fortgesetzt)*

Einstellungen	Beschreibung
IP-Bereichsmaske	Definiert einen bestimmten Bereich von IP-Adressen, die auf den CMC zugreifen können; ein Vorgang, der IP-Bereichsüberprüfung genannt wird. IP-Bereichsüberprüfung lässt den Zugriff auf den CMC nur von Clients oder Management Stations zu, deren IP-Adressen innerhalb des vom Benutzer angegebenen Bereichs liegen. Alle anderen Anmeldeversuche werden abgelehnt. Beispiel: IP-Bereichsmaske: 255.255.255.0 (11111111.11111111.11111111.00000000) IP-Bereichsadresse: 192.168.0.255 (11000000.10101000.00000000.11111111) Der sich ergebende IP-Adressenbereich beinhaltet alle Adressen mit 192.168.0, d. h., eine beliebige Adresse von 192.168.0.0 bis 192.168.0.255.
IP-Blockierung aktiviert	Aktiviert die Funktion des Blockierens der IP-Adresse, wodurch die Anzahl fehlgeschlagener Anmeldeversuche von einer bestimmten IP-Adresse für einen zuvor ausgewählten Zeitraum eingeschränkt wird.
IP-Blockierung, Zählung von Fehlversuchen	Legt die Anzahl von Anmeldungsfehlversuchen einer IP-Adresse fest, bevor die Anmeldungsversuche von dieser Adresse zurückgewiesen werden.
IP-Blockierung, Fenster der Fehlversuche	Legt die Zeitspanne in Sekunden fest, während der Fehler bei der IP-Blockierungsfehlerzählung auftreten müssen, um die Strafzeit für die IP-Blockierung auszulösen.

Tabelle 5-40. Einstellungen der Seite „Netzwerksicherheit“ *(fortgesetzt)*

Einstellungen	Beschreibung
IP-Blockierung, Strafzeit	Die Zeitspanne in Sekunden, während der Anmeldeversuche von einer IP-Adresse aufgrund übermäßiger Fehlversuche zurückgewiesen werden. **ANMERKUNG:** Die Felder „IP-Blockierung, Zählung von Fehlversuchen“, „IP-Blockierung, Fenster der Fehlversuche“ und „IP-Blockierung, Strafzeit“ sind nur dann aktiv, wenn das Kontrollkästchen „IP-Blockierung aktiviert“ (das Eigenschaftsfeld, das diesen Feldern vorausgeht) markiert (aktiviert) ist. In diesem Falle müssen Sie manuell die Eigenschaften „IP-Blockierung, Zählung von Fehlversuchen“, „IP-Blockierung, Fenster der Fehlversuche“ und „IP-Blockierung, Strafzeit“ manuell eingeben.

5 Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

Um den Inhalt der Seite **Netzwerksicherheit** zu aktualisieren, klicken Sie auf **Aktualisieren**.
Um den Inhalt der Seite **Netzwerksicherheit** zu drucken, klicken Sie auf **Drucken**.

VLAN konfigurieren

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. So konfigurieren Sie VLAN:

1 Melden Sie sich bei der Webschnittstelle an.

2 Klicken Sie auf das Unterregister **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.

3 Konfigurieren Sie die CMC/iDRAC-VLAN-Einstellungen.

Tabelle 5-41 beschreibt die **Einstellungen** auf der Seite **Netzwerksicherheit**.

Tabelle 5-41. VLAN-Tag-Einstellungen

Einstellung	Beschreibung
Solt (Steckplatz)	Zeigt den vom Server im Gehäuse besetzten Steckplatz an. Steckplätze sind sequenzielle IDs von 1 bis 16 (für die 16 im Gehäuse verfügbaren Steckplätze), mit denen die Position des Servers im Gehäuse identifiziert werden kann.
Name	Zeigt den Namen des Servers in jedem Steckplatz an.
Enable (Aktivieren)	Aktiviert VLAN, wenn das Kontrollkästchen ausgewählt ist. VLAN ist standardmäßig deaktiviert.
Priority (Priorität)	Gibt die Frame-Prioritätsstufe an, die verwendet werden kann, um unterschiedliche Arten von Verkehr (Sprache, Bild und Daten) mit Prioritäten zu versehen. Gültige Prioritäten sind: 0 bis 7, wobei 0 (Standardeinstellung) die niedrigste Priorität ist und 7 die höchste.
ID	Zeigt die VLAN-ID (Identifikation) an. Gültige VLAN-IDs sind: 1 bis 4000 und 4021 bis 4094. Die Standardeinstellung für VLAN-ID ist 1.

4 Auf **Anwenden klicken**, um die Einstellungen zu speichern.

Sie können auch über das Register **Gehäuse-Übersicht→ Server→ Setup** und das Unterregister→ **VLAN** auf diese Seite zugreifen.

CMC-Benutzer hinzufügen und konfigurieren

Um das System mit dem iDRAC6 zu verwalten und die Systemsicherheit zu erhalten, erstellen Sie eindeutige Benutzer mit spezifischen Verwaltungsberechtigungen (oder *rollenbasierter Autorität*). Für zusätzliche Sicherheit können Sie auch Warnungen konfigurieren, die spezifischen Benutzern per E-Mail geschickt werden, wenn ein bestimmtes Systemereignis vorkommt.

Benutzertypen

Es gibt zwei Typen von Benutzern: CMC-Benutzer und iDRAC-Benutzer. CMC-Benutzer werden auch als „Gehäusebenutzer“ bezeichnet. Da iDRAC auf dem Server resident ist, werden iDRAC-Benutzer auch als „Serverbenutzer“ bezeichnet.

CMC-Benutzer können lokale Benutzer oder Verzeichnisdienstbenutzer sein. iDRAC-Benutzer können auch lokale Benutzer oder Nutzer des Verzeichnisdienstes 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 5-42. Benutzertypen

Berechtigung	Beschreibung
Benutzer: CMC-Anmeldung	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.

Tabelle 5-42. Benutzertypen *(fortgesetzt)*

Berechtigung	Beschreibung
Gehäusekonfigurations-Administrator	Benutzer können Daten hinzufügen oder ändern, die: • das Gehäuse identifizieren, wie z. B. den Gehäusenamen und die Gehäuseposition • speziell dem Gehäuse zugewiesen sind, wie z. B. IP-Modus (statisch oder DHCP), statische IP-Adresse, statisches Gateway und statische Subnetzmaske • dem Gehäuse Dienste zur Verfügung stellen, wie 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.

Tabelle 5-42. Benutzertypen *(fortgesetzt)*

Berechtigung	Beschreibung
Benutzer-konfigurations-Administrator	Ein Benutzer kann: • Einen neuen Benutzer hinzufügen. • Einen vorhandenen Benutzer löschen. • Das Kennwort eines Benutzers ändern. • Die Berechtigungen eines Benutzers ändern. • Die Anmeldungsberechtigung eines Benutzers aktivieren oder deaktivieren, aber den Namen des Benutzers und andere Berechtigungen in der Datenbank beibehalten.
Administrator zum Löschen von Protokollen	Ein Benutzer kann das Hardwareprotokoll und das CMC-Protokoll löschen.
Gehäusesteuerungs-Administrator (Stromsteuer-ungsbefehle)	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.

Tabelle 5-42. Benutzertypen *(fortgesetzt)*

Berechtigung	Beschreibung
Server Administrator	Die Server-Administrator-Berechtigung ist eine Pauschalberechtigung, die einem CMC-Benutzer alle Rechte zum Ausführen beliebiger Vorgänge auf beliebigen, im Gehäuse vorhandenen Servern gewährt. Wenn ein Benutzer mit Berechtigung als **Server-Administrator** eine Maßnahmen zum Ausführen auf einem Server anweist, sendet die CMC-Firmware den Befehl zum Zielserver, ohne die Berechtigungen des Benutzers auf dem Server zu prüfen. Mit anderen Worten: die **Server-Administrator**-Berechtigung setzt alle fehlenden Administratorrechte für dem Server außer Kraft. 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 sind: • Derselbe Benutzername ist auf dem Server vorhanden. • Derselbe Benutzername muss auf dem Server das identische Kennwort besitzen. • Der Benutzer muss über die Berechtigung zum Ausführen des Befehls verfügen. Wenn ein CMC-Benutzer ohne Berechtigung als **Server-Administrator** eine Maßnahme anweist, die auf einem Server ausgeführt werden soll, sendet der CMC einen Befehl an den Zielserver mit dem Anmeldenamen und Kennwort des Benutzers. Wenn der Benutzer auf dem Server nicht vorhanden ist oder das Kennwort nicht übereinstimmt, wird dem Benutzer die Ausführung der Maßnahme verweigert. Wenn der Benutzer auf dem Zielserver vorhanden ist und das Kennwort übereinstimmt, antwortet der Server mit den Berechtigungen, die dem Benutzer auf dem Server gewährt wurden. Basierend auf den Berechtigungen, mit denen der Server antwortet, wird über die CMC-Firmware entschieden, ob der Benutzer das Recht zur Ausführung der Maßnahme besitzt. Im Folgenden werden die Berechtigungen und Maßnahmen auf dem Server aufgeführt, zu denen der **Server Administrator** berechtigt ist. Diese Rechte werden nur dann angewendet, wenn der Gehäusebenutzer nicht über die Server-Administrator-Berechtigung auf dem Gehäuse verfügt.

Tabelle 5-42. Benutzertypen *(fortgesetzt)*

Berechtigung	Beschreibung
Server-Administrator (Forts.)	Serverkonfigurations-Administrator: • IP-Adresse einstellen • Gateway einstellen • Subnetzmaske einstellen • Erstes Startlaufwerk einstellen Benutzer konfigurieren: • iDRAC-Stammkennwort einstellen • iDRAC-Reset Serversteuerungs-Administrator: • Netzstrom ein • Stromversorgung aus • Aus- und einschalten • Ordentliches Herunterfahren • Serverneustart
Warnungstests für Benutzer	Benutzer kann Testwarnungsmeldungen senden.
Debug-Befehl-Administrator	Benutzer kann Systemdiagnosebefehle ausführen.
Struktur A-Administrator	Benutzer kann die Struktur A-EAM festlegen und konfigurieren, die sich entweder in Steckplatz A1 oder Steckplatz A2 der E/A-Steckplätze befindet.
Struktur B-Administrator	Benutzer kann die Struktur B-EAM festlegen und konfigurieren, die sich entweder in Steckplatz B1 oder Steckplatz B2 der E/A-Steckplätze befindet.
Struktur C-Administrator	Benutzer kann die Struktur C-EAM festlegen und konfigurieren, die sich entweder in Steckplatz C1 oder Steckplatz C2 der E/A-Steckplätze befindet.

Tabelle 5-42. Benutzertypen *(fortgesetzt)*

Berechtigung	Beschreibung
Superbenutzer	Benutzer hat Stammzugriff auf den CMC und verfügt über Berechtigungen als **Benutzerkonfigurations-Administrator** und für **CMC-Benutzeranmeldung**. Nur Benutzer mit **Superbenutzer**-Berechtigung können neuen oder bestehenden Benutzern Berechtigungen als **Administrator für Debug-Befehle** und **Superbenutzer** gewähren.

Die CMC-Benutzergruppen bieten eine Reihe von Benutzergruppen, die voreingestellte Benutzerrechte haben.

ANMERKUNG: Wenn Sie Administrator, Hauptbenutzer oder Gastbenutzer auswählen und dann eine Berechtigung zum vordefinierten Satz hinzufügen oder davon entfernen, wird die CMC-Gruppe automatisch zu „benutzerdefiniert" geändert.

Tabelle 5-43. CMC-Gruppenberechtigungen

User Group (Benutzergruppe)	Gewährte Berechtigungen
Administrator	• Benutzer: CMC-Anmeldung • Gehäusekonfigurations-Administrator • Benutzerkonfigurations-Administrator • Administrator zum Löschen von Protokollen • Server Administrator • Warnungstests für Benutzer • Debug-Befehl-Administrator • Struktur A-Administrator • Struktur B-Administrator • Struktur C-Administrator

Tabelle 5-43. CMC-Gruppenberechtigungen *(fortgesetzt)*

User Group (Benutzergruppe)	Gewährte Berechtigungen
Hauptbenutzer	• Anmeldung • Administrator zum Löschen von Protokollen • Gehäusesteuerungs-Administrator • Server Administrator • Warnungstests für Benutzer • Struktur A-Administrator • Struktur B-Administrator • Struktur C-Administrator
Gastbenutzer	Anmeldung
Custom (Benutzerdefiniert)	Wählen Sie eine beliebige Kombination der folgenden Berechtigungen aus: • Benutzer: CMC-Anmeldung • Gehäusekonfigurations-Administrator • Benutzerkonfigurations-Administrator • Administrator zum Löschen von Protokollen • Gehäusesteuerungs-Administrator • Superbenutzer • Server Administrator • Warnungstests für Benutzer • Debug-Befehl-Administrator • Struktur A-Administrator • Struktur B-Administrator • Struktur C-Administrator
Keine	Keine zugewiesenen Berechtigungen

Tabelle 5-44. Vergleich der Berechtigungen zwischen CMC-Administrator, Hauptbenutzer und Gastbenutzer

Berechtigungssatz	Administrator-rechte	Hauptbenutzer Berechtigungen	Gastbenutzer Berechtigungen
Benutzer: CMC-Anmeldung	✔	✔	✔
Gehäusekonfigurations-Administrator	✔	✖	✖
Benutzerkonfigurations-Administrator	✔	✖	✖
Administrator zum Löschen von Protokollen	✔	✔	✖
Gehäusesteuerungs-Administrator	✔	✔	✖
Superbenutzer	✔	✖	✖
Server Administrator	✔	✔	✖
Warnungstests für Benutzer	✔	✔	✖
Debug-Befehl-Administrator	✔	✖	✖
Struktur A-Administrator	✔	✔	✖
Struktur B-Administrator	✔	✔	✖
Struktur C-Administrator	✔	✔	✖

Benutzer hinzufügen und verwalten

Über die Seiten **Benutzer** und **Benutzerkonfiguration** der Webschnittstelle können Sie Informationen zu CMC-Benutzern anzeigen, einen neuen Benutzer hinzufügen und Einstellungen für einen vorhandenen Benutzer ändern.

Sie können bis zu 16 lokale Benutzer konfigurieren. Wenn weitere Benutzer erforderlich sind und Ihr Unternehmen Microsoft Active Directory oder allgemeine Lightweight Directory Access Protocol (LDAP)-Dienste nutzt, können Sie diese so konfigurieren, dass Zugriff auf den CMC möglich ist. Über die Active Directory-Konfiguration können Sie, zusätzlich zu den 16 lokalen Benutzern für Ihre existierenden Benutzer in der Active Directory-Software, CMC-Benutzerberechtigungen hinzufügen und steuern. Weitere Informationen finden Sie unter„CMC-Verzeichnisdienst verwenden“ auf Seite 309. Weitere Informationen über LDAP finden Sie im Abschnitt „CMC mit Lightweight Directory Access Protocol-Diensten verwenden“.

Benutzer können über Webschnittstellen-, serielle Telnet-, SSH- und iKVM-Sitzungen angemeldet sein. Es können maximal 22 aktive Sitzungen (Webschnittstelle, Telnet seriell, SSH und iKVM, in beliebiger Kombination) zwischen Benutzern aufgeteilt werden.

ANMERKUNG: Um die Sicherheit zu erhöhen, wird dringend empfohlen, das vorgegebene Kennwort für das Benutzerkonto „root“ (Benutzer 1) zu ändern. Das Konto „root“ ist das werkseitig voreingestellte Verwaltungskonto des CMC. Um das vorgegebene Kennwort für das Konto „root“ zu ändern, klicken Sie auf **User ID 1** (Benutzer-ID 1), um die Seite **User Configuration** (Benutzerkonfiguration) zu öffnen. Hilfe zu dieser Seite finden Sie über den Link Hilfe, der sich auf dieser Seite oben rechts befindet.

So fügen Sie CMC-Benutzer hinzu und konfigurieren diese:

ANMERKUNG: Zur Ausführung der folgenden Schritte müssen Sie die Berechtigung **„Benutzer konfigurieren“** besitzen.

1. Melden Sie sich bei der Webschnittstelle an.
2. Klicken Sie auf das Register **Benutzer-Authentifizierung.** Die Seite **Lokale Benutzer** wird angezeigt und führt die Benutzer-ID, den Benutzernamen, die CMC-Berechtigung sowie den Anmeldestatus zu jedem Benutzer auf, einschließlich Stammbenutzer. Benutzerkennungen, zu denen keine Benutzerinformationen angezeigt werden, stehen für die Konfiguration zur Verfügung.

3 Klicken Sie auf eine verfügbare Benutzerkennung. Die Seite **Benutzerkonfiguration** wird angezeigt.

Klicken Sie auf **Aktualisieren**, um den Inhalt der Seite **Benutzer** zu aktualisieren. Um den Inhalt der Seite **Benutzer** zu drucken, klicken Sie auf **Drucken**.

4 Wählen Sie die allgemeinen Einstellungen für den Benutzer aus.

Tabelle 5-45. Allgemeine Benutzereinstellungen zur Konfiguration eines neuen oder vorhandenen CMC-Benutzernamens und -kennworts

Eigenschaft	Beschreibung
Benutzer-ID (Nur-Lesen)	Kennzeichnet einen Benutzer anhand einer der 16 voreingestellten, sequenziellen Nummern, die für CLI-Scripting-Zwecke verwendet werden. Die Benutzer-ID kennzeichnet einen bestimmten Benutzer, wenn der Benutzer mit dem CLI-Hilfsprogramm (RACADM) konfiguriert wird. Die Benutzer-ID kann nicht bearbeitet werden. Wenn Sie Informationen für den Benutzer „root“ bearbeiten, ist dieses Feld statisch. Sie können den Benutzernamen für „root“ nicht bearbeiten.
Benutzer aktivieren	Aktiviert oder deaktiviert den Zugriff des Benutzers auf den CMC.
Benutzername	Bestimmt oder zeigt den eindeutigen CMC-Benutzernamen, der dem Benutzer zugeordnet ist. Der Benutzername kann aus bis zu 16 Zeichen bestehen. CMC-Benutzernamen dürfen keine Schrägstriche (/) oder Punkte (.) enthalten. **ANMERKUNG:** Wenn Sie den Benutzernamen ändern, wird der neue Name erst dann auf der Benutzeroberfläche angezeigt, wenn Sie sich das nächste Mal anmelden. Jeder Benutzer, der sich anmeldet, nachdem der neue Benutzername übernommen wurde, kann die Änderung sofort sehen.
Kennwort ändern	Lässt das Ändern des Kennworts eines vorhandenen Benutzers zu. Geben Sie das neue Kennwort in das Feld **Neues Kennwort** ein. Das Kontrollkästchen **Kennwort ändern** kann nicht ausgewählt werden, wenn gerade ein neuer Benutzer konfiguriert wird. Es kann nur dann ausgewählt werden, wenn die Einstellung für einen bestehenden Benutzer geändert wird.

Tabelle 5-45. Allgemeine Benutzereinstellungen zur Konfiguration eines neuen oder vorhandenen CMC-Benutzernamens und -kennworts *(fortgesetzt)*

Eigenschaft	Beschreibung
Kennwort	Legt ein neues Kennwort für einen vorhandenen Benutzer fest. Um ein Kennwort zu ändern, müssen Sie auch das Kontrollkästchen **Kennwort ändern** auswählen. Das Kennwort darf bis zu 20 Zeichen enthalten, die während der Eingabe als Punkte dargestellt werden.
Kennwort bestätigen	Bestätigt das Kennwort, das Sie in das Feld **Neues Kennwort** eingegeben haben. **ANMERKUNG:** Die Felder **Neues Kennwort** und **Neues Kennwort bestätigen** können nur bearbeitet werden, wenn Sie (1) gerade einen neuen Benutzer konfigurieren; oder (2) gerade die Einstellungen eines vorhandenen Benutzers bearbeiten und das Kontrollkästchen **Kennwort ändern** ausgewählt ist.

5 Ordnen Sie den Benutzer einer CMC-Benutzergruppe zu. Tabelle 5-42 beschreibt die CMC-Benutzerrechte.

Wenn Sie eine Benutzerberechtigungseinstellung aus dem Drop-Down-Menü „CMC-Gruppe“ auswählen, werden die aktiven Zugriffsrechte (erkennbar an den markierten Kontrollkästchen in der Liste) entsprechend den vordefinierten Einstellungen für die betreffende Gruppe angezeigt.

Sie können die Einstellungen für Benutzerzugriffsrechte anpassen, indem Sie die Kontrollkästchen aktivieren bzw. deaktivieren. Nachdem Sie eine CMC-Gruppe ausgewählt oder die Benutzerberechtigungseinstellungen individuell festgelegt haben, klicken Sie auf **Änderungen anwenden**, um die Einstellungen beizubehalten.

Um den Inhalt der Seite **Benutzerkonfiguration** zu aktualisieren, klicken Sie auf **Aktualisieren**.

Um den Inhalt der Seite **Benutzerkonfiguration** zu drucken, klicken Sie auf **Drucken**.

Microsoft Active Directory-Zertifikate konfigurieren und verwalten

ANMERKUNG: Um Active Directory-Einstellungen für den CMC zu konfigurieren, müssen Sie die Berechtigung als **Gehäusekonfigurations-Administrator** besitzen.

ANMERKUNG: Weitere Informationen zur Active Directory-Konfiguration und zur Konfiguration von Active Directory mit dem Standardschema oder einem erweiterten Schema finden Sie unter „CMC-Verzeichnisdienst verwenden“ auf Seite 309.

Sie können den Microsoft Active Directory-Dienst zum Konfigurieren der Software für den Zugriff auf den CMC verwenden. Mit dem Active Directory-Dienst können Sie für die vorhandenen Benutzer CMC-Benutzerberechtigungen hinzufügen und diese kontrollieren.

So greifen Sie auf das **Active Directory-Hauptmenü** zu:

1. Melden Sie sich bei der Webschnittstelle an.
2. Klicken Sie auf das Register **Benutzer-Authentifizierung** und dann auf das Unterregister **Verzeichnisdienste**.
3. Wählen Sie die Optionsschaltfläche für das **Microsoft Active Directory-Standardschema** oder das **erweiterte Schema** aus. Es werden die **Active Directory**-Tabellen angezeigt.

Allgemeine Einstellungen

In diesem Bereich können Sie gemeinsame Active Directory-Einstellungen für den CMC konfigurieren und anzeigen.

Tabelle 5-46. Allgemeine Einstellungen

Feld	Beschreibung
Active Directory aktivieren	Aktiviert die Active Directory-Anmeldung auf dem CMC. Sie müssen SSL-Zertifikate für die Active Directory-Server installieren, die von derselben Zertifizierungsstelle unterzeichnet sind und diese auf den CMC hochladen.
Smart Card-Anmeldung aktivieren	Aktiviert die Active Directory-Interoperation auf der Basis der Kerberos-Authentifizierung, die von einem von Dell gelieferten automatisch installierten Browser-Plugin unterstützt werden, und Smart Card-Verwendung. Zur Aktivierung von Smart Card wählen Sie das Kontrollkästchen aus. Zur Deaktivierung von Smart Card löschen Sie die Markierung im Kontrollkästchen. Wenn Sie Smart Card aktivieren, müssen Sie auch Ihre Microsoft Windows Client Workstation konfigurieren, damit diese ordnungsgemäß mit der Smart Card-Leserfunktion funktioniert. Dies umfasst die Installation der korrekten Treiber für den zu verwendenden Smart Card-Leser und auch die Installation der korrekten Treiber für die tatsächlich verwendete Smart Card. Diese Smart Card-Treiber sind von Hersteller zu Hersteller verschieden. Die Smart Card muss unter Verwendung der Smart Card-Aktivierungsdienste, die vom entsprechenden Active Directory-Server zur Verfügung gestellt werden, ordnungsgemäß mit den erforderlichen Anmeldeinformationen programmiert werden. **ANMERKUNG:** Die Smart Card-Anmeldung und einfache Anmeldung schließen sich gegenseitig aus. Sie können jeweils nur einen Typ von Anmeldung auswählen.

Tabelle 5-46. Allgemeine Einstellungen *(fortgesetzt)*

Feld	Beschreibung
Einfache Anmeldung aktivieren	Aktiviert den CMC für die Nutzung von **Active Directory**. Zur Aktivierung der **einfachen Anmeldung** wählen Sie das Kontrollkästchen aus. Zur Deaktivierung der **einfachen Anmeldung** löschen Sie die Markierung im Kontrollkästchen. Wenn Sie die **einfache Anmeldung** aktivieren, müssen Sie auch die **Active Directory**-Eigenschaften einrichten und das Schema auswählen, das Sie verwenden möchten. **ANMERKUNG:** Die Smart Card-Anmeldung und einfache Anmeldung schließen sich gegenseitig aus. Sie können jeweils nur einen Typ von Anmeldung auswählen.

Tabelle 5-46. Allgemeine Einstellungen *(fortgesetzt)*

Feld	Beschreibung
SSL-Zertifikatüberprüfung aktivieren	Aktiviert die SSL-Zertifikatüberprüfung für die Active Directory-SSL-Verbindung des CMC. Zur Deaktivierung der SSL-Zertifikatsüberprüfung löschen Sie die Markierung aus dem Kontrollkästchen. **VORSICHTSHINWEIS: Die Deaktivierung dieser Funktion kann die Authentifizierung für einen Man-in-the-Middle-Angriff öffnen.** Der Browservorgang erfordert, dass auf den CMC über eine HTTP-URL zugegriffen wird, die die vollständige qualifizierte Domänenadresse des CMC enthält, das heißt **http://cmc-6g2wxf1.dom.net**. Eine einfache IP-Adresse für den CMC führt nicht zu einem ordnungsgemäßen einfachen Anmeldevorgang. Um vollständige qualifizierte Domänenadressen zu unterstützen, ist es notwendig, den CMC beim Domänennamendienst des Active Directory-Servers zu registrieren. Wenn eine Browser-Authentifizierung für eine einfache Anmeldung nicht erfolgreich ist, dann wird automatisch die gewöhnliche Browser-Authentifizierung mit lokalem oder Active Directory-Benutzername/Kennwort präsentiert. Analog dazu gibt eine Abmeldemaßname nach einer erfolgreichen einfachen Anmeldung die Methode Benutzername/Kennwort vor. Die Nutzung der einfachen Anmeldung dient der Bequemlichkeit und ist nicht als Einschränkung gedacht. **ANMERKUNG:** Die Smart Card-basierte Browser-Authentifizierung wird nur für Microsoft Windows-Clients und Internet Explorer-Browser unterstützt. Das von Dell gelieferte und automatisch geladene Browser-Plugin (ActiveX-Steuerung) ist davon abhängig, ob auf dem Microsoft Windows Client-Betriebssystem die folgenden Laufzeitkomponenten vorinstalliert sind: Microsoft Visual C++ 2005 Redistributable Package (x86). Der folgende Link kann dabei helfen, die Komponente zu finden: **microsoft.com/downloads/details.aspx?FamilyID=32BC1BEE-A3F9-4C13-9C99-220B62A191EE&displaylang=en**. Der Windows-Client benötigt **erhöhte Berechtigungen**, um die ActiveX-Steuerung erfolgreich zu installieren. Analog dazu muss die Browser-Konfiguration die Installation von „unsignierten“ ActiveX-Steuerungen akzeptieren.

Tabelle 5-46. Allgemeine Einstellungen *(fortgesetzt)*

Feld	Beschreibung
	Die Aktivierung von Smart Card erzwingt eine „Nur Smart Card"-Regel für die Browser-Authentifizierung. Alle anderen Methoden der Browser-Authentifizierung wie beispielsweise die Authentifizierung mit lokalem oder Active Directory-Benutzernamen/Kennwort sind beschränkt. Wenn die „Nur Smart Card"-Erzwingungsrichtlinie angenommen werden soll, ist es wichtig, dass der Betrieb der Smart Card vollständig überprüft wird, bevor alle anderen Zugriffsmethoden auf den CMC deaktiviert werden. Ansonsten kann es sein, dass versehentlich jeglicher Zugriff auf den CMC blockiert wird.
Root-Domänenname	Bestimmt den vom Active Directory verwendeten Domänennamen. Der Root-Domänenname ist der voll qualifizierte Root-Domänenname für die Gesamtstruktur. **ANMERKUNG:** Der Root-Domänenname muss ein gültiger Domänenname sein, für den die Namenskonvention x.y verwendet wird, wobei x eine ASCII-Zeichenkette aus 1-256 Zeichen ohne Leerstellen zwischen den Zeichen und y ein gültiger Domänentyp wie com, edu, gov, int, mil, net oder org ist.
AD-Zeitüberschreitung	Legt die Zeit in Sekunden fest, nach der eine inaktive Active Directory-Sitzung automatisch geschlossen wird. Gültige Werte: 15-300 Sekunden Standardeinstellung: 90 Sekunden
AD-Server zur Suche bestimmen (optional)	Aktiviert (wenn markiert) den weitergeleiteten Aufruf des Domänen-Controllers und globalen Katalogs. Wenn Sie diese Option aktivieren, müssen Sie in den folgenden Einstellungen auch den Domänen-Controller und die globalen Katalogspeicherorte bestimmen. **ANMERKUNG:** Der Name auf dem Active Directory-Zertifizierungsstellenzertifikat wird nicht auf den festgelegten Active Directory-Server oder den globalen Katalogserver abgestimmt sein.
Domänen-Controller	Legt den Server fest, auf dem der Active Directory-Dienst installiert wird. Diese Option ist nur gültig, wenn „AD-Server zur Suche bestimmen (optional)" aktiviert ist.

Tabelle 5-46. Allgemeine Einstellungen *(fortgesetzt)*

Feld	Beschreibung
Globaler Katalog	Legt den Speicherort des globalen Katalogs auf dem Active Directory-Domänen-Controller fest. Der globale Katalog ist eine Ressource zum Durchsuchen einer Active Directory-Gesamtstruktur. Diese Option ist nur gültig, wenn „AD-Server zur Suche bestimmen (optional)“ aktiviert ist.

Einstellungen zum Standardschema

Es werden die Standardschema-Einstellungen angezeigt, wenn Microsoft Active Directory (Standardschema) ausgewählt wird. Dieser Abschnitt beschreibt für alle Rollengruppen, die bereits konfiguriert wurden die Rollengruppen mit zugehörigen Namen, Domänen und Berechtigungen.

Um die Einstellungen für eine Rollengruppe zu ändern, klicken Sie auf die Rollengruppenschaltfläche in der **Rollengruppen**liste.

ANMERKUNG: Wenn Sie auf einen Rollengruppen-Link klicken, bevor Sie die neu von Ihnen vorgenommenen Einstellungen anwenden, gehen diese Einstellungen verloren. Um zu vermeiden, dass neue Einstellungen verloren gehen, klicken Sie auf **Anwenden**, bevor Sie auf eine Rollengruppenschaltfläche klicken.

Die Seite „Rollengruppe“ konfigurieren wird angezeigt.

- Gruppenname - Der Name, der die Rollengruppe im Active Directory identifiziert, die der CMC-Karte zugeordnet ist.
- Gruppendomäne - Die Domäne, in der sich die Gruppe befindet.
- Gruppenberechtigung - Die Berechtigungsebene für die Gruppe.

Auf **Anwenden klicken**, um die Einstellungen zu speichern.

Klicken Sie auf **Zurück zur Seite Konfiguration**, um zur Seite **Verzeichnisdienste** zurückzukehren.

Um den Inhalt der Seite **Verzeichnisdienste** zu aktualisieren, klicken Sie auf **Aktualisieren**.

Um den Inhalt der Seite **Verzeichnisdienste** zu drucken, klicken Sie auf **Drucken**.

Einstellungen zum erweiterten Schema

Es werden diese erweiterten Schema-Einstellungen mit den folgenden Eigenschaften angezeigt, wenn **Microsoft Active Directory (erweitertes Schema)** ausgewählt wird:

- CMC-Gerätename - Zeigt den Namen des RAC-Geräteobjekts an, das Sie für den CMC erstellt haben. Der CMC-Gerätename identifiziert die CMC-Karte im Active Directory eindeutig. Der CMC-Gerätename muss dem gemeinsamen Namen des neuen RAC-Geräteobjekts entsprechen, das Sie in Ihrem Domänen-Controller erstellt haben. Der CMC-Name muss eine ASCII Zeichenkette mit 1 bis 256 Zeichen ohne Leerstellen sein.
- CMC-Domänenname - Zeigt den DNS-Namen (Zeichenkette) der Domäne an, in der sich das Active Directory RAC-Geräteobjekt befindet. Der CMC-Domänenname muss ein gültiger Domänenname sein und aus *x.y* bestehen, wobei *x* eine ASCII-Zeichenkette mit 1 bis 256 Zeichen ohne Leerstellen und *y* ein gültiger Domänentyp wie com, edu, gov, int, mil, net oder org ist.

Active Directory-Zertifikate verwalten

Dieser Bereich zeigt die Eigenschaften für das Active Directory-Zertifikat an, das zuletzt auf den CMC hochgeladen wurde. Wenn Sie ein Zertifikat hochgeladen haben, verwenden Sie diese Informationen, um zu überprüfen, ob das Zertifikat gültig und nicht abgelaufen ist.

ANMERKUNG: Standardmäßig beinhaltet der CMC kein von einer Zertifizierungsstelle ausgegebenes Zertifikat für Active Directory. Sie müssen ein aktuelles, von einer Zertifizierungsstelle signiertes Serverzertifikat, hochladen.

Folgende Eigenschaften für das Zertifikat werden angezeigt:

- Seriennummer - Die Seriennummer des Zertifikats.
- Subjektinformationen - Subjekt des Zertifikats (Name der zertifizierten Person oder Firma).
- Ausstellerinformationen - Aussteller des Zertifikats (Name der Zertifizierungsstelle).
- Gültig ab - Das Anfangsdatum des Zertifikats.
- Gültig bis - Das Ablaufdatum des Zertifikats.

Die folgenden Steuerungen ermöglichen Ihnen das Hoch- und Herunterladen dieses Zertifikats:

- Hochladen - Initiiert den Hochladevorgang für das Zertifikat. Dieses Zertifikat, das Sie vom Active Directory erhalten, gewährt Ihnen Zugang zum CMC.
- Herunterladen - Initiiert den Herunterladevorgang. Sie werden aufgefordert, den Speicherort für die Datei anzugeben. Wenn Sie diese Option wählen und auf **Weiter** klicken, wird das Dialogfeld **Datei herunterladen** eingeblendet. Verwenden Sie dieses Dialogfeld, um auf Ihrer Management Station oder Ihrem freigegebenen Netzwerk einen Speicherort für das Serverzertifikat zu bestimmen.

ANMERKUNG: Standardmäßig beinhaltet der CMC kein von einer Zertifizierungsstelle ausgegebenes Zertifikat für Active Directory. Sie müssen ein aktuelles, von einer Zertifizierungsstelle signiertes Serverzertifikat, hochladen.

Kerberos-Keytab

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.

ANMERKUNG: Der CMC verfügt nicht über eine Kerberos-Keytab-Datei für Active Directory. Sie müssen eine neu erzeugte Kerberos-Keytab-Datei hochladen. Weitere Informationen finden Sie unter „Einfache Anmeldung konfigurieren“ auf Seite 344.

Die folgenden Maßnahmen sind zulässig:

- Durchsuchen - Öffnet das Dialogfeld **Durchsuchen**, von dem aus Sie das Serverzertifikat auswählen können, das Sie hochladen möchten.
- Hochladen - Initiiert den Hochladevorgang für das Zertifikat über den von Ihnen angegebenen Dateipfad.

Konfiguration und Verwaltung von allgemeinen Lightweight Directory Access Protocol-Diensten

Sie können den allgemeinen Lightweight Directory Access Protocol (LDAP)-Dienst zur Konfiguration Ihrer Software verwenden, um Zugriff auf den CMC zu ermöglichen. Mit LDAP können Sie für die vorhandenen Benutzer CMC-Benutzerberechtigungen hinzufügen und diese kontrollieren.

ANMERKUNG: Um LDAP-Einstellungen für den CMC zu konfigurieren, müssen Sie die Berechtigung als **Gehäusekonfiguration-Administrator** besitzen.

So wird LDAP angezeigt und konfiguriert:

1. Melden Sie sich bei der Webschnittstelle an.
2. Klicken Sie auf das Register **Benutzer-Authentifizierung** und dann auf das Unterregister **Verzeichnisdienste**. Die Seite **Verzeichnisdienste** wird angezeigt.
3. Klicken Sie auf die Optionsschaltfläche, die mit dem allgemeinen LDAP verbunden ist.
4. Konfigurieren Sie die angezeigten Optionen und klicken Sie auf **Anwenden**.

Tabelle 5-47 listet die verfügbaren Konfigurationsoptionen auf.

Tabelle 5-47. Allgemeine Einstellungen

Einstellung	Beschreibung
Allgemeiner LDAP-Dienst aktiviert	Aktiviert den allgemeinen LDAP-Dienst auf dem CMC.
Abgegrenzten Namen zur Suche nach Gruppenmitgliedschaft verwenden	Legt den abgegrenzten Namen (DN) der LDAP-Gruppen fest, deren Mitglieder auf das Gerät zugreifen dürfen.
SSL-Zertifikatüberprüfung aktivieren	Wenn markiert, verwendet der CMC das CA-Zertifikat, um das LDAP-Serverzertifikat während des SSL-Handshake zu bestätigen.
Bindungs-DN	Legt den DN (Distinguished Name) eines Benutzers fest, der bei der Suche nach dem DN eines angemeldeten Benutzers zur Bindung an den Server verwendet wird. Wird kein DN angegeben, wird eine anonyme Bindung verwendet.

Tabelle 5-47. Allgemeine Einstellungen *(fortgesetzt)*

Einstellung	Beschreibung
Kennwort	Ein Bindungskennwort, das gemeinsam mit dem Bindungs-DN verwendet wird. **ANMERKUNG:** Beim Bindungskennwort handelt es sich um sensible Daten, die entsprechend geschützt werden müssen.
Base-DN für Suche	Der DN des Verzeichniszweigs, von dem aus alle Suchvorgänge gestartet werden müssen.
Attribut der Benutzeranmeldung	Gibt das Attribut an, nach dem gesucht werden soll. Wenn keine Konfiguration vorliegt, lautet die zu verwendende Standardeinstellung „uid“. Es wird empfohlen, bei der Auswahl des Base-DN Eindeutigkeit zu gewährleisten, da andernfalls ein Suchfilter konfiguriert werden muss, um die Eindeutigkeit des anmeldenden Benutzers sicherzustellen. Wenn der Benutzer-DN nicht eindeutig durch die Suche nach einer Kombination aus Attribut und Suchfilter identifiziert werden kann, schlägt die Anmeldung fehl und es wird eine Fehlermeldung ausgegeben.
Attribut der Gruppenmitgliedschaft	Legt das LDAP-Attribut fest, das zur Prüfung der Gruppenmitgliedschaft verwendet wird. Dies muss ein Attribut der Gruppenklasse sein. Wird hier nichts angegeben, werden die Attribute „member“ und „unique member“ verwendet.
Suchfilter	Gibt einen gültigen LDAP-Suchfilter an. Dieser Filter wird verwendet, wenn das Benutzerattribut den anmeldenden Benutzer innerhalb des ausgewählten Base-DN nicht eindeutig identifizieren kann. Wird hier nichts angegeben, wird der Standardwert (objectClass=*) zugrunde gelegt, mit dem nach allen Objekten in der Struktur gesucht wird. Die maximale Länge dieser Eigenschaft ist 1024 Zeichen.
Netzwerkzeitüberschreitung (Sekunden)	Legt die Zeit in Sekunden fest, nach der eine inaktive LDAP-Sitzung automatisch geschlossen wird.
Suchzeitüberschreitung (Sekunden)	Legt die Zeit in Sekunden fest, nach der eine Suche automatisch geschlossen wird.

Auswahl Ihres LDAP-Servers

Sie können den für allgemeines LDAP zu verwendenden Server auf zwei Arten konfigurieren. Statische Server erlauben es dem Administrator eine FQDN oder IP-Adresse in das Feld zu platzieren. Alternativ kann eine Liste von LDAP-Servern abgerufen werden, indem nach deren SRV-Eintrag in der DNS gesucht wird. Es folgen die Eigenschaften im Abschnitt „LDAP-Server“:

- Statische LDAP-Server verwenden – Wenn diese Option ausgewählt wird, verwendet der LDAP-Dienst die angegebenen Server mit der angegebenen Schnittstellennummer (siehe Details unten).

  ANMERKUNG: Sie müssen „Statisch“ oder „DNS“ auswählen.

- LDAP-Server-Adresse – Legen Sie die FQDN oder IP des LDAP-Servers fest. Um mehrere redundante LDAP-Server anzugeben, die der gleichen Domäne dienen, legen Sie eine Liste aller Server an (kommagetrennt). Der CMC versucht sich nacheinander mit jedem Server zu verbinden, bis ein Verbindungsversuch erfolgreich ist.
- LDAP-Serverschnittstelle – Schnittstelle von LDAP über SSL, Standard ist 636, falls nicht konfiguriert. Nicht-SSL-Schnittstellen werden von CMC Version 3.0 nicht unterstützt, da das Kennwort nicht ohne SSL übertragen werden kann.
- DNS verwenden, um LDAP-Server zu finden – Wenn diese Option gewählt wird, verwendet LDAP die Suchdomäne und den Dienstnamen über DNS. Sie müssen „Statisch“ oder „DNS“ auswählen.

Die folgende DNS-Abfrage wird für SRV-Einträge durchgeführt:

`_[Dienstname]._tcp.[Suchdomäne]`

where <Search Domain> is the root level domain to use within the query and <Service Name> is the service name to use within the query.
For example:

`_ldap._tcp.dell.com`

wobei `ldap` der Dienstname ist und `dell.com` die Suchdomäne.

LDAP-Gruppeneinstellungen verwalten

In der Tabelle im Abschnitt „Gruppeneinstellungen“ werden Rollengruppen aufgelistet, einschließlich zugeordneter Namen, Domänen und Berechtigungen für jede Rollengruppe, die bereits konfiguriert ist.

- Zur Konfiguration einer neuen Rollengruppe klicken Sie auf einen Rollengruppennamen, für den kein Name, keine Domäne und Berechtigung aufgelistet ist.
- Zum Ändern der Einstellungen einer vorhandenen Rollengruppe klicken Sie auf den Rollengruppennamen.

Wenn Sie einen Rollengruppennamen anklicken, erscheint die Seite **Rollengruppe konfigurieren**. Hilfe zu dieser Seite finden Sie über den Link **Hilfe**, der sich auf dieser Seite oben rechts befindet.

LDAP-Sicherheitszertifikate verwalten

In diesem Abschnitt werden die Eigenschaften für das kürzlich auf den CMC hochgeladene LDAP-Zertifikat angezeigt. Wenn Sie ein Zertifikat hochgeladen haben, verwenden Sie diese Informationen, um zu überprüfen, ob das Zertifikat gültig und nicht abgelaufen ist.

ANMERKUNG: Standardmäßig beinhaltet der CMC kein von einer Zertifizierungsstelle ausgegebenes Zertifikat für Active Directory. Sie müssen ein aktuelles, von einer Zertifizierungsstelle signiertes Serverzertifikat, hochladen.

Folgende Eigenschaften für das Zertifikat werden angezeigt:

- Seriennummer - Die Seriennummer des Zertifikats.
- Subjektinformationen - Subjekt des Zertifikats (Name der zertifizierten Person oder Firma).
- Ausstellerinformationen - Aussteller des Zertifikats (Name der Zertifizierungsstelle).
- Gültig ab - Das Anfangsdatum des Zertifikats.
- Gültig bis - Das Ablaufdatum des Zertifikats.

Die folgenden Steuerungen ermöglichen Ihnen das Hoch- und Herunterladen dieses Zertifikats:

- Hochladen - Initiiert den Hochladevorgang für das Zertifikat. Dieses Zertifikat, das Sie von Ihrem LDAP-Server erhalten, gewährt Ihnen Zugang zum CMC.
- Herunterladen - Initiiert den Herunterladevorgang. Sie werden aufgefordert, den Speicherort für die Datei anzugeben. Wenn Sie diese Option wählen und auf **Weiter** klicken, wird das Dialogfeld **Datei herunterladen** eingeblendet. Verwenden Sie dieses Dialogfeld, um auf Ihrer Management Station oder Ihrem freigegebenen Netzwerk einen Speicherort für das Serverzertifikat zu bestimmen.

Sichere CMC-Datenübertragung mit SSL und digitalen Zertifikaten

Dieser Unterabschnitt enthält Informationen über die folgenden Datensicherheitsfunktionen, die im CMC integriert sind:

- „Secure Sockets Layer (SSL)“ auf Seite 212.
- „Zertifikatsignierungsanforderung (CSR)“ auf Seite 213.
- „Zugriff auf das SSL-Hauptmenü“ auf Seite 214.
- „Neue Zertifikatsignierungsanforderung erstellen“ auf Seite 214.
- „Serverzertifikat hochladen“ auf Seite 218.
- „Web Server-Schlüssel und Zertifikat hochladen“ auf Seite 219.
- „Serverzertifikat anzeigen“ auf Seite 220.

Secure Sockets Layer (SSL)

Der CMC beinhaltet einen Web Server, der zur Verwendung des SSL-Sicherheitsprotokolls nach industriellem Standard konfiguriert wurde, um verschlüsselte Daten über das Internet zu übertragen. SSL ist auf öffentlicher und privater Verschlüsselungstechnologie aufgebaut und eine allgemein akzeptierte Methode, um authentifizierte und verschlüsselte Kommunikationen zwischen Clients und Servern bereitzustellen und unbefugtes Abhören in einem Netzwerk zu verhindern.

SSL erlaubt einem SSL-aktivierten System, die folgenden Tasks auszuführen:

- Sich an einem SSL-aktivierten Client authentifizieren
- Dem Client erlauben, sich am Server zu authentifizieren
- Beiden Systemen gestatten, eine verschlüsselte Verbindung herzustellen

Dieses Verschlüsselungsverfahren gewährleistet ein hohes Maß von Datenschutz. Der iDRAC6 verwendet den SSL 128-Bit-Verschlüsselungsstandard, die sicherste Form der Verschlüsselung, die für Webbrowser in Nordamerika allgemein verfügbar ist.

Der CMC-Web Server enthält ein von Dell selbstsigniertes digitales Zertifikat (Server-ID). Um hohe Sicherheit über das Internet zu gewährleisten, ersetzen Sie das Web Server SSL-Zertifikat, indem Sie eine Aufforderung an den CMC senden, eine neue Zertifikatsignierungsanforderung (CSR) zu erstellen.

Zertifikatsignierungsanforderung (CSR)

Eine CSR ist eine digitale Aufforderung an eine Zertifizierungsstelle (in der Webschnittstelle CA genannt) für ein sicheres Serverzertifikat. Sichere Serverzertifikate sind erforderlich zur Sicherstellung der Identität eines entfernten Systems und zur Gewährleistung, dass mit dem entfernten System ausgetauschte Informationen von anderen weder eingesehen noch geändert werden können. Um Sicherheit für den CMC zu gewährleisten, wird dringend empfohlen, eine CSR zu erstellen, die CSR an eine Zertifizierungsstelle zu senden und das von der Zertifizierungsstelle zurückgesendete Zertifikat hochzuladen.

Eine Zertifizierungsstelle ist ein Geschäftsunternehmen, das in der IT-Industrie dafür anerkannt ist, hohe Standards der zuverlässigen Abschirmung, Identifizierung und anderer wichtiger Sicherheitskriterien einzuhalten. Beispiele für CAs umfassen Thawte und VeriSign. Sobald die Zertifizierungsstelle die CSR empfangen hat, werden die in der CSR enthaltenen Informationen eingesehen und überprüft. Wenn der Bewerber die Sicherheitsstandards der Zertifizierungsstelle erfüllt, stellt diese dem Bewerber ein Zertifikat aus, das den Bewerber bei Übertragungen über Netzwerke oder über das Internet eindeutig identifiziert.

Nachdem die Zertifizierungsstelle die CSR genehmigt hat und Ihnen ein Zertifikat sendet, muss das Zertifikat auf die CMC-Firmware hochgeladen werden. Die auf der CMC-Firmware gespeicherten CSR-Informationen müssen mit den im Zertifikat enthaltenen Informationen übereinstimmen.

Zugriff auf das SSL-Hauptmenü

ANMERKUNG: Um SSL-Einstellungen für den CMC zu konfigurieren, müssen Sie die Berechtigung als **Gehäusekonfigurations-Administrator** besitzen.

ANMERKUNG: Jedes von Ihnen hochgeladene Serverzertifikat muss aktuell (nicht abgelaufen) und von einer Zertifizierungsstelle signiert sein.

So greifen Sie auf das SSL-Hauptmenü zu:

1. Melden Sie sich bei der Webschnittstelle an.
2. Klicken Sie auf das Register **Netzwerk** und dann auf das Unterregister **SSL**. Die Seite **SSL-Hauptmenü** wird angezeigt.

Verwenden Sie die Optionen auf der Seite **SSL-Hauptmenü**, um eine CSR zu erstellen und diese an eine Zertifizierungsstelle zu senden. Die CSR-Informationen werden in der CMC-Firmware gespeichert.

Neue Zertifikatsignierungsanforderung erstellen

Um die Sicherheit zu gewährleisten, empfiehlt Dell eindringlich, ein sicheres Serverzertifikat zu erwerben und auf den CMC hochzuladen. Sichere Serverzertifikate garantieren die Identität eines Remote-Systems und stellen sicher, dass Daten, die mit dem Remote-System ausgetauscht werden, nicht von anderen System eingesehen oder geändert werden können. Ohne ein sicheres Serverzertifikat ist der CMC gegenüber Zugriff von unberechtigten Benutzern gefährdet.

Tabelle 5-48. SSL-Hauptmenüoptionen

Feld	Beschreibung
Eine neue Zertifikatsignierungsanforderung erstellen (CSR)	Wählen Sie diese Option aus und klicken Sie auf **Weiter**, um die Seite „Zertifikatsignierungsanforderung (CSR) erstellen“ zu öffnen; auf dieser Seite können Sie eine CSR-Anforderung für ein sicheres Web-Zertifikat erstellen, das an eine Zertifizierungsstelle gesendet wird. **ANMERKUNG:** Jede neue CSR überschreibt die vorherige CSR des CMC. Damit eine Zertifizierungsstelle Ihre CSR anerkennt, muss die CSR im CMC mit dem von der Zertifizierungsstelle zurückgesendeten Zertifikat übereinstimmen.
Serverzertifikat basierend auf erstellter CSR hochladen	Wählen Sie diese Option aus und klicken Sie auf **Weiter**, um die Seite **Zertifikat hochladen** anzuzeigen, auf der Sie ein vorhandenes Zertifikat hochladen können, das im Besitz Ihres Unternehmen ist und für Zugriffssteuerung auf den CMC verwendet wird. **ANMERKUNG:** Der CMC akzeptiert lediglich X509-Base-64-kodierte Zertifikate. DER-kodierte Zertifikate werden nicht angenommen. Durch das Hochladen eines neuen Zertifikats wird das mit dem CMC gelieferte Standardzertifikat ersetzt.
Web Server-Schlüssel und Zertifikat hochladen	Wählen Sie diese Option aus und klicken Sie auf **Weiter**, um die Seite **Web Server-Schlüssel und Zertifikat hochladen** zu öffnen, auf der Sie einen vorhandenen Web Server-Schlüssel und ein vorhandenes Zertifikat hochladen können, das im Besitz Ihres Unternehmen ist und für Zugriffssteuerung auf den CMC verwendet wird. **ANMERKUNG:** Nur X.509-Base-64-kodierte Zertifikate werden vom CMC akzeptiert. Binäre DER-kodierte Zertifikate werden nicht akzeptiert. Durch das Hochladen eines neuen Zertifikats wird das mit dem CMC gelieferte Standardzertifikat ersetzt.
Serverzertifikat anzeigen	Wählen Sie die Option aus und klicken Sie auf die Schaltfläche **Weiter**, um die Seite **Serverzertifikat anzeigen** zu öffnen, auf der Sie das aktuelle Serverzertifikat anzeigen können.

Um ein sicheres Serverzertifikat für den CMC zu erwerben, müssen Sie eine Zertifikatsignierungsanforderung (CSR) an eine Zertifizierungsstelle Ihrer Wahl senden. Unter einer CSR versteht man eine digitale Anforderung für ein signiertes, sicheres Serverzertifikat, das Informationen über Ihre Organisation und einen eindeutigen Identifizierungsschlüssel enthält.

Wenn auf der Seite **Zertifikatsignierungsanforderung (CSR) erstellen** eine CSR erstellt wird, erhalten Sie die Aufforderung, eine Kopie in der Management Station oder im freigegebenen Netzwerk zu speichern, und eindeutige Informationen zur Erstellung der CSR werden im CMC abgelegt. Diese Informationen werden später verwendet, um das Serverzertifikat, das Sie von der Zertifizierungsstelle erhalten, zu beglaubigen. Nachdem Sie das Serverzertifikat von der Zertifizierungsstelle erhalten, müssen Sie es auf den CMC hochladen.

ANMERKUNG: Damit der CMC das von der Zertifizierungsstelle zurückgesendete Serverzertifikat akzeptiert, müssen die Authentifizierungsinformationen, die im neuen Zertifikat enthalten sind, mit den Informationen übereinstimmen, die bei der Erstellung der CSR auf dem CMC gespeichert wurden.

VORSICHTSHINWEIS: Bei der Erstellung einer neuen CSR, wird jede vorherige CSR auf dem CMC überschrieben. Wenn eine wartende CSR überschrieben wird, bevor das Serverzertifikats von der Zertifizierungsstelle bewilligt wird, wird das Serverzertifikat vom CMC nicht angenommen, weil die zur Authentifizierung des Zertifikats verwendeten Informationen verloren gegangen sind. Beachten Sie, dass bei der Erstellung einer CSR keine wartende CSR überschreiben wird.

Um eine CSR zu erstellen:

1. Wählen Sie auf der Seite **SSL-Hauptmenü** die Option **Neue Zertifikatsignierungsanforderung (CSR) erstellen**, und klicken Sie dann auf **Weiter**. Die Seite **Zertifikatsignierungsanforderung (CSR) erstellen** wird angezeigt.
2. Geben Sie für jedes CSR-Attribut einen Wert ein.
3. Klicken Sie auf **Generate** (Erstellen). Ein Dialogfeld **Dateidownload** erscheint.
4. Speichern Sie die Datei **csr.txt** auf der Management Station oder im freigegebenen Netzwerk. (Sie können die Datei auch jetzt öffnen und später speichern.) Diese Datei werden Sie später an die Zertifizierungsstellen senden.

Tabelle 5-49. Optionen der Seite „Zertifikatsignierungsanforderung (CSR) erstellen“

Feld	Beschreibung
Allgemeiner Name	Der genaue Name, der zertifiziert werden soll (normalerweise der Domänenname des Web Servers, z. B. **www.xyzFirma.com/**).
	Gültig: Alphanumerische Zeichen (A-Z, a-z, 0-9); Bindestriche, Unterstriche und Punkte.
	Nicht gültig: Nicht-alphanumerische Zeichen, die oben nicht angegeben sind (z. B., aber nicht beschränkt auf, @ # $ % & *); Zeichen, die hauptsächlich in nicht-englischen Sprachen verwendet werden, wie z. B. ß, å, é, ü.
Name der Organisation	Der Name, der sich auf Ihre Organisation bezieht (z. B. **Unternehmen XYZ**).
	Gültig: Alphanumerische Zeichen (A-Z, a-z, 0-9); Bindestriche, Unterstriche Punkte und Leerzeichen.
	Nicht gültig: Nicht-alphanumerische Zeichen, die nicht oben angegeben sind (wie z. B., aber nicht begrenzt auf, @ # $ % & *).
Organisationseinheit	Der Name, der mit einer organisatorischen Einheit in Verbindung gebracht wird, wie z. B. eine Abteilung (zum Beispiel Unternehmensgruppe).
	Gültig: Alphanumerische Zeichen (A-Z, a-z, 0-9); Bindestriche, Unterstriche Punkte und Leerzeichen.
	Nicht gültig: Nicht-alphanumerische Zeichen, die nicht oben angegeben sind (wie z. B., aber nicht begrenzt auf, @ # $ % & *).
Ort	Die Stadt oder ein anderer Standort Ihrer Organisation (zum Beispiel: **Atlanta**, **Hongkong**).
	Gültig: Alphanumerische Zeichen (A-Z, a-z, 0-9) und Leerzeichen.
	Nicht gültig: Nicht-alphanumerische Zeichen, die nicht oben angegeben sind (wie z. B., aber nicht beschränkt auf, @ # $ % & *).

Tabelle 5-49. Optionen der Seite „Zertifikatsignierungsanforderung (CSR) erstellen“ *(fortgesetzt)*

Feld	Beschreibung
Status	Der Staat, das Land oder Territorium, in denen sich die Einheit befindet, die sich für eine Zertifizierung bewirbt (zum Beispiel: **Texas**, **New South Wales**, **Andhra Pradesh**). **ANMERKUNG:** Verwenden Sie keine Abkürzungen. **Gültig**: Alphanumerische Zeichen (Groß- und Kleinbuchstaben; 0-9) und Leerzeichen. **Nicht gültig**: Nicht-alphanumerische Zeichen, die nicht oben angegeben sind (wie z. B., aber nicht beschränkt auf, @ # $ % & *).
Land	Das Land, in dem sich die Organisation, die sich für die Zertifizierung bewirbt, befindet.
E-Mail	Die E-Mail-Adresse Ihrer Firma. Sie können eine beliebige E-Mail-Adresse eingeben, die der CSR zugeordnet sein soll. Die E-Mail-Adresse muss gültig sein und das @-Zeichen enthalten (z. B. **Name@UnternehmenXYZ.com**). **ANMERKUNG:** Diese E-Mail-Adresse ist ein optionales Feld.

Serverzertifikat hochladen

So laden Sie ein Serverzertifikat hoch:

1. Auf der Seite **SSL-Hauptmenü** wählen Sie **Server-Zertifikat auf Basis von erstellter CSR hochladen** und klicken dann auf **Weiter**. Die Seite **Zertifikat hochladen** wird angezeigt.
2. Geben Sie den Dateipfad im Textfeld ein und klicken Sie auf **Durchsuchen**, um die Datei auszuwählen.
3. Klicken Sie auf **Anwenden**. Wenn das Zertifikat ungültig ist, wird eine Fehlermeldung angezeigt.

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.

Um den Inhalt der Seite **Zertifikat hochladen** zu aktualisieren, klicken Sie auf **Aktualisieren**.

Um den Inhalt der Seite **Zertifikat hochladen** zu drucken, klicken Sie auf **Drucken**.

Web Server-Schlüssel und Zertifikat hochladen

So laden Sie einen Web-Server-Schlüssel und Zertifikat hoch:

1. Wählen Sie die Option **Web Server-Schlüssel und Zertifikat hochladen** und klicken dann auf **Weiter**.
2. Geben Sie die Datei des privaten Schlüssels unter Verwendung des Menüs „Durchsuchen“ ein.
3. Geben Sie die Zertifikatdatei unter Verwendung des Menüs „Durchsuchen“ ein.
4. Nachdem beide Dateien hochgeladen sind, klicken Sie auf **Anwenden**. Falls der Web Server-Schlüssel und das Zertifikat nicht übereinstimmen, wird eine Fehlermeldung angezeigt.

ANMERKUNG: Der CMC akzeptiert lediglich X509-Base-64-kodierte Zertifikate. Zertifikate, die andere Kodierungsschemata verwenden, z. B. DER, werden nicht akzeptiert. Durch das Hochladen eines neuen Zertifikats wird das mit dem CMC gelieferte Standardzertifikat ersetzt.

ANMERKUNG: Um einen Web Server-Schlüssel und ein Serverzertifikat hochzuladen, müssen Sie **Gehäusekonfigurations-Administratorberechtigungen** besitzen.

ANMERKUNG: Nach dem erfolgreichen Hochladen des Zertifikats wird der CMC zurückgesetzt und ist vorübergehend nicht verfügbar. Um zu vermeiden, dass die Verbindung anderer Benutzer während des Resets unterbrochen wird, benachrichtigen Sie berechtigte Benutzer, die sich am CMC anmelden könnten und überprüfen Sie auf aktive Sitzungen, indem Sie die Seite **Sitzungen** im Register **Netzwerk** aufrufen.

Serverzertifikat anzeigen

Auf der Seite **SSL-Hauptmenü** wählen Sie **Server-Zertifikat anzeigen** und klicken dann auf **Weiter**. Die Seite **Serverzertifikat anzeigen** wird angezeigt.

Tabelle 5-50 erläutert die Felder und zugehörigen Beschreibungen, die im Fenster **Zertifikat** aufgeführt werden.

Tabelle 5-50. Zertifikatinformationen

Feld	Beschreibung
Seriell	Seriennummer des Zertifikats
Antragsteller	Vom Bewerber eingegebene Zertifikatsattribute
Aussteller	Vom Aussteller zurückgegebene Zertifikatsattribute.
nicht vor	Ausgabedatum des Zertifikats
nicht nach	Ablaufdatum des Zertifikats

Um den Inhalt der Seite **Serverzertifikat anzeigen** zu aktualisieren, klicken Sie auf **Aktualisieren**.

Um den Inhalt der Seite **Serverzertifikat anzeigen** zu drucken, klicken Sie auf **Drucken**.

Sitzungen verwalten

Die Seite **Sitzungen** zeigt alle aktuellen Verbindungen zum Gehäuse an und ermöglicht Ihnen, beliebige aktive Sitzungen zu beenden.

ANMERKUNG: Um eine Sitzung zu beenden, müssen Sie die Berechtigung als **Gehäusekonfiguration-Administrator** besitzen.

So verwalten oder beenden Sie eine Sitzung:

1. Melden Sie sich über die Webschnittstelle beim CMC an.
2. Klicken Sie auf das Register **Netzwerk** und dann auf das Unterregister **Sitzungen**.
3. Wählen Sie auf der Seite **Sitzungen** die zu beendenden Sitzungen aus und klicken Sie auf die entsprechende Schaltfläche. Tabelle 5-51 zeigt die Sitzungseigenschaften an.

Tabelle 5-51. Sitzungseigenschaften

Eigenschaft	Beschreibung
Sitzungs-ID	Zeigt die sequenziell erstellte ID-Nummer für die einzelnen Instanzen einer Anmeldung an.
Benutzername	Zeigt den Anmeldenamen eines Benutzers an (lokaler Benutzer oder Active Directory-Benutzer). Beispiele von Active Directory-Benutzernamen sind *Name@Domäne.com*, *Domäne.com/Name*, *Domäne.com\Name*.
IP-Adresse	Zeigt die IP-Adresse des Benutzers an.
Sitzungstyp	Beschreibt den Sitzungstyp: Telnet, seriell, SSH, Remote-RACADM, SMASH CLP, WSMAN oder eine GUI-Sitzung.
Beenden	Ermöglicht Ihnen, eine beliebige aufgelistete Sitzung zu beenden (außer der eigenen Sitzung). Um die zugeordnete Sitzung zu beenden, klicken Sie auf die Schaltfläche. Diese Spalte wird nur angezeigt, wenn Sie die Berechtigung zum **Gehäusekonfigurations-Administrator** besitzen.

Dienste konfigurieren

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 übertragen. Der Web Server enthält ein von Dell selbstsigniertes digitales SSL-Zertifikat (Server-ID) und ist dafür verantwortlich, sichere HTTP-Aufforderungen von Clients zu empfangen bzw. darauf zu antworten. Dieser Dienst wird von der Webschnittstelle und dem Remote-CLI-Hilfsprogramm zur Kommunikation mit dem CMC benötigt.

ANMERKUNG: Das Remote-CLI-Hilfsprogramm (RACADM) und die Webschnittstelle verwenden den Web Server. Im Falle, dass der Web Server nicht aktiv ist, stehen Remote-RACADM und die Webschnittstelle nicht zur Verfügung.

ANMERKUNG: Im Falle eines Web Server-Resets warten Sie mindestens eine Minute, bis die Dienste wieder verfügbar werden. Ein Web Server wird normalerweise auf Grund eines der folgenden Ereignisse zurückgesetzt: die Netzwerkkonfiguration oder Netzwerksicherheitseigenschaften wurden über die CMC-Webbenutzerschnittstelle oder RACADM geändert; die Web Server-Schnittstellenkonfiguration wurde über die Webbenutzerschnittstelle oder RACADM geändert; der CMC wurde zurückgesetzt; ein neues SSL-Serverzertifikat wurde hochgeladen.

ANMERKUNG: Zum Modifizieren von Diensteinstellungen müssen Sie die Berechtigung als **Gehäusekonfigurations-Administrator** besitzen.

So konfigurieren Sie die CMC-Dienste:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie auf das Register **Netzwerk**.
3. Klicken Sie auf das Unterregister **Dienste**. Die Seite **Dienste** wird angezeigt.
4. Konfigurieren Sie die folgenden Dienste nach Bedarf:
   - Serielle-CMC-Konsole (Tabelle 5-52)
   - Web Server (Tabelle 5-53)
   - SSH (Tabelle 5-54)
   - Telnet (Tabelle 5-55)
   - Remote-RACADM (Tabelle 5-56)
   - SNMP (Tabelle 5-57)
   - Remote-Syslog (Tabelle 5-58)
5. Klicken Sie auf **Anwenden;** dies aktualisiert alle Standard-Zeitüberschreitungen und alle maximalen Zeitüberschreitungsgrenzwerte.

Tabelle 5-52. Einstellungen der seriellen CMC-Konsole

Einstellung	Beschreibung
Aktiviert	Aktiviert die Telnet-Konsolenschnittstelle auf dem CMC. **Standardeinstellung**: Nicht markiert (deaktiviert)
Umleitung aktiviert	Ermöglicht die serielle bzw. Text-Konsolenumleitung vom CMC zum Server über den seriellen/Telnet/SSH-Client. Der CMC verbindet sich mit dem iDRAC, der intern mit der Server-COM2-Schnittstelle verbunden ist. **Konfigurationsoptionen**: Markiert (aktiviert), nicht markiert (deaktiviert) **Standardeinstellung:** Markiert (aktiviert).
Zeitüberschreitung aufgrund von Inaktivität	Zeigt die Anzahl der Sekunden an, bevor eine inaktive serielle Sitzung automatisch unterbrochen wird. Eine Änderung an der Einstellung **Zeitüberschreitung** wird bei der nächsten Anmeldung wirksam; sie wirkt sich nicht auf die aktuelle Sitzung aus. **Zeitüberschreitungsspanne**: 0 oder 60 bis 10800 Sekunden. Um die Funktion der Zeitüberschreitung zu deaktivieren, geben Sie 0 ein. **Standardeinstellung**: 1800 Sekunden
Baudrate	Zeigt die Datengeschwindigkeit auf der externen seriellen Schnittstelle des CMC an. **Konfigurationsoptionen**: 9600, 19200, 28800, 38400, 57600 und 115200 Bit/s. **Standardeinstellung**: 115200 Bit/s
Authentifizierung deaktiviert	Aktiviert die Anmeldungsauthentifizierung der seriellen CMC-Konsole. **Standardeinstellung**: Nicht markiert (deaktiviert)

Tabelle 5-52. Einstellungen der seriellen CMC-Konsole *(fortgesetzt)*

Einstellung	Beschreibung
Escape-Taste	Ermöglicht Ihnen, die Escape-Tastenkombination festzulegen, die eine serielle bzw. Text-Konsolenumleitung beendet, wenn Sie den Befehl **connect** oder **racadm connect** verwenden. **Standardeinstellung**: ^\ (Halten Sie die Taste <Strg> gedrückt und geben Sie einen umgekehrten Schrägstrich (\) ein). **ANMERKUNG:** Das Caret-Zeichen ^ steht für die Taste <Strg>. Konfigurationsoptionen: • Dezimalwert (Beispiel: 95) • Hexadezimalwert (Beispiel: 0x12) • Oktalwert (Beispiel: 007) • ASCII-Wert (Beispiel: ^a) ASCII-Werte können anhand der folgenden Escape-Tastencodes repräsentiert werden: • Esc, gefolgt von einem beliebigen alphabetischen Zeichen (a-z, A-Z) • Esc, gefolgt von den folgenden Sonderzeichen: [ ] \ ^ _ • Maximal zulässige Länge: 4
Größe Verlaufspuffer	Zeigt die maximale Größe des seriellen Verlaufspuffers an, der die letzten Zeichen enthält, die auf die serielle Konsole geschrieben wurden. **Standardeinstellung**: 8192 Zeichen
Anmeldungsbefehl	Bestimmt den seriellen Befehl, der automatisch ausgeführt wird, wenn sich ein Benutzer an der seriellen CMC-Konsolenschnittstelle anmeldet. **Beispiel**: connect server-1 **Standardeinstellung**: [Null]

Tabelle 5-53. Web Server-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert Web Server-Dienste (Zugriff über Remote-RACADM und die Webschnittstelle) für den CMC. **Standardeinstellung**: Markiert (aktiviert)
Max. Sitzungen	Zeigt die maximale Anzahl der für das Gehäuse zulässigen gleichzeitigen Sitzungen der Web-Benutzerschnittstelle an. Eine Änderung an der Eigenschaft **Max. Sitzungen** wird bei der nächsten Anmeldung wirksam; sie hat keine Auswirkung auf die aktuellen **aktiven Sitzungen** (einschließlich Ihrer eigenen). Remote-RACADM ist von der Eigenschaft **Max. Sitzungen** für den Web Server nicht betroffen. **Zugelassener Bereich**: 1-4 **Standardeinstellung**: 4 **ANMERKUNG:** Wenn Sie die Eigenschaft **Max. Sitzungen** auf einen Wert unter dem Wert der aktuellen Anzahl an aktiven Sitzungen ändern und sich dann abmelden, können Sie sich nicht erneut anmelden, bevor die anderen Sitzungen beendet werden oder ablaufen.
Zeitüberschreitung aufgrund von Inaktivität	Zeigt die Anzahl von Sekunden an, bevor die Verbindung zu einer inaktiven Web-Benutzerschnittstellensitzung automatisch abgebrochen wird. Eine Änderung an der Einstellung **Zeitüberschreitung** wird bei der nächsten Anmeldung wirksam; sie wirkt sich nicht auf die aktuelle Sitzung aus. Der **Zeitüberschreitungsbereich** ist 60 bis 10800 Sekunden. **Standardeinstellung**: 1800 Sekunden

Tabelle 5-53. Web Server-Einstellungen *(fortgesetzt)*

Einstellung	Beschreibung
HTTP-Schnittstellennummer	Zeigt die Standardschnittstelle an, die vom CMC verwendet wird, der eine Serververbindung abhört. **ANMERKUNG:** Wenn Sie die HTTP-Adresse im Browser angeben, führt der Web Server automatisch eine Umleitung aus und verwendet HTTPS. Wenn die Standard-HTTP-Schnittstellennummer (80) geändert wurde, müssen Sie in der Adresse im Adressenfeld des Browsers die Schnittstellennummer wie gezeigt angeben: http://<*IP-Adresse*>:<*Schnittstellennummer*> wobei *IP-Adresse* die IP-Adresse für das Gehäuse ist und *Schnittstellennummer* ist die HTTP-Schnittstellennummer, falls diese vom Standardwert 80 abweicht. **Konfigurationsbereich**: 10 - 65535 **Standardeinstellung**: 80
HTTPS-Schnittstellennummer	Zeigt die Standardschnittstelle an, die vom CMC verwendet wird, der auf eine sichere Serververbindung wartet. Wenn die Standard-HTTPS-Schnittstellennummer (443) geändert wurde, müssen Sie in der Adresse im Adressenfeld des Browsers die Schnittstellennummer wie gezeigt angeben: https://<*IP-Adresse*>:<*Schnittstellennummer*> wobei *IP-Adresse* die IP-Adresse für das Gehäuse ist und *Schnittstellennummer* ist die HTTPS-Schnittstellennummer, falls diese vom Standardwert 443 abweicht. **Konfigurationsbereich**: 10 - 65535 **Standardeinstellung**: 443

Tabelle 5-54. SSH-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert SSH auf dem CMC. **Standardeinstellung**: Markiert (aktiviert)
Max. Sitzungen	Die maximale Anzahl gleichzeitiger, auf dem Gehäuse zulässiger SSH-Sitzungen. Eine Änderung an dieser Eigenschaft wird mit der nächsten Anmeldung wirksam; sie hat keine Auswirkung auf die aktuellen aktiven Sitzungen (einschließlich Ihrer eigenen). **Konfigurierbarer Bereich**: 1–4 **Standardeinstellung**: 4 **ANMERKUNG:** Wenn Sie die Eigenschaft **Max. Sitzungen** auf einen Wert unter dem Wert der aktuellen Anzahl an **aktiven Sitzungen** ändern und sich dann abmelden, können Sie sich nicht erneut anmelden, bevor die anderen Sitzungen beendet werden oder ablaufen.
Zeitüberschreitung aufgrund von Inaktivität	Zeigt die Anzahl der Sekunden an, bevor eine inaktive SSH-Sitzung automatisch unterbrochen wird. Eine Änderung an der Einstellung **Zeitüberschreitung** wird bei der nächsten Anmeldung wirksam; sie wirkt sich nicht auf die aktuelle Sitzung aus. Der **Zeitüberschreitungsbereich** ist 0 oder 60 bis 10800 Sekunden. Um die Funktion der Zeitüberschreitung zu deaktivieren, geben Sie 0 ein. **Standardeinstellung**: 1800 Sekunden
Schnittstellennummer	Vom CMC verwendete Schnittstelle, die eine Serververbindung abhört. **Konfigurationsbereich**: 10 - 65535. **Standardeinstellung**: 22

Tabelle 5-55. Telnet-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert die Telnet-Konsolenschnittstelle auf dem CMC. **Standardeinstellung**: Nicht markiert (deaktiviert)
Max. Sitzungen	Zeigt die für das Gehäuse maximal zulässige Anzahl gleichzeitiger Telnet-Sitzungen an. Eine Änderung an dieser Eigenschaft wird mit der nächsten Anmeldung wirksam; sie hat keine Auswirkung auf die aktuellen aktiven Sitzungen (einschließlich Ihrer eigenen). **Zugelassener Bereich:** 1–4 **Standardeinstellung**: 4 **ANMERKUNG:** Wenn Sie die Eigenschaft „Max. Sitzungen" auf einen Wert unter dem Wert der aktuellen Anzahl an aktiven Sitzungen ändern und sich dann abmelden, können Sie sich nicht erneut anmelden, bevor die anderen Sitzungen beendet werden oder ablaufen.
Zeitüberschreitung aufgrund von Inaktivität	Zeigt die Anzahl der Sekunden an, bevor eine inaktive Telnet-Sitzung automatisch unterbrochen wird. Eine Änderung an der Einstellung Zeitüberschreitung wird bei der nächsten Anmeldung wirksam; sie wirkt sich nicht auf die aktuelle Sitzung aus. Der **Zeitüberschreitungsbereich** ist 0 oder 60 bis 10800 Sekunden. Um die Funktion der Zeitüberschreitung zu deaktivieren, geben Sie 0 ein. **Standardeinstellung**: 1800 Sekunden
Schnittstellennummer	Zeigt die Standardschnittstelle an, die vom CMC verwendet wird, der eine Serververbindung abhört. **Standardeinstellung**: 23

Tabelle 5-56. Remote-RACADM- Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert den Zugriff des Remote-RACADM-Dienstprogramms auf den CMC. **Standardeinstellung**: Markiert (aktiviert)
Max. Sitzungen	Zeigt die für das Gehäuse maximal zulässige Anzahl gleichzeitiger RACADM-Sitzungen an. Eine Änderung an dieser Eigenschaft wird mit der nächsten Anmeldung wirksam; sie hat keine Auswirkung auf die aktuellen **aktiven Sitzungen** (einschließlich Ihrer eigenen). **Zugelassener Bereich:** 1–4 **Standardeinstellung**: 4 **ANMERKUNG:** Wenn Sie die Eigenschaft „Max. Sitzungen" auf einen Wert unter dem Wert der aktuellen Anzahl an aktiven Sitzungen ändern und sich dann abmelden, können Sie sich nicht erneut anmelden, bevor die anderen Sitzungen beendet werden oder ablaufen.
Zeitüberschreitung aufgrund von Inaktivität	Zeigt die Anzahl der Sekunden an, bevor eine inaktive racadm-Sitzung automatisch unterbrochen wird. Bei der nächsten Anmeldung wird eine Änderung an der Einstellung Zeitüberschreitung aufgrund von Inaktivität wirksam; sie wirkt sich nicht auf die aktuelle Sitzung aus. Geben Sie zur Deaktivierung der Funktion „Zeitüberschreitung aufgrund von Inaktivität" den Wert 0 ein. **Zeitüberschreitungsspanne**: 0 oder 10 bis 1920 Sekunden. Um die Funktion der Zeitüberschreitung zu deaktivieren, geben Sie 0 ein. **Standardeinstellung:** 30 Sekunden

Tabelle 5-57. SNMP-Konfiguration

Einstellung	Beschreibung
Aktiviert	Aktiviert SNMP auf dem CMC. **Gültige Werte:** Markiert (aktiviert), nicht markiert (deaktiviert) **Standardeinstellung**: Nicht markiert (deaktiviert)
Community-Name	Gibt die Community-Zeichenkette an, die verwendet wird, um Daten von SNMP-Daemon des CMC zu erhalten.

Tabelle 5-58. Remote-Syslog-Konfiguration

Einstellung	Beschreibung
Aktiviert	Aktiviert die Übertragung und Remote-Erfassung von CMC-Protokoll- und Hardwareprotokolleinträgen an die angegebenen Server. **Gültige Werte:** Markiert (aktiviert), nicht markiert (deaktiviert) **Standardeinstellung**: Nicht markiert (deaktiviert)
Syslog Server 1	Erster von drei möglichen Servern, die eine Kopie der CMC- und Hardwareprotokolleinträge speichern können. Spezifiziert als Host-Name, IPv6-Adresse oder IPv4-Adresse.
Syslog Server 2	Zweiter von drei möglichen Servern, die eine Kopie der CMC- und Hardwareprotokolleinträge speichern können. Spezifiziert als Host-Name, IPv6-Adresse oder IPv4-Adresse.
Syslog Server 3	Dritter von drei möglichen Servern, die eine Kopie der CMC- und Hardwareprotokolleinträge speichern können. Spezifiziert als Host-Name, IPv6-Adresse oder IPv4-Adresse.
Syslog-Schnittstellennummer	Gibt die Schnittstellennummer am Remote-Server an, um eine Kopie der CMC- und Hardwareprotokolleinträge zu erhalten. Die gleiche Schnittstellennummer wird für alle drei Server verwendet. Eine gültige Syslog-Schnittstellennummer liegt im Bereich von 10-65535. **Standardeinstellung**: 514

Strombudget konfigurieren

Sie können mit dem CMC die Stromversorgung des Gehäuses budgetieren und verwalten. Der Stromverwaltungsdienst optimiert den Stromverbrauch und weist den verschiedenen Modulen je nach Bedarf Strom zu.

Anweisungen zur Stromkonfiguration über den CMC finden Sie unter „Strom konfigurieren und verwalten“ auf Seite 386.

Weitere Informationen zu den Strommanagementdiensten des CMC finden Sie unter „Stromverwaltung“ auf Seite 363.

Firmwareaktualisierungen verwalten

In diesem Abschnitt wird die Aktualisierung der Firmware auf den Gehäuse- und Server-Komponenten über die GUI und das RACADM-Dienstprogramm erläutert.

Die folgenden Komponenten können über das RACADM-Dienstprogramm oder über die GUI aktualisiert werden. In der GUI können Sie die Aktualisierung über die Seiten **Gehäuse-Übersicht→ Aktualisieren** oder **Gehäuse-Controller→ Aktualisieren** durchführen:

- CMC – Aktiv und Standby
- iKVM
- iDRAC – Alle iDRAC-Firmware-Versionen vor der Version iDRAC6 müssen über die Wiederherstellungsschnittstelle aktualisiert werden. Die iDRAC6-Firmware kann ebenfalls über die Wiederherstellungsschnittstelle aktualisiert werden, für iDRAC6 und künftige Versionen wird dies jedoch nicht empfohlen.
- EAM-Infrastrukturgeräte

Auf der Seite **Server-Übersicht→ Aktualisieren** in der GUI können Sie die folgenden Serverkomponenten aktualisieren.

- iDRAC
- BIOS
- Unified Server Configurator
- 32-Bit Diagnose
- OS-Treiberpaket

- Netzwerkschnittstellen-Controller
- RAID-Controller

Die Firmware-Aktualisierungen für die Serverkomponente werden mithilfe des Lifecycle Controller-Dienstes ausgeführt, der auf iDRAC verfügbar ist. Der Lifecycle Controller unterstützt Firmware-Abbilder im Dell Update Package (DUP)-Format. Die standardmäßige CMC-Konfiguration hat eine Größenbeschränkung von 48MB für das DUP. Die DUP-Komponente für das BS-Treiberpaket überschreitet diesen Grenzwert und muss separat über die Funktion „Erweiterter Speicher“ aktualisiert werden. Weitere Informationen finden Sie unter „Aktualisieren der Serverkomponenten-Firmware unter Verwendung des Lifecycle Controllers“ auf Seite 242.

Wenn Sie Firmware aktualisieren, sollte das empfohlene Verfahren eingehalten werden, um einen Verlust des Dienstes zu verhindern, falls die Aktualisierung fehlschlägt. Weitere Richtlinien finden Sie unter „Installieren oder Aktualisieren der CMC-Firmware“ auf Seite 56.

Aktuelle Firmware-Versionen anzeigen

Die Seite „Aktualisierung“ zeigt die aktuelle Version aller aktualisierbaren Gehäusekomponenten an. Dies kann die iKVM-Firmware, aktive CMC-Firmware, (gegebenenfalls) die Standby-CMC-Firmware, die iDRAC-Firmware und die Firmware der EAM-Infrastrukturgeräte einschließen Weitere Informationen finden Sie unter„Aktualisierung der Firmware des EAM-Infrastrukturgeräts“ auf Seite 238.

So zeigen Sie die Gehäusekomponenten an, die aktualisiert werden können:

1. Melden Sie sich bei der Webschnittstelle an. Weitere Informationen finden Sie unter „Auf die CMC-Webschnittstelle zugreifen“ auf Seite 121.
2. Klicken Sie in der Systemstruktur auf **Gehäuseübersicht**.

   ANMERKUNG: Klicken Sie alternativ dazu in der Systemstruktur auf Gehäuse-Controller.
3. Klicken Sie auf die Registerkarte **Aktualisieren**. Die Seite **Firmwareaktualisierung** wird eingeblendet.

So zeigen Sie die aktualisierbaren Serverkomponenten an:

1. Melden Sie sich bei der Webschnittstelle an. Weitere Informationen finden Sie unter „Auf die CMC-Webschnittstelle zugreifen“ auf Seite 121.
2. Klicken Sie in der Systemstruktur auf **Serverübersicht**.
3. Klicken Sie auf die Registerkarte **Aktualisieren**. Die Seite **Serverkomponenten-Aktualisierung** erscheint.

So öffnen Sie eine Aktualisierungsseite für ausgewählte Geräte:

1. Klicken Sie auf den Gerätenamen oder markieren Sie die Option **Alle auswählen/abwählen**.
2. Klicken Sie auf **Aktualisierung Anwenden**.

   Eine Aktualisierungsseite für die ausgewählten Geräte wird angezeigt.

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. Lesen Sie unter „iDRAC-Firmware mittels CMC wiederherstellen“ auf Seite 240 nach, um weitere Schritte zur Wiederherstellung der iDRAC-Firmware unter Verwendung des CMC zu erfahren.

Firmware aktualisieren

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

ANMERKUNG: Die Firmware-Aktualisierung bewahrt die derzeitigen CMC- und iKVM-Einstellungen.

ANMERKUNG: Wenn eine Benutzersitzung an der Webschnittstelle verwendet wird, um Systemkomponenten-Firmware zu aktualisieren, müssen die Einstellungen für die **Inaktivitätszeitüberschreitung** hoch genug 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" auf Seite 221.

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

Die grundlegenden Schritte zur Aktualisierung der Geräte-Firmware sind:

1. Geräte zur Aktualisierung auswählen.
2. Auf die Schaltfläche **Anwenden** unter der Gruppierung klicken.
3. Auf **Durchsuchen** klicken, um das Firmware-Image auszuwählen.
4. Auf **Firmware-Aktualisierung starten** klicken, um den Aktualisierungsvorgang zu starten. Die Meldung **Datei-Image übertragen** wird angezeigt, gefolgt von einer Statusfortschrittsseite.

ANMERKUNG: Stellen Sie sicher, dass Sie die neueste Firmware-Version besitzen. Sie können die aktuelle Version der Firmware von der Dell Support-Website unter **support.dell.com** herunterladen.

CMC-Firmware aktualisieren

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.

ANMERKUNG: 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.

ANMERKUNG: Um zu vermeiden, dass die Verbindung anderer Benutzer während des Resets unterbrochen wird, benachrichtigen Sie berechtigte Benutzer, die sich am CMC anmelden könnten und prüfen Sie auf aktive Sitzungen, indem Sie die Seite **Sitzungen** aufrufen. Um die Seite **Sitzungen** zu öffnen, wählen Sie in der Struktur **Gehäuse,** klicken auf das Register **Netzwerk** und dann auf das Unterregister **Sitzungen**. Hilfe zu dieser Seite finden Sie über den Link **Hilfe**, der sich auf dieser Seite oben rechts befindet.

ANMERKUNG: 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. Anleitungen finden Sie unter „Animationen im Internet Explorer erlauben“ auf Seite 43.

ANMERKUNG: Wenn beim Herunterladen von Dateien vom CMC mit dem Internet Explorer Probleme auftreten, aktivieren Sie die Option **Verschlüsselte Seiten nicht auf der Festplatte speichern**. Anleitungen hierzu finden Sie unter „Dateien mit dem Internet Explorer vom CMC herunterladen“ auf Seite 43.

CMC-Firmware aktualisieren

1. Auf der Seite **Firmware-Aktualisierung** wählen Sie die zu aktualisierende(n) CMC(s) aus, indem Sie das Kontrollkästchen **Ziele aktualisieren** für die CMC(s) auswählen. Beide CMCs können gleichzeitig aktualisiert werden.
2. Klicken Sie auf die Schaltfläche **CMC-Aktualisierung anwenden** unterhalb der CMC-Komponentenliste.

   ANMERKUNG: Der standardmäßige Firmware-Image-Name lautet **firmimg.cmc**. Die CMC-Firmware sollte zuerst, vor der Firmware der EAM-Infrastrukturgeräte, aktualisiert werden.
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.

4 Klicken Sie auf **Firmware-Aktualisierung beginnen**. Der Abschnitt **Fortschritt der Firmware-Aktualisierung** bietet Statusinformationen zur Firmwareaktualisierung. Ein Statusindikator wird auf der Seite während des Aktualisierungsvorganges angezeigt. Die Übertragungszeit kann je nach Verbindungsgeschwindigkeit deutlich variieren. Wenn der interne Aktualisierungsprozess beginnt, aktualisiert sich die Seite automatisch und zeigt die Dauer der Firmwareaktualisierung an. Zusätzliche Anweisungen:

- Verwenden Sie während der Dateiübertragen nicht die Schaltfläche **Aktualisieren** und navigieren nicht Sie zu einer anderen Seite.
- Um den Prozess abzubrechen, klicken Sie auf **Dateiübertragung und Aktualisierung abbrechen** - diese Option ist nur während der Dateiübertragung verfügbar.
- Der Status der Aktualisierung wird im Feld **Aktualisierungsstatus** angezeigt; dieses Feld wird automatisch während der Dateiübertragung aktualisiert.

ANMERKUNG: Die Aktualisierung kann einige Minuten für den CMC dauern.

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, da der aktive CMC offline genommen wird. Sie müssen sich nach einigen Minuten neu anmelden, wenn der aktive CMC neu gestartet ist.

Nach dem Reset des CMC wird die neue Firmware auf der Seite **Firmware-Aktualisierung** angezeigt.

ANMERKUNG: Nach der Firmware-Aktualisierung löschen Sie den Cache des Internet-Browsers. Beachten Sie zum Löschen des Browser-Cache die Online-Hilfe Ihres Web-Browsers.

Aktualisieren der iKVM-Firmware

ANMERKUNG: Nach dem erfolgreichen Abschluss der Firmwareaktualisierung wird das iKVM-Modul zurückgesetzt und ist vorübergehend nicht verfügbar.

1 Melden Sie sich erneut bei der CMC-Webschnittstelle an.

2 Klicken Sie in der Systemstruktur auf **Gehäuse-Übersicht**.

3 Klicken Sie auf die Registerkarte **Aktualisieren**. Die Seite **Firmwareaktualisierung** wird eingeblendet.

4 Wählen Sie das zu aktualisierende iKVM, indem Sie das Kontrollkästchen **Ziele aktualisieren** für das iKVM auswählen.

5 Klicken Sie auf die Schaltfläche **iKVM-Aktualisierung anwenden** unterhalb der CMC-Komponentenliste.

6 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.

ANMERKUNG: Der Standardname des iKVM-Firmware-Images ist ikvm.bin; der Name des iKVM-Firmware-Images kann jedoch vom Benutzer verändert werden, um Verwechslungen mit früheren Images zu vermeiden.

7 Klicken Sie auf **Firmware-Aktualisierung beginnen**.

8 Klicken Sie auf **Yes** (Ja), um fortzufahren. 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 deutlich variieren. Wenn der interne Aktualisierungsprozess beginnt, aktualisiert sich die Seite automatisch und zeigt die Dauer der Firmwareaktualisierung an. Zusätzliche Anweisungen:

- Verwenden Sie während der Dateiübertragen nicht die Schaltfläche **Aktualisieren** und navigieren nicht Sie zu einer anderen Seite.
- Um den Prozess abzubrechen, klicken Sie auf **Dateiübertragung und Aktualisierung abbrechen** - diese Option ist nur während der Dateiübertragung verfügbar.
- Der Status der Aktualisierung wird im Feld **Aktualisierungsstatus** angezeigt; dieses Feld wird automatisch während der Dateiübertragung aktualisiert.

ANMERKUNG: Die Aktualisierung für das iKVM kann bis zu zwei Minuten dauern.

Wenn die Aktualisierung abgeschlossen ist, wird das iKVM zurückgesetzt und die neue Firmware wird auf der Seite **Firmware-Aktualisierung** angezeigt.

Aktualisierung der Firmware des EAM-Infrastrukturgeräts

Diese Aktualisierung bewirkt, dass die Firmware für eine Komponente des EAM-Geräts aktualisiert wird, aber nicht die Firmware des EAM-Geräts selbst; die Komponente ist die Schnittstelle zwischen dem EAM-Gerät und dem CMC. Das Aktualisierungs-Image für die Komponente befindet sich im CMC-Dateisystem und die Komponente wird nur als aktualisierbares Gerät auf der CMC-Web-GUI angezeigt, wenn die aktuelle Revision auf der Komponente und das Komponenten-Image nicht übereinstimmen. So aktualisieren Sie die Firmware des EAM-Infrastruktugerätes:

1. Melden Sie sich erneut bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur **Gehäuse-Übersicht** aus.
3. Klicken Sie auf die Registerkarte **Aktualisieren**. Die Seite **Firmwareaktualisierung** wird eingeblendet.
4. Wählen Sie das zu aktualisierende EAM-Gerät, indem Sie das Kontrollkästchen **Ziele aktualisieren** für dieses EAM-Gerät markieren.
5. Klicken Sie auf die Schaltfläche **EAM-Aktualisierung anwenden** unterhalb der CMC-Komponentenliste.

   ANMERKUNG: Das Feld Firmware-Image wird für ein EAM-Infrastrukturgerät-Ziel (IOMINF) nicht angezeigt, da sich das benötigte Image auf dem CMC befindet. Die CMC-Firmware sollte zuerst, vor der IONINF-Firmware, aktualisiert werden.

   IOMINF-Aktualisierungen werden vom CMC zugelassen, wenn der CMC erkennt, dass die IOMINF-Firmware gegenüber dem im CMC-Dateisystem enthaltenen Image veraltet ist. Falls die IOMINF-Firmware auf dem neuesten Stand ist, verhindert der CMC IOMINF-Aktualisierungen. Aktualisierte IOMINF-Geräte sind als aktualisierbare Geräte aufgelistet.

6 Klicken Sie auf **Firmware-Aktualisierung beginnen**. Der Abschnitt **Fortschritt der Firmware-Aktualisierung** bietet Statusinformationen zur Firmwareaktualisierung. Ein Statusindikator wird auf der Seite während des Aktualisierungsvorganges angezeigt. Die Übertragungszeit kann je nach Verbindungsgeschwindigkeit deutlich variieren. Wenn der interne Aktualisierungsprozess beginnt, aktualisiert sich die Seite automatisch und zeigt die Dauer der Firmwareaktualisierung an. Zusätzliche Anweisungen:

- Verwenden Sie während der Dateiübertragung nicht die Schaltfläche **Aktualisierung** und navigieren Sie nicht zu einer anderen Seite.
- Der Status der Aktualisierung wird im Feld **Aktualisierungsstatus** angezeigt; dieses Feld wird automatisch während der Dateiübertragung aktualisiert.

ANMERKUNG: Es wird bei der IOMINF-Firmware-Aktualisierung kein Zeitgeber angezeigt. Der Aktualisierungsprozess kann kurzzeitigen Verlust der Konnektivität zum EAM-Gerät verursachen, da das Gerät einen Neustart durchführt, wenn die Aktualisierung beendet ist. Wenn die Aktualisierung abgeschlossen ist, wird die neue Firmware angezeigt und das aktualisierte System ist nicht mehr auf der Seite **Firmware-Aktualisierung** vorhanden.

iDRAC-Firmware aktualisieren

ANMERKUNG: Der iDRAC (auf einem Server) wird zurückgesetzt und ist vorübergehend nicht verfügbar, nachdem die Firmware-Aktualisierungen erfolgreich hochgeladen wurden.

ANMERKUNG: Die iDRAC-Firmware muss Version 1.4 oder höher für Server mit iDRAC, bzw. 2.0 oder höher für Server mit iDRAC6 Enterprise sein. Wenn die iDRAC-Firmware von einer Version unterhalb von Version 2.3 auf eine Version ab Version 3.0 aktualisiert werden soll, müssen Sie die iDRAC-Firmware zunächst auf die Version 2.3 aktualisieren, bevor Sie sie auf eine Version ab 3.0 aktualisieren können.

1 Melden Sie sich erneut bei der CMC-Webschnittstelle an.

2 Wählen Sie in der Systemstruktur **Gehäuse-Übersicht** aus.

3 Klicken Sie auf die Registerkarte **Aktualisieren**. Die Seite **Firmwareaktualisierung** wird eingeblendet.

4 Wählen Sie die zu aktualisierende(n) iDRAC(s), indem Sie das Kontrollkästchen **Ziele aktualisieren** für diese Geräte wählen.

5 Klicken Sie auf die Schaltfläche **iDRAC-Aktualisierung anwenden** unterhalb der CMC-Komponentenliste.

6 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.

7 Klicken Sie auf **Firmware-Aktualisierung beginnen**. Der Abschnitt **Fortschritt der Firmware-Aktualisierung** bietet Statusinformationen zur Firmwareaktualisierung. Ein Statusindikator wird auf der Seite während des Aktualisierungsvorganges angezeigt. Die Übertragungszeit kann je nach Verbindungsgeschwindigkeit deutlich variieren. Wenn der interne Aktualisierungsprozess beginnt, aktualisiert sich die Seite automatisch und zeigt die Dauer der Firmwareaktualisierung an. 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.
   - Der Status der Aktualisierung wird im Feld **Aktualisierungsstatus** angezeigt; dieses Feld wird automatisch während der Dateiübertragung aktualisiert.

ANMERKUNG: Die Aktualisierung kann einige Minuten für den CMC oder den Server dauern.

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. Wie Sie die iDRAC-Firmware aktualisieren, erfahren Sie im *Benutzerhandbuch zur iDRAC-Firmware*.

Für frühe 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.

So aktualisieren Sie die iDRAC-Firmware:

1. Laden Sie die neueste iDRAC-Firmware von **support.dell.com** auf den Verwaltungscomputer herunter.
2. Melden Sie sich bei der Webschnittstelle an (siehe „Auf die CMC-Webschnittstelle zugreifen“ auf Seite 121).
3. Klicken Sie in der Systemstruktur auf **Gehäuseübersicht**.
4. Klicken Sie auf die Registerkarte **Aktualisieren**. Die Seite **Firmwareaktualisierung** wird eingeblendet.
5. Wählen Sie die zu aktualisierende(n) iDRAC(s) auf demselben Modell aus, indem Sie das Kontrollkästchen **Ziele aktualisieren** für diese Geräte auswählen.
6. Klicken Sie auf die Schaltfläche **iDRAC-Aktualisierung anwenden** unterhalb der CMC-Komponentenliste.
7. Klicken Sie auf **Durchsuchen**, und suchen Sie nach dem von Ihnen heruntergeladenen iDRAC-Firmware-Image. Klicken Sie dann auf **Öffnen**.

   ANMERKUNG: Der Standardname für das iDRAC-Firmware-Image ist **firmimg.imc**. Die CMC-Firmware sollte zuerst, vor der Firmware der EAM-Infrastrukturgeräte, aktualisiert werden.
8. Klicken Sie auf **Firmware-Aktualisierung beginnen**. 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.
   - Der Status der Aktualisierung wird im Feld **Aktualisierungsstatus** angezeigt; dieses Feld wird automatisch während der Dateiübertragung aktualisiert.

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

Aktualisieren der Serverkomponenten-Firmware unter Verwendung des Lifecycle Controllers

Der Lifecycle Controller ist ein Dienst, der auf jedem der Server zur Verfügung steht und durch iDRAC unterstützt wird. Die Seite **Serverkomponenten-Aktualisierung** ermöglicht Ihnen die Verwaltung der Firmware von Komponenten und Geräten auf den Servern unter Verwendung des Lifecycle Controller-Dienstes. Der Lifecycle Controller verwendet für die Aktualisierung der Firmware einen Authentifizierungsalgorithmus, der die Anzahl der Neustarts auf effiziente Art und Weise reduziert.

Vor der Verwendung der Lifecycle Controller-basierten Aktualisierungsfunktion müssen die Server-Firmware-Versionen aktualisiert werden.

ANMERKUNG: Sie müssen die CMC-Firmware vor dem Aktualisieren der Firmware-Module für die Serverkomponente aktualisieren.

Sie müssen die Firmware-Module der Serverkomponente in der folgenden Reihenfolge aktualisieren:

- BIOS
- Lifecycle Controller
- iDRAC

Weitere Informationen finden Sie im Abschnitt „Empfohlene Modul-Firmware-Versionen“ in den CMC-Versionshinweisen unter **support.dell.com/manuals**. 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.

Wenn Sie die Firmware manuell über DUPs aktualisieren, müssen Sie die Firmware in der folgenden Reihenfolge aktualisieren:

• BIOS

• Lifecycle Controller

• iDRAC – Wenn die iDRAC-Firmware von einer Version unterhalb von Version 2.3 auf eine Version ab Version 3.0 aktualisiert werden soll, müssen Sie die iDRAC-Firmware zunächst auf Version 2.3 aktualisieren, bevor Sie sie auf eine Version ab 3.0 aktualisieren können.

Aktivierung des Lifecycle Controllers

Wenn der Server den Lifecycle Controller-Dienst nicht unterstützt, wird im Abschnitt **Firmware-Bestandsliste** `Not Supported` (Nicht unterstützt) angezeigt

Möglicherweise ist der Lifecycle Controller-Dienst auf dem Server deaktiviert und der Abschnitt **Firmware-Bestandsliste** zeigt `Lifecycle Controller may not be enabled` an.

Aktualisieren Sie auf der neuesten Servergeneration zur Aktivierung des Lifecycle Controller-Dienstes die vorhandenen Server, indem Sie die Unified Server Configurator (USC)-Firmware installieren und die iDRAC-Firmware aktualisieren. Für ältere Servergenerationen ist diese Aktualisierung möglicherweise nicht möglich.

Normalerweise wird die USC-Firmware über ein geeignetes Installationspaket installiert, das auf dem Server-OS ausgeführt werden muss. Ein spezielles Reparatur- oder Installationspaket mit der Dateierweiterung.**usc** steht auf der systemeigenen iDRAC Webbrowser-Schnittstelle zur Verfügung. Mit diesem Paket können Sie die USC-Firmware über die gewohnte Firmware-Aktualisierungsfunktion installieren. Lesen Sie für weitere Informationen das *Dell Lifecycle Controller USC/USC-LCE-Benutzerhandbuch*.

Der Lifecycle Controller-Dienst kann im Rahmen des Server-Startvorgangs aktiviert werden. Drücken Sie bei iDRAC6-Servern auf der Startkonsole, wenn Sie dazu über die Nachricht `Press <CTRL-E> for Remote Access Setup within 5 sec` aufgefordert werden, die Tastenkombination <Strg-E>. Aktivieren Sie anschließend auf dem Setup-Bildschirm die Option **Systemdienste**.

Wählen Sie **Systemdienste abbrechen**, um alle geplanten und ausstehenden Aufträge abzubrechen und sie aus der Warteschlange zu entfernen.

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

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

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 irgendeine Art von Lifecycle Controller-Vorgang auf dem Server auswählen.

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

- Die Dell Lifecycle Controller Remote Services-Übersicht.
- **delltechcenter.com/page/Lifecycle+Controller**.

Filtermechanismen

Informationen zu allen Komponenten und Geräten werden über alle Server hinweg auf einmal abgerufen. Um diese große Menge an Informationen zu verwalten, stellt der Lifecycle Controller verschiedene Filtermechanismen zur Verfügung. 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.
- Die ausgewählten Komponenten und Geräte automatisch auswählen, um die Kategorie einer bestimmten Komponente bzw. eines Gerätes basierend auf Typen oder Modellen einzueengen.

  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.

Beispiele

Es folgen einige Beispiele für die Anwendung der Filtermechanismen:

- Bei Auswahl des BIOS-Filters wird nur die BIOS-Bestandsliste für alle 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.

Die Seite **Serverkomponenten-Aktualisierung** enthält die folgenden Abschnitte:

- Komponente/Geräte-Aktualisierungsfilter: Dieser Abschnitt wird zur Steuerung der Anzeige von Komponenten und/oder von Geräten im Abschnitt **Firmware-Bestandsliste** verwendet. Indem Sie den Filter für einen Komponenten- oder Gerätetyp aktivieren, wird der Abschnitt mit der **Firmware-Bestandsliste** geändert, sodass nur die aktivierte Komponente, bzw. das aktivierte Gerät über alle Server hinweg angezeigt wird.

  Nachdem eine Filterauswahl vorgenommen wurde und der gefilterte Satz an Komponenten und Geräten im Bestandslistenabschnitt 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 Bestandslistenabschnitt alle Server nur mit ihrer BIOS-Komponente an. Wenn eine BIOS-Komponente auf einem der Server ausgewählt wird, wird die Bestandsliste weiter gefiltert, um die Server anzuzeigen, die mit der Modellbezeichnung des ausgewählten Servers übereinstimmen.

Wenn kein Filter ausgewählt wird und im Bestandslistenabschnitt 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 Bestandslistenabschnitt 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 Bestandslistenabschnitt zeigt die Server an, die mit der Modellbezeichnung des ausgewählten Servers übereinstimmen.

Das Aktivieren des Filters ermöglicht das Filtern nach der jeweiligen Komponente bzw. dem Gerät im **Firmware-Bestandsliste**nabschnitt. Nach dem Aktivieren eines Filters können nur die jeweilige Komponenten bzw. das Gerät über alle im Gehäuse vorhandenen Server hinweg angezeigt werden. Der Filter ist ein Pass-Filter; das bedeutet, dass er nur Komponenten oder Geräte zulässt, die mit dem Filter verbunden sind und alle anderen ausschließt. Je nach Bedarf können ein oder mehrere Filter (oder alle) ausgewählt werden.

Die Komponenten und Geräte werden in folgende Kategorien gruppiert:

- BIOS
- iDRAC
- Unified Server Configurator (Lifecycle Controller)
- 32-Bit Diagnose
- BS-Treiberpaket
- Network Interface Controller (NICs) und RAID-Controller

- Komponenten/Geräte-Firmwarebestandsliste: Dieser Abschnitt fasst den Status der Firmwareversionen aller Komponenten und Geräte über die aktuell im Gehäuse vorhandenen Server hinweg zusammen. Es stehen Optionen zum Durchführen der verschiedenen Lifecycle Controller-Vorgänge, wie z.B. Aktualisierung, Rollback, Neuinstallation und Auftragslöschung zur Verfügung. 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.

Server, die derzeit den Lifecycle Controller-Dienst nicht unterstützen, werden als **Nicht unterstützt** aufgeführt. Es wird ein Hyperlink bereitgestellt, der die Navigation auf eine alternative Seite ermöglicht, auf der es möglich ist, nur die iDRAC-Firmware direkt zu aktualisieren. Diese Seite unterstützt keine Aktualisierung irgendwelcher der Komponenten oder Geräte des Servers. Auf dieser alternativen Seite kann nur die iDRAC-Firmware aktualisiert werden und sie ist nicht von der Lifecycle Controller-Einrichtung abhängig.

Wenn der Server als **Nicht bereit** aufgeführt wird, bedeutet dies, dass sich zum Zeitpunkt des Abrufens der Firmware-Bestandsliste der iDRAC auf dem Server noch initialisiert hat. Warten Sie ab, bis der iDRAC voll betriebsbereit ist und aktualisieren Sie anschließend die Seite, damit die Firmware-Bestandsliste erneut abgerufen werden kann.

Wenn die Bestandsliste der Komponenten und Geräte nicht dem entspricht, was physikalisch auf dem Server installiert ist, dann müssen Sie während des Server-Startvorgangs die USC-Konsole (Unified Server Configurator) aufrufen. Dies ist beim Aktualisieren der internen Komponenten- und Geräteinformationen hilfreich und stellt eine andere Möglichkeit zur Prüfung der derzeit installierten Komponenten und Geräte dar. Diese Situation tritt auf, wenn:

- Die Server-iDRAC-Firmware aktualisiert wird, um die Lifecycle Controller-Funktionalität neu bei der Serververwaltung einzuführen.
- Die neuen Geräte gerade in den Server eingesetzt wurden.

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

Drücken Sie bei iDRAC6-Servern auf der Startkonsole, wenn Sie dazu über die Nachricht `Press <CTRL-E> for Remote Access Setup within 5 sec.` für die Einrichtung des Remote-Zugriffs die Tastenkombination <Strg-E> aufgefordert werden, die Tastenkombination **<Strg-E>**. Aktivieren Sie anschließend auf dem Setup-Bildschirm die Option **System-Bestandsliste beim Neustart erfassen**.

Klicken Sie für iDRAC7-Server auf der Startkonsole für das System-Setup-Programm auf die Taste F2. Wählen Sie auf dem Setup-Bildschirm die Option „iDRAC-Einstellungen“ aus, und wählen Sie dann „Systemdienste“ (USC) aus. Aktivieren Sie dann auf dem Setup-Bildschirm die Option **System-Bestandsliste beim Neustart erfassen**.

Tabelle 5-59 zeigt Informationen zu Komponenten und Geräten auf dem Server an:

Tabelle 5-59. Komponenten- und Geräteinformationen

Feld	Beschreibung
Steckplatz	Zeigt den vom Server im Gehäuse besetzten Steckplatz an. Steckplatznummern sind sequenzielle IDs von 1 bis 16 (für die 16 im Gehäuse verfügbaren Steckplätze), mit denen die Position des Servers im Gehäuse identifiziert werden kann. Wenn weniger als 16 Steckplätze mit Servern belegt sind, werden nur die mit Servern bestückten Steckplätzen angezeigt.
Name	Zeigt den Namen des Servers in jedem Steckplatz an.
Modell	Zeigt das Modell des Servers an.
Komponente/Gerät	Zeigt eine Beschreibung der Komponente oder des Geräts auf dem Server an. Wenn die Spaltenbreite zu schmal ist, stellt das Mouse-Over-Hilfswerkzeug eine Ansicht mit der Beschreibung bereit.
Aktuelle Version	Zeigt die aktuelle Version der Komponente oder des Geräts auf dem Server an. Wenn neben der aktuellen Version ein Kontrollkästchen angezeigt wird, ist dies ein Hinweis darauf, dass ein Firmware-Image der aktuell installierten Firmware für die Komponente oder das Gerät im Lifecycle Controller für einen **Neuinstallationsvorgang** zur Verfügung steht.
Rollback-Version	Zeigt die aktuelle Rollback-Version der Komponente oder des Geräts auf dem Server an. Wenn neben der Rollback-Version ein Kontrollkästchen angezeigt wird, ist dies ein Hinweis darauf, dass ein Firmware-Image der aktuell installierten Firmware für die Komponente oder das Gerät im Lifecycle Controller für einen **Rollback-**Vorgang zur Verfügung steht. Die Verfügbarkeit unterliegt der Versionskompatibilitätslogik des Lifecycle Controllers. Es wird auch angenommen, dass die vorherige Aktualisierung mittels des Lifecycle Controllers stattgefunden hat.

Tabelle 5-59. Komponenten- und Geräteinformationen *(fortgesetzt)*

Feld	Beschreibung
Auftragsstatus	Zeigt den Auftragsstatus von jeglichen Vorgängen an, die auf dem Server geplant sind. Der Auftragsstatus wird kontinuierlich dynamisch aktualisiert. Wenn ein Auftragsabschluss über den Status **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. Wird neben dem Auftragsstatus ein Kontrollkästchen angezeigt, ist dies ein Hinweis darauf, dass gerade ein Lifecycle Controller-Auftrag durchgeführt wird und sich dieser derzeit im Status **angezeigt** befindet. Er kann für einen **Auftrags-Löschvorgang** ausgewählt werden. Neben dem aktuellen Status ist auch ein Info-Symbol vorhanden, das zusätzliche Informationen über den aktuellen Auftragsstatus bereitstellt. Diese Informationen können angezeigt werden, indem auf das Symbol geklickt wird oder der Mauszeiger über das Symbol bewegt wird.

Tabelle 5-59. Komponenten- und Geräteinformationen *(fortgesetzt)*

Feld	Beschreibung
Aktualisierung	Wählt die Komponente oder das Gerät für die Firmware-Aktualisierung auf dem Server aus. Verwenden Sie das STRG-Tastenkürzel, um einen Komponenten- oder Gerätetyp für die Aktualisierung über alle zutreffenden Server hinweg auszuwählen. Das Drücken und Halten der STRG-Taste markiert alle Komponenten in gelb. Wählen Sie bei gedrückter STRG-Taste die erforderliche Komponente oder das Gerät aus, indem Sie das zugehörige Kontrollkästchen in der Spalte **Aktualisieren** aktivieren. BIOS-Aktualisierungen sind Servermodell-spezifisch. Die Auswahllogik basiert auf dieser Funktionsweise. 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 48MB unterstützt. Wenn die Größe des Aktualisierungsdatei-Images größer ist, zeigt der Auftragsstatus an, dass das Herunterladen fehlgeschlagen ist. Werden auf einem Server mehrere Serverkomponenten-Aktualisierungen versucht, überschreitet die kombinierte Größe aller Firmware-Aktualisierungen möglicherweise 48MB. In einem solchen Fall schlägt eine der Komponenten-Aktualisierungen fehl, da deren Aktualisierungsdatei abgeschnitten wird. Eine empfohlene Strategie zur Aktualisierung mehrerer Komponenten auf einem Server ist es, zuerst die Komponenten des Unified Server Configurators und der 32-Bit Diagnose 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, dass die durch den CMC gehostete Remote-Freigabe nicht länger zur Verfügung steht.

Bei der Auswahl einer Komponente oder eines Geräts für die Aktualisierung muss das DUP (Dell Update Package) angegeben werden. Es wird eine sekundäre Tabelle, die die Komponente/das Gerät identifiziert und ein Wähler für die Firmware-Imagedatei angezeigt. Dadurch kann die Firmware-Imagedatei für die zugehörige Komponente oder das Gerät angegeben werden. Es wird ein spezifischer Wähler für jeden Komponenten-/Gerätetyp angezeigt, der für die Aktualisierung angegeben wird.

ANMERKUNG: Es wird pro Komponente oder Gerätekategorie nur ein Wähler angezeigt.

Dies fällt bei NIC-Geräten (Network Interface Controller) und den RAID-Controller-Geräten eher auf. Diese Geräte 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. Die Firmware-Imagedatei muss ein Microsoft Windows DUP (Dell Update Package) sein. Dabei handelt es sich um eine unter Microsoft Windows ausführbare Datei.

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 „Aktivieren von wechselbaren Flash-Datenträgern" auf Seite 125.

ANMERKUNG: Es wird empfohlen, die Auftragswarteschlange zu löschen, bevor Sie die Aktualisierung einer Serverkomponentenfirmware initialisieren. Auf der Seite **Lifecycle Controller-Aufträge** ist eine Liste mit allen Aufträgen auf den/dem Server(n) vorhanden. Diese Seite ermöglicht die Löschung einzelner/mehrerer Aufträge oder die Bereinigung aller Aufträge auf dem Server. Weitere Informationen finden Sie im Abschnitt „Fehlerbehebung" unter „Lifecycle Controller-Aufträge auf einem Remote-System verwalten" auf Seite 490.

Die Seite **Serverkomponenten-Aktualisierung** ermöglicht Ihnen das Durchführen verschiedener Maßnahmen, indem Sie die vorhandenen Schaltflächen verwenden. Jede Schaltfläche ermöglicht das Durchführen der zugewiesenen Lifecycle Controller-Maßnahme. Damit ein Vorgang durchgeführt werden kann, muss für diesen Vorgang mindestens eine Komponente oder ein Gerät ausge-wählt werden. Wenn für eine Komponente oder ein Gerät ein **Aktualisierungsvorgang** ausgewählt wird, dann muss im Abschnitt **Aktualisierungsfilter** und **Auswahl der Image-Datei** die Firmware-Image-Datei angegeben werden. Verlassen Sie die Seite nicht, nachdem ein Vorgang für die Planung eingereicht wurde. Wird ein Versuch unternommen, wird eine Popup-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 Popup-Bestätigungsmeldung zur Anzeige der erfolgreichen Planung des Vorgangs bestätigt wird. Sobald ein Lifecycle Controller-Vorgang auf einem Server geplant wurde, kann es 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. Der Fortschritt dieses Vorgangs kann durch das Anzeigen der Serverkonsole beobachtet werden. 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.

Tabelle 5-60 beschreibt die vorhandenen Schaltflächen und die Maßnahmen, die auf der Seite **Serverkomponenten-Aktualisierung** durchgeführt werden können:

Tabelle 5-60. Serverkomponenten-Aktualisierungsmaßnahmen

Schaltfläche	Aktion
Aktualisierung	Führt für die ausgewählten Komponenten und/oder Geräte den **Aktualisierungsvorgang** durch, um Firmware-Aktualisierungen über einen oder mehrere Server hinweg zu planen.
Rollback	Führt für die ausgewählten Komponenten und/oder Geräte den **Rollback-**Vorgang durch, um Firmware-Rollbacks über einen oder mehrere Server hinweg zu planen.
Neuinstallation	Führt für die ausgewählten Komponenten und/oder Geräte den **Neuinstallationsvorgang** durch, um Firmware-Neuinstallationen über einen oder mehrere Server hinweg zu planen.
Auftragslöschung	Führt den **Auftragslöschungsvorgang** durch, um zu den ausgewählten Komponenten und/oder Geräten zugehörige Aufträge über einen oder mehrere Server hinweg zu löschen.

Bei einigen Komponenten ist bei den Vorgängen Aktualisieren, Rollback und Neuinstallation der Neustart des Servers erforderlich. Der Neustart kann verschoben werden, indem Sie eine Auswahl aus der Dropdown-Liste treffen. Wählen Sie **Jetzt neu starten** aus, wenn der Server sofort neu gestartet werden soll, oder wählen Sie **Später neu starten** aus, um den Server zu einem späteren Zeitpunkt neu zu starten.

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 Popup-Bestätigungsmeldung angezeigt, die auf die Situation hinweist und der Vorgang wird nicht eingereicht. Warten Sie, bis der Vorgang abgeschlossen wurde und reichen Sie den Vorgang anschließend erneut ein.

iDRAC verwalten

Der CMC liefert die Seite „iDRAC bereitstellen“, um dem Benutzer die Konfi-guration von installierten und neu eingefügten iDRAC-Netzwerkkonfigurations-einstellungen des Servers zu ermöglichen. Ein Benutzer kann ein oder mehrere installierte iDRAC-Geräte von dieser Seite aus konfigurieren. Der Benutzer kann außerdem die Standard- iDRAC-Netzwerkkonfigurationseinstellungen und das Stammkennwort für Server, die zu einem späteren Zeitpunkt installiert werden, konfigurieren; diese Standardeinstellungen sind die Einstellungen der **schnellen iDRAC Bereitstellung**.

Weitere Informationen zum iDRAC-Verhalten finden Sie in den *iDRAC-Benutzerhandbüchern* unter **support.dell.com/manuals**.

Schnelle iDRAC Bereitstellung

Der Abschnitt **Schnelle iDRAC Bereitstellung** auf der Seite **iDRAC bereitstellen** enthält Netzwerkkonfigurationseinstellungen, die auf neu eingefügte Server angewendet werden. Diese Einstellungen können dazu verwendet werden, die Tabelle **iDRAC-Netzwerkeinstellungen,** die sich unter dem Abschnitt „Schnelle Bereitstellung“ befindet, automatisch zu bestücken. Wenn „Schnelle Bereitstellung“ aktiviert ist, werden die Einstellungen der schnellen Bereitstellung auf Server angewendet, wenn der jeweilige Server installiert wird. Weitere Informationen zu den iDRAC QuickDeploy-Einstellungen finden Sie in Schritt 8 unter „Netzwerkbetrieb mit dem LCD-Konfigurationsassistent konfigurieren“ auf Seite 46.

So aktivieren Sie die **iDRAC-Einstellungen für die schnelle Bereitschaft** und stellen sie ein:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur **Server-Übersicht** aus.
3. Klicken Sie auf das Register **Setup**. Die Seite **iDRAC bereitstellen** wird angezeigt.
4. Stellen Sie die Einstellungen zur schnellen Bereitstellung entsprechend ein.

Tabelle 5-61. Einstellungen zur schnellen Bereitstellung

Einstellung	Beschreibung
Schnelle Bereitstellung aktiviert	Aktiviert/deaktiviert die Funktion **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. **ANMERKUNG:** Dies schließt das Stammbenutzer-kennwort ein, wenn das Kontrollkästchen **iDRAC-Stammkennwort bei Servereinfügung einstellen** markiert ist. **Standardeinstellung**: Nicht markiert (deaktiviert)
iDRAC-Stammkennwort bei Servereinfügung einstellen	Gibt an, ob das iDRAC-Stammkennwort eines Servers auf den Wert geändert werden soll, der im Textfeld **iDRAC-Stammkennwort** angegeben wird, wenn der Server eingefügt wird.
iDRAC-Stammkennwort	Wenn **iDRAC-Stammkennwort bei Servereinfügung einstellen** und **Schnelle Bereitstellung aktiviert** markiert sind, wird der Kennwortwert einem Server-iDRAC-Stammbenutzerkennwort zugewiesen, wenn der Server in das Gehäuse eingefügt wird. Das Kennwort kann 1 bis 20 druckbare Zeichen (einschließlich Leerzeichen) aufweisen.
iDRAC-Stammkennwort bestätigen	Bestätigt das Kennwort, das in das Feld **iDRAC-Stammkennwort** eingegeben wurde.
iDRAC-LAN aktivieren	Aktiviert/deaktiviert den iDRAC-LAN-Kanal. **Standardeinstellung**: Nicht markiert (deaktiviert)
iDRAC IPv4 aktivieren	Aktiviert/deaktiviert IPv4 auf dem iDRAC. Die Standardeinstellung lautet „aktiviert“.
IPMI-Über-LAN aktivieren	Aktiviert/deaktiviert den IPMI-über-LAN-Kanal für jeden iDRAC, der sich in dem Gehäuse befindet. **Standardeinstellung**: Nicht markiert (deaktiviert)

Tabelle 5-61. Einstellungen zur schnellen Bereitstellung *(fortgesetzt)*

Einstellung	Beschreibung
iDRAC-DHCP aktivieren	Aktiviert/deaktiviert DHCP für jeden iDRAC, der sich in dem Gehäuse befindet. Wenn diese Option aktiviert ist, sind die Felder **Schnelle Bereitstellung-IP**, **Schnelle Bereitstellung-Subnetzmaske** und **Schnelle Bereitstellung-Gateway** deaktiviert und können nicht geändert werden, da DHCP verwendet wird, um diese Einstellungen automatisch für jeden iDRAC zuzuweisen. **Standardeinstellung**: Nicht markiert (deaktiviert)
iDRAC-IPv4-Adresse (Steckplatz 1) starten	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 schnelle Bereitstellung für Steckplatz 15: 192.168.0.265. Wenn die Subnetzmaske 255.255.255.0 wäre, würde die Fehlermeldung `IP-Adressenbereich für schnelle Bereitstellung befindet sich nicht vollständig innerhalb des Subnetzes für schnelle Bereitstellung` angezeigt, wenn entweder die Schaltfläche **Einstellungen zur schnellen Bereitstellung speichern** oder **Automatische Bestückung mit Einstellungen zur schnellen Bereitstellung** betätigt wird.
iDRAC IPv4-Netzmaske	Gibt die Subnetzmaske für schnelle Bereitstellung an, die allen neu eingefügten Servern zugewiesen ist.
iDRAC IPv4-Gateway	Gibt das Standard-Gateway (für schnelle Bereitstellung) an, das allen iDRACs, die sich im Gehäuse befinden, zugewiesen wird.

Tabelle 5-61. Einstellungen zur schnellen Bereitstellung *(fortgesetzt)*

Einstellung	Beschreibung
iDRAC IPv6 aktivieren	Aktiviert IPv6-Adressierung für jeden iDRAC, der sich in dem Gehäuse befindet und IPv6-fähig ist.
iDRAC IPv6 AutoConfiguration aktivieren	Aktiviert den iDRAC zur Beschaffung von IPv6-Einstellungen (Adresse und Präfixlänge) von einem DHCPv6-Server und aktiviert auch statuslose automatische Adresskonfiguration. Die Standardeinstellung lautet „aktiviert“.
iDRAC IPv6-Gateway	Gibt das Standard-IPv6-Gateway an, das den iDRACs zugewiesen wird. Die Standardeinstellung ist „::“.
iDRAC IPv6-Präfixlänge	Gibt die Präfixlänge an, die den IPv6-Adressen auf dem iDRAC zugewiesen wird. Die Standardeinstellung ist 64.

5 Um die Auswahl zu speichern, klicken Sie auf die Schaltfläche **Einstellungen zur schnellen Bereitstellung speichern**. Wenn Sie die Änderungen an den Einstellungen des iDRAC-Netzwerkes vorgenommen haben, klicken Sie auf die Schaltfläche **iDRAC-Netzwerkeinstellungen anwenden**, um die Einstellungen zur iDRAC bereitzustellen.

6 Um die Tabelle zu den zuletzt gespeicherten Einstellungen zur schnellen Bereitstellung zu aktualisieren und die iDRAC-Netzwerkeinstellungen auf die aktuellen Werten für jeden installierten Server wiederherzustellen, klicken Sie auf **Aktualisieren**.

ANMERKUNG: Durch Klicken auf die Schaltfläche Aktualisieren werden alle iDRAC- und iDRAC-Netzwerkkonfigurationseinstellungen (für schnelle Bereitstellung) gelöscht, die nicht gespeichert wurden.

Die Funktion schnelle Bereitstellung wird nur ausgeführt, wenn sie aktiviert ist und ein Server im Gehäuse eingefügt ist. Wenn **iDRAC-Stammkennwort bei Servereinfügung einstellen** und **Schnelle Bereitstellung aktiviert** markiert sind, wird der Benutzer aufgefordert, die LCD-Schnittstelle zu verwenden, um die Kennwortänderung zu erlauben oder nicht zu erlauben. Wenn Netzwerk-einstellungen 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 schnelle Bereitstellung anzunehmen. Wenn der Unterschied in der DHCP-Einstellung liegt, wird der Benutzer aufgefordert, die Einstellungen der schnellen DHCP-Bereitstellung anzunehmen.

Um die Einstellungen zur schnellen Bereitstellung in den Abschnitt **iDRAC-Netzwerkeinstellungen** zu kopieren, klicken Sie auf **Mit Einstellungen zur schnellen Bereitstellung automatisch bestücken**. Die Netzwerkkonfigurationseinstellungen zur schnellen Bereitstellung werden in die entsprechenden Felder der Tabelle **iDRAC-Netzwerkkonfigurations-einstellungen** kopiert.

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 die Schaltfläche **Aktualisieren** zu früh betätigt wird, werden eventuell nur teilweise richtige Daten für einen oder mehrere iDRAC-Server angezeigt.

iDRAC-Netzwerkeinstellungen

Der Abschnitt **iDRAC-Netzwerkeinstellungen** auf der Seite **iDRAC bereitstellen** enthält eine Tabelle, die die iDRAC IPv4- und IPv6-Netzwerkkonfigurationseinstellungen aller installierten Server aufführt. Mithilfe dieser Tabelle 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. Durch Ändern eines Felds und Klicken auf **iDRAC-Netzwerkeinstellungen anwenden** werden die geänderten Felder auf dem iDRAC gespeichert.

So aktivieren Sie die iDRAC-Netzwerkeinstellungen und stellen sie ein:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur **Server-Übersicht** aus.
3. Klicken Sie auf das Register **Setup**.

   Die Seite **iDRAC bereitstellen** wird angezeigt.
4. Wählen Sie das Kontrollkästchen **Schnelle Bereitstellung aktiviert**, um die Einstellungen zur schnellen Bereitstellung zu aktivieren.
5. Stellen Sie die restlichen **iDRAC-Netzwerkeinstellungen** entsprechend ein.

Tabelle 5-62. iDRAC-Netzwerkeinstellungen

Einstellung	Beschreibung
Steckplatz	Zeigt den vom Server im Gehäuse besetzten Steckplatz an. Steckplatznummern sind sequenzielle IDs von 1 bis 16 (im Gehäuse gibt es 16 verfügbare Steckplätze), die bei der Identifizierung der Position des Servers im Gehäuse hilfreich sind. **ANMERKUNG:** Wenn weniger als 16 Steckplätze mit Servern belegt sind, werden nur die mit Servern bestückten Steckplätzen angezeigt.
Name	Zeigt den Servernamen des Servers in jedem Steckplatz an. Standardmäßig heißen die Steckplätze **STECKPLATZ-01** bis **STECKPLATZ-16**. **ANMERKUNG:** Der Steckplatzname kann nicht leer oder NULL sein.
LAN aktivieren	Aktiviert (markiert) oder deaktiviert (nicht markiert) den LAN-Kanal. **ANMERKUNG:** Wenn LAN nicht ausgewählt ist (deaktiviert), werden alle anderen Netzwerkkonfigura-tionseinstellungen (**IPMI-über-LAN, DHCP, IP-Adresse Subnetzmaske** und **Gateway**) nicht verwendet. Diese Felder sind nicht zugreifbar.
Stammkennwort ändern	Aktiviert (wenn markiert) die Möglichkeit, das Kennwort des iDRAC-Stammbenutzers zu ändern. Die Felder **iDRAC-Stammkennwort** und **iDRAC-Stammkennwort bestätigen** müssen ausgefüllt sein, damit dieser Vorgang erfolgreich ist.

Tabelle 5-62. iDRAC-Netzwerkeinstellungen *(fortgesetzt)*

Einstellung	Beschreibung
DHCP	Wenn markiert, wird DHCP verwendet, um IP-Adresse, Subnetzmaske und Standard-Gateway des iDRAC zu erwerben. Ansonsten werden die in den iDRAC-Netzwerk-konfigurationsfeldern definierten Werte verwendet. LAN muss aktiviert sein, um dieses Feld einzustellen.
IPMI über LAN	Aktiviert (markiert) oder deaktiviert (nicht markiert) den LAN-Kanal. LAN muss aktiviert sein, um dieses Feld einzustellen.
IP-Adresse	Die statische IPv4- oder IPv6-Adresse, die dem iDRAC in diesem Steckplatz zugewiesen ist.
Subnetzmaske	Gibt die Subnetzmaske an, die dem in diesem Steckplatz installierten iDRAC zugewiesen ist.
Gateway	Gibt das Standard-Gateway an, das dem in diesem Steckplatz installierten iDRAC zugewiesen ist.
IPv4 aktivieren	Aktiviert den iDRAC im Steckplatz für die Verwendung des IPv4-Protokolls im Netzwerk. Diese Option kann nur aktiv sein, wenn Sie die Option **LAN aktivieren** auswählen. Die Standardeinstellung lautet „aktiviert“.
IPv6 aktivieren	Aktiviert den iDRAC im Steckplatz für die Verwendung des IPv6-Protokolls im Netzwerk. Diese Option kann nur aktiv sein, wenn Sie die Option **LAN aktivieren** auswählen und die **Autokonfiguration**-Option deaktivieren. Die Standardeinstellung lautet „deaktiviert“. **ANMERKUNG:** Diese Option ist nur verfügbar, wenn der Server IPv6-fähig ist.
AutoConfiguration	Aktiviert den iDRAC zur Beschaffung von IPv6-Einstellungen (Adresse und Präfixlänge) von einem DHCPv6-Server und aktiviert auch statuslose automatische Adresskonfiguration. **ANMERKUNG:** Diese Option ist nur verfügbar, wenn der Server IPv6-fähig ist.
Präfixlänge	Gibt die Länge des IPv6-Subnetzes (in Bit) an, zu dem dieser iDRAC gehört.

6 Um die Einstellung auf dem iDRAC bereitzustellen, klicken Sie auf die Schaltfläche **iDRAC-Netzwerkeinstellungen anwenden**. Wenn Sie Änderungen an den Einstellungen zur schnellen Bereitstellung vorgenommen haben, werden diese ebenfalls gespeichert.

7 Zur Wiederherstellung der iDRAC-Netzwerkeinstellungen auf die aktuellen Werte für die einzelnen installierten Server und zur Aktualisierung der Tabelle für schnelle Bereitstellung auf die zuletzt gespeicherten Einstellungen für schnelle Bereitstellung, klicken Sie auf **Aktualisieren**.

ANMERKUNG: Durch Klicken auf die Schaltfläche Aktualisieren werden alle iDRAC- und iDRAC-Netzwerkkonfigurationseinstellungen (für schnelle Bereitstellung) gelöscht, die nicht gespeichert wurden.

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). Verwenden Sie die Schaltfläche **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 die Schaltfläche Aktualisierung zu früh gedrückt wird, werden eventuell nur teilweise richtige Daten für einen oder mehrere iDRAC-Server angezeigt.

Remote-Konsole von der CMC-GUI starten

Mit dieser Funktion können Sie eine Keyboard-Video-Mouse (KVM)-Sitzung direkt auf dem Server starten.

So starten Sie eine Server-Remote-Konsole von der CMC-GUI-Homepage:

1 Klicken Sie auf den angegebenen Server in der Gehäuse-Grafik.

2 Bei den **Quicklinks** klicken Sie auf den Link **Remote-Konsole starten**.

So starten Sie eine Server-Remote-Konsole von der Seite **Status der Server**:

1. In der Systemstruktur wählen Sie **Server-Übersicht**.
2. Klicken Sie in der Tabelle für den angegebenen Server auf **Remote-Konsole starten**.

So starten Sie eine Server-Remote-Konsole für einen Einzelanwender:

1. Erweitern Sie in der Systemstruktur **Server-Übersicht**. Es werden alle Server (1 - 16) in der erweiterten Liste der Server angezeigt.
2. In der Systemstruktur klicken Sie auf den Server, den Sie anzeigen möchten. Die Seite **Serverstatus** wird angezeigt.
3. Klicken Sie auf **Remote-Konsole starten**.

Die Remote-Konsolen-Funktion wird nur unterstützt, wenn alle folgenden Bedingungen erfüllt sind:

- Das Gehäuse ist eingeschaltet.
- Server, die iDRAC6 und iDRAC7 unterstützen.
- Die LAN-Schnittstelle auf dem Server ist aktiviert.
- Die iDRAC-Version ist 2.20 oder höher.
- 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).

ANMERKUNG: Die Remote-Konsole kann auch vom iDRAC-GUI gestartet werden. Weitere Einzelheiten finden Sie unter iDRAC-GUI.

iDRAC mit einfacher Anmeldung starten

Der CMC bietet eine eingeschränkte Verwaltung individueller Gehäusekompo-nenten, 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).

Start der iDRAC-Verwaltungskonsole von der **Server-**Seite aus:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur **Server-Übersicht** aus. Die Seite **Status der Server** wird angezeigt.

3 Klicken Sie auf die Schaltfläche **iDRAC-GUI starten** für den Server, den Sie verwalten möchten.

So starten Sie die iDRAC-Verwaltungskonsole für einen individuellen Server:

1 Melden Sie sich bei der CMC-Webschnittstelle an.

2 Erweitern Sie in der Systemstruktur **Server-Übersicht**. Es werden alle Server (1–16) in der erweiterten Liste der **Server** angezeigt.

3 Klicken Sie auf den Server, den Sie anzeigen möchten. Die Seite **Serverstatus** wird angezeigt.

4 Klicken Sie auf die Schaltfläche **iDRAC-GUI starten**.

Ein Benutzer kann die iDRAC-GUI starten ohne sich ein zweites Mal anzumelden, da diese Funktion die einfache Anmeldung verwendet. Die Richtlinien der einfachen Anmeldung werden nachfolgend 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 die Schaltfläche **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.

ANMERKUNG: Wenn der Server vom Gehäuse entfernt wird, die iDRAC-IP-Adresse geändert wird oder die iDRAC-Netzwerkverbindung ein Problem aufweist, kann das Klicken des Symbols „iDRAC-GUI starten" zur Anzeige einer Fehlerseite führen.

Erstellen von Server-Klonen

Mit der Funktion zum Erstellen von Server-Klonen können Benutzer alle klonbaren BIOS-Einstellungen von einem spezifizierten Server auf einen oder mehrere Server anwenden. Klonbare BIOS-Einstellungen sind solche BIOS-Einstellungen, die geändert werden können und dazu dienen, auf verschiedenen Servern repliziert zu werden.

Die Funktion zum Klonen von Servern unterstützt iDRAC6- und iDRAC7-Server. Es werden auch frühere Generationen von iDRAC-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. iDRAC6-Server müssen mindestens in Version 3.2 und iDRAC7-Server in der Version 1.0.0 vorliegen.
- Auf dem Server muss die Generierung von iDRAC unterstützt werden.
- Der Server muss eingeschaltet sein.

Sie können die BIOS-Einstellungen mithilfe der Funktion zum Klonen von Servern nur über die CMC-Web-Schnittstelle konfigurieren. Auf der Seite „BIOS-Profile" können Sie diesen Vorgang ausführen.

Klicken Sie zum Zugreifen auf die Seite „Bios-Profile" auf **Server-Übersicht→ Setup→ Profile**.

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

Erfassungsprofil

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

Wenn Sie ein gespeichertes Profil erstellen, stellen Sie einen Namen und eine optionale Beschreibung für jedes Profil bereit. 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“.

Profil anwenden

Wenn gespeicherte Profile auf dem nichtflüchtigen CMC-Medium verfügbar sind, um das Klonen eines Servers zu initiieren, wenden Sie ein Speicherprofil auf einen oder mehrere Server an.

Der Vorgangsstatus, die Einschubnummer, der Einschubname und der Modellname werden für jeden Server in der Tabelle **Profil anwenden** angezeigt. Nach dem Anwenden eines gespeicherten Profils auf einen Server wird der Server umgehend neu gestartet.

BIOS-Einstellungen auf dem Server anzeigen

Klicken Sie zum Anzeigen der Server-BIOS-Einstellungen für einen ausgewählten Server in der Tabelle **Profil anwenden** in der Spalte der BIOS-Einstellungen für den ausgewählten Eintrag auf **Anzeigen**.

Daraufhin wird die Seite **Einstellungen anzeigen** 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 ähnliche Weise in Gruppen partitioniert, wie sie auf dem BIOS-Setup-Bildschirm für iDRAC angezeigt werden.

ANMERKUNG: Sämtliche Änderungen, die an den Blade-BIOS-Einstellungen in der Konsole vorgenommen wurden, werden auf der Seite **Einstellungen anzeigen** erst dann angezeigt, nachdem eine Systembestandsliste auf dem Blade erfolgt ist. Dazu muss die Option **Systembestandsliste beim Neustart erfassen** (CSIOR) im BIOS aktiviert werden.

Gespeicherte Profile verwalten

Um die gespeicherten Profile im CMC zu verwalten, klicken Sie in der Tabelle **Profil anwenden** auf **Profil verwalten**. Daraufhin wird die Seite „BIOS-Profile verwalten“ angezeigt.

Auf der Seite „BIOS-Profile verwalten“ können Sie den Namen oder die Beschreibung eines gespeicherten Profils bearbeiten, die darin enthaltenen BIOS-Einstellungen anzeigen oder ein gespeichertes Profil löschen.

Neu erstelltes Profilprotokoll

In der Tabelle **Neu erstelltes Profilprotokoll** auf der Hauptseite für das Klonen von Blades werden die neu erstellten Profilprotokolleinträge aufgeführt, die direkt aus Server-Klonvorgängen heraus erstellt wurden. Jedes neu erstellte Profilprotokoll zeigt den Schweregrad sowie Uhrzeit und Datum der Bestätigung des Server-Klonvorgangs sowie die Beschreibung der Klonprotokollmeldung an.

Meldungen, die im **neu erstellen Profilprotokoll** ermittelt wurden, werden auch in das RAC-Protokoll geschrieben. Die Tabelle „Neu erstelltes Profilprotokoll“ enthält die zehn neuesten Profilprotokolleinträge. Klicken Sie zum Anzeigen weiterer verfügbarer Einträge auf **Gehe zu Profilprotokoll**.

Fertigstellungsstatus und Fehlerbehebung

So überprüfen Sie den Fertigstellungsstatus für ein angefordertes und angewendetes BIOS-Profil:

1. Erfassen Sie die Job-ID (JID) des übermittelten gewünschten Jobs aus der Tabelle **Neu erstelltes Profilprotokoll** auf der Hauptseite für das Klonen von Servern.
2. Suchen Sie die gleiche JID in der Tabelle **Jobs** auf der Seite **Lifecycle Controller-Jobs** (**Server-Übersicht→ Fehlerbehebung→ Lifecycle Controller-Jobs**).

FlexAddress

Dieser Abschnitt beschreibt die Webschnittstellenbildschirme von FlexAddress. 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: Sie müssen die FlexAddress-Erweiterung kaufen und installieren, um Zugriff auf die Konfigurationsbildschirme zu haben. Wenn die Erweiterung nicht gekauft und installiert wurde, wird der folgende Text in der Webschnittstelle angezeigt:

```
Optional feature not installed. See the Dell
Chassis Management Controller Users Guide for
information on the chassis-based WWN and MAC
address administration feature.

To purchase this feature, please contact Dell at
www.dell.com.
```

Anzeigen des FlexAddress-Status

Sie können die Webschnittstelle nutzen, um Statusinformationen zu FlexAddress anzuzeigen. Sie können die Statusinformationen für das gesamte Gehäuse oder für einen einzelnen Server anzeigen lassen. Die angezeigten Informationen beinhalten:

- Strukturkonfiguration
- FlexAddress aktiv/nicht aktiv
- Steckplatznummer und -name
- Gehäusezugewiesene und serverzugewiesene Adressen
- Verwendete Adressen

ANMERKUNG: Sie können den Status von FlexAddress auch über die Befehlszeilenschnittstelle einsehen. Weitere Befehlsinformationen finden Sie unter „FlexAddress verwenden“ auf Seite 281.

Anzeigen des Gehäuse-FlexAddress-Status

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.

Anzeigen, ob FlexAddress für das Gehäuse aktiv ist:

1. Melden Sie sich bei der Webschnittstelle an (siehe „Auf die CMC-Webschnittstelle zugreifen“ auf Seite 121).
2. Klicken Sie in der Systemstruktur auf **Gehäuseübersicht**.

3 Klicken Sie auf die Registerkarte **Setup**. Die Seite **Allgemeine Einstellungen** erscheint. Der Eintrag für FlexAddress weist den Wert **Aktiv** oder **Nicht Aktiv** auf; der Eintrag „Aktiv“ bedeutet, dass die Funktion für das Gehäuse installiert wurde. Ein Wert „Nicht aktiv“ bedeutet, dass die Funktion nicht für das Gehäuse installiert wurde und nicht verfügbar ist.

Anzeigen einer FlexAddress Statusübersicht für jedes Servermodul:

1 Melden Sie sich bei der Webschnittstelle an („Auf die CMC-Webschnittstelle zugreifen“ auf Seite 121).

2 Klicken Sie auf **Serverübersicht→ Eigenschaften→ WWN/MAC**.

3 Die Seite **FlexAddress-Zusammenfassung** wird angezeigt. Diese Seite erlaubt Ihnen, die WWN-Konfiguration und die MAC-Adressen für alle Steckplätze im Gehäuse anzuzeigen.

Die Statusseite zeigt die folgenden Informationen an:

Strukturkonfiguration	**Struktur A**, **Struktur B** und **Struktur C** zeigen den Typ der installierten Eingabe/Ausgabe-Struktur. **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, und MAC oder WWNs für Struktur B und C anzeigen, wenn diese von den bestückten Steckplätzen verwendet werden.
WWN/MAC-Adressen	Zeigt die FlexAddress-Konfiguration für jeden Steckplatz im Gehäuse an. Die angezeigten Informationen beinhalten: • Der iDRAC-Management-Controller ist keine Struktur, doch seine FlexAddress wird wie eine Struktur behandelt. • Steckplatznummer und -position • FlexAddress-Status aktiv/nicht aktiv • Strukturtyp • Serverzugewiesene und gehäusezugewiesene verwendete WWN/MAC-Adressen Ein grünes Häkchen zeigt den aktiven Adresstyp, entweder serverzugewiesen oder gehäusezugewiesen.

4 Klicken Sie für weitere Informationen auf **Hilfe**.

Anzeigen des Status von Server-FlexAddress

FlexAddress-Statusinformationen können auch für jeden einzelnen Server angezeigt werden. Die Serverebenen-Informationen zeigen eine Statusübersicht für FlexAddress für diesen Server an.

Anzeige von FlexAddress Serverinformationen:

1. Melden Sie sich bei der Webschnittstelle an (siehe „Auf die CMC-Webschnittstelle zugreifen“ auf Seite 121).
2. Erweitern Sie in der Systemstruktur **Server-Übersicht**. Es werden alle Server (1–16) in der erweiterten Liste der **Server** angezeigt.
3. Klicken Sie auf den Server, den Sie anzeigen möchten.

   Die Seite **Serverstatus** wird angezeigt.
4. Klicken Sie auf das Register **Setup** und dann das Unterregister **FlexAddress**. Die Seite **FlexAddress bereitstellen** wird angezeigt. Diese Seite erlaubt Ihnen, die WWN-Konfiguration und die MAC-Adressen für ausgewählten Server anzuzeigen.

   Die Statusseite zeigt die folgenden Informationen an:

Tabelle 5-63. Statusseiteninformationen

FlexAddress aktiviert	Zeigt an, ob die Funktion FlexAddress für einen bestimmten Steckplatz aktiviert oder deaktiviert ist.
Aktueller Zustand	Zeigt die derzeitige FlexAddress-Konfiguration an: • **Gehäusezugewiesen** - die ausgewählte Steckplatz-Adresse ist mittels FlexAddress dem Gehäuse zugewiesen. Die steckplatzbasierten WWN/MAC-Adressen bleiben die gleichen, selbst wenn ein neuer Server installiert wird. • **Serverzugewiesen** - der Server verwendet eine serverzugewiesen Adresse oder die standardmäßig in die Controller-Hardware eingebettete Adresse.
Stromzustand	Status: Zeigt den aktuellen Stromstatus der Server an. Werte sind: **An**, **Hochfahren**, **Herunterfahren**, **Aus** und **k.A.** (wenn kein Server vorhanden ist).

Tabelle 5-63. Statusseiteninformationen *(fortgesetzt)*

Seite „Funktionszustand“		OK	Zeigt an, dass FlexAddress aktiv ist und liefert den Status an den CMC. Im Falle eines Fehlers bei der Datenübertragung zwischen dem CMC und FlexAddress, kann der CMC den Funktionszustand von FlexAddress weder abrufen noch anzeigen.
		Informativ	Zeigt Informationen über FlexAddress an, wenn beim Funktionsstatus (OK, Warnung, Kritisch) keine Änderung eingetreten ist.
		Warnung	Zeigt an, dass Warnungen ausgegeben wurden und **Korrekturmaßnahmen getroffen werden müssen**. Falls keine Korrekturmaßnahmen getroffen werden, können kritische Fehler die Integrität des Servers beinträchtigen.
		Kritisch	Zeigt an, dass mindestens eine Fehlerwarnung ausgegeben wurde. Ein kritischer Status stellt einen Systemfehler auf dem Server dar. **Es müssen umgehend Korrekturmaßnahmen getroffen werden**.
		Kein Wert	Wenn FlexAddress nicht verfügbar ist, werden keine Informationen zum Funktionszustand geliefert.
iDRAC Firmware	Zeigt die derzeit auf dem Server installierte iDRAC-Version an.		
BIOS-Version	Zeigt die derzeit auf dem Servermodul installierte BIOS-Version an.		
Steckplatz	Steckplatznummer des Servers, der mit der Strukturposition verbunden ist.		
Standort	Zeigt die Position des Eingabe/Ausgabe-Moduls (E/A) im Gehäuse nach Gruppennummer (A, B oder C) und Steckplatznummer (1 oder 2) an. Steckplatznamen: A1, A2, B1, B2, C1 oder C2.		

Tabelle 5-63. Statusseiteninformationen *(fortgesetzt)*

Fabric	Zeigt die Struktur an.
Serverzugewiese n	Zeigt die dem Server zugewiesenen WWN/MAC-Adressen an, die in die Hardware des Controllers eingebettet sind.
Gehäusezugewiesen	Zeigt die dem Gehäuse zugewiesenen WWN/MAC-Adressen an, die für einen bestimmten Steckplatz verwendet werden.

5 Klicken Sie für weitere Informationen auf **Hilfe**.

FlexAddress konfigurieren

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 CMC *Secure Digital (SD) Card Technical Specification* installieren. Sie finden dieses Dokument unter **support.dell.com/manuals**.

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/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.

Für die ausgewählten Steckplätze wird FlexAddress für alle Strukturen aktiviert, die aktiviert sind. So ist es zum Beispiel nicht möglich, Struktur-A und -B zu aktivieren und FlexAddress auf Steckplatz 1 nur für Struktur-A, nicht aber für Struktur-B, zu aktivieren.

ANMERKUNG: Sie können den Status von FlexAddress auch über die Befehlszeilenschnittstelle einsehen. Weitere Befehlsinformationen finden Sie unter „FlexAddress verwenden“ auf Seite 281.

ANMERKUNG: Stellen Sie sicher, dass Sie die Blade-Server ausschalten, bevor Sie die Flex-Adresse für die Fabric-Ebene (A, B, C oder DRAC) ändern.

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 zu aktivieren, und dann werden die Steckplätze ausgewählt, die davon betroffen sein sollen. Sowohl Strukturen, als auch Steckplätze müssen für einen erfolgreiche FlexAddress-Konfiguration aktiviert sein.

Führen Sie folgende Schritte durch, um Strukturen und Steckplätze für die Nutzung von FlexAddress zu aktivieren oder zu deaktivieren:

1. Melden Sie sich bei der Webschnittstelle an (siehe „Auf die CMC-Webschnittstelle zugreifen“ auf Seite 121).
2. Klicken Sie in der Systemstruktur auf **Serverübersicht**.
3. Klicken Sie auf das Unterregister Setup→ **FlexAddress**. Die Seite **FlexAddress-Zusammenfassung** wird angezeigt.
4. Der Abschnitt **Struktur auswählen für gehäuseyugewiesene WWN/MACs** zeigt ein Kontrollkästchen für **Struktur A**, **Struktur B**, **Struktur C** und **iDRAC**.
5. Klicken Sie auf das Kontrollkästchen für jede Struktur, für die Sie FlexAddress aktivieren möchten. Um eine Struktur zu deaktivieren, klicken Sie auf das Kontrollkästchen, um die Auswahl zu löschen.

   ANMERKUNG: Sind keine Strukturen ausgewählt, wird FlexAddress für die ausgewählten Steckplätze nicht aktiviert.

   Die Seite **Steckplatz auswählen für gehäusezugewiesene WWN/MACs** zeigt das Kontrollkästchen **Aktiviert** für jeden Steckplatz im Gehäuse (1-16) an.
6. Klicken Sie auf das Kontrollkästchen **Aktiviert** für jeden Steckplatz, für den Sie FlexAddress aktivieren möchten. Wenn Sie alle Steckplätze auswählen möchten, verwenden Sie das Kontrollkästchen **Alle auswählen/abwählen**. Um einen Steckplatz zu deaktivieren, klicken Sie auf das Kontrollkästchen **Aktiviert**, um die Auswahl zu löschen.

ANMERKUNG: Ist ein Server im Steckplatz vorhanden, muss dieser zunächst ausgeschaltet werden, bevor die Funktion FlexAddress für diesen Steckplatz aktiviert werden kann.

ANMERKUNG: Sind keine Steckplätze ausgewählt, wird FlexAddress für die ausgewählten Strukturen nicht aktiviert.

7 Klicken Sie auf **Anwenden**, um die Änderungen zu speichern. Klicken Sie für weitere Informationen auf **Hilfe**.

Serverseitige FlexAddress-Steckplatzkonfiguration

Auf Serverebene können Sie FlexAddress für einzelne Steckplätze aktivieren oder deaktivieren

Aktivieren oder Deaktivieren eines einzelnen Steckplatzes für die Verwendung mit der FlexAddress-Funktion:

1 Melden Sie sich bei der Webschnittstelle an (siehe „Auf die CMC-Webschnittstelle zugreifen“ auf Seite 121).

2 Erweitern Sie in der Systemstruktur **Server-Übersicht**. Es werden alle Server (1 - 16) in der erweiterten Liste der **Server** angezeigt.

3 Klicken Sie auf den Server, den Sie anzeigen möchten. Die Seite **Serverstatus** wird angezeigt.

4 Klicken Sie auf das Register **Setup** und dann das Unterregister **FlexAddress**. Die Seite **FlexAddress-Status** wird angezeigt.

5 Verwenden Sie das Pulldown-Menü für **FlexAddress aktiviert**, um Ihre Auswahl zu treffen; wählen Sie **Ja**, um FlexAddress zu aktivieren oder wählen Sie **Nein**, um FlexAddress zu deaktivieren.

6 Klicken Sie auf **Anwenden**, um die Änderungen zu speichern. Klicken Sie für weitere Informationen auf **Hilfe**.

Remote-Dateifreigabe

Die Option 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.

1 Melden Sie sich bei der Webschnittstelle an (siehe „Auf die CMC-Webschnittstelle zugreifen“ auf Seite 121).

2 Klicken Sie in der Systemstruktur auf **Server-Übersicht**.

3 Klicken Sie im Register **Setup** auf das Unterregister **Remote-Dateifreigabe**. Die Seite **Remote-Dateifreigabe bereitstellen** wird angezeigt.

4 Legen Sie die Einstellungen für die Remote-Dateifreigabe fest.

Tabelle 5-64. Remote-Dateifreigabe-Einstellungen

Einstellung	Beschreibung

Image-Dateipfad	Image-Dateipfad ist nur erforderlich für Verbindungs- und Bereitstellungsvorgänge. Die Einstellung wirkt sich nicht auf Trennvorgänge aus. Der Pfadname des Netzwerklaufwerks wird über ein Windows-SMB- oder Linux/Unix-NFS-Protokoll auf dem Server eingebunden.
	Zum Verbinden mit CIFS geben Sie zum Beispiel Folgendes ein:
	`//<IP to connect for CIFS file system>/<file path>/<image name>`
	`//<IP to connect for NFS file system>:/<file path>/<image name>`
	Dateinamen, die mit **.img** enden, sind als virtuelle Disketten verbunden. Dateinamen, die mit **.iso** enden, sind als virtuelle CDs/DVDs verbunden. Die maximale Zeichenzahl beträgt 511.

Benutzername	Benutzername ist nur erforderlich für Verbindungs- und Bereitstellungsvorgänge. Die Einstellung wirkt sich nicht auf Trennvorgänge aus. Sie können in diesem Feld maximal 40 Zeichen angeben.
Kennwort	Kennwort ist nur erforderlich für Verbindungs- und Bereitstellungsvorgänge. Die Einstellung wirkt sich nicht auf Trennvorgänge aus. Sie können in diesem Feld maximal 40 Zeichen angeben.
Steckplatz	Identifiziert den Standort des Steckplatzes. Steckplatznummern sind sequenzielle IDs von 1 bis 16 (für die 16 im Gehäuse verfügbaren Steckplätze).
Name	Zeigt den Namen des Steckplatzes an. Steckplätze werden nach ihrer Position im Gehäuse benannt.
Modell	Zeigt den Modellnamen des Servers an.

Tabelle 5-64. Remote-Dateifreigabe-Einstellungen *(fortgesetzt)*

Einstellung	Beschreibung
Stromzustand	Zeigt den Stromzustand des Servers: **k.A.** - Der CMC hat den Stromzustand des Servers noch nicht bestimmt. **Aus** – Entweder der Server oder das Gehäuse sind ausgeschaltet. **Ein** – Sowohl das Gehäuse als auch der Server sind eingeschaltet. **Einschalten –** Vorübergehender Zustand zwischen Aus und Ein. Ein erfolgreich, der Stromzustand ist Ein. **Ausschalten** – Vorübergehender Zustand zwischen Ein und Aus. Ein erfolgreich, der Stromzustand ist Aus.
Verbindungsstatus	Zeigt den Verbindungsstatus der Remote-Dateifreigabe an.
Alle auswählen/ Aus wahl rückgängig	Wählen Sie diese Option aus, bevor Sie einen Remote-Dateifreigabe-Vorgang initiieren. Remote-Dateifreigabe-Vorgänge sind: Verbinden, Trennen und Bereitstellen.

5 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: Speichern Sie alle Arbeitsdateien, bevor Sie den Befehl `Bereitstellen` ausführen, da diese Maßnahme den Server neu startet.

Dieser Befehl schließt Folgendes ein:

- Die Remote-Dateifreigabe wird verbunden.
- Die Datei wird als das erste Startgerät für die Server ausgewählt.
- Der Server ist wird neu gestartet.
- Strom wird an den Server angelegt, falls der Server ausgeschaltet ist.

Häufig gestellte Fragen

Tabelle 5-65 zeigt die häufig gestellten Fragen zur Verwaltung oder Wiederherstellung eines Remote-Systems an.

Tabelle 5-65. Remote-System verwalten und wiederherstellen

Frage	Antwort
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** Kicken Sie in der **Systemstruktur** auf **Gehäuse-Übersicht**. **2** Klicken Sie auf das Register **Netzwerk** und dann auf **Netzwerk**. Die Seite **Netzwerkkonfiguration** wird angezeigt. **3** Aktivieren Sie das Kontrollkästchen **CMC auf DNS registrieren**. **4** Geben Sie den CMC-Namen in das Feld **DNS-CMC-Name** ein. **5** Klicken Sie auf **Änderungen übernehmen**. Weitere Informationen über die Erstellung von Zertifikatsignierungsanforderungen und die Ausgabe von Zertifikaten finden Sie unter „Sichere CMC-Datenübertragung mit SSL und digitalen Zertifikaten“ auf Seite 212.

Tabelle 5-65. Remote-System verwalten und wiederherstellen *(fortgesetzt)*

Frage	Antwort
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-Web Servers wieder verfügbar sind. Der CMC-Web Server führt nach den folgenden Ereignissen einen Reset durch: • Wenn die Netzwerkkonfiguration oder Netzwerksicherheitseigenschaften über die CMC-Webschnittstelle geändert werden. • Wenn die Eigenschaft **cfgRacTuneHttpsPort** geändert wird (einschließlich der Änderung durch eine config -f-<*config file*>). • Bei Verwendung von **racresetcfg** oder Wiederherstellen einer Gehäusekonfigurationssicherung. • Wenn der CMC zurückgesetzt wird. • Wenn ein neues SSL-Serverzertifikat hochgeladen wird.
Warum registriert mein DNS-Server meinen CMC nicht?	Einige DNS-Server registrieren nur Namen mit maximal 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. Weitere Informationen zur Ausgabe von Zertifikaten finden Sie unter „Sichere CMC-Datenübertragung mit SSL und digitalen Zertifikaten“ auf Seite 212.

Tabelle 5-65. Remote-System verwalten und wiederherstellen *(fortgesetzt)*

Frage	Antwort

Die folgende Meldung wird aus unbekannten Gründen angezeigt:
`Remote-Zugriff: SNMP-Authentifizierungsfehler`
Warum geschieht dies?
	Als Teil der Ermittlung versucht IT Assistant, die Get- und Set-Community-Namen des Geräts zu überprüfen. In IT Assistant gibt es den Get-**Community-Name = public** und den 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.
	Sie können den CMC-Community-Namen mit RACADM ändern.
	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, müssen Sie Community-Namen eingeben, die vom Agenten akzeptiert werden. Da der CMC nur einen Community-Namen zulässt, müssen Sie den gleichen **Get-** und **Set-**Community-Namen für das IT Assistant-Ermittlungs-Setup eingeben.

CMC Fehlerbehebung

Die CMC-Webschnittstelle enthält Hilfsprogramme zum Erkennen, Diagnostizieren und Beheben von Problemen mit dem Gehäuse. Weitere Informationen zur Problembehandlung finden Sie unter „Fehlerbehebung und Wiederherstellung“ auf Seite 469.

6

FlexAddress verwenden

Die FlexAddress-Funktion ist eine optionale Erweiterung, die es Servermodulen ermöglicht, die werkseitig zugewiesenen WWN- und MAC-Netzwerkken-nungen (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 vor der Einführung von FlexAddress ein Servermodul durch ein anderes ersetzt werden musste, änderten sich die WWN/MAC-IDs und die Ethernet-Netzwerkverwal-tungshilfsprogramme und die SAN-Ressourcen (Storage Area Network) mussten neu konfiguriert werden, 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.

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; die Formel lautet
<*mac_start*> + <*mac_count*> - 1 = <*mac_end*>

Zum 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.

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 die 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 aufgelistet sind, umfassen Servermodul-BIOS, E/A-Mezzanine-BIOS oder -Firmware sowie CMC-Firmware. Diese Updates müssen angewendet werden, bevor FlexAddress aktiviert wird. Wenn diese Aktualisierungen nicht angewendet werden, funktioniert FlexAddress nicht wie vorgesehen.

Komponente	Erforderliche Mindestversion
Ethernet-Mezzanine-Karte - Broadcom M5708t, 5709, 5710	Bootcode-Firmware 4.4.1 oder höher iSCSI-Bootfirmware 2.7.11 oder höher PXE-Firmware 4.4.3 oder höher
FC Mezzanine-Karte - QLogic QME2472, FC8	BIOS 2.04 oder höher

Komponente	Erforderliche Mindestversion
FC Mezzanine-Karte - Emulex LPe1105-M4, FC8	BIOS 3.03a3 und Firmware 2.72A2 oder höher
Servermodul-BIOS	PowerEdge M600 – BIOS 2.02 oder höher PowerEdge M605 – BIOS 2.03 oder höher PowerEdge M805 PowerEdge M905 PowerEdge M610 PowerEdge M710 PowerEdge M710hd
PowerEdgeM600/M605 LAN auf der Hauptplatine (LOM)	Bootcode-Firmware 4.4.1 oder höher iSCSI-Bootfirmware 2.7.11 oder höher
iDRAC	Version 1.50 oder höher für PowerEdge *xx*0*x* Systeme Version 2.10 oder höher für PowerEdge *xx*1*x* Systeme
CMC	Version 1.10 oder höher

ANMERKUNG: Alle Systeme, die nach Juni 2008 bestellt wurden, haben die korrekten Firmwareversionen.

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

1. Aktualisieren Sie die gesamte Mezzanine-Kartenfirmware und das BIOS.
2. Aktualisieren Sie das Servermodul-BIOS.
3. Aktualisieren Sie die iDRAC-Firmware auf dem Servermodul.
4. Aktualisieren Sie die gesamte CMC-Firmware im Gehäuse; falls redundante CMCs vorhanden sind, stellen Sie sicher, dass beide aktualisiert sind.
5. 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.

Beachten Sie auch das Dokument *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification* für Anleitungen zur SD-Karteninstallation.

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* für Informationen zur Aktivierung eines redundanten CMC.

Wenn der CMC neu startet, bestätigen Sie den Aktivierungsprozess, indem Sie die Schritte im nächsten Abschnitt, „Bestätigung FlexAddress-Aktivierung“ auf Seite 284, durchführen.

Bestätigung FlexAddress-Aktivierung

Für eine Prüfung der korrekten Aktivierung von FlexAddress können RACADM-Befehle verwendet werden, um die SD-Funktionskarte und die FlexAddress-Aktivierung zu bestätigen.

Verwenden Sie den folgenden RACADM-Befehl, um die SD-Funktionskarte und ihren Status zu bestätigen:

```
racadm featurecard -s
```

Tabelle 6-1. 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 FlexAddress-Funktionen: Die Funktionskarte ist an dieses Gehäuse gebunden.	Keine Maßnahme erforderlich.
Die eingesetzte SD-Karte ist gültig und enthält die folgenden FlexAddress-Funktionen: Die Funktionskarte ist 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 eingesetzte Funktionskarte ist gültig und enthält die folgenden Funktionen; FlexAddress: Die Funktionskarte ist an kein Gehäuse 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 des Gehäuses anzuzeigen.

```
racadm feature -s
```

Der Befehl gibt die folgende Statusmeldung aus:

```
Feature = FlexAddress

Date Activated = 8. April 2008 - 10:39:40

Feature installed from SD-card SN = 01122334455
```

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

```
racadm feature -s

No features active on the chassis.
```

Dell-Funktionskarten können mehr als eine Funktion enthalten. Sobald eine auf einer Dell-Funktionskarte enthaltene Funktion auf einem Gehäuse aktiviert ist, können keine anderen Funktionen, die möglicherweise auf der Dell-Funktionskarte enthalten sind, auf einem anderen Gehäuse aktiviert werden. In diesem Fall zeigt der Befehl „racadm feature -s“ die folgende Meldung für die betroffenen Funktionen an:

```
ERROR: One or more features on the SD card are active
on another chassis.
```

Lesen Sie für weitere Informationen zu den RACADM-Befehlen, die Abschnitte zu den Befehlen **feature** und **featurecard** des *RACADM - Befehlszeilen-Referenzhandbuchs für iDRAC6 und CMC*.

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.

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

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

Deaktivierung von FlexAddress

Verwenden Sie den folgenden RACADM-Befehl zur Deaktivierung der FlexAddress-Funktion und zur Wiederherstellung der SD-Karte:

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

Der Befehl gibt die folgende Statusmeldung bei erfolgreicher Ausführung zurück:

```
feature FlexAddress is deactivated on the chassis
successfully.
```

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

```
ERROR: Unable to deactivate the feature because the
chassis is powered ON
```

Lesen Sie für weitere Informationen zu diesem Befehl den Abschnitte zum **feature-Befehl** des *RACADM-Befehlszeilen-Referenzhandbuchs für iDRAC6 und CMC*.

FlexAddress mittels CLI konfigurieren

ANMERKUNG: Sie müssen beides aktivieren, Steckplatz und Struktur, sodass die dem Gehäuse zugewiesene MAC-Adresse auf den iDRAC übertragen wird.

ANMERKUNG: Sie können den Status von FlexAddress auch über die grafische Benutzeroberfläche einsehen. Weitere Informationen finden Sie unter„FlexAddress“ auf Seite 266.

Sie können die Befehlszeilenschnittstelle nutzen, um FlexAddress auf Strukturbasis zu aktivieren oder zu deaktivieren. Zusätzlich können Sie die Funktion steckplatzbasiert aktivieren/deaktivieren. Nachdem Sie die Funktion auf Strukturbasis aktiviert haben, können Sie die zu aktivierenden Steckplätze auswählen. Ist zum Beispiel nur Struktur-A aktiviert, haben alle aktivierten Steckplätze FlexAddress nur für die Struktur-A aktiviert. In allen anderen Strukturen werden die werkseitigen WWN/MAC-IDs des Servers verwendet. Diese Funktion funktioniert nur, wenn die Struktur aktiviert und der Server ausgeschaltet ist.

Aktivierte Steckplätze sind für alle aktivierten Strukturen FlexAddress-fähig. So ist es zum Beispiel nicht möglich, Struktur-A und -B zu aktivieren und FlexAddress auf Steckplatz 1 nur für Struktur-A, nicht aber für Struktur-B, zu aktivieren.

Verwenden Sie den folgenden RACADM-Befehl zum Aktivieren/Deaktivieren von Strukturen:

```
racadm setflexaddr [-f <fabricName> <state>]

<fabricName> = A, B, C oder iDRAC

<state> = 0 oder 1
```

Wobei **0** deaktiviert und **1** aktiviert bedeuten.

Verwenden Sie den folgenden RACADM-Befehl zum Aktivieren/Deaktivieren von Steckplätzen:

```
racadm setflexaddr [-i <slot#> <state>]

<slot#> = 1 bis 16

<state> = 0 oder 1
```

Wobei **0** deaktiviert und **1** aktiviert bedeuten.

Lesen Sie für weitere Informationen zu diesem Befehl den Abschnitte zum **setflexaddr-Befehl** des *RACADM-Befehlszeilen-Referenzhandbuchs für iDRAC6 und CMC*.

Zusätzliche Konfiguration von FlexAddress für Linux

Wenn Sie von einer serverzugewiesenen MAC-ID zu einer gehäusezugewiesenen MAC-ID auf Linux-basierten Betriebssystemen wechseln, sind zusätzliche Konfigurationsschritte erforderlich:

- SUSE Linux Enterprise Server 9 und 10: Sie müssen u. U. YAST (Yet another Setup Tool) auf dem Linux-System ausführen, um die Netzwerkgeräte zu konfigurieren, und dann die Netzwerkdienste neu starten.
- Red Hat Enterprise Linux 4 (RHEL) und RHEL 5: Sie müssen Kudzu ausführen (Dienstprogramm zur Erkennung und Konfiguration neuer/geänderter Hardware im System). Kudzu präsentiert das Hardware Discovery-Menü (Hardwareerkennung), das die MAC-Adressänderung erkennt, wenn Hardware entfernt und durch neue Hardware ersetzt wird.

Anzeigen des FlexAddress-Status mittels CLI

Sie können die Befehlszeilenschnittstelle nutzen, um Statusinformationen von FlexAddress anzuzeigen. Sie können Statusinformationen für das gesamte Gehäuse oder für einen bestimmten Steckplatz anzeigen. Die angezeigten Informationen beinhalten:

- Strukturkonfiguration
- FlexAddress aktiviert/deaktiviert
- Steckplatznummer und -name
- Gehäusezugewiesene und serverzugewiesene Adressen
- Verwendete Adressen

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

```
racadm getflexaddr
```

Um den FlexAddress-Status für einen bestimmten Steckplatz anzuzeigen:

```
racadm getflexaddr [-i <slot#>]

<slot#> = 1 bis 16
```

Unter „FlexAddress mittels CLI konfigurieren“ auf Seite 287 finden Sie weitere Details zur FlexAddress-Konfiguration. Lesen Sie für weitere Informationen zu diesem Befehl den Abschnitte zum **getflexaddr-Befehl** des *RACADM-Befehlszeilen-Referenzhandbuchs für iDRAC6 und CMC*.

FlexAddress mittels GUI konfigurieren

Wake-On-LAN mit FlexAddress verwenden

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.

Fehlerbehebung FlexAddress

Dieser Abschnitt enthält Informationen zur Fehlerbehebung für FlexAddress.

1. Was geschieht bei Entfernen einer Funktionskarte?

   Es geschieht nichts. Funktionskarten können entfernt und aufbewahrt oder im System belassen werden.

2. Was passiert, wenn eine Funktionskarte, die in einem Gehäuse verwendet wurde, entfernt und in ein anderes Gehäuse gesteckt wird?

   Die Webschnittstelle zeigt den folgenden Fehler 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
   ```

   Der folgende Eintrag wird dem CMC-Protokoll hinzugefügt:

   ```
   cmc <date timestamp> : feature
   'FlexAddress@XXXXXXX' not activated; chassis ID=
   'YYYYYYY'
   ```

3. Was passiert, wenn die Funktionskarte entfernt und eine Karte, die FlexAddress nicht unterstützt, eingesetzt wird?

   Es findet keine Aktivierung oder Änderung der Karte statt. Die Karte wird vom CMC ignoriert. In dieser Situation gibt der Befehl **$racadm featurecard -s** folgende Meldung zurück:

   ```
   No feature card inserted
   ```

   ```
   ERROR: can't open file
   ```

4 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 den folgenden Fehler 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.

5 Erhalte ich eine Fehlermeldung, wenn ich in meinem redundanten CMC-System zwei Funktionskarten installiert habe?

Die Funktionskarte im aktiven CMC wird aktiv und im Gehäuse installiert sein. Die zweite Karte wird vom CMC ignoriert.

6 Hat die SD-Karte einen Schreibschutz?

Ja. Bevor Sie die SD-Karte in das CMC-Modul installieren, bestätigen Sie, dass sich die Schreibschutzsperre in der „Entsperr"-Position befindet. Die FlexAddress-Funktion kann nicht aktiviert werden, wenn die SD-Karte schreibgeschützt ist. In dieser Situation gibt der Befehl **$racadm feature -s** folgende Meldung zurück:

```
No features active on the chassis. ERROR: read
only file system
```

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

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

```
Keine Funktionskarte eingesetzt.
```

8 Was passiert mit der FlexAddress-Funktion, wenn das Server-BIOS von Version 1.*xx* auf Version 2.*xx* aktualisiert wird?

Das Servermodul muss heruntergefahren 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.

9 Was geschieht, wenn ein Gehäuse mit einem einzigen CMC auf Firmware vor der Version 1.10 heruntergestuft wird?

- Die FlexAddress-Funktion und die Konfiguration werden aus dem Gehäuse entfernt.
- Die Funktionskarte, die zum Aktivieren der Funktion auf diesem Gehäuse verwendet wurde, bleibt unverändert und an das Gehäuse gebunden. Wenn die CMC-Firmware des Gehäuses nachfolgend auf 1.10 oder höher erweitert wird, wird die FlexAddress-Funktion durch Wiedereinführen der Original-Funktionskarte (falls erforderlich), Zurücksetzen des CMC (falls Funktionskarte nach Abschluss der Firmwareerweiterung eingeführt wurde) und Neukonfigurieren der Funktion reaktiviert.

10 Was geschieht, wenn in einem Gehäuse mit redundanten CMCs eine CMC-Einheit mit einer Einheit ersetzt wird, die eine Firmware vor Version 1.10 hat?

Wenn Sie in einem Gehäuse mit redundanten CMCs einen CMC durch einen CMC mit einer Firmware vor Version 1.10 ersetzen, muss das folgende Verfahren verwendet werden, um sicherzustellen, dass die derzeitige FlexAddress-Funktion und die Konfiguration NICHT entfernt werden.

a Versichern Sie sich, dass der aktive CMC stets die Firmwareversion 1.10 oder höher aufweist.

b Entfernen Sie den Standby-CMC und setzen Sie den neuen CMC ein.

c Erweitern Sie die Firmware des neuen Standby-CMC über den aktiven CMC auf Version 1.10 oder höher.

ANMERKUNG: Wenn Sie die Standby-CMC-Firmware nicht auf Version 1.10 oder höher aktualisieren und es findet ein Failover statt, wird die Funktion FlexAddress nicht konfiguriert und Sie müssen die Funktion reaktivieren und neu konfigurieren.

11 Die SD-Karte war nicht im Gehäuse, als der Deaktivierungsbefehl auf der FlexAddress ausgeführt wurde. Wie stelle ich die SD-Karte jetzt wieder her?

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 erneut.

12 Ich habe eine SD-Karte sowie sämtliche Firmware/Software-Aktualisierungen korrekt installiert. Ich sehe, dass FlexAddress aktiv ist, kann aber auf dem Serverbereitstellungsbildschirm nichts zum Bereitstellen erkennen? Was ist falsch?

Das ist ein Problem des Browser-Cache; schließen Sie den Browser und starten Sie ihn neu.

13 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 herunterfahren, bevor Sie den RACADM-Befehl `racresetcfg` verwenden.

Befehlsmeldungen

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

Tabelle 6-2. FlexAddress-Befehle und -Ausgaben

Situation	Befehl	Ausgabe

SD-Karte im aktiven CMC-Modul ist an eine andere Service-Tag-Nummer gebunden.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)FlexAddress: The feature card is bound to another chassis, svctag = <Service tag`
		`Number> SD card SN =<Valid flex address serial number>`
		`(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>)`

Tabelle 6-2. FlexAddress-Befehle und -Ausgaben *(fortgesetzt)*

Situation	Befehl	Ausgabe

SD-Karte im aktiven CMC-Modul ist an die gleiche Service-Tag-Nummer gebunden.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s) FlexAddress: The feature card is bound to this chassis`
		`(Die eingesetzte Funktionskarte ist ungültig und enthält die folgenden Funktionen`
		`FlexAddress: Die Funktionskarte ist an dieses Gehäuse gebunden)`

Tabelle 6-2. FlexAddress-Befehle und -Ausgaben *(fortgesetzt)*

Situation	Befehl	Ausgabe

Die SD-Karte im aktiven CMC-Modul ist an keine Service-Tag-Nummer gebunden.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s) FlexAddress: The feature card is not bound to any chassis`
		`(Die eingesetzte Funktionskarte ist ungültig und enthält die folgenden Funktionen`
		`FlexAddress: Die Funktionskarte ist an kein Gehäuse 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.	`$racadm setflexaddr [-f <fabricName> <slot-State>] OR` `$racadm setflexaddr [-i <slot#> <slotState>]`	`ERROR: Flexaddress feature is not active on the chassis` `(FEHLER: Die Funktion FlexAddress ist nicht auf dem Gehäuse aktiviert)`

Tabelle 6-2. FlexAddress-Befehle und -Ausgaben *(fortgesetzt)*

Situation	Befehl	Ausgabe
Gastbenutzer versucht FlexAddress für Steckplätze/Strukturen festzulegen	`$racadm setflexaddr [-f <fabricName> <slotState>]` `$racadm setflexaddr [-i <slot#> <slotState>]`	`ERROR: Insufficient user privileges to perform operation` `(FEHLER: Unzureichende Benutzerrechte, zur Ausführung der Operation)`
Die Funktion FlexAddress bei eingeschaltetem Gehäuse deaktivieren.	`$racadm feature -d -c flexaddress`	`ERROR: Unable to deactivate the feature because the chassis is powered ON` `(FEHLER: Die Funktion kann nicht deaktiviert werden, da das Gehäuse eingeschaltet ist.)`
Gastbenutzer versucht die Funktion auf dem Gehäuse zu deaktivieren.	`$racadm feature -d -c flexaddress`	`ERROR: Insufficient user privileges to perform operation` `(FEHLER: Unzureichende Benutzerrechte, zur Ausführung der Operation)`

Tabelle 6-2. FlexAddress-Befehle und -Ausgaben *(fortgesetzt)*

Situation	Befehl	Ausgabe
Ändern der FlexAddress-Einstellungen für einen Steckplatz/eine Struktur, während die Servermodule eingeschaltet sind.	`$racadm setflexaddr -i 1 1`	`ERROR: Unable to perform the set operation because it affects a powered ON server` `(FEHLER: Die Einstell-Operation kann nicht vorgenommen werden, da sie einen eingeschalteten Server betrifft.)`
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.

FlexAddress DELL SOFTWARE-LIZENZVEREINBARUNG

Dies ist eine rechtsgültige Vereinbarung 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 Vereinbarungen geschützt. Sie sind berechtigt, eine einzige 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 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 Disketten auf einem anderen Computer zu verwenden oder sie durch Verleih, Vermietung, Leasing oder Übertragung anderen Benutzern zugänglich zu machen, es sei denn, diese Vereinbarung gewährt Ihnen dieses Recht.

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.

USA STAATLICH BESCHRÄNKTE RECHTE

Die Software und Dokumentation sind „Handelswaren" gemäß Definition in 48 C.F.R. (Code of Federal Regulations) 2.101, bestehend aus „kommerzieller Computersoftware" und „kommerzielle Computersoftwaredokumentation", wie verwendet in 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, jegliche U.S. Regierungs-Endnutzer beziehen 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.

Häufig gestellte Fragen

Tabelle 6-3 listet die häufigsten Fragen zur FlexaddressPlus-Funktion auf.

Tabelle 6-3. FlexaddressPlus

Frage	Antwort
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.

7

Verwenden von 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.

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 Kennzeichnung FlexAddress enthält nur FlexAddress, und die Karte mit der Kennzeichnung FlexAddress Plus enthält FlexAddress und FlexAddress Plus. Die Karte muss in den CMC eingesetzt werden, um das Funktionsmerkmal zu aktivieren.

Einige Server wie z.B. der PowerEdge M710HD benötigen möglicherweise, je nach Konfiguration, mehr MAC-Adressen als FA für den CMC bereitstellen kann. Für diese Server ermöglicht die Erweiterung auf FA+ die vollständige Optimierung der WWN/MACs-Konfiguration. Wenden Sie sich bitte an Dell, um Unterstützung für die FlexAddress Plus-Funktion zu erhalten.

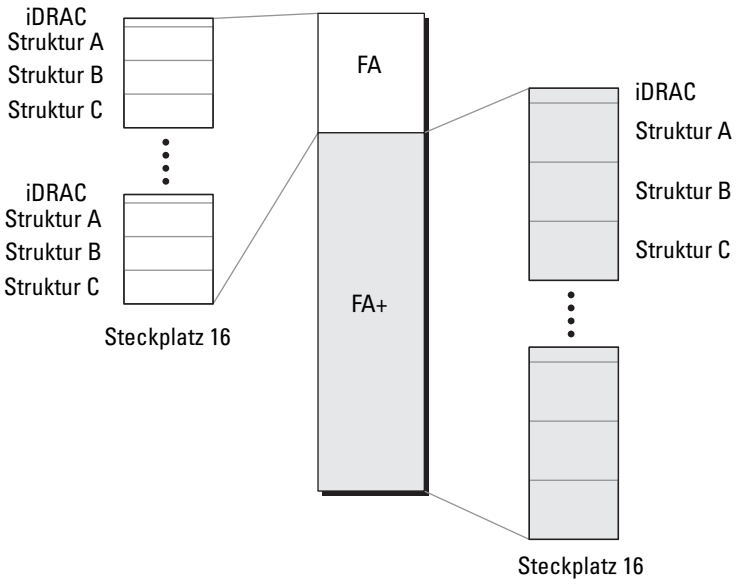
Zur Aktivierung der FlexAddress Plus-Funktion sind die folgenden Softwareaktualisierungen erforderlich: Server-BIOS, Server-iDRAC und CMC-Firmware. Wenn diese Aktualisierungen nicht angewendet werden, steht nur die FlexAddress-Funktion zur Verfügung. Weitere Informationen zu den erforderlichen Mindestversionen dieser Komponenten finden Sie in den Versionshinweisen zu CMC 4.0 unter **support/dell.com/manuals**.

FlexAddress im Vergleich mit FlexAddress Plus

FlexAddress verfügt über 208 Adressen, die auf 16 Servertsteckplätze aufgeteilt sind, so dass jedem Steckplatz 13 MACs zugewiesen sind. FlexAddress verfügt über 2928 Adressen, die auf 16 Servertsteckplätze aufgeteilt sind, so dass jedem Steckplatz 183 MACs zugewiesen sind. Die Tabelle unten zeigt die Bereitstellung der MAC-Adressen in beiden Funktionen.

	Struktur A	Struktur B	Struktur C	iDRAC-Management	Summe der MACs
Flex-Address	4	4	4	1	13
Flex-Address Plus	60	60	60	3	183

Abbildung 7-1. Funktionsvergleich FlexAddress (FA) gegenüber FlexPlusAddress (FA+)



8

CMC-Verzeichnisdienst verwenden

Ein Verzeichnisdienst führt eine allgemeine Datenbank aller Informationen, die für die Steuerung von Netzwerkbenutzern, Computern, Druckern usw. erforderlich sind. Wenn Ihr Unternehmen die Microsoft Active Directory-Software oder die LDAP Verzeichnisdienst-Software verwendet, können Sie den CMC so konfigurieren, dass dieser verzeichnisbasierte Benutzerauthentifizierung verwendet.

CMC mit Microsoft Active Directory verwenden

ANMERKUNG: Die Verwendung von Active Directory zur Erkennung von CMC-Benutzern wird auf den Microsoft Windows 2000- und Windows-Server 2003-Betriebssystemen unterstützt. Active Directory über IPv6 und IPv4 wird nur auf Windows 2008 unterstützt.

Active Directory-Schemaerweiterungen

Sie können mit Active Directory den Benutzerzugriff auf den CMC mittels zweier Methoden definieren:

- Das Standardlösungsschema, das nur die Standardgruppenobjekte von Active Directory verwendet.
- Das erweiterte Lösungsschema, das Active Directory-Objekte verwendet, die von Dell definiert wurden.

Standardschema gegenüber erweitertem Schema

Wenn Sie den Zugang zum CMC mit Active Directory konfigurieren, müssen Sie entweder die Lösung „Erweitertes Schema“ oder „Standardschema“ wählen.

Bei der Standardschemalösung:

- Es ist keine Schemaerweiterung erforderlich, da das Standardschema nur Active Directory-Standardobjekte verwendet.
- Die Konfiguration von Active Directory ist einfach.

Bei der erweiterten Schemalösung:

- Alle Zugriffssteuerungsobjekte werden im Active Directory verwahrt.
- Konfiguration des Benutzerzugriffs auf verschiedenen CMCs mit verschiedenen Berechtigungsebenen ermöglicht maximale Flexibilität.

Übersicht des Standardschema-Active Directory

Bei Verwendung des Standardschemas für die Active Directory-Integration ist die Konfiguration sowohl auf dem Active Directory als auch auf dem CMC erforderlich.

Auf der Seite des 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 eine spezifische CMC-Karte zu gewähren, müssen der Rollengruppenname und sein Domänenname auf der spezifischen CMC-Karte konfiguriert werden. Im Unterschied zur Lösung des erweiterten Schemas, sind die Rollen- und Berechtigungsebenen auf jeder CMC-Karte und nicht im Active Directory definiert. Es können bis zu fünf Rollengruppen in jedem CMC konfiguriert und definiert werden. Abbildung 8-1 veranschaulicht die Konfiguration des CMC mit Active Directory und Standardschema Tabelle 5-43 zeigt die Berechtigungsebene der Rollengruppen an und Tabelle 8-1 zeigt die standardmäßigen Einstellungen der Rollengruppen an.

Abbildung 8-1. Konfiguration des CMC mit Active Directory und Standardschema

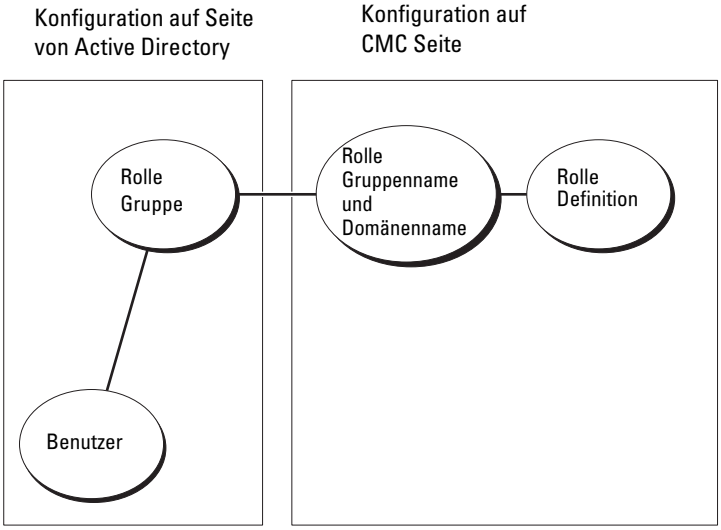


Tabelle 8-1. Standardeinstellungsberechtigungen der Rollengruppe

Rollen-gruppe	Standard-berechtigung Stufe	Gewährte Berechtigungen	Bitmaske
1	-	• Benutzer: CMC-Anmeldung • Gehäusekonfigurations-Administrator • Benutzerkonfigurations-Administrator • Administrator zum Löschen von Protokollen • Gehäusesteuerungs-Administrator • Superbenutzer • Server Administrator • Warnungstests für Benutzer • Debug-Befehl-Administrator • Struktur A-Administrator • Struktur B-Administrator • Struktur C-Administrator	0x00000fff
2	-	• Benutzer: CMC-Anmeldung • Administrator zum Löschen von Protokollen • Gehäusesteuerungs-Administrator • Server Administrator • Warnungstests für Benutzer • Struktur A-Administrator • Struktur B-Administrator • Struktur C-Administrator	0x00000ed9
3	-	Benutzer: CMC-Anmeldung	0x00000001
4	-	Keine zugewiesenen Berechtigungen	0x00000000
5	-	Keine zugewiesenen Berechtigungen	0x00000000

ANMERKUNG: Die Bitmaskenwerte werden nur verwendet, wenn das Standardschema mit dem RACADM eingerichtet wird.

ANMERKUNG: Weitere Informationen über CMC-Benutzerberechtigungen finden Sie unter „Benutzertypen“ auf Seite 188.

Das Standardschema-Active Directory kann auf zwei Arten aktiviert werden:

- Mit der CMC-Webschnittstelle. Siehe „Konfigurieren des CMC mit dem Standardschema von Active Directory und der Webschnittstelle“ auf Seite 314.
- Mit dem RACADM-CLI-Hilfsprogramm. Siehe „CMC mit dem Standardschema von Active Directory und RACADM konfigurieren“ auf Seite 316.

Standardschema von Active Directory konfigurieren um den CMC zuzugreifen

Sie müssen die folgenden Schritte ausführen, um Active Directory zu konfigurieren, bevor ein Active Directory-Benutzer auf den CMC zugreifen kann:

1. Öffnen Sie auf einem Active Directory-Server (Domänen-Controller) das Active Directory-Benutzer- und -Computer-Snap-In.
2. Erstellen Sie eine Gruppe oder wählen Sie eine bestehende Gruppe aus. Der Name der Gruppe und der Name dieser Domäne müssen auf dem CMC entweder mit der Webschnittstelle oder mit RACADM konfiguriert werden.

   Weitere Informationen finden Sie unter „Konfigurieren des CMC mit dem Standardschema von Active Directory und der Webschnittstelle“ auf Seite 314 und „CMC mit dem Standardschema von Active Directory und RACADM konfigurieren“ auf Seite 316.
3. Fügen Sie den Active Directory-Benutzer als ein Mitglied der Active Directory-Gruppe hinzu, um auf den CMC zuzugreifen.

Konfigurieren des CMC mit dem Standardschema von Active Directory und der Webschnittstelle

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur **Gehäuse** aus.
3. Klicken Sie auf **Benutzer-Authentifizierung→ Verzeichnisdienste**. Die Seite **Verzeichnisdienste** wird angezeigt.
4. Wählen Sie die Optionsschaltfläche neben Microsoft Active Directory (Standardschema) aus. Die Seite **Active Directory-Konfiguration und Verwaltung** wird aufgerufen.
5. Im Abschnitt **Allgemeine Einstellungen**:
   a. Wählen Sie das Kontrollkästchen **Active Directory aktivieren** aus.
   b. Geben Sie den **Root-Domänennamen** ein.

   ANMERKUNG: Der **Root-Domänenname** muss ein gültiger Domänenname sein, für den die Namenskonvention *x.y* verwendet wird, wobei *x* eine ASCII-Zeichenkette aus 1-256 Zeichen ohne Leerstellen zwischen den Zeichen und *y* ein gültiger Domänentyp wie com, edu, gov, int, mil, net oder org ist.

   c. Geben Sie die **Zeitüberschreitung** in Sekunden ein. Der Zeitüberschreitungsbereich ist **15–300** Sekunden. Die Standard-Zeitüberschreitung ist **90** Sekunden
6. Wenn der gezielte Aufruf den Domänen-Controller und den globalen Katalog durchsuchen soll, wählen Sie das Kontrollkästchen **AD-Server für Suche durchsuchen (optional)** aus und gehen Sie wie folgt vor:
   a. Geben Sie im Textfeld **Domänen-Controller** den Server ein, auf dem der Active Directory-Dienst installiert ist.
   b. Geben Sie im Textfeld **Globaler Katalog** den Standort des globalen Katalogs auf dem Active Directory-Domänen-Controller ein. Der globale Katalog ist eine Ressource zum Durchsuchen einer Active Directory-Gesamtstruktur.
7. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

   ANMERKUNG: Sie müssen Ihre Einstellungen anwenden, bevor Sie mit dem nächsten Schritt fortfahren. Wenn Sie die Einstellungen nicht anwenden, verlieren Sie die eingegebenen Einstellungen, wenn Sie zur nächsten Seite wechseln.

8. Klicken Sie im Abschnitt **Standardschemaeinstellungen** auf eine **Rollengruppe**. Die Seite **Rollengruppe konfigurieren** wird aufgerufen.
9. Geben Sie den **Gruppennamen** ein. Der Gruppenname identifiziert die Rollengruppe im Active Directory, das mit der CMC-Karte verbunden ist.
10. Geben Sie die **Gruppendomäne** ein. Die **Gruppendomäne** ist der vollständig qualifizierte root-Domänenname der Gesamtstruktur.
11. Wählen Sie auf der Seite **Rollengruppenberechtigungen** die Berechtigungen für die Gruppe aus.

    Wenn Sie Berechtigungen modifizieren, wird die vorhandene **Rollengruppenberechtigung** (Administrator, Hauptbenutzer oder Gastbenutzer) entweder zur benutzerdefinierten Gruppe oder zur entsprechenden Rollengruppenberechtigung wechseln. Siehe Tabelle 5-43.
12. Klicken Sie auf **Anwenden**, um die Einstellungen der Rollengruppe zu speichern.
13. Klicken Sie auf **Zurück zur Seite Konfiguration**.
14. Laden Sie das von der Zertifizierungsstelle signierte Root-Zertifikat Ihrer Domänengesamtstruktur auf den CMC. Geben Sie auf der Seite **Zertifikatverwaltung** den Dateipfad des Zertifikats ein oder suchen Sie nach der Zertifikatsdatei. Klicken Sie auf die Schaltfläche **Hochladen**, um die Datei zum CMC zu übertragen.

    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.
15. Klicken Sie auf **Anwenden**. Der CMC-Webserver startet automatisch neu, nachdem Sie auf **Anwenden** klicken.
16. Melden Sie sich ab und dann beim CMC an, um die CMC Active Directory-Funktionskonfiguration abzuschließen.
17. Wählen Sie in der Systemstruktur **Gehäuse** aus.
18. Klicken Sie auf das Register **Netzwerk**.

19 Klicken Sie auf das Unterregister **Netzwerk**. Die Seite **Netzwerkkonfiguration** wird eingeblendet.

20 Wenn **DHCP verwenden (für Netzwerkschnittstellen-IP-Adresse)** unter **Netzwerkeinstellungen** 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.

21 Klicken Sie auf **Änderungen übernehmen**.

Die Funktionskonfiguration CMC-Standardschema von Active Directory ist abgeschlossen.

CMC mit dem Standardschema von Active Directory und RACADM konfigurieren

Verwenden Sie die folgenden Befehle, um den CMC mit dem Standardschema von Active Directory unter Verwendung von RACADM-CLI zu konfigurieren.

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

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1

racadm config -g cfgActiveDirectory -o cfgADType 2

racadm config -g cfgActiveDirectory -o
cfgADRootDomain <fully qualified root domain name>

racadm config -g cfgStandardSchema -i <Index> -o
cfgSSADRoleGroupName <common name of the role
group>

racadm config -g cfgStandardSchema -i <Index> -o
cfgSSADRoleGroupDomain <fully qualified domain
name>

racadm config -g cfgStandardSchema -i <Index> -o
cfgSSADRoleGroupPrivilege <Bit mask number for
specific user permissions>
```

```
racadm sslcertupload -t 0x2 -f <ADS root CA
certificate>

racadm sslcertdownload -t 0x1 -f <RAC SSL
certificate>
```

ANMERKUNG: Lesen Sie für Bitmaskennummerwerte in Tabelle 3-1 des Kapitels Datenbankeigenschaften im *RACADM Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC.*

2 Legen Sie einen DNS-Server anhand einer der folgenden Optionen fest:

- Wenn DHCP auf dem CMC aktiviert ist und Sie die vom DHCP-Server automatisch abgefragte DNS-Adresse verwenden wollen, geben Sie den folgenden Befehl ein:

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

- Wenn DHCP auf dem CMC deaktiviert ist oder Sie Ihre DNS-IP-Adresse manuell eingeben wollen, geben Sie die folgenden Befehle ein:

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

  racadm config -g cfgLanNetworking -o
  cfgDNSServer1 <primary DNS IP address>

  racadm config -g cfgLanNetworking -o
  cfgDNSServer2 <secondary DNS IP address>
  ```

Erweitertes Schema - Übersicht

Das Active Directory mit erweitertem Schema kann auf zwei Arten aktiviert werden:

- Mit der CMC-Webschnittstelle. Anleitungen hierzu finden Sie unter „Konfiguration des CMC mit der Schema-Erweiterung des Active Directory und der Webschnittstelle“ auf Seite 335.
- Mit dem RACADM-CLI-Hilfsprogramm. Anleitungen hierzu finden Sie unter „CMC mit dem erweiterten Schema von Active Directory und RACADM konfigurieren“ auf Seite 338.

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. Benutzerklassenattribute können den Vornamen, den Nachnamen, die Telefonnummer usw. des Benutzers umfassen.

Sie können die Active Directory-Datenbank erweitern, indem Sie Ihre eigenen einzigartigen Attribute und Klassen hinzufügen, um umgebungsspezifische Bedürfnisse Ihres Unternehmens zu lösen. 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 in der gesamten Branche eindeutige IDs zu unterhalten, führt Microsoft eine Datenbank mit Active Directory Object Identifiers (OIDs). Um das Schema in Microsofts Active Directory zu erweitern, hat Dell eindeutige OIDs, eindeutige Namenserweiterungen und eindeutig verknüpfte Attribut-IDs für Dell-spezifische Attribute und Klassen eingeführt:

Dell-Erweiterung: dell

Grund-OID von Dell: 1.2.840.113556.1.8000.1280

RAC-LinkID-Bereich: 12070–2079

Übersicht der RAC-Schema-Erweiterungen

Dell stellt eine Gruppe von Eigenschaften bereit, die Sie konfigurieren können. Das von Dell erweiterte Schema enthält Zuordnungs-, Geräte- und Berechtigungseigenschaften.

Die Zuordnungseigenschaft verknüpft Benutzer oder Gruppen mit einem spezifischen Satz von Berechtigungen mit einem oder mehreren RAC-Geräten. Dieses Modell verleiht dem Administrator höchste Flexibilität über die verschiedenen Kombinationen von Benutzern, RAC-Berechtigungen und RAC-Geräten im Netzwerk, ohne zu viel Komplexität hinzuzufügen.

Active Directory - Objektübersicht

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.

Jedoch kann jedes Zuordnungsobjekt nur mit einem Berechtigungsobjekt verknüpft werden bzw. darf jedes Benutzer-, Benutzergruppen- oder RAC-Geräteobjekt-Zuordnungsobjekt nur mit einem Berechtigungsobjekt verknüpft werden. Dieses Beispiel ermöglicht dem Administrator, die Berechtigungen jedes Benutzers auf spezifischen CMCs zu steuern.

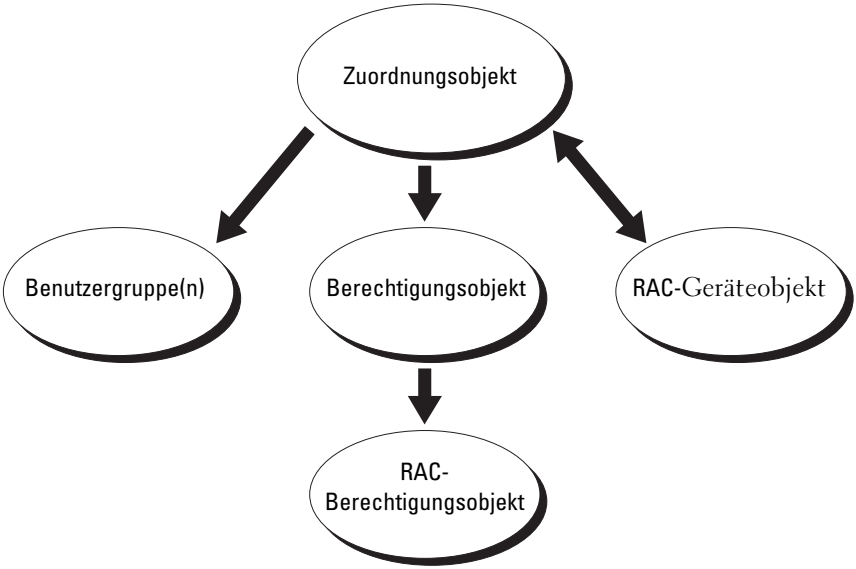
Das RAC-Geräteobjekt ist die Verknüpfung zur RAC-Firmware für die Active Directory-Abfrage zur Authentifizierung und Autorisierung. Wird ein RAC zu einem Netzwerk hinzugefügt, muss der Administrator den RAC und sein Geräteobjekt mit seinem Active Directory-Namen konfigurieren, damit Benutzer mit dem Active Directory Authentifizierungen und Autorisierungen durchführen können. Der Administrator muss außerdem auch mindestens einen RAC zum Zuordnungsobjekt hinzufügen, damit Benutzer Authentifizierungen vornehmen können.

Abbildung 8-2 zeigt, dass das Zuordnungsobjekt die Verbindung bereitstellt, die für die gesamte Authentifizierung und Autorisierung erforderlich ist.

ANMERKUNG: Das RAC-Berechtigungsobjekt gilt für DRAC 4, DRAC 5 und den CMC.

Sie können eine beliebige Anzahl an Zuordnungsobjekten erstellen. Sie müssen jedoch mindestens ein Zuordnungsobjekt erstellen und für jedes RAC (CMC) im Netzwerk, das Sie in Active Directory integrieren möchten, ein RAC-Geräteobjekt haben.

Abbildung 8-2. Typisches Setup für Active Directory-Objekte

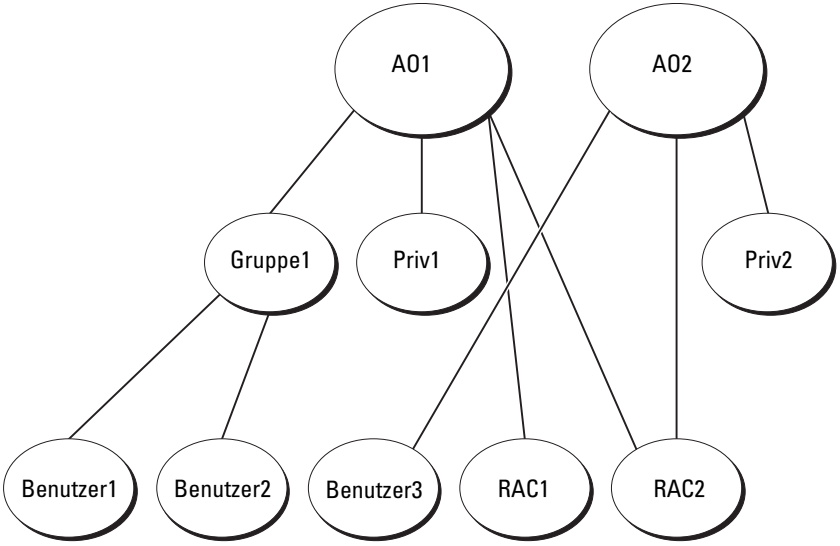


Das Zuordnungsobjekt lässt ebenso viele oder wenige Benutzer und/oder Gruppen sowie RAC-Geräteobjekte zu. Das Zuordnungsobjekt enthält jedoch nur ein Berechtigungsobjekt pro Zuordnungsobjekt. Das Zuordnungsobjekt verbindet die „Benutzer", die „Berechtigungen" auf den RACs (CMCs) haben.

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. Abbildung 8-3 zeigt, wie Sie die Active Directory-Objekte in diesem Szenario einrichten können.

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.

Abbildung 8-3. Active Directory-Objekte in einer einzelnen Domäne einrichten



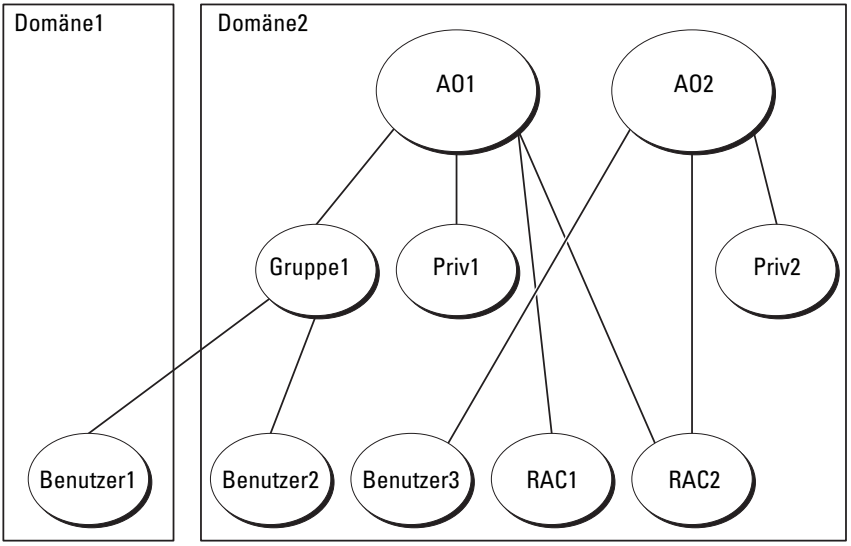
So konfigurieren Sie die Objekte für das Einzeldomänen-Szenario:

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.

Eine detaillierte Anleitung finden Sie unter „CMC-Benutzer und -Berechtigungen zum Active Directory hinzufügen“ auf Seite 332.

Abbildung 8-4 enthält ein Beispiel von Active Directory-Objekten in mehreren Domänen. Dieses Szenario weist zwei CMCs (RAC1 und RAC2) und drei vorhandene Active Directory-Benutzer (Benutzer1, Benutzer2 und Benutzer3) auf. Benutzer1 ist in Domäne1 und Benutzer2 und Benutzer3 sind in Domäne2. In diesem Szenario konfigurieren Sie Benutzer1 und Benutzer2 mit Adminis-tratorrechten für beide CMCs und Benutzer3 mit Anmeldungsberechtigungen für die RAC2-Karte.

Abbildung 8-4. Active Directory-Objekte in mehreren Domänen einrichten



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.

   Abbildung 8-4 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. Gruppieren Sie Benutzer1 und Benutzer2 in Gruppe1. Die Gruppenreichweite von Gruppe1 muss „Universal" 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.

Erweitertes Schema von Active Directory konfigurieren um auf den CMC zuzugreifen

Bevor Sie mit Active Directory auf den CMC zugreifen, konfigurieren Sie die Active Directory-Software und den CMC:

1. Erweitern Sie das Active Directory-Schema (siehe „Erweitern des Active Directory-Schemas" auf Seite 324).
2. Erweitern Sie das Active Directory-Benutzer- und -Computer-Snap-In (siehe „Dell-Erweiterung zum Active Directory-Benutzer und -Computer-Snap-In installieren" auf Seite 331).
3. Fügen Sie dem Active Directory CMC-Benutzer und deren Berechtigungen hinzu (siehe „CMC-Benutzer und -Berechtigungen zum Active Directory hinzufügen" auf Seite 332).
4. Aktivieren Sie SSL auf allen Domänen-Controllern.
5. Konfigurieren Sie die Active Directory-Eigenschaften des CMC über die CMC-Webschnittstelle oder das RACADM (siehe „Konfiguration des CMC mit der Schema-Erweiterung des Active Directory und der Webschnittstelle" auf Seite 335 bzw. „CMC mit dem erweiterten Schema von Active Directory und RACADM konfigurieren" auf Seite 338).

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, vergewissern Sie sich, dass Sie Schema-Admin-Berechtigung auf dem Schema-Master Flexible Single Master Operation (FSMO)-Rollenbesitzer der Domänengesamtstruktur haben.

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 Verzeichnissen:

- <DVD-Laufwerk>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\<*installation type*>\LDIF Files
- <DVD-Laufwerk>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_ Tools\<*installation type*>\Schema Extender

Lesen Sie zur Verwendung der LDIF-Dateien die Anleitungen in der Infodatei im Verzeichnis **LDIF_Files**. Eine Anleitung zur Verwendung von Dell Schema Extender, um das Active Directory-Schema zu erweitern, finden Sie unter „Dell Schema Extender verwenden“ auf Seite 325.

Sie können Schema Extender oder die LDIF-Dateien an einem beliebigen Standort kopieren und ausführen.

Dell Schema Extender verwenden

VORSICHTSHINWEIS: Das Dell Schema Extender-Dienstprogramm 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 auf dem **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-Administratorberechtigungen 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 und prüfen Sie die Existenz der folgenden Elemente:

   - Klassen (siehe Tabelle 8-2 bis Tabelle 8-7)
   - Eigenschaften – siehe Tabelle 8-8

   Weitere Informationen über das Aktivieren und die Verwendung von Active Directory-Schema-Snap-In in MMC finden Sie in der Microsoft-Dokumentation.

Tabelle 8-2. Klassendefinitionen für Klassen, die zum Active Directory-Schema hinzugefügt wurden

Klassenname	Zugewiesene Objekt-Identifikationsnummer (OID)
dellRacDevice	1.2.840.113556.1.8000.1280.1.1.1.1
dellAssociationObject	1.2.840.113556.1.8000.1280.1.1.1.2
dellRACPrivileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Tabelle 8-3. dellRacDevice Class

OID	1.2.840.113556.1.8000.1280.1.1.1.1
Beschreibung	Repräsentiert das Dell RAC-Gerät. Das RAC-Gerät muss als dellRacDevice im Active Directory konfiguriert werden. 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 8-4. dellAssociationObject Class

OID	1.2.840.113556.1.8000.1280.1.1.1.2
Beschreibung	Repräsentiert das Dell-Zuordnungsobjekt. Das Zuordungsobjekt ist die Verbindung zwischen Benutzern und Geräten.
Klassentyp	Strukturklasse
SuperClasses	Gruppe
Attribute	**dellProductMembers** **dellPrivilegeMember**

Tabelle 8-5. dellRAC4Privileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Beschreibung	Definiert Autorisierungsrechte (Berechtigungen) für das CMC-Gerät.
Klassentyp	Erweiterungsklasse
SuperClasses	NONE
Attribute	**dellIsLoginUser** **dellIsCardConfigAdmin** **dellIsUserConfigAdmin** **dellIsLogClearAdmin** **dellIsServerResetUser** **dellIsTestAlertUser** **dellIsDebugCommandAdmin** **dellPermissionMask1** **dellPermissionMask2**

Tabelle 8-6. dellPrivileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Beschreibung	Container-Klasse für die Dell-Berechtigungen (Autorisierungsrechte).
Klassentyp	Strukturklasse
SuperClasses	Benutzer
Attribute	**dellRAC4Privileges**

Tabelle 8-7. 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 8-8. 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:** Liste mit **dellRacDevices**-Objekten, die zu dieser Rolle gehören. Dieses Attribut ist die Vorwärtsverbindung zur **dellAssociationMembers**-Rückwärtsverbindung. **Link-ID:** 12070 **OID:** 1.2.840.113556.1.8000.1280.1.1.2.2 **Eindeutiger Name:** (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
Attribut: dellIsCardConfigAdmin **Beschreibung:** TRUE, wenn der Benutzer Kartenkonfigurationsrechte auf dem Gerät hat. **OID:** 1.2.840.113556.1.8000.1280.1.1.2.4 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut: dellIsLoginUser **Beschreibung:** TRUE, wenn der Benutzer Anmeldungsrechte auf dem Gerät hat. **OID:** 1.2.840.113556.1.8000.1280.1.1.2.3 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut: 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

Tabelle 8-8. Liste von Attributen, die dem Active Directory-Schema hinzugefügt wurden *(fortgesetzt)*

Zugewiesener OID/Syntax-Objektkennzeichner	Einzelbewertung
Attribut: dellIsUserConfigAdmin	
Beschreibung: TRUE, wenn der Benutzer Benutzerkonfigurationsrechte auf dem Gerät hat.	
OID: 1.2.840.113556.1.8000.1280.1.1.2.5	TRUE
Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
Attribut: delIsLogClearAdmin	
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	TRUE
Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
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	TRUE
Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
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	TRUE
Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
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	TRUE
Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	

Tabelle 8-8. Liste von Attributen, die dem Active Directory-Schema hinzugefügt wurden *(fortgesetzt)*

Zugewiesener OID/Syntax-Objektkennzeichner	Einzelbewertung
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	TRUE
Case Ignore String(LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	
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	TRUE
Case Ignore String(LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	
Attribut: dellAssociationMembers	
Beschreibung: Die Liste von dellAssociationObjectMembers, die zu diesem Produkt gehören. Dieses Attribut ist die Rückwärtsverknüpfung zum Attribut dellProductMembers.	
Link-ID: 12071	
OID: 1.2.840.113556.1.8000.1280.1.1.2.14	FALSE
Eindeutiger Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
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 zum 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 Systemverwaltungssoftware auf der DVD *Dell Systems Management Tools and Documentation* installieren, können Sie das Snap-In erweitern, indem Sie während des Installationsverfahrens die Option **Dell-Erweiterung von Active Directory-Benutzer- und -Computern-Snap-In** auswählen. Lesen Sie das *Dell OpenManage Server Administrator-Installationshandbuch* und *Dell OpenManage Management Station Software-Installationshandbuch* für zusätzliche Informationen über die Installation von Systemverwaltungssoftware.

Weitere Informationen zum Active Directory-Benutzer und -Computer-Snap-In finden Sie in der Microsoft-Dokumentation.

Administratorpaket installieren

Sie müssen das Administratorpaket auf jedem System installieren, das die Active Directory-CMC-Objekte verwaltet. Wenn Sie das Administratorpaket nicht installieren, können Sie das Dell-RAC-Objekt nicht im Container anzeigen.

Öffnen des Active Directory-Benutzer- und -Computer-Snap-In

So öffnen Sie die Active Directory-Benutzer und Computer-Snap-In:

1. Wenn Sie auf dem Domänen-Controller angemeldet sind, klicken Sie auf **Start Verwaltungstools→ Active Directory-Benutzer und -Computer**.

   Wenn Sie nicht auf dem Domänen-Controller angemeldet sind, muss das entsprechende Microsoft-Administratorpaket auf dem lokalen System installiert sein. Um dieses Administratorpaket zu installieren, klicken Sie auf **Start→ Ausführen**, geben Sie `MMC` ein und drücken Sie die Taste <Eingabe>. Die Microsoft-Verwaltungskonsole (MMC) wird eingeblendet.

2. Klicken Sie im Fenster **Konsole 1** auf **Datei** (oder auf **Konsole** bei Systemen, auf denen Windows 2000 ausgeführt wird).

3 Klicken Sie auf **Add/Remove Snap-in** (Snap-In hinzufügen/entfernen).

4 Wählen Sie **Active Directory-Benutzer- und Computer** -Snap-In aus und klicken Sie auf **Hinzufügen**.

5 Klicken Sie auf **Schließen**.

CMC-Benutzer und -Berechtigungen zum Active Directory hinzufügen

Mit dem Dell-erweiterten Active Directory-Benutzer- und Computer-Snap-In können Sie CMC-Benutzer und -Berechtigungen hinzuzufügen, indem Sie RAC-, Zuordnungs- und Berechtigungsobjekte erstellen. Hinzufügen der verschiedenen Objekttypen:

1 RAC-Geräteobjekt erstellen

2 Berechtigungsobjekt erstellen

3 Zuordnungsobjekt erstellen

4 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 RAC-Objekt** aus.

Das Fenster **Neues Objekt** wird geöffnet.

3 Geben Sie einen Namen für das neue Objekt ein. Der Name muss mit dem CMC-Namen übereinstimmen, den Sie in Schritt avon „Konfiguration des CMC mit der Schema-Erweiterung des Active Directory und der Webschnittstelle“ auf Seite 335eingeben.

4 Wählen Sie **RAC-Geräteobjekt** und klicken Sie auf **OK**.

Erstellen von Berechtigungsobjekten

ANMERKUNG: Ein Berechtigungsobjekt muss in derselben Domäne wie das zugehörige Zuordnungsobjekt erstellt werden.

So erstellen Sie ein Berechtigungsobjekt:

1. Klicken Sie im Fenster **Console Root** (MMC) mit der rechten Maustaste auf einen Container.
2. Wählen Sie **Neu→ Dell RAC-Objekt** aus.

   Das Fenster **Neues Objekt** wird geöffnet.
3. Geben Sie 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 **Eigenschaften** aus.
6. Klicken Sie auf das Register **RAC-Berechtigungen** und wählen Sie die Berechtigungen aus, die der Benutzer haben soll. Weitere Informationen über CMC-Benutzerberechtigungen finden Sie unter „Benutzertypen“ auf Seite 188.

Erstellen von Zuordnungsobjekten

Das Zuordnungsobjekt wird von einer Gruppe abgeleitet und muss einen Gruppentyp enthalten. Die Zuordnungsreichweite legt den Sicherheitsgruppen-typ für das Zuordnungsobjekt fest. Wenn Sie ein Zuordnungsobjekt erstellen, müssen Sie die Zuordnungsreichweite wählen, die sich auf den Typ der Objekte bezieht, die hinzugefügt werden sollen.

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 RAC-Objekt** aus.

   Hierdurch wird das Fenster **Neues Objekt** geöffnet.
3. Geben Sie einen Namen für das neue Objekt ein.
4. Wählen Sie **Zuordnungsobjekt**.
5. Wählen Sie den Bereich für das **Zuordnungsobjekt** und **klicken** Sie auf **OK**.

Hinzufügen von Objekten zu einem Zuordnungsobjekt

Durch die Verwendung des Fensters **Zuordnungsobjekt-Eigenschaften** können Sie Benutzer oder Benutzergruppen, Berechtigungsobjekte und RAC-Geräte oder RAC-Gerätegruppen zuordnen. Wenn das System 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. Die Verfahren zum Erstellen von Dell-bezogenen Gruppen und nicht-Dell-bezogenen Gruppen sind identisch.

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**.

Klicken Sie auf das Register **Berechtigungsobjekt**, um das Berechtigungsobjekt der Zuordnung hinzuzufügen, die die Berechtigungen des Benutzers bzw. der Benutzergruppe bei der Authentifizierung eines RAC-Geräts definiert. Einem Zuordnungsobjekt kann nur ein Berechtigungsobjekt hinzugefügt werden.

Berechtigungen hinzufügen

So fügen Sie Berechtigungen hinzu:

1. Wählen Sie das Register **Berechtigungsobjekt** und klicken Sie auf **Hinzufügen**.
2. Geben Sie den Berechtigungsobjektnamen ein und klicken Sie 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.

RAC-Geräte oder RAC-Gerätegruppen hinzufügen

Um RAC-Geräte oder RAC-Gerätegruppen hinzufügen:

1. Wählen Sie das Register **Produkte** und klicken Sie auf **Hinzufügen**.
2. Geben Sie den Namen des RAC-Geräts oder der RAC-Gerätegruppe ein und klicken Sie auf **OK**.
3. Im Fenster **Eigenschaften** klicken Sie auf **Anwenden** und dann auf **OK**.

Konfiguration des CMC mit der Schema-Erweiterung des Active Directory und der Webschnittstelle

Konfiguration des CMC mit der Schema-Erweiterung des Active Directory und der Webschnittstelle:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf **Gehäuse**.
3. Klicken Sie auf **Benutzer-Authentifizierung→ Verzeichnisdienste**.

   Die Seite **Verzeichnisdienste** wird angezeigt.
4. Wählen Sie **Microsoft Erweitertes Schema** aus.
5. Im Abschnitt **Allgemeine Einstellungen**:
   a. Vergewissern Sie sich, dass das Kontrollkästchen **Active Directory aktivieren** ausgewählt ist.
   b. Geben Sie den **Root-Domänennamen** ein.

   ANMERKUNG: Der **Root-Domänenname** muss ein gültiger Domänenname sein, für den die Namenskonvention *x.y* verwendet wird, wobei *x* eine ASCII-Zeichenkette aus 1 - 256 Zeichen ohne Leerstellen zwischen den Zeichen und *y* ein gültiger Domänentyp wie com, edu, gov, int, mil, net oder org ist.

   c. Geben Sie die **Zeitüberschreitung** in Sekunden ein. **Konfigurationsbereich:** 15 - 300 Sekunden. **Standardeinstellung:** 90 Sekunden

6 **Optional:** Wenn der gezielte Aufruf den Domänen-Controller und den globalen Katalog durchsuchen soll, wählen Sie das Kontrollkästchen **AD-Server für Suche durchsuchen (optional)** aus und gehen Sie wie folgt vor:

   a Geben Sie im Textfeld **Domänen-Controller** den Server ein, auf dem der Active Directory-Dienst installiert ist.

   b Geben Sie im Textfeld **Globaler Katalog** den Standort des globalen Katalogs auf dem Active Directory-Domänen-Controller ein. Der globale Katalog ist eine Ressource zum Durchsuchen einer Active Directory-Gesamtstruktur.

   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 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.

7 Im Abschnitt **Erweiterte Schemaeinstellungen**:

   a Geben Sie den **CMC-Gerätenamen** ein. Der **CMC-Name** identifiziert die CMC-Karte im Active Directory eindeutig. Der **CMC-Name** muss dem allgemeinen Namen des neuen CMC-Objekts entsprechen, das Sie in Ihrem Domänen-Controller erstellt haben. Der **CMC-Name** muss eine ASCII-Zeichenkette mit 1 bis 256 Zeichen und ohne Leerstellen sein.

   b Geben Sie den **CMC-Domänennamen** ein (z. B. `cmc.com`). Der **CMC-Domänenname** ist der DNS-Name (Zeichenkette) der Domäne, bei der sich das Active Directory-CMC-Objekt befindet. Der Name muss ein gültiger Domänenname sein und aus *x.y* bestehen, wobei *x* eine ASCII-Zeichenkette mit 1 bis 256 Zeichen ohne Leerstellen und *y* ein gültiger Domänentyp wie com, edu, gov, int, mil, net, org ist.

8 Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

ANMERKUNG: Sie müssen Ihre Einstellungen anwenden, bevor Sie mit dem nächsten Schritt fortfahren und zu einer anderen Seite wechseln. Wenn Sie die Einstellungen nicht anwenden, verlieren Sie die eingegebenen Einstellungen, wenn Sie zur nächsten Seite wechseln.

9 Geben Sie im Abschnitt **Zertifikate verwalten** den Dateipfad des Zertifikats in das Textfeld ein oder klicken Sie auf **Durchsuchen**, um die Zertifikatdatei auszuwählen. Klicken Sie auf die Schaltfläche **Hochladen**, um die Datei zum CMC zu übertragen.

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-Zertifikatüberprüfung ist standardmäßig erforderlich. Es gibt eine neue Einstellung in der **cfgActiveDirectory** RACADM-Gruppe und innerhalb der GUI, um die Zertifikatsprüfung zu deaktivieren.

VORSICHTSHINWEIS: Das Deaktivieren dieses Zertifikats ist mit Risiken verbunden.

So schalten Sie die SSL-Zertifikatüberprüfung ein (Standard):

```
racadm config -g cfgActiveDirectory -o
cfgADCertValidationEnable 1
```

So schalten Sie die SSL-Zertifikatüberprüfung aus:

```
racadm config -g cfgActiveDirectory -o
cfgADCertValidationEnable 0
```

Die SSL-Zertifikate für den Domänen-Controller müssen von der root-Zertifizierungsstelle signiert werden. Das von der Root-Zertifizierungsstelle signierte Zertifikat muss auf der Management Station verfügbar sein, die auf den CMC zugreift.

10 Klicken Sie auf **Anwenden**. Der CMC-Webserver startet automatisch neu, wenn Sie auf **Anwenden** klicken.

11 Melden Sie sich erneut bei der CMC-Webschnittstelle an.

12 Wählen Sie in der Systemstruktur **Gehäuse** aus, klicken Sie auf das Register **Netzwerk** und anschließend auf das Unterregister **Netzwerk**. Die Seite **Netzwerkkonfiguration** wird angezeigt.

13 Wenn **DHCP verwenden (für Netzwerkschnittstellen-IP-Adresse)** aktiviert ist, wählen Sie eine der folgenden Vorgehensweisen:

- 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.

14 Klicken Sie auf **Änderungen übernehmen**.

Die CMC-Funktionskonfiguration für das erweiterte Schema von Active Directory ist abgeschlossen.

CMC mit dem erweiterten Schema von Active Directory und RACADM konfigurieren

Verwenden Sie die folgenden Befehle, um die CMC-Active Directory-Funktion mit erweitertem Schema mit Hilfe des RACADM-CLI-Hilfsprogramms, anstatt der webbasierten Schnittstelle, zu konfigurieren.

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

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1

racadm config -g cfgActiveDirectory -o cfgADType 1

racadm config-g cfgActiveDirectory-o
cfgADRacDomain <fully qualified CMC domain name>

racadm config -g cfgActiveDirectory -o
cfgADRootDomain <fully qualified CMC domain name>

racadm config-g cfgActiveDirectory-o cfgADRacName
<CMC common name>

racadm sslcertupload -t 0x2 -f <ADS root CA
certificate> -r

racadm sslcertdownload-t 0x1-f <CMC SSL
certificate>
```

ANMERKUNG: Sie können diesen Befehl nur über Remote-RACADM verwenden. Weitere Informationen zum Remote-RACADM finden Sie unter „RACADM im Remote-Zugriff aufrufen“ auf Seite 88.

Optional: Wenn Sie ein LDAP oder einen Server des globalen Katalogs festlegen möchten, anstatt die Server zu verwenden, die vom DNS-Server für die Suche nach einem Benutzernamen zurückgegeben wurden, geben Sie den folgenden Befehl ein, um die Option **Server festlegen** zu aktivieren:

```
racadm config -g cfgActiveDirectory -o
cfgADSpecifyServerEnable 1
```

ANMERKUNG: Wenn Sie die Option **Server festlegen** verwenden, wird der Host-Name in dem von der Zertifizierungsstelle signierten Zertifikat nicht mit dem Namen des angegebenen Servers abgeglichen. Dies ist besonders nützlich, wenn Sie ein CMC-Administrator sind, weil es Ihnen hierdurch möglich ist, sowohl einen Host-Namen als auch eine IP-Adresse einzugeben.

Nachdem Sie die Option **Server festlegen** aktiviert haben, können Sie einen LDAP-Server und globalen Katalog mit IP-Adressen oder vollständig qualifizierten Domänennamen (FQDNs) der Server festlegen. Die FQDNs bestehen aus den Host-Namen und Domänennamen der Server.

Geben Sie zur Angabe eines LDAP-Servers Folgendes ein:

```
racadm config -g cfgActiveDirectory -o cfgADDomain-
Controller <AD domain controller IP address>
```

Um einen Server anzugeben, der den globalen Katalog enthält, geben Sie Folgendes ein:

```
racadm config -g cfgActiveDirectory -o
cfgADGlobalCatalog <AD global catalog IP address>
```

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 LDAP-Servern oder von Servern, die den globalen Katalog enthalten, angeben. Der CMC ermöglicht Ihnen, bis zu drei IP-Adressen oder Host-Namen festzulegen.

ANMERKUNG: LDAPs, die nicht korrekt für alle Domänen und Anwendungen konfiguriert sind, können zu unerwarteten Ergebnissen bei der Funktionsweise der vorhandenen Anwendungen/Domänen führen.

2 Legen Sie einen DNS-Server anhand einer der folgenden Optionen fest:

- Wenn DHCP auf dem CMC aktiviert ist und Sie die vom DHCP-Server automatisch abgefragte DNS-Adresse verwenden wollen, geben Sie den folgenden Befehl ein:

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

- Wenn DHCP auf dem CMC deaktiviert ist oder wenn DHCP aktiviert ist, Sie aber Ihre DNS-IP-Adresse manuell eingeben wollen, geben Sie die folgenden Befehle ein:

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

  ```
  racadm config -g cfgLanNetworking -o
  cfgDNSServer1 <primary DNS IP address>
  ```

  ```
  racadm config -g cfgLanNetworking -o
  cfgDNSServer2 <secondary DNS IP address>
  ```

Die Funktionskonfiguration des erweiterten Schemas ist abgeschlossen.

Häufig gestellte Fragen

Tabelle 8-9. CMC mit Active Directory verwenden: Häufig gestellte Fragen

Frage	Antwort
Kann ich mich beim CMC anmelden, indem ich Active Directory über mehrfache Strukturen verwende?	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).

Tabelle 8-9. CMC mit Active Directory verwenden: Häufig gestellte Fragen *(fortgesetzt)*

Frage	Antwort
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 müssen Sie diese zwei Objekte in derselben Domäne erstellen. Andere Objekte können sich in verschiedenen Domänen befinden.
Gibt es Beschränkungen bei der SSL-Konfiguration der Domänen-Controller?	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.

Tabelle 8-9. CMC mit Active Directory verwenden: Häufig gestellte Fragen *(fortgesetzt)*

Frage	Antwort

Ich habe ein neues RAC-Zertifikat erstellt und hochgeladen und jetzt startet die Webschnittstelle nicht.	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 dann ein neues Webzertifikat von Microsoft Certificate Services und laden Sie es mit Hilfe der folgenden RACADM-Befehle hoch:
	`racadm sslcsrgen [-g] [-f {filename}]`
	`racadm sslcertupload -t 1 -f {web_sslcert}`

Tabelle 8-9. CMC mit Active Directory verwenden: Häufig gestellte Fragen *(fortgesetzt)*

Frage	Antwort
Was kann ich tun, wenn ich mich mittels Active Directory-Authentifizierung nicht beim CMC anmelden kann? Wie kann ich das Problem beheben?	**1** Stellen Sie sicher, dass Sie während einer Anmeldung den korrekten Benutzerdomänennamen und nicht den NetBIOS-Namen verwenden. **2** Wenn Sie ein lokales CMC-Benutzerkonto haben, melden Sie sich mit Ihren lokalen Anmeldeinformationen beim CMC an. Nachdem Sie angemeldet sind, führen Sie die folgenden Schritte aus: **a** Stellen Sie sicher, dass Sie das Kästchen **Active Directory aktivieren** auf der CMC Active Directory-Konfigurationsseite markiert haben. **b** Stellen Sie sicher, dass die DNS-Einstellung auf der CMC-Netzwerkkonfigurationsseite richtig ist. **c** Stellen Sie sicher, dass Sie das Active Directory-Zertifikat von dem von Ihrer Active Directory-Root-Zertifizierungsstelle signierten Zertifikat zum CMC hochgeladen haben. **d** Überprüfen Sie die SSL-Zertifikate der Domänen-Controller, um sicherzustellen, dass sie nicht abgelaufen sind. **e** Stellen Sie sicher, dass **CMC-Name**, **Root-Domänenname** und **CMC-Domänenname** mit Ihrer Active Directory-Umgebungskonfiguration übereinstimmen. **f** Stellen Sie sicher, dass das CMC-Kennwort maximal 127 Zeichen aufweist. Während der CMC Kennwörter von bis zu 256 Zeichen unterstützt, unterstützt Active Directory nur Kennwörter, die maximal 127 Zeichen lang sind.

Einfache Anmeldung konfigurieren

Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista und Windows Server 2008 können Kerberos (ein Netzwerk-Authentifizier-ungsprotokoll) als Authentifizierungsmethode verwenden und Benutzern, die sich bei der Domäne angemeldet haben, automatische oder einfache Anmeldung für nachfolgende Anwendungen wie Exchange ermöglichen.

Beginnend mit CMC Version 2.10 kann der CMC Kerberos verwenden, um zwei zusätzliche Authentifizierungsmechanismen, einfache Anmeldung und Smart Card-Anmeldung, zu unterstützen. 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.

ANMERKUNG: Die Auswahl einer Anmeldemethode legt keine Richtlinien-attribute 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.

Systemanforderungen

Zu Verwendung der Kerberos-Authentifizierung muss Ihr Netzwerk Folgendes enthalten:

- DNS-Server
- Microsoft Active Directory-Server

  ANMERKUNG: Falls Sie Active Directory unter Windows 2003 verwenden, müssen Sie sicherstellen, dass die neuesten Service-Packs und Patches auf dem Clientsystem installiert sind. Falls Sie Active Directory unter 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 Dienstpro-gramm *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.

Clientsysteme

- 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 und Smart Card-Anmeldung muss das Clientsystem ein Teil der Active Directory-Domäne und des Kerberos-Bereichs sein.

CMC

- Der CMC muss Firmwareversion 2.10 oder neuer aufweisen.
- Jeder CMC muss ein Active Directory-Konto haben.
- Der CMC muss ein Teil der Active Directory-Domäne und des Kerberos-Bereichs sein.

Einstellungen konfigurieren

Vorbedingungen

- Der Kerberos-Bereich und das Kerberos-Schlüsselverteilungscenter (KDC) für Active Directory (AD) wurden eingerichtet (ksetup).
- Gewährleisten Sie eine robuste NTP- und DNS-Infrastruktur zur Vermeidung von Problemen mit Clock-Drift und Reverse-Lookup.
- Die CMC-Standardschema-Rollengruppe mit autorisierten Mitgliedern

Active Directory konfigurieren

Konfigurieren Sie im Dialogfeld **CMC-Eigenschaften** im Optionsabschnitt **Konten** die folgenden Einstellungen:

- **Dem Konto wird für Delegierungszwecke vertraut** – Der CMC verwendet derzeit keine weitergeleiteten Anmeldeinformationen, wenn diese Option ausgewählt ist. Sie können diese Option abhängig von anderen Dienstanforderungen auswählen oder nicht auswählen.
- **Konto ist vertraulich und kann nicht delegiert werden** – Sie können diese Option abhängig von anderen Dienstanforderungen auswählen oder nicht auswählen.
- **DES-Verschlüsselungstypen für dieses Konto verwenden** – Wählen Sie diese Option aus.
- **Keine Kerberos-Vorauthentifizierung erforderlich** – Wählen Sie diese Option nicht aus.

Führen Sie das Dienstprogramm ktpass (Teil von Microsoft Windows) auf dem Domänen-Controller (Active Directory-Server) aus, auf dem Sie den CMC einem Benutzerkonto in Active Directory zuordnen möchten. Beispiel:

```
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: `cmcname.domainname.com` muss gemäß RFC in Kleinbuchstaben und der REALM-Name `@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 unter: **technet2.microsoft.com/windowsserver/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.mspx?mfr=true**.

Den CMC konfigurieren

ANMERKUNG: Die in diesem Abschnitt beschriebenen Konfigurationsschritte gelten nur für den Webzugriff des CMC.

Konfigurieren Sie den CMC zur Verwendung von Standardschema-Rollengruppen, die in Active Directory eingerichtet sind. Weitere Informationen finden Sie unter„Standardschema von Active Directory konfigurieren um den CMC zuzugreifen“ auf Seite 313.

Kerberos-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.

So laden Sie die Keytab-Datei hoch:

1. Navigieren Sie zum Register **Benutzer-Authentifizierung**→ Unterregister **Verzeichnisdienste**. Stellen Sie sicher, dass **Microsoft Active Directory Standard** oder **Erweitertes Schema** ausgewählt ist. Falls nicht, wählen Sie Ihre Einstellungen aus und klicken auf **Anwenden**.
2. Klicken Sie auf **Durchsuchen** im Abschnitt **Kerberos-Keytab-Hochladen** und navigieren Sie zu dem Ordner, in dem die Keytab-Datei gespeichert ist, und klicken auf **Hochladen**.

   Wenn der Vorgang beendet ist, wird ein Meldungsfenster eingeblendet, das anzeigt, ob der Upload erfolgreich oder fehlerhaft war.

Einfache Anmeldung aktivieren

1. Klicken Sie auf das Register **Chassis Management Controller Netzwerksicherheit**→ **Active Directory**→ **Active Directory konfigurieren**.

   Die Seite **Active Directory-Konfiguration und Verwaltung** wird angezeigt.
2. Wählen Sie auf der Seite **Active Directory-Konfiguration und Verwaltung** Folgendes aus:
   - Einfache Anmeldung – diese Option ermöglicht die Anmeldung beim CMC unter Verwendung der zwischengespeicherten Anmeldeinformationen, die bei der Anmeldung beim Active Directory verwendet wurden.

ANMERKUNG: Alle bandexternen Befehlszeilenschnittstellen, einschließlich Secure Shell (SSH), Telnet, Seriell und Remote-RACADM, bleiben für diese Option unverändert.

3 Klicken Sie am unteren Rand auf **Anwenden**.

Sie können das Active Directory mit Kerberos-Authentifizierung testen, indem Sie die Testfunktion des CLI-Befehls verwenden.

```
testfeature -f adkrb -u <user>@<domain>
```

wobei Benutzer 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 wiederholen. Lesen Sie für weitere Informationen das *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC* auf **support.dell.com/manuals**.

Browser für einfache Anmeldung konfigurieren

Einfache Anmeldung wird von Internet Explorer Version 6.0 und neuer und Firefox Version 3.0 und neuer 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 **This might void your warranty** (Das kann Ihre Garantie ungültig machen) anzeigt, klicken Sie auf **I'll be careful. I promise** (Ich werde vorsichtig sein, ich verspreche es).

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**.

Anmelden beim CMC unter Verwendung einfacher Anmeldung

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

So melden Sie sich am CMC unter Verwendung einfacher Anmeldung an:

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

2 Greifen Sie auf die CMC-Webseite zu. Verwenden Sie:

https://<*cmcname.domain-name***>**

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.domaine-name>:<port number>* auf den CMC zu, wobei ***cmcname*** der CMC-Hostname für den CMC ist; ***domain-name*** ist der Domänenname und ***port number*** die HTTPS-Schnittstellennummer.

Die Seite **CMC – einfache Anmeldung** wird angezeigt.

3 Klicken Sie auf **Anmelden.**

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.

Smart Card-Zweifaktor-Authentifizierung konfigurieren

Für herkömmliche Authentifizierungsschemata werden der Benutzername und das Kennwort zum Authentifizieren von Benutzern verwendet. Bei der Zweifaktor-Authentifizierung wird andererseits eine höhere Sicherheitsstufe geboten, indem Benutzer aufgefordert werden, ein Kennwort oder eine PIN sowie eine physische Karte mit einem privaten Schlüssel oder einem digitalen Zertifikat bereitzustellen. Kerberos, ein Netzwerk-Authentifizierungsprotokoll, verwendet diesen Zweifaktor-Authentifizierungsmechanismus und ermöglicht es Systemen, ihre Authentizität zu beweisen. Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista und Windows Server 2008 verwenden Kerberos als bevorzugte Authentifizierungsmethode. Beginnend mit CMC Version 2.10 Version kann der CMC Kerberos verwenden, um Smart Card-Anmeldung zu unterstützen.

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.

Systemanforderungen

Die „Systemanforderungen“ auf Seite 344 für Smart Card entsprechen denen für einfache Anmeldung.

Einstellungen konfigurieren

Die „Vorbedingungen“ auf Seite 345 für Smart Card entsprechen denen für einfache Anmeldung.

Active Directory konfigurieren

So konfigurieren Sie Active Directory:

1. Richten Sie den Kerberos-Bereich und das Kerberos-Schlüsselverteilungscenter (KDC) für Active Directory ein, falls diese Komponenten noch nicht konfiguriert sind (ksetup).

   ANMERKUNG: Gewährleisten Sie eine robuste NTP- und DNS-Infrastruktur zur Vermeidung von Problemen mit Clock-Drift und Reverse-Lookup.

2. Erstellen Sie Active Directory-Benutzer für jeden CMC und konfigurieren Sie Kerberos-DES-Verschlüsselung, jedoch nicht Vorauthentifizierung.
3. Registrieren Sie die CMC-Benutzer mit Ktpass beim Schlüsselverteilungscenter (dies erzeugt auch einen Schlüssel zum Hochladen auf den CMC).

Den CMC konfigurieren

ANMERKUNG: Die in diesem Abschnitt beschriebenen Konfigurationsschritte gelten nur für den Webzugriff des CMC.

Konfigurieren Sie den CMC zur Verwendung von Standardschema-Rollengruppen, die in Active Directory eingerichtet sind. Weitere Informationen finden Sie unter „Standardschema von Active Directory konfigurieren um den CMC zuzugreifen“ auf Seite 313.

Kerberos-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.

So laden Sie die Keytab-Datei hoch:

1. Navigieren Sie zum Register **Benutzer-Authentifizierung**→ Unterregister **Verzeichnisdienste**. Stellen Sie sicher, dass **Microsoft Active Directory Standard** oder **Erweitertes Schema** ausgewählt ist. Falls nicht, wählen Sie Ihre Einstellungen aus und klicken auf **Anwenden**.
2. Klicken Sie auf **Durchsuchen** im Abschnitt **Kerberos-Keytab-Hochladen** und navigieren Sie zu dem Ordner, in dem die Keytab-Datei gespeichert ist, und klicken Sie auf **Hochladen**.

   Wenn der Vorgang beendet ist, wird ein Meldungsfenster eingeblendet, das anzeigt, ob der Upload erfolgreich oder fehlerhaft war.

Smart Card-Authentifizierung aktivieren

So aktivieren Sie die Smart Card-Authentifizierung:

1. Navigieren Sie zum Register **Benutzer-Authentifizierung**→ Unterregister **Verzeichnisdienste**. Stellen Sie sicher, dass **Microsoft Active Directory Standard** oder **Erweitertes Schema** ausgewählt ist.
2. Im Abschnitt **Allgemeine Einstellungen** wählen Sie:
   - Smart Card – diese Option erfordert das Einführen einer Smart Card in den Leser und die Eingabe der PIN-Nummer.

   ANMERKUNG: Alle bandexternen Befehlszeilenschnittstellen, einschließlich Secure Shell (SSH), Telnet, Seriell und Remote-RACADM, bleiben für diese Option unverändert.
3. Klicken Sie am unteren Rand auf **Anwenden**.

Sie können das Active Directory mit Kerberos-Authentifizierung testen, indem Sie die Testfunktion des CLI-Befehls verwenden.

Geben Sie Folgendes ein:

```
testfeature -f adkrb -u <user>@<domain>
```

wobei *Benutzer* 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 wiederholen. Weitere Informationen finden Sie in der Dokumentation zur Testfunktion für RACADM-Befehle.

Browser für Smart Card-Anmeldung konfigurieren

Mozilla Firefox

CMC 2.10 unterstützt Smart Card-Anmeldung über Firefox-Browser nicht.

Internet Explorer

Stellen Sie sicher, dass der Webbrowser zum Herunterladen von Active-X-Plug-Ins konfiguriert ist.

Anmeldung beim CMC mit Smart Card

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

So melden Sie sich am CMC unter Verwendung einer Smart Card an:

1. Melden Sie sich unter Verwendung Ihres Netzwerkkontos beim Clientsystem an.
2. Greifen Sie auf die CMC-Webseite zu. Verwenden Sie:

   https://<*cmcname.domain-name*>

   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.domaine-name>:<port number>* auf den CMC zu, wobei cmcname der CMC-Hostname für den CMC ist; **domain-name** ist der Domänenname und **port number** die HTTPS-Schnittstellennummer.

   Die Seite **CMC – einfache Anmeldung** wird eingeblendet. Sie werden aufgefordert, die Smart Card einzuführen.
3. Führen Sie die Smart Card in den Leser ein und klicken Sie auf **OK**.

   Das **PIN-Popup-**Dialogfeld wird angezeigt.

4 Optional können Sie eine Sitzungszeitüberschreitung wählen. Dies ist die Zeit, die Sie angemeldet bleiben, auch wenn keine Aktivität stattfindet. Der Standardwert ist als Web Service-Inaktivitätszeitüberschreitung definiert. Weitere Einzelheiten finden Sie unter „Dienste konfigurieren“.

5 Geben Sie die PIN ein und klicken Sie auf **OK**.

Fehlerbehebung Smart Card-Anmeldung

Die folgenden Tipps helfen beim Debuggen einer Smart Card, auf die nicht zugegriffen werden kann.

Das ActiveX-Plug-In kann das Smart Card-Laufwerk nicht erkennen.

Stellen Sie sicher, dass die Smart Card auf dem Microsoft Windows-Betriebssystem unterstützt wird. Windows unterstützt eine beschränkte Anzahl von Cryptographic Service Providers (CSP) für die Smart Card.

Sie können generell überprüfen, ob die Smart Card-CSPs auf einem bestimmten Client vorhanden sind, indem Sie die Smart Card bei der Windows-Anmeldung (Strg-Alt-Entf) in das Laufwerk einlegen, um zu sehen, ob Windows die Smart Card erkennt und das PIN-Dialogfeld einblendet.

Falsche Smart Card-PIN

Prüfen Sie, ob die Smart Card aufgrund übermäßiger Versuche mit einer falschen PIN gesperrt wurde. In solchen Fällen kann Ihnen der Aussteller der Smart Card in der Organisation helfen, eine neue Smart Card zu beschaffen.

Anmeldung beim CMC als Active Directory-Benutzer nicht möglich.

Wenn Sie sich als Active Directory-Benutzer nicht beim CMC anmelden können, versuchen Sie sich anzumelden, ohne die Smart Card-Anmeldung zu aktivieren. Sie haben auch die Möglichkeit, die Smart Card-Anmeldung über den lokalen RACADM zu deaktivieren, indem Sie die folgenden Befehle eingeben:

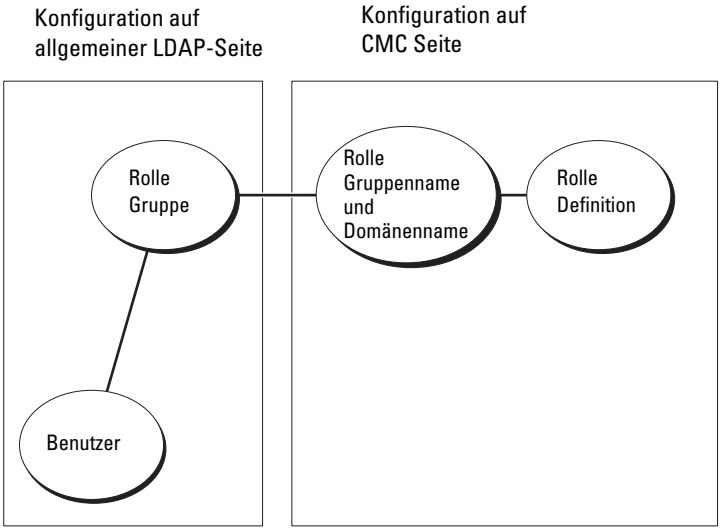
```
racadm config -g cfgActiveDirectory -o cfgADSCLEnable 0
racadm config -g cfgActiveDirectory -o cfgADSSOEnable 0
```

CMC mit allgemeinem LDAP verwenden

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. Tabelle 5-43 zeigt die Zugriffsebene der Rollengruppen und Tabelle 8-1 die standardmäßigen Einstellungen der Rollengruppen. Abbildung 8-5veranschaulicht die CMC-Konfiguration bei allgemeinem LDAP

Abbildung 8-5. CMC-Konfiguration bei allgemeinem LDAP



Allgemeines LDAP-Verzeichnis für Zugriff auf CMC konfigurieren

Die allgemeine LDAP-Implementierung des CMC verwendet zwei Phasen, um einem Benutzer Zugriff zu gewähren. Phase 1 beginnt mit der Benutzer-Authentifizierung, gefolgt von Phase 2 mit der Benutzerautorisierung.

Authentifizierung und Autorisierung von LDAP-Benutzern

Manche Verzeichnisserver erfordern eine Bindung, bevor eine Suche auf einem spezifischen LDAP-Server durchgeführt werden kann. Die Schritte zur Authentifizierung sind:

1. Optionale Bindung zum Verzeichnisdienst. Standard ist die anonyme Bindung.
2. Suche nach dem Benutzer auf Basis von dessen Benutzeranmeldung. Das Standardattribut ist **uid**.
3. Wenn mehr als ein Objekt gefunden wird, dann meldet der Prozess einen Fehler.
4. Bindung lösen und Bindung mit dem DN und Kennwort des Benutzers herstellen.
5. Falls die Bindung fehlschlägt, schlägt auch die Anmeldung fehl.

Wenn diese Schritte erfolgreich sind, dann gilt der Benutzer als authentifiziert. Die nächste Phase ist die Autorisierung. Der CMC speichert maximal 5 Gruppen und deren entsprechende Berechtigungen. 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.

Die Autorisierungsschritte sind Folgende:

1. Durchsuchen aller konfigurierten Gruppen nach dem DN des Benutzers und zwar innerhalb der Attribute **member** bzw. **uniqueMember**. Dieses Feld kann vom Administrator konfiguriert werden.
2. Hinzufügen der Berechtigungen für jede Gruppe, der der Benutzer als Mitglied angehört.

Konfiguration des allgemeinen LDAP-Verzeichnisdienstes mit der CMC-Webschnittstelle

Sie können den allgemeinen Lightweight Directory Access Protocol (LDAP)-Dienst zur Konfiguration Ihrer Software verwenden, um Zugriff auf den CMC zu ermöglichen. Mit LDAP können Sie für die vorhandenen Benutzer CMC-Benutzerberechtigungen hinzufügen und diese kontrollieren.

ANMERKUNG: Um LDAP-Einstellungen für den CMC zu konfigurieren, müssen Sie die Berechtigung als **Gehäusekonfiguration-Administrator** besitzen.

Weitere Informationen zur LDAP-Konfiguration zur Konfiguration eines allgemeinen LDAP finden Sie unter „CMC mit allgemeinem LDAP verwenden“ auf Seite 355.

So wird LDAP angezeigt und konfiguriert:

1. Melden Sie sich bei der Webschnittstelle an.
2. Klicken Sie auf das Register **Benutzer-Authentifizierung** und dann auf das Unterregister **Verzeichnisdienste**. Die Seite **Verzeichnisdienste** wird angezeigt.
3. Klicken Sie auf die Optionsschaltfläche, die mit dem allgemeinen LDAP verbunden ist.
4. Konfigurieren Sie die angezeigten Optionen und klicken Sie auf **Anwenden**.

Tabelle 8-10 zeigt die verfügbaren Optionen an:

Tabelle 8-10. Allgemeine Einstellungen

Einstellung	Beschreibung
Allgemeiner LDAP-Dienst aktiviert	Aktiviert den allgemeinen LDAP-Dienst auf dem CMC.
Abgegrenzten Namen zur Suche nach Gruppenmitgliedschaft verwenden	Legt den abgegrenzten Namen (DN) der LDAP-Gruppen fest, deren Mitglieder auf das Gerät zugreifen dürfen.
SSL-Zertifikatüberprüfung aktivieren	Wenn markiert, verwendet der CMC das CA-Zertifikat, um das LDAP-Serverzertifikat während des SSL-Handshake zu bestätigen.
Bindungs-DN	Legt den DN (Distinguished Name) eines Benutzers fest, der bei der Suche nach dem DN eines angemeldeten Benutzers zur Bindung an den Server verwendet wird. Wird kein DN angegeben, wird eine anonyme Bindung verwendet.
Kennwort	Ein Bindungskennwort, das gemeinsam mit dem Bindungs-DN verwendet wird. **ANMERKUNG:** Beim Bindungskennwort handelt es sich um sensible Daten, die entsprechend geschützt werden müssen.
Base-DN für Suche	Der DN des Verzeichniszweigs, von dem aus alle Suchvorgänge gestartet werden müssen.
Attribut der Benutzeranmeldung	Gibt das Attribut an, nach dem gesucht werden soll. Wenn keine Konfiguration vorliegt, lautet die zu verwendende Standardeinstellung „uid“. Es wird empfohlen, bei der Auswahl des Base-DN Eindeutigkeit zu gewährleisten, da andernfalls ein Suchfilter konfiguriert werden muss, um die Eindeutigkeit des anmeldenden Benutzers sicherzustellen. Wenn der Benutzer-DN nicht eindeutig durch die Suche nach einer Kombination aus Attribut und Suchfilter identifiziert werden kann, schlägt die Anmeldung fehl und es wird eine Fehlermeldung ausgegeben.

Tabelle 8-10. Allgemeine Einstellungen *(fortgesetzt)*

Einstellung	Beschreibung
Attribut der Gruppenmitgliedschaft	Legt das LDAP-Attribut fest, das zur Prüfung der Gruppenmitgliedschaft verwendet wird. Dies muss ein Attribut der Gruppenklasse sein. Wird hier nichts angegeben, werden die Attribute „member“ und „unique member“ verwendet.
Suchfilter	Gibt einen gültigen LDAP-Suchfilter an. Dieser Filter wird verwendet, wenn das Benutzerattribut den anmeldenden Benutzer innerhalb des ausgewählten Base-DN nicht eindeutig identifizieren kann. Wird hier nichts angegeben, wird der Standardwert (objectClass=*) zugrunde gelegt, mit dem nach allen Objekten in der Struktur gesucht wird. Die maximale Länge dieser Eigenschaft ist 1024 Zeichen.
Netzwerkzeitüberschreitung (Sekunden)	Legt die Zeit in Sekunden fest, nach der eine inaktive LDAP-Sitzung automatisch geschlossen wird.
Suchzeitüberschreitung (Sekunden)	Legt die Zeit in Sekunden fest, nach der eine Suche automatisch geschlossen wird.

Auswahl Ihres LDAP-Servers

Sie können den für allgemeines LDAP zu verwendenden Server auf zwei Arten konfigurieren. Statische Server erlauben es dem Administrator eine FQDN oder IP-Adresse in das Feld zu platzieren. Alternativ kann eine Liste von LDAP-Servern abgerufen werden, indem nach deren SRV-Eintrag in der DNS gesucht wird.

Es folgen die Eigenschaften im Abschnitt „LDAP-Server“:

- Statische LDAP-Server verwenden – Wenn diese Option ausgewählt wird, verwendet der LDAP-Dienst die angegebenen Server mit der angegebenen Schnittstellennummer (siehe Details unten).

  ANMERKUNG: Sie müssen „Statisch“ oder „DNS“ auswählen.

- LDAP-Server-Adresse – Geben Sie den FQDN oder die IP des LDAP-Servers an. Um mehrere redundante LDAP-Server anzugeben, die der gleichen Domäne dienen, legen Sie eine Liste aller Server an (kommagetrennt). Der CMC versucht sich nacheinander mit jedem Server zu verbinden, bis ein Verbindungsversuch erfolgreich ist.

- LDAP-Serverschnittstelle – Schnittstelle des LDAP über SSL, Standard ist 636, falls nicht konfiguriert. Nicht-SSL-Schnittstellen werden von CMC Version 3.0 nicht unterstützt, da das Kennwort nicht ohne SSL übertragen werden kann.
- DNS verwenden, um LDAP-Server zu finden – Wenn diese Option gewählt wird, verwendet der LDAP die Suchdomäne und den Dienstnamen über DNS. Sie müssen „Statisch“ oder „DNS“ auswählen.

Die folgende DNS-Abfrage wird für SRV-Einträge durchgeführt:

`_<Service Name>._tcp.<Search Domain>`

wobei <*Suchdomäne*> die root-Ebenendomäne ist, die für die Abfrage verwendet wird, und <*Dienstname*> der Dienstname, der für die Abfrage verwendet wird. Beispiel:

`_ldap._tcp.dell.com`

wobei `ldap` der Dienstname ist und `dell.com` die Suchdomäne.

LDAP-Gruppeneinstellungen verwalten

In der Tabelle im Abschnitt „Gruppeneinstellungen“ werden Rollengruppen aufgelistet, einschließlich zugeordneter Namen, Domänen und Berechtigungen für jede Rollengruppe, die bereits konfiguriert ist.

- Zur Konfiguration einer neuen Rollengruppe klicken Sie auf einen Rollengruppennamen, für den kein Name, keine Domäne und Berechtigung aufgelistet ist.
- Zum Ändern der Einstellungen einer vorhandenen Rollengruppe klicken Sie auf den Rollengruppennamen.

Wenn Sie einen Rollengruppennamen anklicken, erscheint die Seite **Rollengruppe konfigurieren**. Hilfe zu dieser Seite finden Sie über den Link **Hilfe**, der sich auf dieser Seite oben rechts befindet.

LDAP-Sicherheitszertifikate verwalten

In diesem Abschnitt werden die Eigenschaften für das kürzlich auf den CMC hochgeladene LDAP-Zertifikat angezeigt. Wenn Sie ein Zertifikat hochgeladen haben, verwenden Sie diese Informationen, um zu überprüfen, ob das Zertifikat gültig und nicht abgelaufen ist.

ANMERKUNG: Standardmäßig beinhaltet der CMC kein von einer Zertifizierungsstelle ausgegebenes Zertifikat für Active Directory. Sie müssen ein aktuelles, von einer Zertifizierungsstelle signiertes Serverzertifikat, hochladen.

Folgende Eigenschaften für das Zertifikat werden angezeigt:

- Seriennummer - Die Seriennummer des Zertifikats.
- Subjektinformationen - Subjekt des Zertifikats (Name der zertifizierten Person oder Firma).
- Ausstellerinformationen - Aussteller des Zertifikats (Name der Zertifizierungsstelle).
- Gültig ab - Das Anfangsdatum des Zertifikats.
- Gültig bis - Das Ablaufdatum des Zertifikats.

Die folgenden Steuerungen ermöglichen Ihnen das Hoch- und Herunterladen dieses Zertifikats:

- Hochladen - Initiiert den Hochladevorgang für das Zertifikat. Dieses Zertifikat, das Sie von Ihrem LDAP-Server erhalten, gewährt Ihnen Zugang zum CMC.
- Herunterladen - Initiiert den Herunterladevorgang. Sie werden aufgefordert, den Speicherort für die Datei anzugeben. Wenn Sie diese Option wählen und auf **Weiter** klicken, wird das Dialogfeld **Datei herunterladen** eingeblendet. Verwenden Sie dieses Dialogfeld, um auf Ihrer Management Station oder Ihrem freigegebenen Netzwerk einen Speicherort für das Serverzertifikat zu bestimmen.

Konfiguration des allgemeinen LDAP-Verzeichnisdienstes mittels RACADM

ANMERKUNG: Diese Funktion unterstützt sowohl IPv4 wie auch IPv6.

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.

Erforderliche 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.

Seite „Verwendung"

Um sich unter Verwendung eines LDAP-Benutzers am CMC anzumelden, verwenden Sie den Benutzernamen in der Anmeldeaufforderung und das Benutzerkennwort in der Kennwortaufforderung. Wenn ein LDAP-Benutzer aus bestimmten Gründen nicht angemeldet werden kann, geht der CMC zurück und versucht eine lokale Anmeldung mit demselben Benutzernamen und Kennwort. Dies ermöglicht eine Anmeldung, wenn die Netzwerkverbindung unterbrochen ist oder der LDAP-Server nicht erreichbar ist.

Wie Sie Hilfe bekommen

Das Ablaufverfolgungsprotokoll des CMC enthält einige Informationen darüber, warum ein Benutzer möglicherweise nicht angemeldet werden kann. Zur Untersuchung von LDAP-Anmeldefehlern wird die Verwendung des Befehls `racadm testfeature -f LDAP` mit eingeschalteter Debug-Funktion empfohlen.

9

Stromverwaltung

Das Dell PowerEdge M1000e-Servergehäuse 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 und die Stromumgebung umfassend kontrollieren.

Das modulare PowerEdge M1000e-Gehäuse nimmt Wechselstrom auf und verteilt die Last auf alle aktiven internen Netzteileinheiten. Das System kann bis zu 11637 Watt Wechselstrom übertragen, der Servermodulen und der damit verbundenen Gehäuseinfrastruktur zugeteilt wird.

Sie können die Energieverwaltung auch über die **Konsole zum Messen, Verteilen und Steuern** (PM3) steuern. Wenn die Energie über PM3 extern gesteuert wird, setzt CMC die Verwaltung der folgenden Aktivitäten fort:

- Redundanzregel
- Remote-Energieprotokollierung
- Serverleistung über Stromredundanz
- Dynamische Netzteilzuschaltung
- 110 V-Betrieb

PM3 verwaltet dann:

- Server-Stromversorgung
- Server-Priorität
- Eingangsstromkapazität des Systems
- Maximalen Stromsparmodus

Weitere Informationen finden Sie unter„Externe Energieverwaltung“ auf Seite 415.

ANMERKUNG: Die tatsächliche Stromzuteilung hängt von der Konfiguration und der Auslastung ab.

Die Stromverwaltungsfunktionen des M1000e helfen Administratoren, das Gehäuse zu konfigurieren, um den Stromverbrauch zu reduzieren und die Stromverwaltung auf die individuellen Bedürfnisse und Umgebungen zuzuschneiden.

Das M1000e-Gehäuse kann für eine von drei Redundanzregeln konfiguriert werden, die das Netzteileinheit-Verhalten beeinflussen und bestimmen, wie der Gehäuse-Redundanzstatus Administratoren gemeldet wird.

Wechselstrom-Redundanzmodus

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, 2 und 3 befinden sich im ersten Netz und die Netzteileinheiten in den Steckplätzen 4, 5 und 6 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: Da es eine Aufgabe der Wechselstromredundanz ist, für nahtlosen Serverbetrieb zu sorgen, selbst bei Ausfall eines ganzen Stromnetzes, ist der meiste Strom für die Aufrechterhaltung der Wechselstromredundanz verfügbar, wenn die Kapazitäten der beiden Netze etwa gleich sind.

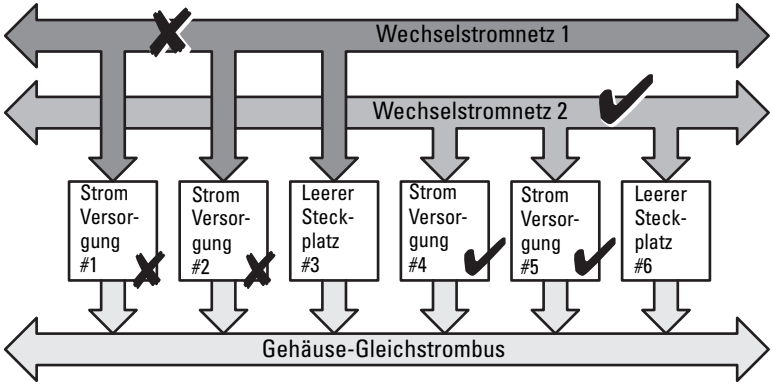
ANMERKUNG: Wechselstromredundanz besteht nur dann, wenn die Ladungsanforderungen nicht die Kapazität des schwächeren Stromnetzes übersteigen.

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. Abbildung 9-1 veranschaulicht 2 Netzteileinheiten pro Netz und ein Stromausfall in Netz 1.

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.

Abbildung 9-1. 2 Netzteileinheiten pro Netz und ein Stromausfall in Netz 1



ANMERKUNG: 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 „Keine Redundanz“ gemeldet und der Gehäusezustand als „Kritisch“ angezeigt.

Netzteilredundanz-Modus

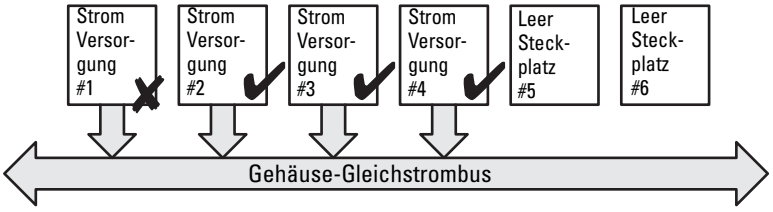
Der Netzteilredundanz-Modus ist nützlich, wenn keine redundanten Stromnetze zur Verfügung stehen und Schutz gegen den Ausfall einer einzelnen Netzteil-einheit erwünscht ist, um den Ausfall der Server in einem modularen Gehäuse zu vermeiden. Für diesen Zweck wird die Netzteileinheit mit der größten Kapazität als Onlinereserve gehalten. Das bildet einen Netzteilredundanzpool. Abbildung 9-2 veranschaulicht den Netzteilredundanz-Modus.

Etwaige über die für die Stromversorgung und Redundanz erforderlichen Netz-teileinheiten sind weiterhin verfügbar und werden dem Pool im Falle eines Ausfalls hinzugefügt.

Im Gegensatz zur Wechselstromredundanz ist es so, dass wenn Netzteilredun-danz 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 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.

Abbildung 9-2. Netzteilredundanz: Insgesamt 4 Netzteileinheiten bei Ausfall einer Netzteileinheit.



Zweifaches oder einfaches Stromnetz:
Die Stromversorgungsredundanz schützt gegen den Ausfall eines einzelnen Netzteils.

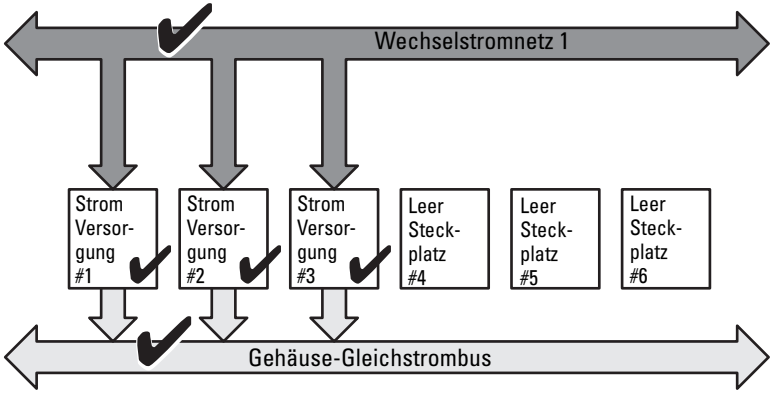
Keine-Redundanz-Modus

Der Modus **Keine Redundanz** ist die Standardwerkseinstellung für eine Konfiguration mit drei Netzteileinheiten und zeigt an, dass für das Gehäuse keine Stromredundanz konfiguriert ist. Bei dieser Konfiguration ist der Gesamt-Redundanzstatus des Gehäuses immer **Keine Redundanz**. Abbildung 9-3 veranschaulicht, dass der Modus **Keine Redundanz** die Standardwerkseinstellung für eine Konfiguration mit 3 Netzteileinheiten ist.

Der CMC verlangt nicht, dass die Netzteileinheiten an bestimmten Netzteileinheit-Steckplatzpositionen vorhanden sind, wenn **Keine Redundanz** konfiguriert ist.

ANMERKUNG: Alle Netzteileinheiten im Gehäuse werden als **Online** aufge-führt, falls DPSE im Modus **Keine Redundanz** deaktiviert wird. Wenn DPSE aktiviert ist, dann werden alle aktiven Netzteileinheiten im Gehäuse als **Online** aufgeführt und zusätzliche Netzteileinheiten können auf **Standby** gesetzt werden, um die Stromeffizienz des Systems zu erhöhen.

Abbildung 9-3. „Keine Redundanz" bei drei Netzteileinheiten im Gehäuse



Einfaches Stromnetz:
Kein Schutz gegen Stromnetz- oder Netzteilausfall

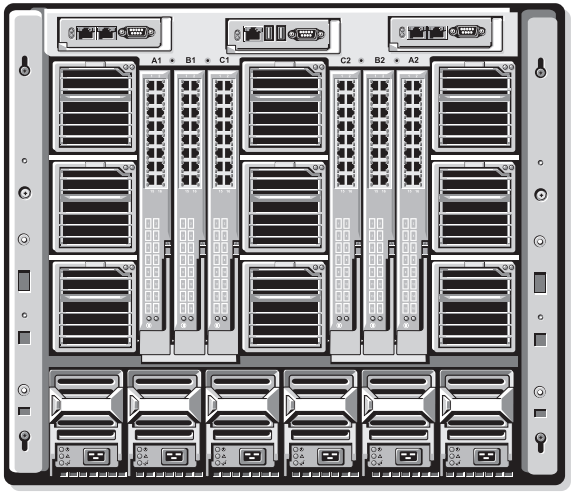
Der Ausfall einer Netzteileinheit bewirkt, dass die anderen Netzteileinheiten nach Bedarf aus dem Standby-Modus geschaltet werden, um die Gehäusestromzuteilungen zu unterstützen. Wenn Sie 4 Netzteileinheiten haben und nur drei benötigen, dann wird die vierte Netzteileinheit im Falle eines Ausfalls online gesetzt. Ein Gehäuse kann alle 6 Netzteileinheiten online haben.

Bei Aktivierung von DPSE werden die zusätzlichen Netzteileinheiten in den Standby-Modus gesetzt, um die Effizienz zu erhöhen und Energie zu sparen. Weitere Informationen finden Sie unter„Dynamische Netzteilzuschaltung“ auf Seite 372.

Strombudget für Hardwaremodule

Abbildung 9-4 zeigt ein Gehäuse mit einer Konfiguration für 6 Netzteileinheiten. Die Netzteileinheiten im Gehäuse sind von links nach rechts von 1 bis 6 nummeriert.

Abbildung 9-4. Gehäuse mit einer Konfiguration für 6 Netzteileinheiten



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 und iKVM (falls vorhanden). Das Gehäuse kann bis zu 16 Server aufweisen, die über den iDRAC mit dem Gehäuse kommunizieren. Weitere Informationen finden Sie im *iDRAC-Benutzerhandbuch* unter **support.dell.com/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.

Der CMC gewährt 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 den tatsächlichen Stromverbrauch. Der iDRAC-Strombereich kann, abhängig von den tatsächlichen Stromanforderungen, sich im Lauf der Zeit ändern. Der iDRAC verlangt nur 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 M1000e-Gehäuse kann ausreichend Strom für die Spitzenleis-tung der meisten Serverkonfigurationen bereitstellen, aber viele verfügbare Serverkonfigurationen verbrauchen nicht die maximale Strommenge, die das Gehäuse liefern kann. Um Rechenzentren bei der Strombereitstellung für ihre Gehäuse zu unterstützen, erlaubt das M1000e dem Benutzer, eine **System-eingangsstromobergrenze** anzugeben. Damit kann sichergestellt werden, dass der Gesamt-Wechselstromverbrauch des Gehäuses unter einem festgelegten Schwellenwert bleibt. Zunächst stellt der CMC sicher, dass ausreichend Strom für die Lüfter, E/A-Module, iKVM (falls vorhanden) 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 dem tatsächlichen Verbrauch anzusetzen, schlägt fehl.

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 maximale Strommenge vor Servern der Priorität 2 usw. Server mit niedrigerer Priorität erhalten basierend auf der Einstellung **Maximale System-eingangskapazität** und der benutzerdefinierten Einstellung **Systemeingangs-stromobergrenze** möglicherweise weniger Strom als Server der Priorität 1.

Konfigurationsänderungen, z. B. ein zusätzlicher Server im 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 von E/A-Modulen und iKVM 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 16685 Watt erhöht werden, um das Einschalten von zusätzlichen Servern zu ermöglichen.

Änderungen im modularen Gehäuse, die die Stromzuteilung verringern, sind:

- Ausschalten des Servers
- Server
- E/A-Modul
- iKVM-Entfernung
- Gehäuse in einen ausgeschalteten Zustand versetzen

Die **Systemeingangsstromobergrenze** kann neu konfiguriert werden, wenn das Gehäuse eingeschaltet (EIN) oder ausgeschaltet (AUS) ist.

ANMERKUNG: Wird ein Server mit einer anderen Geometrie als der einfachen Bauhöhe eingesetzt und es steht nicht ausreichend Strom für den iDRAC zur Verfügung, wird der Server als mehrere Server mit einfacher Bauhöhe angezeigt.

Serversteckplatz-Stromprioritätseinstellungen

Der CMC ermöglicht es Ihnen, eine Strompriorität für jeden der 16 Serversteck-plätze 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-Servers teckplatzpriorität 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 dann 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 einschaltet, vor denen mit höherer Priorität, dann wird die Stromzuteilung die 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 iKVM (falls vorhanden) erhalten die höchste Priorität. Der CMC fordert Strom nur von Geräten mit niedrigerer Priorität zurück, um den Strombedarf eines Moduls oder Servers mit höherer Priorität zu erfüllen.

Dynamische Netzteilzuschaltung

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.

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.

So werden die verbleibenden Netzteileinheiten mit maximaler Effizienz betrieben:

- Der Modus **Keine Redundanz** mit dynamischer Zuschaltung von Netzteileinheiten (DPSE) ist sehr energieeffizient – optimale Anzahl von Netzteileinheiten online. Nicht benötigte Netzteileinheiten werden in den Standby-Modus gesetzt.
- Auch der **Netzteilredundanzmodus** 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. Es besteht 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 drei oben erläuterten Redundanzkonfigurationen aktiviert werden: **Keine Redundanz**, **Netzteilredundanz** und **Wechselstromredundanz**.

- Bei der Konfiguration **Keine Redundanz** mit dynamischer Zuschaltung von Netzteileinheiten (DPSE) kann das M1000e bis zu fünf Netzteileinheiten in den Zustand **Standby** versetzen. In einer Konfiguration mit 6 Netzteileinheiten werden einige Netzteileinheiten in Standby versetzt und bleiben unbenutzt, um die Energieeffizienz zu verbessern. Die Entfernung oder der Ausfall einer Online-Netzteileinheit in dieser Konfiguration setzt eine Netzteileinheit vom Zustand **Standby** in den Zustand **Online**; es kann allerdings 2 Sekunden dauern, bis Standby-Netzteileinheiten aktiv werden, sodass es bei einigen Servern während dieser Umschaltung in der Konfiguration **Keine Redundanz** zu einem Stromverlust kommen kann.

ANMERKUNG: In einer Konfiguration mit drei Netzteileinheiten kann die Serverlast verhindern, dass Netzteileinheiten in den Zustand **Standby** 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. Es können je nach Gesamtsystemlast bis zu vier Netzteileinheiten in den Zustand **Standby** gesetzt werden. In einer Konfiguration mit sechs Netzteileinheiten sind immer mindestens zwei Netzteileinheiten eingeschaltet.

Da ein Gehäuse mit der Konfiguration **Netzteilredundanz** immer über eine zusätzliche Netzteileinheit verfügt, kann das Gehäuse den Ausfall einer Online-Netzteileinheit überbrücken und trotzdem noch genug Strom für die installierten Servermodule zur Verfügung stellen. Der Ausfall der Online-Netzteileinheit führt dazu, dass eine Standby-Netzteileinheit online geschaltet wird. Der gleichzeitige Ausfall mehrerer Netzteileinheiten kann zum Stromverlust bei einigen Servermodulen führen, während die Standby-Netzteileinheiten hochfahren.

- 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 wiederspiegelt, 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 drei Wechselstromredundanzmodi Strom anzufordern.

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
- Keine Redundanz

Die Standard-Redundanzkonfiguration eines Gehäuses hängt von der Zahl der enthaltenen Netzteileinheiten ab, wie in Tabelle 9-1 dargestellt.

Tabelle 9-1. Standard-Redundanzkonfiguration

Konfiguration der Netzteileinheiten	Standard-Redundanzregel	Standardeinstellung für die dynamische Zuschaltung von Netzteileinheiten
Sechs Netzteileinheiten	Wechselstromredundanz	Deaktiviert
Drei Netzteileinheiten	Keine Redundanz	Deaktiviert

Wechselstromredundanz

Im Wechselstromredundanzmodus mit 6 Netzteileinheiten sind alle Netzteileinheiten aktiv. Die drei Netzteileinheiten links müssen mit einen Wechselstromnetz verbunden sein, während die drei Netzteileinheiten rechts mit einem anderen Wechselstromnetz verbunden sein müssen.

VORSICHTSHINWEIS: 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.

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

Netzteilredundanz

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 bis zu vier 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.

Keine Redundanz

Es wird Strom bereitgestellt, der das zum Betreiben des Gehäuses erforderliche Maß übersteigt, sodass dem Gehäuse selbst bei einem Ausfall weiterhin Strom zur Verfügung steht.

VORSICHTSHINWEIS: Der „Keine Redundanz"-Modus verwendet optimale Netzteileinheiten, wenn DPSE entsprechend den Erfordernissen des Gehäuses aktiviert ist. Der Ausfall einer einzigen Netzteileinheit kann in diesem Modus den Strom- und Datenverlust von Servern zur Folge haben.

Stromeinsparung und Strombudgetänderungen

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.

Anleitungen zum Zuweisen von Serverprioritätsstufen finden Sie unter „RACADM verwenden" auf Seite 405.

Sie können Serverpriorität über die GUI zuweisen:

1. Klicken Sie in der Systemstruktur auf **Server.**
2. Klicken Sie auf **Strom→ Priorität**.

Stromspar- und maximaler Sparmodus

Der CMC sorgt für maximale Stromeinsparung, wenn:

- Der Benutzer den maximalen Stromsparmodus wählt, unter Verwendung der Webschnittstelle oder RACADM.
- Ein von einem UPS-Gerät automatisch ausgegebenes Befehlszeilenskript den maximalen Sparmodus wählt.

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 Benutzer oder ein automatische Befehlszeilenskript den maximalen Stromsparmodus aufhebt.

Webschnittstelle verwenden

Der maximale Stromsparmodus kann mithilfe der GUI ausgewählt oder aufgehoben werden:

1. Klicken Sie in der Systemstruktur auf **Gehäuseübersicht**.
2. Klicken Sie auf **Strom→ Konfiguration**.
3. Wählen Sie das Feld **Maximaler Stromsparmodus** aus, um die maximale Stromeinsparung zu aktivieren und klicken Sie auf **Anwenden**.
4. Löschen Sie das Feld **Maximaler Stromsparmodus**, um zum normalen Betrieb zurückzukehren und klicken dann auf **Anwenden**.

RACADM verwenden

Öffnen Sie eine serielle, Telnet- oder SSH-Konsole für den CMC und melden Sie sich an.

- 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
  ```

110 V Betrieb von Netzteileinheiten

Manche Netzteile unterstützen den Betrieb mit 110 V Wechselstromversorgung. Dieser Eingang kann den für den Stromkreis erlaubten Wert überschreiten. Wenn Netzteile an 110 V Wechselstrom angeschlossen sind, muss der Benutzer den CMC für den normalen Betrieb des Gehäuses einstellen. Wenn er nicht so eingestellt ist und 110 V Netzteileinheiten erkannt werden, werden alle nachfolgenden Stromzuteilungsanfragen von Servern abgelehnt. In diesem Fall können zusätzliche Server nicht eingeschaltet werden, unabhängig von ihrer Priorität. Sie können den CMC so einstellen, dass 110 V Netzteile unter Verwendung der Webschnittstelle oder RACADM verwendet werden.

Webschnittstelle verwenden

Vergewissern Sie sich, dass der 110 V Stromkreis für den erwarteten Strom ausgelegt ist, und führen Sie dann die folgenden Schritte durch:

1. Klicken Sie in der Systemstruktur auf **Gehäuseübersicht**.
2. Klicken Sie auf **Strom→ Konfiguration**.
3. Wählen Sie **110 V Wechselstrombetrieb erlauben** und klicken dann auf **Anwenden**.

RACADM verwenden

Vergewissern Sie sich, dass der 110 V Stromkreis für den erwarteten Strom ausgelegt ist, und führen Sie dann die folgenden Schritte aus:

1. Öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC und melden Sie sich an.
2. 110 V Wechselstrom-Netzteileinheiten aktivieren:

```
racadm config -g cfgChassisPower -o
cfgChassisAllow110VACOperation 1
```

Serverleistung über Stromredundanz

Wenn diese Option aktiviert ist, hat die Serverleistung und der Serverstart gegenüber der Aufrechterhaltung der Stromredundanz Vorrang. Wenn diese Option deaktiviert ist, bevorzugt das System die Stromredundanz gegenüber der Serverleistung. Wenn diese Option deaktiviert ist und die Netzteile des Gehäuses dann nicht ausreichend Strom liefern, weder für die Redundanz, noch für die volle Leistung, trifft für einige Server möglicherweise das Folgende nicht zu, um die Redundanz beizubehalten:

- Bereitstellung von ausreichend Strom für die volle Leistung.
- Netzstrom eingeschaltet.

Webschnittstelle verwenden

Führen Sie zur Aktivierung von „Serverleistung über Stromredundanz“ die folgenden Schritte durch:

1. Klicken Sie in der Systemstruktur auf **Gehäuseübersicht**.
2. Klicken Sie auf **Strom→ Konfiguration**.
3. Wählen Sie **Serverleistung über Stromredundanz** und klicken Sie auf **Anwenden**.

Führen Sie zur Deaktivierung von „Serverleistung über Stromredundanz“ die folgenden Schritte durch:

1. Klicken Sie in der Systemstruktur auf **Gehäuseübersicht**.
2. Klicken Sie auf **Strom→ Konfiguration**.
3. Wählen Sie **Serverleistung über Stromredundanz** und klicken Sie auf **Anwenden**.

RACADM verwenden

Führen Sie zur Aktivierung von „Serverleistung über Stromredundanz“ die folgenden Schritte durch:

1. Öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC und melden Sie sich an.
2. Aktivieren von „Serverleistung über Stromredundanz“:

```
racadm config -g cfgChassisPower -o
cfgChassisPerformanceOverRedundancy 1
```

Führen Sie zur Deaktivierung von „Serverleistung über Stromredundanz“ die folgenden Schritte durch:

1. Öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC und melden Sie sich an.
2. Deaktivieren von „Serverleistung über Stromredundanz“:

```
racadm config -g cfgChassisPower -o
cfgChassisPerformanceOverRedundancy 0
```

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- bzw. Protokollierungszeitraums die entsprechenden folgenden Abschnitte.

Webschnittstelle verwenden

Sie können die Remote-Protokollierung des Stromverbrauchs unter Verwendung der GUI aktivieren. Melden Sie sich dazu an der GUI an und verfahren Sie folgendermaßen:

1. Klicken Sie in der Systemstruktur auf **Gehäuseübersicht**.
2. Klicken Sie auf **Strom→ Konfiguration**.
3. Wählen Sie **Remote-Protokollierung des Stromverbrauchs**, um Stromverbrauchsereignisse auf einem Remote-Host zu protokollieren.
4. Geben Sie den erforderlichen Protokollierungszeitraum an (1–1440 Minuten).
5. Klicken Sie auf **Übernehmen,** um Änderungen zu speichern.

RACADM verwenden

Öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC, melden Sie sich an und konfigurieren Sie die Remote-Stromverbrauchsprotokollierung wie hier gezeigt:

1. Geben Sie zur Aktivierung der Remote-Stromverbrauchsprotokollierungsfunktion den folgenden Befehl ein:

   ```
   racadm config -g cfgRemoteHosts -o
   cfgRhostsSyslogPowerLoggingEnabled 1
   ```

2. 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.

3. Geben Sie zur Bestimmung dessen, ob die Remote-Stromverbrauchsprotokollierungsfunktion aktiviert ist den folgenden Befehl ein:

   ```
   racadm getconfig -g cfgRemoteHosts -o
   cfgRhostsSyslogPowerLoggingEnabled
   ```

4. Geben Sie zur Bestimmung des Remote-Stromverbrauchsprotokollierungszeitraums den folgenden Befehl ein:

   ```
   racadm getconfig -g cfgRemoteHosts -o
   cfgRhostsSyslogPowerLoggingInterval
   ```

   ANMERKUNG: 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. Lesen Sie für weitere Details die Remote-Syslog Konfigurationsanweisungen.

Ausfall einer Netzteileinheit unter der Regeloption „Herabgesetzt“ oder „Keine Redundanz“

Im Stromeinsparungsmodus verringert der CMC die Stromzufuhr zu Servern, wenn das Ereignis „unzureichende Stromversorgung“ auftritt, z. B. der Ausfall einer Netzteileinheit. Nachdem der Strom in Servern verringert wurde, berechnet der CMC den Strombedarf des Gehäuses neu. Wenn die Stromanforderungen nach wie vor nicht erfüllt werden, dann schaltet der CMC die Server mit niedrigerer Priorität ab.

Der Strom für Server mit höherer Priorität wird stufenweise wiederhergestellt, wobei der Strombedarf innerhalb des Strombudgets verbleibt.

ANMERKUNG: Informationen, um die Redundanzregel festzulegen, finden Sie unter „Konfiguration von Stromversorgungsbudget und Redundanz“ auf Seite 401.

Regel zur Zuschaltung neuer Server

Wenn ein neuer Server eingeschaltet wird, muss der CMC die Stromzufuhr zu Servern mit niedriger Priorität möglicherweise verringern, um den neuen Server mit mehr Strom zu versorgen, wenn das Hinzufügen des neuen Servers den verfügbaren Strom für das System überschreitet. 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 für den Minimalstromverbrauch aller Server im Gehäuse verfügbar ist. Wenn durch die Reduktion des zugewiesenen Stroms der Server mit niedriger Priorität nicht genügend Strom freigesetzt werden kann, kann es sein, dass der neue Server nicht hochfährt.

Der höchste erforderliche Strombedarf im Dauerbetrieb von Gehäuse und allen Servern, einschließlich des neuen Servers, entspricht bei Volllast dem Strombedarf im ungünstigsten Fall. Ist diese Strommenge verfügbar, wird keinem Server mehr Strom zugewiesen, als im ungünstigsten Fall notwendig und somit kann der neue Server hochfahren.

Kann der Strombedarf für den ungünstigsten Fall nicht geliefert werden, wird der Strom der Server mit niedrigerer Priorität soweit reduziert, bis genügend Strom für den Startvorgang des neuen Servers freigesetzt ist.

Tabelle 9-2 beschreibt die vom CMC ergriffenen Maßnahmen, wenn ein neuer Server im oben beschriebenen Szenario eingeschaltet wird.

Tabelle 9-2. 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 zugelassen

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 im ungünstigsten Fall herunterfahren. Beide Bedingungen wirken sich zuerst auf Server mit niedriger Priorität aus.

Tabelle 9-3beschreibt die Firmware-Reaktion, wenn eine Netzteileinheit heruntergefahren oder entfernt wird, hinsichtlich verschiedener Redundanzkonfigurationen von Netzteileinheiten.

Tabelle 9-3. Auswirkung auf das Gehäuse bei Ausfall oder Entfernung einer Netzteileinheit

Konfiguration der Netzteileinheiten	Dynamische Netzteileinheit Zuschaltung	Firmware-Reaktion
Wechselstromredundanz	Deaktiviert	Der CMC alarmiert bei Verlust der Wechselstromredundanz.
Netzteilredundanz	Deaktiviert	Der CMC alarmiert bei Verlust der Netzteilredundanz.

Tabelle 9-3. Auswirkung auf das Gehäuse bei Ausfall oder Entfernung einer Netzteileinheit *(fortgesetzt)*

Konfiguration der Netzteileinheiten	Dynamische Netzteileinheit Zuschaltung	Firmware-Reaktion
Keine Redundanz	Deaktiviert	Verringerung der Stromversorgung für Server mit niedriger Priorität, falls nötig.
Wechselstromredundanz	Aktiviert	Der CMC alarmiert bei Verlust der Wechselstromredundanz. Netzteile im Standby-Modus (wenn vorhanden) werden eingeschaltet, um den Stromverlust in Folge eines Netzteileinheitfehlers oder -ausfalls zu kompensieren.
Netzteilredundanz	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.
Keine Redundanz	Aktiviert	Verringerung der Stromversorgung für Server mit niedriger Priorität, falls nötig.

Entfernung von Netzteileinheiten unter der Regeloption „Herabgesetzt" oder „Keine Redundanz"

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 Herunterfahren 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 drei in der Liste „Redundanzregeln“ auf Seite 374aufgeführten Redundanzkonfigurationseinstellungen von Netzteileinheiten auswählen.

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.

Tabelle 9-4 listet die SEL-Einträge auf, die mit Netzteiländerungen zusammenhängen.

Tabelle 9-4. SEL-Ereignisse für Netzteiländerungen

Netzteilereignis	Systemereignisprotokoll (SEL)-Eintrag
Einfügen	Vorhandenes Netzteil festgestellt
Entfernen	Vorhandenes Netzteil nicht mehr feststellbar
Wechselstromeingang	Netzteileingangsverlust nicht mehr feststellbar
Wechselstrom-Eingangsverlust	Netzteileingangsverlust festgestellt
Gleichstromausgabe hergestellt	Netzteilausfall nicht mehr feststellbar
Gleichstromausgabeverlust	Netzteilausfall festgestellt
Unbestätigter 110 V Betrieb erkannt	Stromversorgung mit niedriger Eingangsspannung (110 V) wurde festgestellt
110 V Betrieb bestätigt	Stromversorgung mit niedriger Eingangsspannung (110 V) nicht mehr feststellbar

Ereignisse, die mit Änderungen der Stromredundanzregeln zusammenhängen, die Einträge im SEL verursachen, sind Redundanzverlust und Redundanzwiederherstellung für das modulare Gehäuse, das entweder für eine **Wechselstromredundanzregel** oder eine **Netzteilredundanzregel** konfiguriert ist. Tabelle 9-5 listet die SEL-Einträge auf, die mit Änderungen der Stromredundanzregeln zusammenhängen.

Tabelle 9-5. SEL-Ereignisse für Änderungen des Stromredundanzstatus

Stromregelereignis	Systemereignisprotokoll (SEL)-Eintrag
Redundanzverlust	Redundanzverlust wurde festgestellt
Redundanz wiederhergestellt	Redundanzverlust nicht mehr feststellbar

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.

Strom konfigurieren und verwalten

Sie können die webbasierten und RACADM-Benutzeroberflächen zum Verwalten und Konfigurieren der Stromsteuerung im CMC verwenden. Genauer gesagt können Sie:

- Stromzuteilungen, Verbrauch und Status des Gehäuses, der Server und der Netzteile anzeigen
- Systemeingangsstromobergrenze und Redundanzregel für das Gehäuse konfigurieren
- Stromsteuerungsvorgänge (Einschalten, Ausschalten, System-Reset, Aus- und Einschalten) für das Gehäuse ausführen

Funktionszustand der Netzteileinheiten anzeigen

Die Seite **Netzteilstatus** zeigt den Status und die Messwerte der Netzteileinheiten an, die dem Gehäuse zugeordnet sind.

Webschnittstelle verwenden

Der Funktionszustand der Netzteileinheiten kann auf zwei Arten eingesehen werden: im Abschnitt **Gehäuse-Grafiken** auf der Seite **Gehäusestatus** oder auf der Seite **Netzteilstatus**. Die Seite **Gehäuse-Grafiken** bietet einen grafischen Überblick über alle Netzteileinheiten, die im Gehäuse installiert sind.

Um den Funktionszustand aller Netzteileinheiten mittels **Gehäuse-Grafiken** einzusehen:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Die Seite **Gehäusestatus** wird angezeigt. Der untere Abschnitt der **Gehäuse-Grafiken** stellt die Rückansicht des Gehäuses dar und enthält den Funktionszustand aller Netzteileinheiten. Der Netzteileinheit-Funktionszus-tand wird durch die Farbe des Netzteil-Untergrafik angegeben:
   - Grün – Netzteileinheit wird erkannt, mit Strom versorgt und kommuniziert mit dem CMC; es gibt keine Anzeichen eines ungünstigen Zustands.
   - Gelb – Zeigt den Ausfall einer Netzteileinheit an. Einzelheiten zur Fehlerbedingung finden Sie im CMC-Protokoll.
   - Grau – Tritt bei der Initialisierung der Netzteileinheit auf, wenn die Netzteileinheit auf Standby gesetzt wird, während des Gehäusestarts oder bei der Einführung der Netzteileinheit. Netzteileinheit ist vorhanden und nicht eingeschaltet. Es gibt kein Anzeichen für einen ungünstigen Zustand.
3. Bewegen Sie den Cursor über eine einzelne Netzteil-Untergrafik und ein entsprechender Texthinweis oder Bildschirmtipp wird angezeigt. Der Texthinweis liefert zusätzliche Informationen zu diesem Netzteil.
4. Die Netzteil-Untergrafik ist mit der entsprechenden Seite der CMC-GUI verknüpft, um sofortige Navigation zur Seite **Netzteilstatus** für alle Netzteileinheiten zu ermöglichen.

Um den Funktionszustand der Netzteileinheiten einzusehen, verwenden Sie die Seite **Netzteilstatus**:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur **Netzteile** aus. Die Seite **Netzteilstatus** wird angezeigt.

Tabelle 9-6 und Tabelle 9-7 enthalten Erläuterungen zu den Informationen auf der Seite Stromversorgung-Status.

Tabelle 9-6. Netzteile

Element	Beschreibung	
Name	Zeigt den Namen des Netzteils an: PS-[n], wobei [n] die Nummer des Netzteils ist.	
Präsentation	Gibt an, ob die Netzteileinheit **Vorhanden** oder **Nicht vorhanden** ist.	
Seite „Funktionszustand“	OK	Zeigt an, dass die Netzteileinheit vorhanden ist und mit dem CMC kommuniziert. Im Falle eines Fehlers bei der Kommunikation zwischen dem CMC und dem Netzteil kann der CMC den Funktionsstatus der Netzteileinheit weder abrufen noch anzeigen.
	Warnung	Zeigt an, dass Warnungen ausgegeben wurden und Korrekturmaßnahmen ergriffen werden müssen. Wenn keine Korrekturmaßnahmen ergriffen werden, könnte dies zu kritischen oder schwerwiegenden Stromausfällen und somit zu einer Beeinträchtigung der Integrität des Gehäuses führen.
	Schwerwiegend	Gibt an, dass mindestens eine Fehlerwarnung für das Netzteil ausgegeben wurde. Der Status „Schwerwiegend“ zeigt einen Stromausfall im Gehäuse an; **es müssen umgehend Korrekturmaßnahmen ergriffen werden**.

Tabelle 9-6. Netzteile *(fortgesetzt)*

Element	Beschreibung
Stromstatus	Zeigt den Betriebszustand der Netzteile an (einer der Folgenden): **Initialisierung**, **Online**, **Standby**, **Diagnosemodus**, **Fehler**, **Offline**, **Unbekannt** oder **Abwesend**.
Kapazität	Zeigt die Stromkapazität des Netzteils in Watt.

Tabelle 9-7. Systemstromstatus

Element	Beschreibung
Gesamt-Stromfunktionszustand	Zeigt den Funktionszustand (**OK, Nicht-kritisch, Kritisch, Nicht behebbar, Anderer, Unbekannt**) für die Stromverwaltung des gesamten Gehäuses an.
Systemstromstatus	Zeigt den Stromstatus (**Ein, Aus, Einschalten, Ausschalten**) des Gehäuses an.
Redundancy (Redundanz)	Zeigt den Netzteilredundanzstatus an. Zu den Werten gehören: **Nein**: Netzteile sind nicht redundant. **Ja**: Volle Redundanz wirksam.

RACADM verwenden

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

```
racadm getpminfo
```

Lesen Sie für weitere Informationen über **getpminfo**, einschließlich der Ausgabedetails, das *RACADM Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC auf der* Dell Support-Website unter **support.dell.com/manuals**.

Anzeige des Stromverbrauchsstatus

Der CMC zeigt den tatsächlichen Eingangsstromverbrauch für das gesamte System auf der Seite **Stromverbrauchsstatus** an.

Webschnittstelle verwenden

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, müssen Sie die Berechtigung als **Gehäusekonfigurations-Administrator** besitzen.

So zeigen Sie den Stromverbrauchsstatus mithilfe der Webschnittstelle an:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur **Gehäuse-Übersicht** aus.
3. Klicken Sie auf **Strom→ Stromverbrauch**. Die Seite **Stromverbrauch** wird angezeigt.

ANMERKUNG: Der Stromredundanzstatus wird auch unter **Netzteile** in der Systemstruktur **System** auf dem Register→ **Status** angezeigt.

RACADM verwenden

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
```

Tabelle 9-8 bis Tabelle 9-11 beschreiben die auf der Seite **Stromverbrauch** angezeigten Informationen.

Tabelle 9-8. Stromstatistik in Echtzeit

Element	Beschreibung
Systemeingangsleistung	Zeigt den aktuellen kumulativen Stromverbrauch aller Module im Gehäuse an, gemessen von der Eingangsseite der Netzteileinheiten. Der Wert für die?Systemeingangsleistung wird sowohl in Watt, als auch in BTU/h (British Thermal Unit per hour) angegeben.
Systemspitzenleistung	Zeigt den Maximalstromverbrauch auf Systemeingangsebene an, seit dieser Wert zuletzt gelöscht wurde. Über diese Eigenschaft können Sie den maximalen Stromverbrauch des Systems (Gehäuse und Module) verfolgen, der über einen bestimmten Zeitraum aufgezeichnet wurde. Klicken Sie auf die Schaltfläche **Spitzen-/Min.-Stromstatistik zurücksetzen** unter der Tabelle, um diesen Wert zu löschen. Der Wert für die?Systemspitzenleistung wird sowohl in Watt, als auch in BTU/h (British Thermal Unit per hour) angegeben.

Tabelle 9-8. Stromstatistik in Echtzeit *(fortgesetzt)*

Element	Beschreibung
Startzeit der Systemspitzenleistung	Zeigt das aufgezeichnete Datum und die Uhrzeit an, zu der der Wert des Stromverbrauchs (Systemspitzenwert) zuletzt gelöscht wurde. Der Zeitstempel wird im Format **hh:mm:ss MM/TT/JJJJ** angezeigt, wobei **hh** die Stunden (0 - 24), **mm** die Minuten (00 - 60), **ss** die Sekunden (00 - 60), **MM** den Monat (1 - 12), **TT** die Tage (1 - 31) und **JJJJ** das Jahr angeben. Dieser Wert wird über die Schaltfläche **Spitzen-/Min.-Stromstatistik zurücksetzen** und bei CMC-Reset oder -Ausfall zurückgesetzt.
Spitzenstromverbrauch des Systems, Zeitstempel	Zeigt das aufgezeichnete Datum und die Uhrzeit des in dem festgelegten Aufzeichnungszeitraum gemessenen Spitzenstromverbrauchs des Systems an. Der Zeitstempel wird im Format **hh:mm:ss MM/TT/JJJJ** angezeigt, wobei **hh** die Stunden (0 - 24), **mm** die Minuten (00 - 60), **ss** die Sekunden (00 - 60), **MM** den Monat (1 - 12), **TT** den Tag (1 - 31) und **JJJJ** das Jahr angeben.
Minimalsystemstrom	Zeigt den niedrigsten Wert des Wechselstromverbrauchs des Systems (in Watt) über den Zeitraum an, seit der Benutzer diesen Wert das letzte Mal zurückgesetzt hat. Über diese Eigenschaft können Sie den minimalen Stromverbrauch des Systems (Gehäuse und Module) verfolgen, der über einen bestimmten Zeitraum aufgezeichnet wurde. Klicken Sie auf die Schaltfläche **Spitzen-/Min.-Stromstatistik zurücksetzen** unter der Tabelle, um diesen Wert zu löschen. Der Wert für den?Systemminimalstrom wird sowohl in Watt, als auch in BTU/h (British Thermal Unit per hour) angegeben. Dieser Wert wird über die Schaltfläche **Spitzen-/Min.-Stromstatistik zurücksetzen** und bei CMC-Reset oder -Failover zurückgesetzt.

Tabelle 9-8. Stromstatistik in Echtzeit *(fortgesetzt)*

Element	Beschreibung
Startzeit der Systemminimalleistung	Zeigt das aufgezeichnete Datum und die Uhrzeit an, zu der der Wert des minimalen Systemstromverbrauchs zuletzt gelöscht wurde. Der Zeitstempel wird im Format **hh:mm:ss MM/TT/JJJJ** angezeigt, wobei **hh** die Stunden (0 - 24), **mm** die Minuten (00 - 60), **ss** die Sekunden (00 - 60), **MM** den Monat (1 - 12), **TT** die Tage (1 - 31) und **JJJJ** das Jahr angeben. Dieser Wert wird über die Schaltfläche **Spitzen-/Min.-Stromstatistik zurücksetzen** und bei CMC-Reset oder -Failover zurückgesetzt.
Minimaler Stromverbrauch des Systems, Zeitstempel	Zeigt das aufgezeichnete Datum und die Uhrzeit des in dem festgelegten Aufzeichnungszeitraum gemessenen minimalen Stromverbrauchs des Systems an. Das Format des Zeitstempels entspricht dem unter **Spitzenstromverbrauch des Systems**, **Zeitstempel** beschriebenen Format.
Systemleerlaufleistung	Zeigt den geschätzten Stromverbrauch des Gehäuses im Leerlauf an. Der Leerlaufzustand wird definiert als Zustand, bei dem das Gehäuse eingeschaltet ist und alle Module Strom verbrauchen, während sie sich im Leerlauf befinden. *Dies ist ein geschätzter, kein gemessener Wert.* Er wird berechnet aus der kumulativen Strommenge, die den Gehäuseinfrastruktur-komponenten Strommenge (E/A-Module, Lüfter, iKVM, iDRAC-Controller und Vorderseiten-LCDs) zugewiesen ist und dem Minimalbedarf aller Server, denen Strom zugewiesen ist und die sich im eingeschalteten Zustand befinden. Der Wert für die Systemleerlaufleistung wird sowohl in Watt, als auch in BTU/h (British Thermal Unit per hour) angegeben.

Tabelle 9-8. Stromstatistik in Echtzeit *(fortgesetzt)*

Element	Beschreibung
Systempotentialleistung	Zeigt den geschätzten Stromverbrauch des Gehäuses, wenn es mit maximalem Stromverbrauch betrieben wird. Der maximale Stromverbrauch wird als der Zustand definiert, bei dem das Gehäuse eingeschaltet ist und alle Module maximal Strom verbrauchen. *Dies ist ein geschätzter Wert, abgeleitet vom historischen Gesamtstromverbrauch der Systemkonfiguration und nicht ein gemessener Wert.* Er wird berechnet aus der kumulativen Strommenge, die den Gehäuseinfrastruktur-komponenten (E/A-Module, Lüfter, iKVM, iDRAC-Controller und Vorderseiten-LCDs) zugeteilt ist, und dem Maximalbedarf aller eingeschalteten Server, denen Strom zugeteilt ist. Der Wert für die?Systempotentialleistung wird sowohl in Watt, als auch in BTU/h (British Thermal Unit per hour) angegeben.
Auslesen des Systemeingangsstroms	Zeigt die gesamte Eingangsstromaufnahme des Gehäuses an, basierend auf der Summe der Eingangsstromaufnahme jedes einzelnen Netzteilmoduls im Gehäuse. Der Wert für die Systemeingangsstromaufnahme wird in Ampere angezeigt.

Tabelle 9-9. Status der Echtzeit-Energiestatistik

Element	Beschreibung
Systemenergieverbrauch	Zeigt den aktuellen gesamten Stromverbrauch aller Module im Gehäuse an, gemessen von der Stromeingangsseite der Netzteileinheiten. Der Wert wird in kWh angezeigt; es handelt sich um einen kumulativen Wert.
Startzeit der Systemenergiedaten	Zeigt das aufgezeichnete Datum und die Uhrzeit an, zu der der Wert für den Systemenergieverbrauch zuletzt gelöscht wurde und der neue Messzyklus begann. Der Zeitstempel wird im Format **hh:mm:ss MM/TT/JJJJ** angezeigt, wobei **hh** für die Stunden (0-24) steht, **mm** für die Minuten (00-60), **ss** die Sekunden bezeichnet (00-60), **MM** den Monat angibt (1-12), **DD** für die Tage steht (1-31) und **JJJJ** das Jahr angeben. Dieser Wert wird über die Schaltfläche **Energiestatistik zurücksetzen** zurückgesetzt und bleibt bei CMC-Reset oder -Failover erhalten.

Tabelle 9-9. Status der Echtzeit-Energiestatistik *(fortgesetzt)*

Element	Beschreibung
Systemenergieverbrauch, Zeitstempel	Zeigt das Datum und die Uhrzeit an, zu der der System-energie-verbrauch für die Anzeige berechnet wurde. Der Zeitstempel wird im Format **hh:mm:ss MM/TT/JJJJ** angezeigt, wobei **hh** für die Stunden (0-24) steht, **mm** für die Minuten (00-60), **ss** die Sekunden bezeichnet (00-60), **MM** den Monat angibt (1-12), **DD** für die Tage steht (1-31) und **JJJJ** das Jahr angeben.

Tabelle 9-10. Systemstromstatus

Element	Beschreibung
Gesamt-Stromfunktionszustand	Zeigt den Funktionsstatus des Stromuntersystems des Gehäuses an: • Grünes Prüfsymbol für **OK** • Gelbes Ausrufezeichensymbol für **Nicht kritisch** • Rotes X-Symbol für **Kritisch**
Systemstromstatus	Zeigt den Stromstatus (**Ein**, **Aus**, **Netzstrom ein**, **Ausschalten**) des Gehäuses an.
Redundanz	Zeigt den Redundanzstatus an. Gültige Werte sind: **Nein** – Netzteileinheiten sind nicht redundant **Ja** – Volle Redundanz wirksam.

Tabelle 9-11. Servermodule

Element	Beschreibung
Steckplatz	Zeigt die Position des Servermoduls an. Die **Steckplatznummer** ist eine sequenzielle Nummer (1-16), die das Servermodul nach seiner Position im Gehäuse identifiziert.
Name	Zeigt den Servernamen an. Der Servername kann vom Benutzer neu definiert werden.
Präsentation	Zeigt an, ob der Server im Steckplatz vorhanden ist (**Ja** oder **Nein**). Wenn dieses Feld die **Erweiterung von #** (wobei das Zeichen **#** für 1 - 8 steht) anzeigt, dann bezeichnet die darauf folgende Nummer den Hauptsteckplatz eines Mehrfach-Steckplatz-Servers.

Tabelle 9-11. Servermodule *(fortgesetzt)*

Element	Beschreibung
Tatsächlicher Verbrauch (Wechselstrom)	Echtzeit-Messung des tatsächlichen Stromverbrauchs des Servers. Die Messung ist in Watt angegeben.
Startzeit kumulativer Strom	Echtzeitmessung des kumulativen Stroms, den der Server seit der Zeitangabe im Feld **Startzeit** verbraucht hat. Die Messung wird in Kilowattstunden (kWh) angegeben.
Spitzenverbrauch-Zeitstempel	Zeigt den Spitzenstromverbrauch des Servers an, der zu einem bestimmten Zeitpunkt aufgetreten ist. Die Zeit, zu der der Spitzenstromverbrauch aufgetreten ist, wird im **Zeitstempel-**Feld angegeben. Die Messung wird in Watt angezeigt.

Strombudgetstatus anzeigen

Der CMC enthält auf der Seite **Strombudgetstatus** Übersichten zum Stromstatus der Stromsubsysteme.

Webschnittstelle verwenden

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, müssen Sie die Berechtigung als **Gehäusekonfigurations-Administrator** besitzen.

So zeigen Sie den Strombudgetstatus mithilfe der Webschnittstelle an:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf **Gehäuse-Übersicht**.
3. Klicken Sie auf **Strom→ Budgetstatus**.

   Die Seite **Strombudgetstatus** wird angezeigt.

Tabelle 9-12 bis Tabelle 9-15 beschreiben die auf der Seite **Strombudgetstatus** angezeigten Informationen.

Weitere Informationen zur Konfiguration der Einstellungen für diese Daten finden Sie unter „Konfiguration von Stromversorgungsbudget und Redundanz“ auf Seite 401.

RACADM verwenden

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

```
racadm getpbinfo
```

Lesen Sie für weitere Informationen über **getpbinfo,** einschließlich der Ausgabedetails, den Abschnitt zum **getpbinfo-**Befehl im *RACADM Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*.

Tabelle 9-12. Regelkonfiguration des Systemstroms

Element	Beschreibung
Systemeingangs-stromobergrenze	Zeigt die benutzerdefinierte Grenze für den maximalen Stromverbrauch des gesamten Systems an (Gehäuse, CMC, Server, E/A-Module, Netzteileinheiten, iKVM und Lüfter). Der CMC wird diese Grenze über reduzierte Serverstromzuweisungen oder durch Abschalten von Servermodulen mit niedrigerer Priorität, einhal-ten. Der Wert für die Systemeingangsstromobergrenze wird in Watt, BTU/h und Prozent angezeigt. Übersteigt der Stromverbrauch des Gehäuses die **Systemeingangsstromobergrenze**, wird die Leistung der Server mit niedrigerer Priorität soweit reduziert, dass der Gesamtstromverbrauch unter die Grenze fällt. In Fällen, in denen die Server auf die **gleiche** Priorität gesetzt sind, basiert die Auswahl der Server zur Stromreduktion oder Abschaltung auf der Reihenfolge der Steckplatznummern. So wird beispielsweise der Server in Steckplatz 1 zuerst und der Server in Steckplatz 16 zuletzt ausgewählt.

Tabelle 9-12. Regelkonfiguration des Systemstroms *(fortgesetzt)*

Element	Beschreibung
Redundanzregel	Zeigt die aktuelle Redundanzkonfiguration an: **Wechselstromredundanz**, **Netzteilredundanz** oder **Keine Redundanz**. **Wechselstromredundanz** – die Stromaufnahme wird entsprechend der Last über alle Netzteileinheiten verteilt. Die Hälfte der Netzteileinheiten sollte mit einem Wechselstromnetz verkabelt sein und die andere Hälfte mit einem anderen Stromnetz. Wenn das System im Modus „Wechselstromredun-danz“ optimal läuft, wird die Leistung auf alle aktiven Netzteile verteilt. In dem Fall, dass ein Stromnetz ausfällt, übernehmen die Netzteileinheiten des funktionierenden Wechselstromnetzes ohne Unterbrechung. **Netzteilredundanz** – Die Netzteileinheit mit der höchsten Kapazität im Gehäuse verbleibt als Reserve, sodass ein Ausfall einer der Netzteileinheiten nicht dazu führt, dass die Servermodule oder das Gehäuse herunterfahren. **Netzteilredundanz** verwendet nicht unbedingt alle sechs Netzteileinheiten; sie verwendet genügend Netzteileinheiten, um sicherzustellen, dass im Falle eines Ausfalls einer Netzteileinheit, die verbleibenden Netzteileinheiten das Gehäuse weiter mit Strom versorgen können. Die anderen Netzteileinheiten können in den Standby-Modus gesetzt werden, wenn DPSE aktiviert ist. **Keine Redundanz** – Der Strom von allen aktiven Netzteileinheiten ist ausreichend, um das gesamte Gehäuse einschließlich Gehäuse, Servern, EAMs, iKVMs und CMC zu versorgen. Die verbleibenden Netzteileinheiten können in den Standby-Modus gesetzt werden, wenn DPSE aktiviert ist. **VORSICHTSHINWEIS: Der Modus Keine Redundanz verwendet nur die Mindestanzahl von Netzteileinheiten gleichzeitig, ohne Backup. Der Ausfall einer der verwendeten Netzteileinheiten kann dazu führen, dass die Servermodule nicht mit Strom versorgt werden und Daten verloren gehen.**

Tabelle 9-12. Regelkonfiguration des Systemstroms *(fortgesetzt)*

Element	Beschreibung
Dynamische Netzteilzuschaltung	Zeigt an, ob die **Dynamische Zuschaltung von Netzteilen** aktiviert oder deaktiviert ist. Wenn diese Funktion aktiviert ist, kann der CMC ungenügend genutzte Netzteileinheiten anhand der festgelegten Redundanzregel und der Stromanforderungen des Systems in den Standby-Modus setzen. Werden ungenügend genutzte Netzteileinheiten in den Standby-Modus gesetzt, erhöht sich die Nutzung und der Wirkungsgrad der angeschlossenen Netzteileinheiten, wodurch Strom eingespart wird.

Tabelle 9-13. Energiebudgetierung

Element	Beschreibung
Maximale Eingangsstromkapazität des Systems	Der maximale Eingangsstrom, der dem System von den verfügbaren Netzteilen zur Verfügung gestellt werden kann (in Watt).
Eingangsredundanzreserve	Zeigt die redundante Strommenge (in Watt) in Reserve an, die im Falle eines Ausfalls des Wechselstromnetzes oder der Netzteileinheit zur Verfügung steht. Wenn das Gehäuse so konfiguriert ist, dass es im Modus **Wechselstromredundanz** ausgeführt wird, entspricht die **Eingangsleistungsredundanzreserve** der Reserve-strommenge, die bei einem Ausfall eines Wechselstromnetzes zur Verfügung steht. Wenn das Gehäuse so konfiguriert ist, dass es im Modus **Netzteilredundanz** betrieben wird, entspricht die Angabe unter **Eingangsleistungsredundanzreserve** der Reservestrommenge, die im Falle eines Ausfalls einer Netzteileinheit zur Verfügung steht.
Serverzugewiesene Eingangsleistung	Zeigt (in Watt) die kumulative Eingangsleistung an, die der CMC auf der Basis der Konfiguration den Servern zuweist.
Gehäuseinfrastruktur-zugewiesene Eingangsleistung	Zeigt (in Watt) die kumulative Eingangsleistung, die der CMC der Gehäuseinfrastruktur (Lüfter, E/A-Module, iKVM, CMC, Standby-CMC und iDRAC auf den Servern) zuweist.

Tabelle 9-13. Energiebudgetierung *(fortgesetzt)*

Element	Beschreibung
Gesamter, für die Zuteilung verfügbarer, Eingangsstrom	Zeigt die gesamte Gehäuseleistung in Watt an, die noch zugeteilt werden kann.
Standby-Eingangsstromkapazität	Zeigt die Menge des Standby-Eingangsstroms (in Watt) an, die im Falle eines Netzteilfehlers oder der Entfernung eines Netzteils aus dem System, zur Verfügung steht. Dieses Feld zeigt Werte an, wenn das System mehrere Netzteile aufweist und die dynamische Netzteilzuschaltung (DPSE) aktiviert ist. **ANMERKUNG:** Es ist möglich, dass eine Netzteileinheit im Standby-Modus angezeigt wird, ohne dass sie den Wert der Standby-Eingangsstromkapazität erhöht. In diesem Fall trägt die Stromleistung dieser Netzteileinheit zum **Gesamten, für die Zuteilung verfügbaren, Eingangsstrom** bei.

Tabelle 9-14. Servermodule

Element	Beschreibung
Steckplatz	Zeigt die Position des Servermoduls an. Die **Steckplatznummer** ist eine sequenzielle Nummer (1-16), die das Servermodul nach seiner Position im Gehäuse identifiziert.
Name	Zeigt den Servernamen an. Der Servername wird vom Benutzer festgelegt.
Typ	Zeigt den Typ des Servers an.

Tabelle 9-14. Servermodule *(fortgesetzt)*

Element	Beschreibung
Priorität	Zeigt die Prioritätsstufe an, die dem Serversteckplatz im Gehäuse zur Strombudgetierung zugewiesen ist. Der CMC verwendet diesen Wert in seinen Berechnungen, wenn Strom basierend auf benutzerdefinierten Stromgrenzen oder auf Netzteil- oder Stromnetzausfällen reduziert oder neu zugeteilt werden muss. **Prioritätsstufen**: 1 (höchste) bis 9 (niedrigste) Standardeinstellung: **1** **ANMERKUNG:** Die Prioritätsstufe des Serversteckplatzes wird dem Serversteckplatz zugewiesen, nicht dem im Steckplatz eingesetzten Server. Wenn Sie einen Server in einen anderen Steckplatz im Gehäuse oder in ein anderes Gehäuse einsetzen, bestimmt die zuvor dem neuen Steckplatz zugewiesene Priorität die Priorität des neu eingesetzten Servers.
Stromzustand	Zeigt den Stromzustand des Servers: • Der CMC hat den Stromzustand des Servers nicht bestimmt. • **AUS**: Sowohl Gehäuse als auch Server sind ausgeschaltet. • **EIN**: Sowohl Gehäuse als auch Server sind eingeschaltet. • **Einschalten**: Vorrübergehender Zustand zwischen AUS und EIN. Ist der Einschaltvorgang abgeschlossen ändert sich der Stromzustand zu EIN. • **Abschalten**: Vorrübergehender Zustand zwischen EIN und AUS. Ist der Abschaltvorgang abgeschlossen ändert sich der Stromzustand zu AUS.
Budgetzuweisung - Tatsächlich	Zeigt die Strombudgetzuweisung für die Servermodule an. • **Tatsächlich:** Aktuelle Strombudgetzuweisung für jeden Server.

Tabelle 9-15. Gehäuse-Netzteile

Element	Beschreibung
Name	Zeigt den Namen der Netzteileinheit im Format NT-*n* an, wobei *n* die Nummer der Netzteileinheit ist.
Stromzustand	Zeigt den Stromzustand des Netzteils an – **Initialisieren**, **Online**, **Standby**, **Diagnose**, **Fehlerhaft**, **Unbekannt** oder **Nicht vorhanden** (fehlend).
Eingangsspannung	Zeigt die derzeitige Eingangsspannung des Netzteils an.
Eingangsstrom	Zeigt die derzeitige Eingangsstromstärke des Netzteils an.
Ausgangsnennleistung	Zeigt die maximale Ausgangsnennleistung des Netzteils an.

Konfiguration von Stromversorgungsbudget und Redundanz

Der Stromverwaltungsdienst des CMC optimiert den Stromverbrauch für das gesamte Gehäuse (Gehäuse, Server, E/A-Module, iKVM, CMC und Netzteileinheiten) und teilt den unterschiedlichen Modulen je nach Bedarf Strom neu zu.

Webschnittstelle verwenden

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, müssen Sie die Berechtigung als **Gehäusekonfigurations-Administrator** besitzen.

So konfigurieren Sie den Strombudgetstatus mithilfe der Webschnittstelle an:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf **Gehäuse-Übersicht**.
3. Klicken Sie auf **Strom→ Konfiguration**.

   Die Seite **Budget/Redundanzkonfiguration** wird angezeigt.
4. Legen Sie einige oder alle in Tabelle 9-16 beschriebenen Eigenschaften entsprechend Ihrer Bedürfnisse fest.
5. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

Um den Inhalt der Seite **Budget-/Redundanzkonfiguration** zu aktualisieren, klicken Sie auf **Aktualisieren**. Um den Inhalt auszudrucken, klicken Sie auf **Drucken**.

Tabelle 9-16. Konfigurierbare Strombudget-/Redundanzeigenschaften

Element	Beschreibung
Systemeingangs-stromobergrenze	Die Systemeingangsstromobergrenze ist der maximale Wechselstrom, den das System den Servern und der Gehäuseinfrastruktur zuweisen kann. Sie kann vom Benutzer auf einen beliebigen Wert gesetzt werden, der den Minimalstrombedarf der eingeschalteten Server und Gehäuseinfrastruktur **übersteigt**; Versuche einen Wert zu konfigurieren, der unter dem Minimalstrombedarf der Server und der Gehäuseinfrastruktur liegt, schlagen fehl. Den Wert für den der Server- und Gehäuseinfrastruktur zugewiesenen Strom finden Sie über die Benutzerschnittstelle auf der Statusseite **Gehäuse-Übersicht** → **Strom** → **Strombudget** im Abschnitt **Strombudgetierung** oder über das CLI RACADM-Dienstprogramm (`racadm getpbinfo`). Benutzer können einen oder mehrere Server ausschalten, um die aktuelle Stromzuweisung zu reduzieren und erneut versuchen, einen niedrigeren Wert für die **Systemeingangs-stromobergrenze** (falls gewünscht) einzustellen, oder die Obergrenze einfach vor dem Einschalten der Server festlegen. Um diese Einstellung zu ändern, kann ein Wert in einer beliebigen Einheit eingegeben werden. Die Schnittstelle sorgt dafür, dass das Einheitenfeld, das als letztes geändert wurde, der übermittelte Wert sein wird, wenn diese Änderungen angewendet werden. **ANMERKUNG:** Das Hilfsprogramm Datacenter Capacity Planner (DCCP) unter **www.dell.com/calc** enthält Informationen zur Kapazitätsplanung. **ANMERKUNG:** Wenn Wertänderungen in Watt angegeben werden, repräsentiert der übergebene Wert exakt, was angewendet wird. Werden die Änderungen jedoch entweder in BTU/h oder in Prozent übergeben, repräsentiert der übergebene Wert u. U. nicht exakt, was angewendet wird. Das liegt daran, dass diese Werte in Watt umgerechnet und dann angewandt werden; bei einer solchen Konvertierung können Rundungsfehler auftreten.

Tabelle 9-16. Konfigurierbare Strombudget-/Redundanzeigenschaften *(fortgesetzt)*

Element	Beschreibung
Redundanzregel	Diese Option ermöglicht das Auswählen folgender Möglichkeiten: • **Keine Redundanz**: Der Strom von den Netzteilen wird dazu verwendet, das gesamte Gehäuse einschließlich Gehäuse, Servern, EAMs, iKVM und CMC zu versorgen. Es müssen keine Netzteile in Reserve gehalten werden. **ANMERKUNG:** Der Modus **Keine Redundanz** verwendet nur die Mindestanzahl von Netzteilen gleichzeitig. Wenn die Mindestanzahl von Netzteileinheiten installiert ist, dann steht kein Backup zur Verfügung. Der Ausfall eines der drei verwendeten Netzteile kann dazu führen, dass den Servern der Strom ausgeht und/oder sie Daten verlieren. Falls mehr als die Mindestanzahl von Netzteileinheiten vorhanden ist, dann können die zusätzlichen Netzteileinheiten in den Standby-Modus gesetzt werden, um die Stromeffizienz zu verbessern, wenn DPSE aktiviert ist. • **Netzteilredundanz**: Die Kapazität des leistungsstärksten Netzteils im Gehäuse wird als Reserve bewahrt, um so sicherzustellen, dass ein Ausfall irgendeines Netzteils nicht zum Herunterfahren der Servermodule oder des Gehäuses führt (aktive Reserve). **Es kann sein, dass der Netzteilredundanz-Modus** nicht alle installierten Netzteile verwendet. Zusätzliche Netzteile können zur Verbesserung der Energieeffizienz in den Standby-Modus gesetzt werden, falls die dynamische Zuschaltung von Netzteileinheiten (DPSE) aktiviert ist. Der Modus **Netzteilredundanz** verhindert, dass Servermodule hochgefahren werden, wenn der Stromverbrauch des Gehäuses die Nennleistung übersteigt. Ein Ausfall von **zwei** Netzteilen in diesem Modus kann dazu führen, dass einige oder alle Servermodule im Gehäuse herunterfahren. Die Servermodulleistung wird in diesem Modus nicht herabgesetzt. • **Wechselstromredundanz**: Dieser Modus teilt die Netzteileinheiten in zwei Stromnetze auf (die Netzteileinheiten 1 - 3 bilden z. B. Stromnetz 1 und die Netzteileinheiten 4 - 6 bilden z. B. Stromnetz 2). Der Ausfall einer Netzteileinheit oder der Verlust von Wechselstrom an einem Stromnetz führt zum Status „Redundanzverlust“.

Tabelle 9-16. Konfigurierbare Strombudget-/Redundanzeigenschaften *(fortgesetzt)*

Element	Beschreibung
Serverleistung über Stromredundanz	Diese Option gibt der Serverleistung und dem Serverstart gegenüber der Aufrechterhaltung der Stromredundanz Vorrang. Lesen Sie für weitere Informationen über diese Funktion „Serverleistung über Stromredundanz“ auf Seite 379.
Aktivieren der Dynamische Netzteilzuschaltung	Aktiviert bei Auswahl die dynamische Stromverwaltung. Im Modus **Dynamische Netzteilzuschaltung** werden die Netzteile auf der Basis des Stromverbrauch **eingeschaltet** (Online) oder **ausgeschaltet** (Standby), um den Energieverbrauch des gesamten Gehäuses zu optimieren. Sie haben beispielsweise ein Strombudget von 5000 Watt, Ihre Redundanzregeln sind auf Wechselstromredundanz konfiguriert und Sie haben sechs Netzteileinheiten im Einsatz. Der CMC legt fest, dass vier Netzteileinheiten die Wechselstromredundanz leisten und die anderen beiden im Standby-Modus bleiben. Wenn beispielsweise zusätzliche 2000 W Strom für neu installierte Server benötigt wird, oder wenn die Energieeffizienz der bestehenden Systemkonfiguration verbessert werden muss, dann werden die zwei Standby-Netzteileinheiten in Betrieb genommen.
Netzschalter des Gehäuses deaktivieren	Deaktiviert bei Auswahl den Netzschalter des Gehäuses. Wenn das Kontrollkästchen ausgewählt ist und Sie versuchen, den Stromstatus des Gehäuses über den Gehäusenetzschalter zu ändern, wird die Maßnahme ignoriert.
Erlaubt den 110 V Wechselstrombetrieb	Erlaubt bei Auswahl Normalbetrieb, wenn Netzteileinheiten an 110 V Wechselstromversorgung angeschlossen sind. Weitere Informationen finden Sie unter „110 V Betrieb von Netzteileinheiten“ auf Seite 378.
Maximaler Stromsparmodus	Geht bei Auswahl sofort in den maximalen Stromsparmodus über. Weitere Informationen finden Sie unter „Stromspar- und maximaler Sparmodus“ auf Seite 377.

RACADM verwenden

So aktivieren Sie die Redundanz und legen die Redundanzregel fest:

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, müssen Sie die Berechtigung als **Gehäusekonfigurations-Administrator** besitzen.

1. Öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC und melden Sie sich an.
2. Legen Sie die Eigenschaften nach Bedarf fest:
   - Um eine Redundanzregel auszuwählen, geben Sie Folgendes ein:

     ```
     racadm config -g cfgChassisPower -o
     cfgChassisRedundancyPolicy <value>
     ```

     wobei der <*Wert*> **0** für „Keine Redundanz“, 1 für „Wechselstromredundanz“ und **2** für „Netzteilredundanz“ steht. Die Standardeinstellung ist 0.

     Zum Beispiel legt der folgende Befehl:

     ```
     racadm config -g cfgChassisPower -o
     cfgChassisRedundancyPolicy 1
     ```

     die Redundanzregel auf 1 fest.

   - Um die dynamische Zuschaltung von Netzteileinheiten zu aktivieren oder deaktivieren, geben Sie Folgendes ein:

     ```
     racadm config -g cfgChassisPower -o
     cfgChassisDynamicPSUEngagementEnable <value>
     ```

     wobei der <*Wert*> **0** für „Deaktivieren“ und 1 für „Aktivieren“ steht. Die Standardeinstellung ist 0.

     Zum Beispiel legt der folgende Befehl:

     ```
     racadm config -g cfgChassisPower -o
     cfgChassisDynamicPSUEngagementEnable 0
     ```

     die dynamische Zuschaltung von Netzteileinheiten fest.

Weitere Informationen zu den RACADM-Befehlen für die Gehäusestromversorgung finden Sie in den Abschnitten **config**, **getconfig**, **getpbinfo** und **cfgChassisPower** im *RACADM Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC*.

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.

Webschnittstelle verwenden

So weisen Sie Prioritätsstufen unter Verwendung der CMC-Webschnittstelle zu:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur **Gehäuse-Übersicht** aus. Die Seite **Status der Server** wird angezeigt.
3. Klicken Sie auf **Strom→ Serverpriorität**.

   Die Seite **Serverpriorität** wird angezeigt. Hier sind alle Server in Ihrem Gehäuse aufgeführt.
4. Wählen Sie 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.
5. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

RACADM verwenden

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 cfgServerPriority -i
<slot number> <priority level>
```

wobei sich <*Steckplatznummer*> (1-16) auf die Position des Servers bezieht und der Wert für die <*Prioritätsstufe*> zwischen 1 und 9 liegt.

Zum Beispiel legt der folgende Befehl:

```
racadm config -g cfgServerInfo -o cfgServerPriority -i 5 1
```

die Prioritätsstufe 1 für den Server in Steckplatz 5 fest.

Strombudget einrichten

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, müssen Sie die Berechtigung als **Gehäusekonfigurations-Administrator** besitzen.

Webschnittstelle verwenden

So legen Sie das Strombudget unter Verwendung der CMC-Webschnittstelle fest:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf **Gehäuseübersicht**. Die Seite **Gehäuse-Funktionszustand** wird angezeigt.
3. Klicken Sie auf die Registerkarte **Strom**. Die Seite **Stromverbrauchsstatus** wird angezeigt.
4. Klicken Sie auf das Unterregister **Konfiguration**.

   Die Seite **Budget/Redundanzkonfiguration** wird angezeigt.
5. Geben Sie einen Budgetwert von bis zu 11637 Watt in das Textfeld **Systemeingangsstromobergrenze** ein.

   ANMERKUNG: Das Strombudget ist auf einen Maximalwert begrenzt, der anhand des jeweils schwächsten Satzes von drei Netzteileinheiten bestimmt wird. Wenn Sie versuchen, einen Wechselstrombudgetwert festzulegen, der diesen Wert überschreitet, zeigt der CMC eine Fehlermeldung an.

   ANMERKUNG: Wenn Wertänderungen in Watt angegeben werden, repräsentiert der übergebene Wert exakt, was angewendet wird. Werden die Änderungen jedoch entweder in BTU/h oder in Prozent übergeben, repräsentiert der übergebene Wert u. U. nicht exakt, was angewendet wird. Das liegt daran, dass diese Werte in Watt umgerechnet und dann angewandt werden; bei einer solchen Konvertierung können Rundungsfehler auftreten.
6. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

RACADM verwenden

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

```
racadm config -g cfgChassisPower -o
cfgChassisPowerCap <value>
```

wobei <*Wert*> eine Zahl zwischen 2715 und 11637 ist und die maximale Stromgrenze in Watt angibt. Die Standardeinstellung ist 16685.

Zum Beispiel legt der folgende Befehl:

```
racadm config -g cfgChassisPower -o
cfgChassisPowerCap 5400
```

das maximale Strombudget mit 5400 Watt fest.

ANMERKUNG: Das Strombudget ist auf 16685 Watt begrenzt. Wenn versucht wird, einen Wechselstrombudgetwert festzulegen, der die Stromleistungskapazität des Gehäuses überschreitet, zeigt das CMC-Modul eine Fehlermeldung an.

Herabsetzen des Serverstroms zur Einhaltung des Strombudgets

Der CMC reduziert Stromzuteilungen von Servern mit niedriger Priorität, wenn zusätzlicher Strom benötigt wird, 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** (siehe „Strombudget einrichten“ auf Seite 407).
- Ein Stromausfall tritt in einer nicht-redundanten Konfiguration auf.

Informationen zur Zuweisung von Prioritäten zum Server finden Sie unter „Durchführen von Energieverwaltungsmaßnahmen am Gehäuse“ auf Seite 409.

Durchführen von Energieverwaltungsmaßnahmen am Gehäuse

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, müssen Sie die Berechtigung als **Gehäusekonfigurations-Administrator** besitzen.

ANMERKUNG: Stromsteuerungsvorgänge wirken sich auf das gesamte Gehäuse aus. Anleitungen zu Energieverwaltungsmaßnahmen an einem EAM finden Sie unter „Stromsteuerungsvorgänge für ein E/A-Modul ausführen" auf Seite 411. Anleitungen zu Energieverwaltungsmaßnahmen an Servern finden Sie unter „Durchführen von Energieverwaltungsmaßnahmen an einem Server" auf Seite 412.

Mit dem CMC können Sie im Remote-Zugriff verschiedene Stromverwaltungsmaßnahmen auf dem gesamten Gehäuse (Gehäuse, Server, E/A-Module, iKVM und Netzteileinheiten) ausführen, z. B. ordnungsgemäßes Herunterfahren.

Webschnittstelle verwenden

So führen Sie auf dem Gehäuse Stromsteuerungsvorgänge unter Verwendung der CMC-Webschnittstelle durch:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf **Gehäuse-Übersicht**.
3. Klicken Sie auf die Registerkarte **Strom**.

   Die Seite **Stromverbrauchsstatus** wird angezeigt.
4. Klicken Sie auf das Unterregister **Steuerung**. Die Seite **Gehäuse-Stromsteuerung** wird angezeigt.
5. Klicken Sie auf die entsprechende Optionsschaltfläche, um eine der folgenden **Stromsteuerungsvorgänge** auszuwählen:
   - **System einschalten** – Schaltet den Systemstrom ein (entspricht dem Drücken des Netzschalters, wenn der Systemstrom **ausgeschaltet** ist). Diese Option ist deaktiviert, wenn das Gehäuse bereits **eingeschaltet** ist.

     ANMERKUNG: Diese Maßnahme schaltet das Gehäuse und andere Untersysteme ein (iDRAC auf den Servern, EAMs und iKVM). Die Server werden nicht eingeschaltet.
   - **System ausschalten** - Schaltet den Systemstrom aus. Diese Option ist deaktiviert, wenn das Gehäuse bereits **ausgeschaltet** ist.

ANMERKUNG: Diese Maßnahme schaltet den Systemstrom aus (Gehäuse, Server, EAMs, iKVM und Netzteile). Der CMC bleibt eingeschaltet, befindet sich aber im Standby-Modus; ein Netzteil und Lüfter liefern Kühlung für den CMC in diesem Zustand. Das Netzteil liefert auch den mit niedriger Geschwindigkeit laufenden Lüftern Strom.

- **System aus- und einschalten (Hardwareneustart)** - Schaltet den Server aus und startet ihn daraufhin neu. Diese Option ist deaktiviert, wenn das Gehäuse bereits **ausgeschaltet** ist.

ANMERKUNG: Diese Maßnahme schaltet des gesamte System aus und startet anschließend neu (Gehäuse, dauerhaft eingeschaltete Server, EAMs, iKVM und Netzteile).

- **CMC zurücksetzen** - Setzt den CMC zurück, ohne diesen auszuschalten (Softwareneustart). (Diese Option ist deaktiviert, wenn der CMC bereits ausgeschaltet ist.)

ANMERKUNG: Diese Maßnahme setzt nur den CMC zurück. Es sind keine anderen Komponenten betroffen.

- **Nicht-ordnungsgemäßes Herunterfahren** - Diese Maßnahme erzwingt ein nicht-ordnungsgemäßes Herunterfahren des gesamten Systems (Gehäuse, Server, EAMs, iKVM und Netzteile). Es wird nicht versucht, das Betriebssystem ordnungsgemäß herunterzufahren, bevor die Server ausgeschaltet werden.

6. Klicken Sie auf **Anwenden**. Daraufhin werden Sie über ein Dialogfeld zur Bestätigung des Vorgangs aufgefordert.
7. Klicken Sie auf **OK**, um die Stromverwaltungsmaßnahme durchzuführen (z. B. das System zurücksetzen).

RACADM verwenden

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

```
racadm chassisaction -m chassis <action>
```

wobei `<action>` `powerup`, `powerdown`, `powercycle`, `nongraceshutdown` oder `reset` ist.

Stromsteuerungsvorgänge für ein E/A-Modul ausführen

Sie können im Remote-Zugriff ein einzelnes E/A-Modul zurücksetzen oder ein- und ausschalten.

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, müssen Sie die Berechtigung als **Gehäusekonfigurations-Administrator** besitzen.

Webschnittstelle verwenden

So führen Sie auf einem EAM Stromsteuerungsvorgänge unter Verwendung der CMC-Webschnittstelle durch:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie die Option **E/A-Module-Übersicht** aus.

   Die Seite **E/A-Modulstatus** wird angezeigt.
3. Klicken Sie auf die Registerkarte **Strom**.

   Die Seite **Stromsteuerung** wird angezeigt.
4. Wählen Sie den Vorgang, den Sie ausführen möchten (**Zurücksetzen** oder **Aus- und einschalten**), aus dem Drop-Down-Menü neben dem in der Liste aufgeführten E/A-Modul aus.
5. Klicken Sie auf **Anwenden**.

   Daraufhin werden Sie über ein Dialogfeld zur Bestätigung des Vorgangs aufgefordert.
6. Klicken Sie auf **OK**, um die Stromverwaltungsmaßnahme durchzuführen (z. B. um zu veranlassen, dass das E/A-Modul aus- und eingeschaltet wird).

RACADM verwenden

So führen Sie auf einem EAM Stromsteuerungsvorgänge unter Verwendung von RACADM durch:

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

```
racadm chassisaction -m switch-<n> <action>
```

wobei *<n>*, Ziffern 1 - 6, das EAM angeben (A1, A2, B1, B2, C1, V2) und *<Maßnahme>* den Vorgang anzeigt, den Sie ausführen möchten: `powercycle` oder `reset`.

Durchführen von Energieverwaltungsmaßnahmen an einem Server

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, müssen Sie die Berechtigung als **Gehäusekonfigurations-Administrator** besitzen.

Mit dem CMC können Sie im Remote-Zugriff verschiedene Stromverwaltungsmaßnahmen durchführen, z. B. das ordnungsgemäße Herunterfahren eines individuellen Servers im Gehäuse.

Webschnittstelle verwenden

So führen Sie auf einem Server Stromsteuerungsvorgänge unter Verwendung der Webschnittstelle durch:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Erweitern Sie den Eintrag **Server** in der Systemstruktur, und wählen Sie den Server aus, an dem Sie eine Energieverwaltungsmaßnahme durchführen möchten. Die Seite **Serverstatus** wird angezeigt.
3. Klicken Sie auf die Registerkarte **Strom**.

   Die Seite **Server-Stromverwaltung** wird angezeigt.
4. **Stromstatus** zeigt den Stromzustand des Servers (einer der Folgenden Zustände):
   - **k.A.** - Der CMC hat den Stromzustand des Servers noch nicht bestimmt.
   - **Aus** - Entweder der Server oder das Gehäuse sind ausgeschaltet.
   - **Ein** - Sowohl Gehäuse, als auch Server sind eingeschaltet.
   - **Einschalten** - vorübergehender Zustand zwischen Aus und Ein. Ist der Vorgang erfolgreich abgeschlossen, wird der **Stromzustand** auf **Ein** stehen.
   - **Ausschalten** - vorübergehender Zustand zwischen Ein und Aus. Ist der Vorgang erfolgreich abgeschlossen, wird der **Stromzustand** auf **Aus** stehen.

5 Wählen Sie eine der folgenden **Stromsteuerungsvorgänge** aus, indem Sie auf die Optionsschaltfläche klicken:

- **Server einschalten**- Schaltet den Serverstrom ein (entspricht dem Drücken des Netzschalters, wenn der Serverstrom ausgeschaltet ist). Diese Option ist deaktiviert, wenn der Server bereits eingeschaltet ist.
- **Server ausschalten** - Schaltet den Serverstrom aus (entspricht dem Drücken des Netzschalters, wenn der Serverstrom eingeschaltet ist).
- **Ordentliches Herunterfahren** - Schaltet den Server aus und startet ihn daraufhin neu.
- **System zurücksetzen (Softwareneustart)** - Startet den Server neu, ohne ihn auszuschalten. Diese Option ist deaktiviert, wenn der Server ausgeschaltet ist.
- **System aus- und einschalten (Hardwareneustart)** - Schaltet den Server aus und startet ihn daraufhin neu. Diese Option ist deaktiviert, wenn der Server ausgeschaltet ist.

6 Klicken Sie auf **Anwenden**. Daraufhin werden Sie über ein Dialogfeld zur Bestätigung des Vorgangs aufgefordert.

7 Klicken Sie auf **OK**, um die Stromverwaltungsmaßnahme durchzuführen (z. B. den Server zurückzusetzen).

ANMERKUNG: Alle Stromsteuerungsvorgänge können über die Seite **Server**→ **Strom**→ **Steuerung** auf mehreren Servern durchgeführt werden.

RACADM verwenden

So führen Sie auf einem Server Stromsteuerungsvorgänge unter Verwendung von RACADM durch:

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

```
racadm serveraction -m <module> <action>
```

wobei *<Modul>* den Server nach Steckplatznummer (1-16) im Gehäuse angibt und *<Maßnahme>* den Vorgang, den Sie ausführen möchten: `powerup`, `powerdown`, `powercycle`, `nongradeshutdown` oder `hardreset`.

110 V Betrieb

Einige der Netzteilmodelle können sowohl an einem 220 V Netz als auch an einem 110 V Netz betrieben werden. 110 V Strom kann eingeschränkte Kapazität aufweisen. Wenn demnach ein 110 V Anschluss erkannt wird, dann gewährt das Gehäuse keine zusätzlichen Serverstromanfragen, bis der Benutzer den 110 V Betrieb bestätigt hat, indem er die Stromkonfigurationseigenschaften ändert. Der Benutzer muss vor der Bestätigung überprüfen, ob der verwendete 110 V Stromkreis die für die Gehäusekonfiguration erforderliche Stromleistung liefern kann. Nach der Bestätigung gewährt das Gehäuse alle künftigen angemessenen Serverstromanfragen und verwendet die gesamte verfügbare Stromversorgungskapazität.

Der Benutzer kann die 110 V Bestätigung über die GUI oder RACADM jederzeit nach der anfänglichen Installation zurücksetzen. Stromversorgungseinträge werden im SEL-Protokoll protokolliert, wenn 110 V Netzteile ermittelt werden und wenn 110 V Netzteile entfernt werden. Einträge werden auch im SEL-Protokoll protokolliert, wenn diese vom Benutzer bestätigt werden oder die Bestätigung aufgehoben wird.

Der Gesamt-Stromfunktionszustand ist mindestens im Status „Nicht Kritisch“, wenn das Gehäuse im 110 V Modus betrieben wird und der Benutzer den 110 V Betrieb nicht bestätigt hat. Das Symbol „Warnung“ wird auf der Hauptseite des GUI angezeigt , wenn der Zustand „Nicht-kritisch“ ist.

Ein Mischbetrieb bei 110 V und 220 V wird 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.

Externe Energieverwaltung

Die CMC-Energieverwaltung wird optional über die Konsole zum Messen, Verteilen und Steuern (PM3) steuern. Weitere Informationen finden Sie im Symantec-Benutzerhandbuch.

Wenn eine externe Energieverwaltung aktiviert ist, verwaltet PM3 die folgenden Aktivitäten:

- Server-Stromversorgung für Server der zwölften Generation
- Server-Priorität für Server der zwölften Generation
- Eingangsstromkapazität des Systems
- Maximalen Stromsparmodus

CMC setzt die Aufrechterhaltung oder Verwaltung der folgenden Aktivitäten fort:

- Redundanzregel
- Remote-Energieprotokollierung
- Serverleistung über Stromredundanz
- Dynamische Netzteilzuschaltung
- Stromversorgung für Server bis einschließlich zur elften Generation

PM3 verwaltet daraufhin die Priorisierung und die Stromversorgung für Blade-Server der zwölften Generation mithilfe des Budgets, das nach der Zuteilung der Energie auf die Gehäuseinfrastruktur und vor der Generierung von Blade-Servern zur Verfügung steht. Die Remote-Energieprotokollierung ist von der externen Energieverwaltung nicht betroffen.

Webschnittstelle verwenden

So aktivieren Sie die externe PM3-Verwaltung:

1. Melden Sie sich mit **Gehäuseadministratorrechten** am Mitgliedsgehäuse an.
2. Wählen Sie in der Systemstruktur **Gehäuse-Übersicht** aus.
3. Klicken Sie auf „Strom→ Konfiguration“.

   Die Seite Budget/Redundancy Configuration (Budget-/Redundanzkonfiguration) wird angezeigt.
4. Legen Sie den **serverbasierten Energieverwaltungsmodus** fest.
5. Klicken Sie auf Anwenden.

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.

So deaktivieren Sie die externe Energieverwaltung:

1. Melden Sie sich mit **Gehäuseadministratorrechten** am Mitgliedsgehäuse an.
2. Klicken Sie in der Systemstruktur auf **Gehäuse-Übersicht**.
3. Klicken Sie auf **Strom→ Konfiguration**.

   Die Seite **Budget/ Redundanz-Konfiguration** wird angezeigt.
4. Löschen Sie den **serverbasierten Energieverwaltungsmodus**.
5. Klicken Sie auf **Anwenden**.

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 zu der früheren Einstellung zur manuellen Wiederherstellung des Wertes finden Sie im **CMC-Protokoll**.

RACADM verwenden

Öffnen Sie eine serielle/Telnet-/SSH-Text-Konsole für CMC mit Berechtigungen als **Administrator für die Gehäusekonfiguration**.

Um die Remote-Energieverwaltung durch PM3 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
```

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 zurück. Weitere Informationen zur früheren Einstellung für die manuelle Wiederherstellung des Wertes finden Sie im **CMC-Protokoll**.

Fehlerbehebung

Weitere Informationen zur Fehlerbehebung bei Netzteilen und bei der Stromversorgung finden Sie unter „Fehlerbehebung und Wiederherstellung“ auf Seite 469.

10

iKVM-Modul verwenden

Übersicht

Der Name des Lokalzugriffs-KVM-Modul für das Dell M1000e-Servergehäuse lautet Avocent Integrated KVM Switch-Modul (iKVM). Das iKVM ist ein analoger Tastatur-, Video- und Maus-Switch, der in das Gehäuse eingesteckt wird. Es handelt sich um ein optionales, hotplug-fähiges Modul für das Gehäuse und bietet lokalen Tastatur-, Maus- und Videozugriff auf die Server im Gehäuse und auf die aktive Befehlszeile des CMC.

iKVM-Benutzeroberfläche

Das iKVM verwendet die graphische Benutzeroberfläche OSCAR (On Screen Configuration and Reporting), die über einen Hotkey aktiviert wird. Mit OSCAR können Sie einen Server oder die Dell CMC-Befehlszeile auswählen, sodass Sie über die lokale Tastatur oder Maus bzw. die lokale Anzeige zugreifen können.

Es ist nur eine iKVM-Sitzung pro Gehäuse zulässig.

Sicherheit

Die OSCAR-Benutzeroberfläche ermöglicht Ihnen, Ihr System mit einem Bildschirmschonerkennwort zu schützen. Nach einer benutzerdefinierten Zeit wird der Bildschirmschonermodus aktiviert und der Zugriff verhindert, bis das richtige Kennwort zum Reaktivieren von OSCAR eingegeben wird.

Suchen

Mit OSCAR können Sie eine Liste mit Servern auswählen, die in der ausgewählten Reihenfolge angezeigt werden, während sich OSCAR im Scan-Modus befindet.

Serveridentifikation

Der CMC weist allen Servern im Gehäuse Steckplatznamen zu. Obwohl Sie mit der OSCAR-Benutzerschnittstelle von einer Reihenverbindung aus den Servern Namen zuweisen können, haben die vom CMC zugewiesenen Namen Vorrang. Neue Namen, die Sie Servern mit OSCAR zuweisen, werden überschrieben.

Der CMC identifiziert einen Steckplatz, indem er ihm einen eindeutigen Namen zuweist. Weitere Informationen zum Ändern von Einschubnamen über die CMC-Webschnittstelle finden Sie unter „Steckplatznamen bearbeiten“. Informationen zum Ändern eines Einschubnamens mit RACADM finden Sie im Abschnitt **setslotname** im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC.*

Grafikkarte

Die iKVM-Videoverbindungen unterstützen Video-Bildschirmauflösungen von 640 x 480 bei 60 Hz bis zu 1280 x 1024 bei 60 Hz.

Plug-and-Play

Das iKVM unterstützt Plug-and-Play des Bildschirmdatenkanals (DDC), was die Videomonitorkonfiguration automatisiert und mit dem VESA DDC2B-Standard kompatibel ist.

FLASH-erweiterbar

Die iKVM-Firmware kann über die CMC-Webschnittstelle oder mit dem RACADM-Befehl **fwupdate** aktualisiert werden. Weitere Informationen finden Sie unter„iKVM vom CMC aus verwalten“ auf Seite 440.

Physische Verbindungsschnittstellen

Sie können eine Verbindung zu einem Server oder zur CMC-CLI-Konsole über das iKVM von der Frontblende des Gehäuses, von einer analogen Konsolenschnittstelle (ACI) und von der rückseitigen Abdeckung des Gehäuses aus herstellen.

ANMERKUNG: Die Anschlüsse auf dem Bedienfeld an der Vorderseite des Gehäuses wurden speziell für das iKVM konzipiert, das optional ist. Falls Sie das iKVM nicht haben, können Sie die Schnittstellen am vorderen Bedienfeld nicht verwenden.

iKVM-Verbindungsrangfolge

Es ist nur eine iKVM-Verbindung auf einmal verfügbar. Das iKVM weist jedem Verbindungstyp eine Rangfolge zu; wenn mehrere Verbindungen vorhanden sind, ist somit nur eine Verbindung verfügbar und die anderen sind deaktiviert.

Die Rangfolge für iKVM-Verbindungen lautet folgendermaßen:

1. Frontblende
2. ACI
3. Rückseitige Abdeckung

Wenn beispielsweise iKVM-Verbindungen an der Frontblende und ACI bestehen, bleibt die Frontblendenverbindung aktiv, während die ACI-Verbindung deaktiviert wird. Wenn ACI- und rückseitige Verbindungen bestehen, hat die ACI-Verbindung Vorrang.

Reihenabstufung über die ACI-Verbindung

Das iKVM lässt Reihenverbindungen mit Servern und der CMC-Befehlszeilenkonsole des iKVM zu, entweder lokal über einen Remote-Konsolen-Switch-Anschluss oder im Remote-Zugriff über die Dell RCS-Software. Das iKVM unterstützt ACI-Verbindungen von den folgenden Produkten aus:

- 180AS, 2160AS, 2161DS*, 2161DS-2 bzw. 4161DS Dell Remote Console Switches
- Avocent AutoView Switching-System
- Avocent DSR Switching-System
- Avocent AMX Switching-System

* Unterstützt die Dell CMC-Konsolenverbindung nicht.

ANMERKUNG: Das iKVM unterstützt auch eine ACI-Verbindung zum Dell 180ES und 2160ES, aber die Reihenabstufung ist nicht nahtlos. Diese Verbindung erfordert einen USB-zu-PS2-SIP.

OSCAR verwenden

In diesem Abschnitt erhalten Sie eine Übersicht über die OSCAR-Benutzeroberfläche.

Navigationsgrundlagen

Tabelle 10-1. OSCAR-Tastatur- und Mausnavigation

Taste oder Tastenfolge	Ergebnis
• <Druck>-<Druck> • <Umsch>-<Umsch> • <Alt>-<Alt> • <Strg>-<Strg>	OSCAR kann über jede dieser Tastenfolgen aufgerufen werden, abhängig von Ihren Einstellungen unter **OSCAR aufrufen**. Sie können zwei, drei oder alle dieser Tastenfolgen aktivieren, indem Sie das jeweilige Kontrollkästchen im Abschnitt **OSCAR aufrufen** des **Hauptdialogfeldes** auswählen und anschließend auf **OK** klicken.
<F1>	Öffnet den **Hilfe**-Bildschirm für das aktuelle Dialogfeld.
<Esc>	Schließt das aktuelle Dialogfeld, ohne die Änderungen zu speichern, und kehrt zum vorhergehenden Dialogfeld zurück. Im **Hauptdialogfeld** schließt die Taste <Esc> die OSCAR-Benutzeroberfläche und kehrt zum ausgewählten Server zurück. In einem Meldungsfenster wird damit das Popup-Fenster geschlossen und zum aktuellen Dialogfeld zurückgekehrt.
<Alt>	Öffnet Dialogfelder, wählt bzw. aktiviert Optionen und führt Maßnahmen aus, wenn in Verbindung mit unterstrichenen Buchstaben oder gekennzeichneten Zeichen verwendet.
<Alt>+<X>	Schließt das aktuelle Dialogfeld und kehrt zum vorhergehenden Dialogfeld zurück.
<Alt>+<O>	Wählt die **OK**-Schaltfläche aus und kehrt zum vorhergehenden Dialogfeld zurück.
<Eingabe>	Führt einen Umschaltvorgang im **Hauptdialogfeld** durch und beendet OSCAR.

Tabelle 10-1. OSCAR-Tastatur- und Mausnavigation *(fortgesetzt)*

Taste oder Tastenfolge	Ergebnis
Einfaches Klicken, <Eingabe>	In einem Textfeld: wählt den Text zum Bearbeiten aus und aktiviert die Tasten „Nach links“ und „Nach rechts“, um den Cursor zu bewegen. Drücken Sie erneut <Eingabe>, um den Bearbeitungsmodus zu beenden.
<Druck>, <Rücktaste>	Wechselt zur vorhergehenden Auswahl zurück, wenn keine weiteren Tasten betätigt wurden.
<Druck>, <Alt>+<0>	Trennt umgehend die Verbindung eines Benutzers zu einem Server; es ist kein Server ausgewählt. Status-Flag zeigt „Frei“ an. (Diese Maßnahme gilt nur für =<0> auf der Tastatur und nicht auf dem numerischen Tastenblock.)
<Druck>, <Pause>	Schaltet umgehend den Bildschirmschonermodus ein und verhindert den Zugriff auf die spezifische Konsole, falls sie kennwortgeschützt ist.
Tasten „Nach oben“/„Nach unten“	Bewegt den Cursor in Listen von Zeile zu Zeile.
Tasten „Nach rechts“/„Nach links“	Bewegt den Cursor beim Bearbeiten eines Textfeldes innerhalb der Spalten.
<Pos1>/<Ende>	Bewegt den Cursor ganz nach oben (Pos1) oder unten (Ende) in einer Liste.
<Entf>	Löscht Zeichen in einem Textfeld.
Nummerntasten	Eingabe über die Tastatur oder den numerischen Tastenblock.
<Feststelltaste>	Deaktiviert. Verwenden Sie zum Ändern der Groß-/Kleinschreibung die <Umsch>-Taste.

OSCAR konfigurieren

Tabelle 10-2. OSCAR-Setup-Menüfunktionen

Funktion	Zweck
Menü	Ändert die Serverauflistung zwischen numerisch nach Steckplatz und alphabetisch nach Name.
Sicherheit	• Legt ein Kennwort fest, um den Zugriff auf Server einzuschränken. • Aktiviert einen Bildschirmschoner und legt eine Inaktivitätszeit fest, bevor der Bildschirmschoner aufgerufen und der Bildschirmschonermodus aktiviert wird.
Flag	Ändert Anzeige, Zeitmessung, Farbe oder Standort des Status-Flags.
Sprache	Ändert die Sprache aller OSCAR-Bildschirme.
Broadcast	Richtet die gleichzeitige Steuerung mehrerer Server mittels Tastatur- und Mausmaßnahmen ein.
Suchen	Richtet ein benutzerdefiniertes Suchmuster für bis zu 16 Server ein.

So rufen Sie das **Setup-Dialogfeld** auf:

1. Drücken Sie die Taste <Druck>, um die OSCAR-Benutzerschnittstelle aufzurufen. Das **Hauptdialogfeld** wird geöffnet.
2. Klicken Sie auf **Setup**. Das **Setup**-Dialogfeld wird aufgerufen.

Anzeigeverhalten ändern

Ändern Sie im **Menü**-Dialogfeld die Anzeigereihenfolge von Servern, und legen Sie eine Bildschirmverzögerungszeit für OSCAR fest.

So rufen Sie das **Menü-Dialogfeld** auf:

1. Drücken Sie <Druck>, um OSCAR zu starten. Das **Hauptdialogfeld** wird geöffnet.
2. Klicken Sie auf **Setup** und anschließend auf **Menü**. Das Dialogfeld **Menü** wird geöffnet.

So wählen Sie die standardmäßige Anzeigereihenfolge von Servern im **Hauptdialogfeld** aus:

1. Wählen Sie **Name** aus, um die Server alphabetisch nach Namen sortiert anzuzeigen.

   oder

   Markieren Sie die Option **Steckplatz**, um die Server nach Steckplatznummer anzuzeigen.

2. Klicken Sie auf **OK**.

So weisen Sie eine oder mehrere Tastenfolgen für die OSCAR-Aktivierung zu:

Wählen Sie eine Tastenfolge aus dem Menü **OSCAR-Aktivierung** aus und klicken Sie auf **OK**.

Die Standardtaste zum Aktivieren von OSCAR ist <Druck>.

So legen Sie eine Anzeigeverzögerungszeit für OSCAR fest:

1. Geben Sie die Anzahl der Sekunden ein (0 bis 9), mit der die Anzeige von OSCAR verzögert werden soll, nachdem Sie auf <Druck> gedrückt haben.

   Bei der Eingabe von <0> wird OSCAR ohne Verzögerung gestartet.

2. Klicken Sie auf **OK**.

Das Festlegen einer Verzögerungszeit für die Anzeige von OSCAR ermöglicht Ihnen, einen Soft-Switch durchzuführen. Informationen zum Umschalten mit Soft-Switching finden Sie unter „Soft-Switch ausführen“ auf Seite 430.

Status-Flag steuern

Das Status-Flag erscheint auf Ihrem Desktop und zeigt den Namen des ausgewählten Servers bzw. den Status des ausgewählten Steckplatzes an. Konfigurieren Sie mit dem Dialogfeld **Flag** das Flag, um nach Server anzuzeigen oder Flag-Farbe, -Transparenz, -Anzeigezeit und -Standort auf dem Desktop zu ändern.

Tabelle 10-3. OSCAR-Status-Flags

Flag	Beschreibung
	Flag-Typ nach Name
	Flag, das angibt, dass die Verbindung des Benutzers bei allen Systemen abgebrochen wurde
	Flag, das angibt, dass der Broadcast-Modus aktiviert ist

So rufen Sie das **Flag-Dialogfeld** auf:

1. Drücken Sie die Taste <Druck>. Das **Hauptdialogfeld** wird geöffnet.
2. Klicken Sie auf **Setup** und anschließend auf **Flag**. Das Dialogfeld **Flag** wird aufgerufen.

So legen Sie fest, wie das Status-Flag angezeigt wird:

1. Wählen Sie **Angezeigt** aus, damit das Flag die ganze Zeit über angezeigt wird, oder **Angezeigt und zeitlich bestimmt**, um das Flag nur fünf Sekunden lang nach dem Umschalten einzublenden.

   ANMERKUNG: Wenn Sie **Zeitlich bestimmt** allein auswählen, wird das Flag nicht angezeigt.

2. Wählen Sie eine Flag-Farbe aus dem Abschnitt **Anzeigefarbe** aus. Es stehen Schwarz, Rot, Blau und Lila zur Auswahl.
3. Wählen Sie im **Anzeigemodus** die Option **Opak** für ein Flag in Volltobfarbe aus oder **Transparent**, damit der Desktop durch das Flag zu sehen ist.
4. So platzieren Sie das Status-Flag auf dem Desktop:
   a. Klicken Sie auf **Position festlegen.** Das Dialogfeld **Flag-Position festlegen** wird aufgerufen.
   b. Klicken Sie mit der linken Maustaste auf die Titelleiste und ziehen Sie sie an den gewünschten Speicherort auf dem Desktop.
   c. Klicken Sie mit der rechten Maustaste, um zum Dialogfeld **Flag** zurückzukehren.

ANMERKUNG: Änderungen an der Flag-Position werden erst gespeichert, wenn Sie im Dialogfeld **Flag** auf **OK** klicken.

5 Klicken Sie auf **OK**, um die Einstellungen zu speichern.

Um zu beenden, ohne zu speichern, klicken Sie auf ☒.

Server mit iKVM verwalten

Das iKVM ist eine analoge Switch-Matrix, die bis zu 16 Server unterstützt. Der iKVM-Switch verwendet die OSCAR-Benutzeroberfläche, um Server auszuwählen und zu konfigurieren. Zusätzlich umfasst das iKVM eine Systemeingabe, um eine CMC-Befehlszeilenkonsolenverbindung zum CMC herzustellen.

Peripheriegerätekompatibilität und -unterstützung

Das iKVM ist mit folgenden Peripheriegeräten kompatibel:

- Standardmäßige PC-USB-Tastaturen mit den Layouts QWERTY, QWERTZ, AZERTY und Japanisch 109.
- VGA-Monitore mit DDC-Unterstützung.
- Standardmäßige USB-Zeigegeräte.
- USB 1.1-Hubs mit eigener Stromversorgung, die am lokalen USB-Anschluss des iKVM angeschlossen sind.
- Mit Strom versorgte USB 2.0-Hubs, die an der Frontblendenkonsole des Dell M1000e-Gehäuses angeschlossen sind.

ANMERKUNG: Es können mehrere Tastaturen und Mäuse am lokalen iKVM-USB-Anschluss verwendet werden. Das iKVM aggregiert die Eingabesignale. Wenn gleichzeitige Eingabesignale von mehreren USB-Tastaturen oder -Mäusen auftreten, kann dies unvorhergesehene Ergebnisse zur Folge haben.

ANMERKUNG: Die USB-Verbindungen sind ausschließlich für unterstützte Tastaturen, Mäuse und USB-Hubs konzipiert. Das iKVM unterstützt keine Daten, die von anderen USB-Geräten übertragen wurden.

Anzeigen und Auswählen von Servern

Verwenden Sie das **Hauptdialogfeld** von OSCAR, um Server über das iKVM anzuzeigen, zu konfigurieren und zu verwalten. Sie können Ihre Server nach Name oder Steckplatz anzeigen. Die Steckplatznummer ist die Nummer des Gehäusesteckplatzes, in dem der Server installiert ist. Die Steckplatznummer eines installierten Servers wird in der Spalte **Slot** (Steckplatz) angezeigt.

ANMERKUNG: Die Dell CMC-Befehlszeile belegt Steckplatz 17. Beim Auswählen dieses Steckplatzes wird die CMC-Befehlszeile angezeigt, in der Sie RACADM-Befehle ausführen oder eine Verbindung zur seriellen Konsole von Servern oder E/A-Modulen herstellen können.

ANMERKUNG: Servernamen und Steckplatznummern werden vom CMC-Modul zugewiesen.

So öffnen Sie das Dialogfeld **Hauptdialog**:

Drücken Sie die Taste <Druck>, um die OSCAR-Benutzerschnittstelle aufzurufen. Das **Hauptdialogfeld** wird geöffnet.

oder

Wenn ein Kennwort zugewiesen ist, wird das Dialogfeld **Kennwort** angezeigt. Geben Sie das Kennwort ein und klicken Sie auf **OK**. Das **Hauptdialogfeld** wird geöffnet.

Weitere Informationen zum Definieren eines Kennwortes finden Sie unter „Konsolensicherheit einstellen“ auf Seite 432.

ANMERKUNG: Es gibt vier Optionen zum Aufrufen von OSCAR. Sie können eine oder alle dieser Tastenfolgen aktivieren, indem Sie das jeweilige Kontrollkästchen im Bereich **OSCAR aufrufen** des **Hauptdialogfeldes** auswählen und anschließend auf **OK** klicken.

Status der Server anzeigen

Der Status der Server im Gehäuse wird in den rechten Spalten des **Hauptdialogfeldes** angezeigt. In der folgenden Tabelle werden die Statussymbole beschrieben.

Tabelle 10-4. Statussymbole der OSCAR-Benutzeroberfläche

Symbole	Beschreibung
	(Grüner Punkt.) Server ist online.
	(Rotes X.) Server ist offline oder nicht im Gehäuse.
	(Gelber Punkt.) Server ist nicht verfügbar.
	(Grün A oder B.) Server wird über den Benutzerkanal genutzt, der mit den folgenden Buchstaben gekennzeichnet ist: A=

Server auswählen

Wählen Sie über das **Hauptdialogfeld** Server aus. Wenn Sie einen Server auswählen, konfiguriert das iKVM die Tastatur und Maus mit den ordnungsgemäßen Einstellungen für diesen Server neu.

- So wählen Sie Server aus:

  Doppelklicken Sie auf den Servernamen oder die Steckplatznummer.

  oder

  Wenn die Anzeigereihenfolge der Serverliste nach Steckplatz ist (d. h. die Schaltfläche **Steckplatz** ist aktiviert), geben Sie die Steckplatznummer ein und drücken Sie <Eingabe>.

  oder

  Wenn die Serverliste nach dem Namen sortiert ist (d. h. die Schaltfläche **Name** ist aktiviert), geben Sie die ersten Zeichen des Servernamens ein, machen den Sie den Eintrag eindeutig und drücken Sie zweimal <Eingabe>.

- So wählen Sie den vorhergehenden Server aus:

  Drücken Sie die Taste <Druck> und anschließend die <Rücktaste>. Mit dieser Tastenkombination wird zwischen der vorhergehenden und der aktuellen Verbindung umgeschaltet.

- So unterbrechen Sie die Verbindung eines Benutzers zu einem Server:

  Drücken Sie die Taste <Druck>, um OSCAR aufzurufen, und klicken Sie dann auf **Unterbrechen**.

  oder

  Drücken Sie die Taste <Druck> und anschließend <Alt><0>. Dadurch wird ein freier Zustand ohne ausgewählten Server bewahrt. Das Status-Flag auf dem Desktop (falls aktiv) zeigt „Frei“ an. Siehe „Status-Flag steuern“ auf Seite 425.

Soft-Switch ausführen

Bei einem Soft-Switch wird mittels einer Hotkey-Tastenfolge zwischen Servern umgeschaltet. Um per Soft-Switching zu einem Server zu wechseln, drücken Sie die Taste <Druck> und geben Sie die ersten Zeichen des Namens bzw. der Nummer des gewünschten Servers ein. Falls Sie zuvor eine **Verzögerungszeit** (die Anzahl der Sekunden, bevor das **Hauptdialogfeld** nach Drücken von <Druck> aufgerufen wird) festgelegt haben und die Tastenfolgen verwenden, bevor diese Zeit abgelaufen ist, wird die OSCAR-Benutzeroberfläche nicht angezeigt.

So konfigurieren Sie OSCAR für einen Soft-Switch:

1. Drücken Sie die Taste <Druck>, um die OSCAR-Benutzerschnittstelle aufzurufen. Das **Hauptdialogfeld** wird geöffnet.
2. Klicken Sie auf **Setup** und anschließend auf **Menü**. Das Dialogfeld **Menü** wird geöffnet.
3. Wählen Sie **Name** oder **Steckplatz** für die Anzeige-/Sortiertaste aus.
4. Geben Sie im Feld **Anzeigeverzögerungszeit** die gewünschte Verzögerungszeit (in Sekunden) ein.
5. Klicken Sie auf **OK**.

So führen Sie einen Soft-Switch zu einem Server aus:

- Um einen Server auszuwählen, drücken Sie die Taste <Druck>.

  Wenn die Anzeigereihenfolge der Serverliste gemäß Ihrer Auswahl in Schritt 3 nach Steckplatz sortiert ist (d. h. die Schaltfläche **Steckplatz** ist aktiviert), geben Sie die Steckplatznummer ein und drücken Sie <Eingabe>.

  oder

  Wenn die Serverliste gemäß Ihrer Auswahl in Schritt 3 nach Namen sortiert ist (d. h. die Schaltfläche **Name** ist aktiviert), geben Sie die ersten Zeichen des Servernamens ein, um ihn eindeutig zu machen und drücken Sie zweimal <Eingabe>.

- Um zum vorhergehenden Server zurückzuschalten, drücken Sie <Druck> und dann die <Rücktaste>.

Videoverbindungen

Das iKVM hat Videoanschlüsse an der Vorderseite und der rückseitigen Abdeckung des Gehäuses. Die Verbindungssignale an der Frontblende haben Vorrang vor denen der rückseitigen Abdeckung. Wenn ein Monitor an der Frontblende angeschlossen ist, geht die Videoverbindung nicht weiter an die rückseitige Abdeckung; es wird eine OSCAR-Meldung angezeigt, die angibt, dass die KVM- und ACI-Verbindungen der rückseitigen Abdeckung deaktiviert sind. Wenn der Monitor deaktiviert wird (d. h. er wird von der Frontblende entfernt oder durch einen CMC-Befehl deaktiviert), wird die ACI-Verbindung aktiv, während das KVM der rückseitigen Abdeckung deaktiviert bleibt. (Informationen über Verbindungsrangfolgen finden Sie unter „iKVM-Verbindungsrangfolge“.)

Informationen zum Aktivieren/Deaktivieren der Frontblendenanschlüsse finden Sie unter „Frontblende aktivieren oder deaktivieren“.

Verdrängungswarnung

Normalerweise hat sowohl ein Benutzer, der über das iKVM, als auch ein anderer Benutzer, der über die iDRAC-GUI-Konsolenumleitungsfunktion mit derselben Serverkonsole verbunden ist, Zugriff auf die Konsole, und beide können gleichzeitig Eingaben vornehmen.

Um dieses Szenario zu vermeiden, kann der Remote-Benutzer vor dem Starten der GUI-Konsolenumleitung die lokale Konsole in der iDRAC-Webschnittstelle deaktivieren. Der lokale iKVM-Benutzer erfährt durch die OSCAR-Meldung, dass die Verbindung in einer festgelegten Zeitspanne verdrängt wird. Der lokale Benutzer sollte seine Arbeit abschließen, bevor die iKVM-Verbindung zum Server abgebrochen wird.

Für den iKVM-Benutzer steht keine Verdrängungsfunktion zur Verfügung.

ANMERKUNG: Wenn ein Remote-iDRAC-Benutzer das lokale Video für einen bestimmten Server deaktiviert hat, sind das Video, die Tastatur und die Maus des Servers nicht für das iKVM verfügbar. Der Serverstatus ist mit einem gelben Punkt im OSCAR-Menü gekennzeichnet, um anzuzeigen, dass er für lokale Nutzung gesperrt bzw. nicht verfügbar ist (siehe „Status der Server anzeigen").

Konsolensicherheit einstellen

OSCAR ermöglicht Ihnen, Sicherheitseinstellungen auf der iKVM-Konsole zu konfigurieren. Sie können einen Bildschirmschonermodus einrichten, der aktiviert wird, wenn die Konsole für eine bestimmte Zeitspanne nicht genutzt wird. Nach dem Aktivieren bleibt die Konsole gesperrt, bis Sie eine beliebige Taste drücken oder die Maus bewegen. Geben Sie das Kennwort des Bildschirmschoners ein, um fortzufahren.

Sperren Sie mit Hilfe des Dialogfelds **Sicherheit** Ihre Konsole mit einem Kennwortschutz, legen Sie Ihr Kennwort fest bzw. ändern Sie es oder aktivieren Sie den Bildschirmschoner.

ANMERKUNG: Falls das iKVM-Kennwort verloren geht oder vergessen wird, können Sie es über die CMC-Webschnittstelle oder RACADM auf die iKVM-Werkseinstellung zurücksetzen. Siehe „Verlorenes oder vergessenes Kennwort löschen".

Sicherheitsdialogfeld aufrufen

So zeigen Sie das Dialogfeld „Sicherheit" an:

1. Drücken Sie die Taste <Druck>. Das **Hauptdialogfeld** wird geöffnet.
2. Klicken Sie auf **Setup** und dann auf **Sicherheit**. Das Dialogfeld **Sicherheit** wird angezeigt.

Kennwort festlegen oder ändern

So setzen oder ändern Sie das Kennwort:

1. Klicken Sie einmal und drücken Sie die Taste <Eingabe> oder doppelklicken Sie auf das Feld **Neu**.
2. Geben Sie im Feld **Neu** das neue Kennwort ein und drücken Sie dann <Eingabe>. Bei Kennwörtern wird zwischen Groß- und Kleinschreibung unterschieden und sie müssen zwischen 5 und 12 Zeichen lang sein. Sie müssen mindestens einen Buchstaben und eine Zahl enthalten. Erlaubte Zeichen sind A-Z, a-z, 0-9, Leerstelle und Bindestrich.
3. Geben Sie im Feld **Wiederholen** das Kennwort erneut ein und drücken Sie dann <Eingabe>.
4. Klicken Sie auf **OK**, wenn Sie nur das Kennwort ändern möchten, und schließen Sie dann das Dialogfeld.

Konsole mit Kennwort schützen

So sichern Sie die Konsole mit einem Kennwort:

1. Legen Sie das Kennwort, wie im vorhergehenden Verfahren beschrieben, fest.
2. Wählen Sie das Feld **Bildschirmschoner aktivieren** aus.
3. Geben Sie die Anzahl Minuten für die **Inaktivitätszeit** (von 1 bis 99) ein, mit der der Kennwortschutz und die Bildschirmschoneraktivierung verzögert werden sollen.
4. Bei **Modus**: Wenn Ihr Monitor ENERGY STAR-kompatibel ist, wählen Sie **Energie** aus, andernfalls, wählen Sie **Bildschirm** aus.

ANMERKUNG: Wenn der Modus auf **Energie** gesetzt wird, versetzt das Gerät den Monitor in den Energiesparmodus. Dies ist normalerweise ersichtlich, wenn der Monitor ausschaltet und die grüne LED-Betriebsanzeige durch ein gelbes Licht ersetzt wird. Wird der Modus auf **Bildschirm** gesetzt, springt das OSCAR-Flag für die Dauer des Tests auf dem Bildschirm hin und her. Bevor der Test startet, wird in einem Warnungs-Popup-Feld die folgende Meldung angezeigt: „Der Energiemodus kann einen Monitor, der nicht ENERGY STAR-kompatibel ist, beschädigen. Nach dem Start kann der Test jedoch umgehend per Maus oder Tastatur beendet werden."

VORSICHTSHINWEIS: Monitore, die nicht Energy Star-kompatibel sind, können bei Verwendung des Energiemodus beschädigt werden.

5 Optional: Um den Bildschirmschonertest zu aktivieren, klicken Sie auf **Test**. Das Dialogfeld **Bildschirmschonertest** wird angezeigt. Klicken Sie auf **OK**, um den Test zu starten.

Der Test dauert 10 Sekunden. Nach Abschluss kehren Sie zum Dialogfeld **Sicherheit** zurück.

Anmeldung

So starten Sie Oscar:

1 Drücken Sie <Druck>, um OSCAR zu starten. Das Dialogfeld **Kennwort** wird aufgerufen.

2 Geben Sie das Kennwort ein und klicken Sie dann auf **OK**. Das **Haupt**dialogfeld wird angezeigt.

Automatische Abmeldung einstellen

Sie können OSCAR so einstellen, dass nach einer Phase von Inaktivität automatisches Abmelden auf einem Server erfolgt.

1 Klicken Sie im **Hauptdialogfeld** auf **Setup** und anschließend auf **Sicherheit**.

2 Geben Sie im Feld **Inaktivitätszeit** die Zeitspanne ein, wie lange Sie mit einem Server verbunden sein möchten, bevor er die Verbindung automatisch trennt.

3 Klicken Sie auf **OK**.

Kennwortschutz von Konsole entfernen

So heben Sie den Kennwortschutz für die Konsole auf:

1 Klicken Sie im **Hauptdialogfeld** auf **Setup** und anschließend auf **Sicherheit**.

2 Klicken Sie im Dialogfeld **Sicherheit** einmal und drücken Sie die Taste <Eingabe> oder doppelklicken Sie auf das Feld **Neu**.

3 Lassen Sie das Feld **Neu** frei und drücken Sie <Eingabe>.

4 Klicken Sie einmal und drücken Sie <Eingabe> oder doppelklicken Sie auf das Feld **Wiederholen**.

5 Lassen Sie das Feld **Wiederholen** frei und drücken Sie <Eingabe>.

6 Klicken Sie auf **OK**, wenn Sie lediglich das Kennwort löschen möchten.

Bildschirmschonermodus ohne Kennwortschutz aktivieren

ANMERKUNG: Falls die Konsole kennwortgeschützt ist, müssen Sie zuerst den Kennwortschutz entfernen. Folgen Sie den Schritten im vorhergehenden Verfahren, bevor Sie die unteren Schritte durchführen.

So aktivieren Sie den Bildschirmschoner-Modus ohne Kennwortschutz:

1. Wählen Sie **Bildschirmschoner aktivieren** aus.
2. Geben Sie die Anzahl Minuten (zwischen 1 und 99) ein, die vergehen soll, bevor der Bildschirmschoner aktiviert wird.
3. Wählen Sie **Energie** aus, wenn Ihr Monitor ENERGY STAR-kompatibel ist; wählen Sie ansonsten **Bildschirm** aus.

   VORSICHTSHINWEIS: Monitore, die nicht Energy Star-kompatibel sind, können bei Verwendung des Energiemodus beschädigt werden.
4. Optional: Um den Bildschirmschonertest zu aktivieren, klicken Sie auf **Test**. Das Dialogfeld **Bildschirmschonertest** wird angezeigt. Klicken Sie auf **OK**, um den Test zu starten.

   Der Test dauert 10 Sekunden. Nach Abschluss kehren Sie zum Dialogfeld **Sicherheit** zurück.

   ANMERKUNG: Durch das Aktivieren des Bildschirmschonermodus wird die Verbindung des Benutzers zu einem Server getrennt; es ist kein Server mehr ausgewählt. Das Status-Flag zeigt „Frei“ an.

Bildschirmschonermodus beenden

Um den Bildschirmschonermodus zu beenden und zum **Hauptdialogfels** zurückzukehren, drücken Sie eine beliebige Taste oder bewegen Sie die Maus.

So schalten Sie den Bildschirmschoner aus:

Deaktivieren Sie im Dialogfeld **Sicherheit** das Feld **Bildschirmschoner aktivieren** und klicken Sie auf **OK**.

Um den Bildschirmschoner umgehend einzuschalten, drücken Sie die Taste <Druck> und dann <Pause>.

Verlorenes oder vergessenes Kennwort löschen

Wenn das iKVM-Kennwort verloren geht oder vergessen wird, können Sie es auf den iKVM-Werksstandard zurücksetzen und anschließend das Kennwort ändern. Sie können das Kennwort entweder über die CMC-Webschnittstelle oder RACADM zurücksetzen.

So setzen Sie ein verloren gegangenes oder vergessenes iKVM-Kennwort mit der CMC-Webschnittstelle zurück:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie im Gehäuse-Untermenü **iKVM** aus.
3. Klicken Sie auf das Register **Setup**. Die Seite **iKVM-Konfiguration** wird angezeigt.
4. Klicken Sie auf **Standardwerte wiederherstellen**.

Sie können nun die Standardeinstellung des Kennworts über OSCAR ändern. Siehe „Kennwort festlegen oder ändern“.

Um ein verlorenes oder vergessenes Kennwort mit RACADM zurückzusetzen, öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole zum CMC, melden sich an und geben Folgendes ein:

```
racadm racresetcfg -m kvm
```

ANMERKUNG: Der Befehl **racresetcfg** setzt die Einstellungen „Frontblende aktivieren“ und „Dell CMC-Konsole aktivieren“ zurück, wenn sie von den Standardwerten abweichen.

Lesen Sie für weitere Informationen über den **racresetcfg**-Unterbefehl den Abschnitt „racresetcfg“ im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*.

Sprache ändern

Ändern Sie mit dem Dialogfeld **Sprache** die Sprache des OSCAR-Texts in eine der unterstützten Sprachen. Der Text ändert auf allen OSCAR-Bildschirmen umgehend in die ausgewählte Sprache.

So ändern Sie die OSCAR-Sprache:

1. Drücken Sie die Taste <Druck>. Das **Hauptdialogfeld** wird geöffnet.
2. Klicken Sie auf **Setup** und anschließend auf **Sprache**. Das Dialogfeld **Sprache** erscheint.
3. Klicken Sie auf die Optionsschaltfläche für die gewünschte Sprache und anschließend auf **OK**.

Versionsinformationen anzeigen

Verwenden Sie das Dialogfeld **Version**, um die iKVM-Firmware- und Hardwareversion anzuzeigen und die Sprach- und Tastaturkonfiguration zu identifizieren.

So zeigen Sie Versionsinformationen an:

1. Drücken Sie die Taste <Druck>. Das **Hauptdialogfeld** wird geöffnet.
2. Klicken Sie auf **Befehl** und dann auf **Versionen anzeigen**. Das Dialogfeld **Version** wird angezeigt.

   In der oberen Hälfte des Dialogfelds **Version** werden die Subsystemversionen im Gerät angezeigt.
3. Klicken Sie auf ☒ oder drücken Sie <Esc>, um das Dialogfeld **Version** zu schließen.

System scannen

Im Scan-Modus scannt das iKVM automatisch von Steckplatz zu Steckplatz (Server zu Server). Sie können bis zu 16 Server scannen, indem Sie die Server angeben, die gescannt werden sollen, sowie die Anzahl Sekunden, während denen jeder Server angezeigt wird.

So fügen Sie der Scan-Liste Server hinzu:

1. Drücken Sie die Taste <Druck>. Das **Hauptdialogfeld** wird geöffnet.
2. Klicken Sie auf **Setup** und dann auf **Suchen**. Das Dialogfeld **Suchen** wird aufgerufen, in dem alle Server im Gehäuse aufgelistet werden.
3. Wählen Sie das Kontrollkästchen neben den Servern aus, die gescannt werden sollen.

   oder

   Doppelklicken Sie auf den Servernamen oder den Steckplatz.

   oder

   Drücken Sie die Taste <Alt > und die Nummer des Servers, der gescannt werden soll. Es können bis zu 16 Server ausgewählt werden.
4. Geben Sie im Feld **Zeit** die Anzahl Sekunden ein (zwischen 3 und 99), die iKVM abwarten soll, bevor der Scan zum nächsten Server der Folge übergeht.

5 Klicken Sie auf die Schaltfläche **Hinzufügen/Entfernen** und anschließend auf **OK**.

So entfernen Sie einen Server aus der **Scan**-Liste:

1 Wählen Sie im Dialogfeld **Suchen** das Kontrollkästchen neben dem zu entfernenden Server aus.

oder

Doppelklicken Sie auf den Servernamen oder den Steckplatz.

oder

Klicken Sie auf die Schaltfläche **Löschen**, um alle Server aus der **Scan**-Liste zu entfernen.

2 Klicken Sie auf die Schaltfläche **Hinzufügen/Entfernen** und anschließend auf **OK**.

So starten Sie den Scan-Modus:

1 Drücken Sie die Taste <Druck>. Das **Hauptdialogfeld** wird geöffnet.
2 Klicken Sie auf **Befehle**. Das Dialogfeld **Befehl** wird aufgerufen.
3 Wählen Sie das Feld **Scan aktivieren** aus.
4 Klicken Sie auf **OK**. Es wird eine Meldung angezeigt, die angibt, dass die Maus und die Tastatur zurückgesetzt wurden.
5 Klicken Sie auf ☒, um das Meldungsfenster zu schließen.

So brechen Sie den Scan-Modus ab:

1 Wenn OSCAR geöffnet ist und das **Hauptdialogfeld** angezeigt wird, wählen Sie einen Server aus der Liste aus.

oder

Ist OSCAR *nicht* geöffnet, bewegen Sie die Maus, oder drücken Sie eine beliebige Taste auf der Tastatur. Der Scan-Vorgang wird beim derzeit ausgewählten Server gestoppt.

oder

Drücken Sie die Taste <Druck>. Das **Hauptdialogfeld** wird angezeigt; wählen Sie einen Server aus der Liste aus.

2 Klicken Sie auf die Schaltfläche **Befehle**. Das Dialogfeld **Befehle** wird aufgerufen.

3 Deaktivieren Sie das Kästchen **Scan aktivieren**.

Broadcast zu Servern

Sie können mehrere Server eines Systems gleichzeitig steuern, um sicherzustellen, dass alle ausgewählten Server die gleiche Eingabe erhalten. Sie können Tastenanschläge und/oder Mausbewegungen unabhängig voneinander senden lassen.

ANMERKUNG: Sie können einen Broadcast an bis zu 16 Server gleichzeitig senden.

So führen Sie einen Broadcast an Server durch:

1 Drücken Sie die Taste <Druck>. Das **Hauptdialogfeld** wird geöffnet.

2 Klicken Sie auf **Setup** und anschließend auf **Broadcast**. Das Dialogfeld **Broadcast** wird angezeigt.

ANMERKUNG: Tastenanschläge senden: Wenn Sie Tastenanschläge verwenden, muss der Tastaturstatus bei allen Servern, die einen Broadcast empfangen, identisch sein, damit die Tastenanschläge auf identische Weise interpretiert werden können. Genauer gesagt müssen die Modi <Feststelltaste> und <Num-Taste> bei allen Tastaturen gleich sein. Während das iKVM versucht, Tastenanschläge gleichzeitig an die ausgewählten Server zu senden, ist es möglich, dass einige Server die Übertragung beeinträchtigen und dadurch verzögern.

ANMERKUNG: Mausbewegungen senden: Damit die Maus korrekt funktioniert, müssen alle Server über den gleichen Maustreiber, Desktop (z. B. identisch platzierte Symbole) und Grafikauflösungen verfügen. Auch die Maus muss sich bei allen Bildschirmen an genau der gleichen Position befinden. Da diese Betriebszustände außerordentlich schwierig zu erzielen sind, kann der Broadcast von Mausbewegungen an mehrere Server unberechenbare Ergebnisse zur Folge haben.

3 Aktivieren Sie die Maus und/oder die Tastatur für die Server, welche die Broadcast-Befehle erhalten sollen, indem Sie die jeweiligen Kontrollkästchen auswählen.

   oder

   Drücken Sie die Tasten „Nach oben“ oder „Nach unten“, um den Cursor zu einem Zielserver zu bewegen. Drücken Sie dann <Alt><K>, um das Tastaturfeld auszuwählen, und/oder <Alt><M>, um das Mausfeld auszuwählen. Wiederholen Sie diesen Vorgang für weitere Server.

4 Klicken Sie auf **OK**, um die Einstellungen zu speichern und zum Dialogfeld **Setup** zurückzukehren. Klicken Sie auf ☒ oder drücken Sie <Esc>, um zum **Hauptdialogfeld** zurückzukehren.

5 Klicken Sie auf **Befehle**. Das Dialogfeld **Befehle** wird aufgerufen.

6 Klicken Sie auf das Feld **Broadcast aktivieren**, um Broadcasts zu aktivieren. Das Dialogfeld **Broadcast-Warnung** wird angezeigt.

7 Klicken Sie auf **OK**, um den Broadcast zu aktivieren.

   Um den Vorgang abzubrechen und zum Dialogfeld **Befehle** zurückzukehren, klicken Sie auf ☒ oder drücken Sie <Esc>.

8 Wenn Broadcasts aktiviert sind, geben Sie die Informationen ein und/oder führen Sie die Mausbewegungen aus, die von der Management Station gesendet werden sollen. Nur Server aus der Liste sind verfügbar.

So schalten Sie Broadcasts aus:

Deaktivieren Sie im Dialogfeld **Befehle** das Kontrollkästchen **Broadcast aktivieren**.

iKVM vom CMC aus verwalten

Frontblende aktivieren oder deaktivieren

Um den Zugriff auf das iKVM von der Frontblende mit RACADM zu aktivieren oder zu deaktivieren, öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole zum CMC, melden sich an und geben folgendes ein:

```
racadm config -g cfgKVMInfo -o cfgKVMFrontPanelEnable
<value>
```

wobei <*Wert*> 1 (aktivieren) oder 0 (deaktivieren) bedeutet.

Lesen Sie für weitere Informationen über den **config**-Unterbefehl den Abschnitt „config“ im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*.

So aktivieren oder deaktivieren Sie den Zugriff auf das iKVM über die Webschnittstelle von der Frontblende aus:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur iKVM aus. Die Seite **iKVM-Status** wird angezeigt.
3. Klicken Sie auf das Register **Setup**. Die Seite **iKVM-Konfiguration** wird angezeigt.
4. Wählen Sie zur Aktivierung das Kontrollkästchen **Frontblenden-USB/Video aktiviert** aus.

   Entfernen Sie zum Deaktivieren das Häkchen im Kontrollkästchen **Frontblenden-USB/Video aktiviert**.
5. Klicken Sie auf **Anwenden**, um die Einstellung zu speichern.

Dell CMC-Konsole über iKVM aktivieren.

Um dem iKVM den Zugriff auf die Dell CMC-Konsole mit RACADM zu ermöglichen, öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole zum CMC, melden sich an und geben Folgendes ein:

```
racadm config -g cfgKVMInfo -o
cfgKVMAccessToCMCEnable 1
```

So aktivieren Sie die Dell-CMC-Konsole über die Webschnittstelle:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur iKVM aus. Die Seite **iKVM-Status** wird angezeigt.
3. Klicken Sie auf die Registerkarte **Setup**. Die Seite **iKVM-Konfiguration** wird angezeigt.
4. Wählen Sie das Kontrollkästchen **Zugang zu CMC-CLI über iKVM zulassen** aus.
5. Klicken Sie auf **Anwenden**, um die Einstellung zu speichern.

iKVM-Status und -Eigenschaften anzeigen

Der Name des Lokalzugriffs-KVM-Modul für das Dell M1000e-Servergehäuse lautet Avocent Integrated KVM Switch-Modul (iKVM). Der Funktionszustand des mit dem Gehäuse verbundenen iKVM kann auf der Seite **Gehäuseeigenschaftszustand** im Abschnitt **Gehäuse-Grafiken** eingesehen werden.

So zeigen Sie den Funktionszustand des iKVM über **Gehäuse-Grafiken** an:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Die Seite **Gehäusestatus** wird angezeigt. Der rechte Abschnitt von **Gehäuse-Grafiken** zeigt die Rückansicht des Gehäuses und enthält den Funktionszustand des iKVM an. Der iKVM-Funktionszustand wird durch die Farbe der iKVM-Grafik angezeigt:
   - Grün - iKVM ist vorhanden, wird mit Strom versorgt und kommuniziert mit dem CMC. Es gibt keine Anzeichen eines unerwünschten Status.
   - Bernstein - iKVM wird erkannt, wird oder wird nicht mit Strom versorgt oder kommuniziert oder kommuniziert nicht mit dem CMC; ein ungünstiger Status könnte vorhanden sein.
   - Grau - iKVM wird erkannt und nicht mit Strom versorgt. Sie kommuniziert nicht mit dem CMC und es gibt keine Anzeichen eines ungünstigen Zustands.
3. Bewegen Sie den Cursor über die iKVM-Grafik und ein entsprechender Texthinweis oder Bildschirmtipp wird angezeigt. Der Texthinweis liefert zusätzliche Informationen zu diesem iKVM.
4. Die iKVM-Grafik ist mit der entsprechenden GUI-Seite des CMC verknüpft, um sofort die Navigation zur Seite **iKVM-Status** zu ermöglichen.

Weitere Informationen zum iKVM finden Sie unter „iKVM-Modul verwenden“.

Um den Status des iKVM einzusehen, verwenden Sie die Seite **iKVM-Status**:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur **iKVM** aus. Die Seite **iKVM-Status** wird aufgerufen.

Tabelle 10-5. iKVM Statusinformationen

Element	Beschreibung
Vorhandensein	Zeigt an, ob das iKVM-Modul **Vorhanden** oder **Nicht vorhanden** ist.
Stromzustand	Zeigt den iKVM-Stromstatus an: **Ein**, **Aus** oder **Nicht vorhanden**.
Name	Zeigt den Produktnamen des iKVM an.
Hersteller	Zeigt den Hersteller des iKVM an.
Teilenummer	Zeigt die Teilenummer des iKVM an. Die Teilenummer ist eine vom Hersteller eindeutig identifizierbare Nummer.
Firmware-Version	Zeigt die iKVM-Firmware-Version an.
Hardwareversion	Zeigt die iKVM-Hardwareversion an.
Frontblende angeschlossen	Zeigt an, ob der Monitor mit dem Frontblenden-VGA-Anschluss **verbunden ist** (**Ja** oder **Nein**). Diese Informationen werden dem CMC zur Verfügung gestellt, damit er bestimmen kann, ob ein lokaler Benutzer Zugriff auf das Gehäuse von der Frontblende aus hat.
Rückseite angeschlossen	Zeigt an, ob der Monitor mit dem rückseitigen VGA-Anschluss **verbunden ist** (**Ja** oder **Nein**). Diese Informationen werden dem CMC zur Verfügung gestellt, damit er bestimmen kann, ob ein lokaler Benutzer Zugriff auf das Gehäuse von der Rückseite aus hat.
Reihenanschluss verbunden	iKVM unterstützt nahtlose Reihenabstufung mit externen iKVM-Anwendungen von Dell und Avocent unter Verwendung eingebauter Hardware. Wenn das iKVM über Reihenabstufung verfügt, kann auf die Server im Gehäuse durch die Bildschirmanzeige des externen KVM-Switch zugegriffen werden, von denen aus iKVM abgestuft ist.
Frontblenden-USB/Video aktiviert	Zeigt an, ob der Frontblenden-VGA-Anschluss aktiviert ist (**Ja** oder **Nein**).
Zugriff von iKVM auf CMC zulassen	Zeigt an, ob die CMC-Befehlskonsole durch iKVM aktiviert ist (**Ja** oder **Nein**).

Aktualisieren der iKVM-Firmware

Die iKVM-Firmware kann mit der CMC-Webschnittstelle oder RACADM aktualisiert werden.

So aktualisieren Sie die iKVM-Firmware mit der CMC-Webschnittstelle:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf **Gehäuse**.
3. Klicken Sie auf die Registerkarte **Aktualisieren**. Die Seite **Aktualisierbare Komponenten** wird angezeigt.
4. Klicken Sie auf den Namen des iKVM-Moduls. Die Seite **Firmware-Aktualisierung** wird eingeblendet.
5. 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.

ANMERKUNG: Der Standardname des iKVM-Firmware-Image ist ikvm.bin; der Dateiname des iKVM-Firmware-Image kann jedoch vom Benutzer verändert werden.

6. Klicken Sie auf **Firmware-Aktualisierung beginnen**. Ein Dialogfeld fordert Sie auf die Maßnahme zu bestätigen.
7. Klicken Sie auf **Ja**, um fortzufahren. Der Abschnitt **Fortschritt der Firmware-Aktualisierung** bietet Statusinformationen zur Firmwareaktualisierung. Ein Statusindikator wird auf der Seite während des Aktualisierungsvorganges angezeigt. Die Zeit Übertragungszeit kann je nach Verbindungsgeschwindigkeit deutlich variieren. Wenn der interne Aktualisierungsprozess beginnt, wird die Seite laufend aktualisiert und zeigt den Firmwareaktualisierungszeitgeber an. Zusätzliche Anweisungen:
   - Verwenden Sie während der Dateiübertragen nicht die Schaltfläche **Aktualisieren** und navigieren nicht Sie zu einer anderen Seite.
   - Um den Prozess abzubrechen, klicken Sie auf **Dateiübertragung und Aktualisierung abbrechen** - diese Option ist nur während der Dateiübertragung verfügbar.

- Der Status der Aktualisierung wird im Feld **Aktualisierungsstatus** angezeigt; dieses Feld wird automatisch während der Dateiübertragung aktualisiert. Bestimmte ältere Browser unterstützen diese automatischen Aktualisierungen nicht. Um das Feld **Aktualisierungsstatus** manuell zu aktualisieren, klicken Sie auf **Aktualisieren**.

ANMERKUNG: Die Aktualisierung für das iKVM kann bis zu einer Minute dauern.

Wenn die Aktualisierung abgeschlossen ist, wird das iKVM zurückgesetzt und die neue Firmware wird aktualisiert und auf der Seite **Aktualisierbare Komponenten** angezeigt.

Um die iKVM-Firmware mit RACADM zu aktualisieren, öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole zum CMC, melden Sie sich an und geben Sie Folgendes ein:

```
racadm fwupdate -g -u -a <TFTP Server IP Address or
FQDN> -d <filepath/filename> -m kvm
```

Beispiel:

```
racadm fwupdate -gua 192.168.0.10 -d ikvm.bin -m kvm
```

Lesen Sie für weitere Informationen über den **fwupdate**-Unterbefehl den Abschnitt **„fwupdate“** im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC*.

Fehlerbehebung

ANMERKUNG: Wenn eine aktive Konsolenumleitungssitzung vorhanden ist und ein Monitor mit niedriger Auflösung an der iKVM angeschlossen ist, kann die Serverkonsolenauflösung u. U. zurückgesetzt werden, wenn der Server auf der lokalen Konsole ausgewählt wird. Wenn der Server ein Linux-Betriebssystem ausführt, kann eine X11-Konsole auf dem lokalen Monitor u. U. nicht angezeigt werden. Durch Drücken auf <Strg><Alt><F1> auf der iKVM wird Linux auf eine Textkonsole geschaltet.

Tabelle 10-6. Fehlerbehebung beim iKVM

Problem	Wahrscheinliche Ursache und Lösung
Die Meldung „Benutzer wurde durch die CMC-Steuerung deaktiviert“ wird auf dem Monitor angezeigt, der an der Frontblende angeschlossen ist.	Die Frontblendenverbindung wurde vom CMC deaktiviert. Sie können die Frontblende entweder mit der CMC-Webschnittstelle oder RACADM aktivieren. So aktivieren Sie die Frontblende über die Webschnittstelle: **1** Melden Sie sich bei der CMC-Webschnittstelle an. **2** Wählen Sie in der Systemstruktur iKVM aus. **3** Klicken Sie auf das Register **Setup**. **4** Wählen Sie das Kontrollkästchen **Frontblenden-USB/Video aktiviert** aus. **5** Klicken Sie auf **Apply** (Anwenden), um die Einstellung zu speichern. Um die Frontblende mit RACADM zu aktivieren, öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole zum CMC, melden Sie sich an und geben Sie Folgendes ein: `racadm config -g cfgKVMInfo -o cfgKVMAccesToCMCEnable 1`
Der Zugriff auf die rückseitige Abdeckung funktioniert nicht.	Die Frontblendeneinstellung ist durch den CMC aktiviert, und an der Frontblende ist gegenwärtig ein Monitor angeschlossen. Es ist jeweils nur eine Verbindung zulässig. Die Frontblendenverbindung hat Vorrang vor ACI und der rückseitigen Abdeckung. Weitere Informationen über Verbindungsrangfolgen finden Sie unter „iKVM-Verbindungsrangfolge“.

Tabelle 10-6. Fehlerbehebung beim iKVM *(fortgesetzt)*

Problem	Wahrscheinliche Ursache und Lösung
Die Meldung „Benutzer wurde deaktiviert, da ein weiteres Gerät derzeit Vorrang hat“ wird auf dem Monitor angezeigt, der an der rückseitigen Abdeckung angeschlossen ist.	Es ist ein Netzwerkkabel am iKVM ACI-Anschluss und an einem sekundären KVM-Gerät angeschlossen. Es ist jeweils nur eine Verbindung zulässig. Die ACI-Reihenverbindung hat Vorrang vor dem Monitoranschluss an der rückseitigen Abdeckung. Die Rangfolge ist Frontblende, ACI und dann rückseitige Abdeckung.

Tabelle 10-6. Fehlerbehebung beim iKVM *(fortgesetzt)*

Problem	Wahrscheinliche Ursache und Lösung
Die gelbe iKVM-LED blinkt.	Es gibt drei mögliche Ursachen: **Es liegt ein Problem mit dem iKVM vor**, für welches das iKVM eine Neuprogrammierung erfordert. Um das Problem zu beheben, folgen Sie den Anweisungen zur Aktualisierung der iKVM-Firmware (siehe „Aktualisieren der iKVM-Firmware“). **Das iKVM programmiert die CMC-Konsolenschnittstelle neu.** In diesem Fall ist die CMC-Konsole vorübergehend nicht verfügbar und wird durch einen gelben Punkt in der OSCAR-Benutzeroberfläche dargestellt. Dieser Vorgang dauert bis zu 15 Minuten. **Die iKVM-Firmware hat einen Hardwarefehler festgestellt.** Weitere Informationen entnehmen Sie dem iKVM-Status. So zeigen Sie den iKVM-Status mithilfe der Webschnittstelle an: **1** Melden Sie sich bei der CMC-Webschnittstelle an. **2** Wählen Sie in der Systemstruktur iKVM aus. Um den iKVM-Status mit RACADM anzuzeigen, öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole zum CMC, melden Sie sich an und geben Sie Folgendes ein: `racadm getkvminfo`

Tabelle 10-6. Fehlerbehebung beim iKVM ***(fortgesetzt)***

Problem	Wahrscheinliche Ursache und Lösung
Das iKVM wird über den ACI-Anschluss an einen externen KVM-Switch abgestuft, wobei jedoch sämtliche Einträge für die ACI-Verbindungen nicht verfügbar sind. Alle Zustände weisen einen gelben Punkt in der OSCAR-Benutzeroberfläche auf.	Der Frontblendenanschluss ist aktiviert, und es ist ein Monitor daran angeschlossen. Da die Frontblende Vorrang vor allen anderen iKVM-Anschlüssen hat, sind die ACI-Anschlüsse und die Anschlüsse der rückseitigen Abdeckung deaktiviert. Um die ACI-Anschlussverbindung zu aktivieren, müssen Sie zuerst den Frontblendenzugriff deaktivieren oder den Monitor entfernen, der an der Frontblende angeschlossen ist. Die OSCAR-Einträge des externen KVM-Switch werden aktiv und verfügbar. So deaktivieren Sie die Frontblende unter Verwendung der Webschnittstelle: **1** Melden Sie sich bei der CMC-Webschnittstelle an. **2** Wählen Sie in der Systemstruktur iKVM aus. **3** Klicken Sie auf das Register **Setup**. **4** Entfernen Sie zum Deaktivieren das Häkchen aus dem Kontrollkästchen **Frontblenden-USB/Video aktiviert**. **5** Klicken Sie auf **Apply** (Anwenden), um die Einstellung zu speichern. Um die Frontblende mit RACADM zu deaktivieren, öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole zum CMC, melden Sie sich an und geben Sie Folgendes ein: `racadm config -g cfgKVMInfo -o cfgKVMFrontPanelEnable 0`

Tabelle 10-6. Fehlerbehebung beim iKVM ***(fortgesetzt)***

Problem	Wahrscheinliche Ursache und Lösung
Im OSCAR-Menü zeigt die Dell-CMC-Verbindung ein rotes X an, und ein Verbindungsaufbau zum CMC ist nicht möglich.	Es gibt zwei mögliche Ursachen: **Die Dell-CMC-Konsole wurde deaktiviert.** In diesem Fall können Sie sie entweder über die CMC-Webschnittstelle oder RACADM aktivieren. So aktivieren Sie die Dell-CMC-Konsole über die Webschnittstelle: **1** Melden Sie sich bei der CMC-Webschnittstelle an. **2** Wählen Sie in der Systemstruktur **iKVM** aus. **3** Klicken Sie auf das Register **Setup**. **4** Wählen Sie das Kontrollkästchen **Zugang zu CMC-CLI über iKVM zulassen** aus. **5** Klicken Sie auf **Apply** (Anwenden), um die Einstellung zu speichern. Um die Dell CMC-Verbindung mit RACADM zu aktivieren, öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole zum CMC, melden Sie sich an und geben Sie Folgendes ein: `racadm config -g cfgKVMInfo -o cfgKVMAccessToCMCEnable 1` **Der CMC ist nicht verfügbar, da er initialisiert wird, zum Standby-CMC wechselt oder eine Neuprogrammierung durchführt.** Warten Sie in diesem Falle einfach ab, bis der CMC die Initialisierung abgeschlossen hat.

Tabelle 10-6. Fehlerbehebung beim iKVM ***(fortgesetzt)***

Problem	Wahrscheinliche Ursache und Lösung
Der Steckplatzname für einen Server wird in OSCAR als „Initialisiert“ angezeigt und er kann nicht ausgewählt werden.	Entweder führt der Server eine Initialisierung durch, oder iDRAC konnte auf diesem Server keine Initialisierung durchführen. Warten Sie zuerst 60 Sekunden. Falls der Server weiterhin initialisiert wird, wird der Steckplatzname angezeigt, sobald die Initialisierung abgeschlossen ist. Sie können dann den Server auswählen. Falls OSCAR nach 60 Sekunden weiterhin angibt, dass der Steckplatz eine Initialisierung durchführt, nehmen Sie den Server aus dem Gehäuse heraus und setzen Sie ihn wieder ein. Diese Maßnahme ermöglicht dem iDRAC die Reinitialisierung.

11

Verwaltung der E/A-Struktur

Das Gehäuse kann bis zu sechs E/A-Module (EAMs) aufnehmen, die entweder Switch- oder Passthrough-Module sein können.

Diese EAMs werden in drei Gruppen unterteilt: A, B und C. Jede Gruppe besitzt zwei Steckplätze: Steckplatz 1 und Steckplatz 2. Die Steckplätze sind auf der Geräterückseite von links nach rechts mit Buchstaben gekennzeichnet: A1 | B1 | C1 | C2 | B2 | A2. Jeder Server verfügt über Steckplätze für zwei Mezzanine-Karten (MCs) zum Anschließen an die EAMs. Die MC und das entsprechende EAM müssen dieselbe Struktur aufweisen.

Der Gehäuse-E/A ist in 3 diskrete Datenpfade aufgeteilt, die mit folgenden Buchstaben gekennzeichnet sind: A, B und C. Diese Pfade werden als STRUKTUREN bezeichnet und unterstützen Ethernet, Fibre Channel und InfiniBand. Diese diskreten Strukturpfade sind in 2 E/A-„Bänke“ aufgeteilt: Bank eins und Bank zwei. Jeder Server-E/A-Adapter (Mezzanine-Karte oder LOM) kann entweder 2 oder 4 Schnittstellen haben, je nach Kapazität. Diese Schnittstellen sind gleichmäßig auf die E/A-Modulbänke eins und zwei aufgeteilt, um Redundanz zu ermöglichen. Wenn Sie Ihre Ethernet-, iSCSI- oder FibreChannel-Netzwerke bereitstellen, sollten Sie deren redundante Links über die Bänke eins und zwei spannen, um maximale Verfügbarkeit zu erzielen. Wir kennzeichnen das diskrete E/A-Modul mit der Strukturkennung und der Banknummer.

Beispiel: „A1“ benennt Struktur „A“ auf Bank „1“. „C2“ benennt Struktur „C“ auf Bank „2“.

Das Gehäuse unterstützt drei Struktur- oder Protokolltypen. Alle EAMs und MCs in einer Gruppe müssen dieselben oder kompatible Strukturtypen aufweisen.

- EAMs der **Gruppe A** sind immer mit den integrierten Ethernet-Adaptern des Servers verbunden. Der Strukturtyp von Gruppe A ist immer Ethernet.
- Für **Gruppe B** sind die EAM-Steckplätze permanent mit dem **ersten MC (Mezzanine-Karte)**-Steckplatz in jedem Servermodul verbunden.

- Für **Gruppe C** sind die EAM-Steckplätze permanent mit dem **zweiten MC (Mezzanine-Karte)-**Steckplatz in jedem Servermodul verbunden.

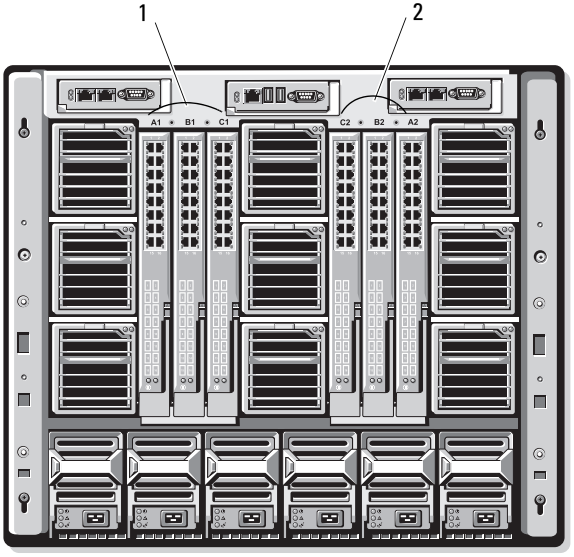
ANMERKUNG: In der CMC-CLI wird über die folgende Konvention auf EAMs Bezug genommen, switch-*n*:
A1=Switch-1, A2=Switch-2, B1=Switch-3, B2=Switch-4, C1=Switch-5

Strukturverwaltung

Strukturverwaltung hilft elektrische, Konfigurations- oder Konnektivitätsprobleme zu vermeiden, die aufgrund der Installation eines EAMs oder einer MC auftreten, das/die einen Strukturtyp aufweist, der nicht mit dem bekannten Strukturtyp des Gehäuses kompatibel ist. Ungültige Hardwarekonfigurationen können zu elektrischen oder funktionalen Problemen des Gehäuses oder seiner Komponenten führen. Die Strukturverwaltung verhindert, dass der Netzstrom bei ungültigen Konfigurationen eingeschaltet wird.

Abbildung 11-1 zeigt den Standort der EAMs im Gehäuse. Der Standort jedes E/A-Moduls wird über dessen Gruppennummer (A, B oder C) angegeben. Diese diskreten Strukturpfade sind in zwei E/A-Banken unterteilt: Bank eins und zwei. Am Gehäuse sind die Steckplatznamen der EAMs mit A1, A2, B1, B2, C1 und C2 gekennzeichnet.

Abbildung 11-1. Rückansicht eines Gehäuses mit ausgewiesenen EAM-Standorten



1 Bank 1 (Steckplätze A1, B1, C1) 2 Bank 2 (Steckplätze A2, B2, C2)

Der CMC erstellt im Hardwareprotokoll und in den CMC-Protokollen Einträge zu ungültigen Hardwarekonfigurationen.

Beispiel:

- Eine mit einem Fibre Channel-EAM verbundene Ethernet-MC ist eine ungültige Konfiguration. Eine Ethernet-MC, die sowohl mit einem in der gleichen EAM-Gruppe installierten Ethernet-Switch als auch mit einem Ethernet-Passthrough-EAM verbunden ist, ist eine gültige Verbindung.

- Ein Fibre Channel-Passthrough-EAM und ein Fibre Channel-Switch-EAM in den Steckplätzen B1 und B2 ist eine gültige Konfiguration, wenn die ersten MCs auf allen Servern ebenfalls Fibre Channels sind. In diesem Fall schaltet der CMC die IOMs und Server ein. Bestimmte Arten von Fibre Channel-Redundanzsoftware unterstützt diese Konfiguration jedoch möglicherweise nicht; nicht alle gültigen Konfigurationen sind zwangsläufig auch unterstützte Konfigurationen.

ANMERKUNG: Strukturbestätigung für Server-EAMs und MCs wird nur ausgeführt, wenn das Gehäuse eingeschaltet ist. Wenn das Gehäuse nur im Standby läuft, bleiben die iDRACs auf den Servermodulen ausgeschaltet und können somit den MC-Strukturtyp des Servers nicht melden. Der MC-Strukturtyp wird möglicherweise erst auf der CMC-Benutzeroberfläche gemeldet, wenn der iDRAC auf dem Server eingeschaltet wird. Wenn das Gehäuse eingeschaltet ist, wird außerdem die Strukturbestätigung ausgeführt, wenn ein Server oder EAM eingesetzt wird (optional). Wenn festgestellt wird, dass die Struktur nicht übereinstimmt, dann erhält der Server oder das EAM die Genehmigung, einzuschalten, und die Status-LED blinkt **gelb**.

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.
- Eine ungültige EAM-MC-Konfiguration liegt vor, wenn eine neu installierte EAM-Struktur und die vorhandenen MC-Strukturen nicht übereinstimmen oder nicht kompatibel sind.
- 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.

Ungültige Konfiguration der Mezzanine-Karte (MC)

Eine ungültige MC-Konfiguration liegt vor, wenn das LOM oder die MC eines einzelnen Servers vom entsprechenden EAM nicht unterstützt wird. In diesem Fall können alle anderen Server im Gehäuse ausgeführt werden, aber der Server mit der nicht übereinstimmenden MC-Karte kann nicht eingeschaltet werden. Der Netzschalter am Server blinkt gelb und warnt über eine Nichtüberein-stimmung der Struktur. Informationen zu den CMC- und Hardwareprotokollen finden Sie unter „Ereignisprotokolle anzeigen“ auf Seite 497.

Ungültige Konfiguration der Mezzanine-Karte (MC)

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. Informationen zu den CMC- und Hardwareproto-kollen finden Sie unter „Ereignisprotokolle anzeigen“ auf Seite 497.

Ungültige EAM-EAM-Konfiguration

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. Informationen zu den CMC- und Hardwareprotokollen finden Sie unter „Ereignisprotokolle anzeigen“ auf Seite 497.

Neues Einschaltszenario

Wenn der Netzstecker des Gehäuses eingesteckt und das Gehäuse eingeschaltet ist, haben die EAMs Priorität gegenüber den Servern. Dem ersten EAM jeder Gruppe wird erlaubt, vor den anderen einzuschalten. Zu diesem Zeitpunkt wird keine Überprüfung der Strukturtypen durchgeführt. Wenn sich im ersten Steckplatz einer Gruppe kein EAM befindet, wird das Modul im zweiten Steckplatz dieser Gruppe eingeschaltet. Wenn sich in beiden Steckplätzen EAMs befinden, wird das Modul im zweiten Steckplatz hinsichtlich Konsistenz mit dem im ersten Steckplatz verglichen.

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

Der Funktionszustand der EAMs kann auf zwei Arten eingesehen werden: im Abschnitt **Gehäuse-Grafiken** auf der Seite **Gehäusestatus** oder auf der Seite **E/A-Module-Status**. Die Seite **Gehäuse-Grafiken** bietet einen grafischen Überblick über die im Gehäuse installierten EAMs.

Um den Funktionszustand der EAMs mittels Gehäuse-Grafiken anzuzeigen:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Die Seite **Gehäusestatus** wird angezeigt. Die rechte Sektion der **Gehäuse-Grafiken** stellt die Rückansicht des Gehäuses dar und enthält den Funktionszustand der EAMs. Der EAM-Funktionszustand wird durch die Farbe der EAM-Grafik angegeben:
   - Grün - EAM ist vorhanden, wird mit Strom versorgt und kommuniziert mit dem CMC; es gibt keine Anzeichen eines ungünstigen Zustands.
   - Bernstein - EAM wird erkannt, kann jedoch mit Strom versorgt sein, oder nicht, kann mit dem CMC kommunizieren oder nicht; ein ungünstiger Zustand könnte vorhanden sein.

- Grau - EAM ist vorhanden und wird nicht mit Strom versorgt. Sie kommuniziert nicht mit dem CMC und es gibt keine Anzeichen eines ungünstigen Zustands.

3 Bewegen Sie den Cursor über eine EAM-Grafik, sodass ein entsprechender Texthinweis oder ein Bildschirmtipp angezeigt wird. Der Texthinweis liefert zusätzliche Informationen zu diesem EAM.

4 Die EAM-Grafik ist mit der entsprechenden Seite der CMC-GUI verknüpft, um sofortige Navigation zur Seite **E/A-Modulstatus** für dieses EAM zu ermöglichen.

Um den Funktionszustand für alle EAMs einzusehen, verwenden Sie bitte die Seite **E/A-Module-Status**:

1 Melden Sie sich bei der CMC-Webschnittstelle an.

2 Wählen Sie im Menü **Gehäuse** der Systemstruktur den Eintrag **I/O Modules** (E/A-Module) aus.

3 Klicken Sie auf das Register **Eigenschaften.**

4 Klicken Sie auf das Unterregister **Status**. Die Seite **E/A-Module-Status** wird angezeigt.

Tabelle 11-1. E/A-Module-Statusinformationen

Element	Beschreibung
Steckplatz	Zeigt den Standort des E/A-Moduls im Gehäuse nach Gruppennummer (A, B oder C) und Bank (1 oder 2) an. EAM-Auflistung: **A1**, **A2**, **B1**, **B2**, **C1** oder **C2**.
Präsentation	Zeigt an, ob das EAM vorhanden ist (**Ja** oder **Nein**).

Tabelle 11-1. E/A-Module-Statusinformationen *(fortgesetzt)*

Element	Beschreibung	
Seite „Funktionszustand“	OK	Zeigt an, dass das EAM vorhanden ist und mit dem CMC kommuniziert. Im Falle eines Fehlers bei der Datenübertragung zwischen dem CMC und dem Server kann der CMC den Funktionszustand für das EAM nicht abrufen bzw. anzeigen.
	Informativ	Zeigt Informationen zum EAM an, wenn keine Änderung im Funktionszustand (OK, Warnung, Schwerwiegend) aufgetreten ist.
	Warnung	Zeigt an, dass Warnungen ausgestellt wurden und **Korrekturmaßnahmen ergriffen werden müssen.** Wenn keine Korrekturmaßnahmen ergriffen werden, kann dies zu kritischen oder schwerwiegen-den Fehlern führen, die Auswirkungen auf die Integrität des EAMs haben können. Beispiele von Zuständen, die Warnungen verursachen: Nichtübereinstimmung der EAM-Struktur mit der Struktur der Mezzanine-Karte des Servers; ungültige EAM-Konfiguration, wobei das neu installierte EAM nicht mit dem vorhandenen EAM auf derselben Gruppe übereinstimmt.
	Schwerwiegend	Zeigt an, dass mindestens eine Fehlerwarnung ausgegeben wurde. Ein schwerwiegender Zustand weist auf einen Systemfehler im EAM hin; es müssen **sofort Korrekturmaßnahmen ergriffen werden**. Beispiele von Zuständen, die einen schwerwiegenden Zustand verursachen: Fehler im EAM erkannt; EAM wurde entfernt.

ANMERKUNG: Alle Änderungen des Funktionszustands werden sowohl im Hardware- als auch im CMC-Protokoll aufgezeichnet. Weitere Informationen finden Sie unter„Ereignisprotokolle anzeigen“ auf Seite 497.

Tabelle 11-1. E/A-Module-Statusinformationen *(fortgesetzt)*

Element	Beschreibung
Fabric	Zeigt den Strukturtyp für das EAM an: Gigabit Ethernet, 10GE XAUI, 10GE KR, 10GE XAUI KR, FC 4 GBit/s, FC 8 GBit/s, SAS 3 GBit/s, SAS 6 GBit/s, Infiniband SDR, Infiniband DDR, Infiniband QDR, PCIe Bypass Generation 1, PCIe Bypass Generation 2. **ANMERKUNG:** Um EAM-Nichtübereinstimmungen innerhalb derselben Gruppe zu verhindern, ist es äußerst wichtig, dass Sie die Strukturtypen der EAMs im Gerät kennen. Informationen zur E/A-Struktur finden Sie unter „Verwaltung der E/A-Struktur“ auf Seite 453.
Name	Zeigt den EAM-Produktnamen an.
EAM-Verwaltungskonsole starten	 Wenn die Schaltfläche für ein bestimmtes E/A-Modul vorhanden ist, kann man darauf klicken, um die EAM-Verwaltungskonsole für dieses E/A-Modul in einem neuen Fenster oder einem neuen Register des Browsers zu starten. **ANMERKUNG:** Diese Option ist nur für die verwalteten Switch-E/A-Module verfügbar. Sie ist nicht verfügbar für Passthrough-E/A-Module oder nicht verwaltete Infiniband-Switches. **ANMERKUNG:** Wenn ein EAM nicht zugreifbar ist, weil es ausgeschaltet ist, seine LAN-Schnittstelle deaktiviert ist oder dem Modul keine gültige IP-Adresse zugewiesen ist, wird die Option „EAM-GUI starten“ für dieses EAM nicht angezeigt. **ANMERKUNG:** Sie werden aufgefordert, sich bei der E/A-Modul-Verwaltungsschnittstelle anzumelden. **ANMERKUNG:** Die E/A-Modul-IP-Adresse kann mit der CMC-GUI konfiguriert werden, Beschreibung in „Konfigurieren der Netzwerkeinstellungen für ein einzelnes EAM“ auf Seite 465.
Rolle	Wenn E/A-Module miteinander verbunden werden, zeigt die Rolle die Stack-Zugehörigkeit der E/A-Module an. **Mitglied** bedeutet, dass das Modul Teil eines Stack-Satzes ist. **Besitzer** bedeutet, dass das Modul ein primärer Zugangspunkt ist.
Stromstatus	Zeigt den Stromstatus des EAMs an: **Ein**, **Aus** oder **-** (Nicht vorhanden).

Tabelle 11-1. E/A-Module-Statusinformationen *(fortgesetzt)*

Element	Beschreibung
Service-Tag-Nummer	Zeigt die Service-Tag-Nummer für das EAM an. Die Service-Tag-Nummer ist eine eindeutige Kennung von Dell für Support- und Wartungsbelange. Alle Änderungen des Funktionszustands werden sowohl im Hardware- als auch im CMC-Protokoll aufgezeichnet. Weitere Informationen finden Sie unter„Ereignisprotokolle anzeigen“ auf Seite 497. **ANMERKUNG:** Passthrough-Module haben keine Service-Tag-Nummern. Nur Switch-Module haben Service-Tag-Nummern.

Anzeigen des Funktionszustands eines einzelnen EAMs

Die Seite **E/A-Modulstatus** (zu unterscheiden von der Seite *E/A-Module*-**Status**) enthält eine Übersicht zu einem einzelnen E/A-Modul.

So zeigen Sie den Funktionszustand eines einzelnen EAMs an:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Erweitern Sie in der Systemstruktur das Verzeichnis **E/A-Module**. Es werden alle EAMs (1–6) in der erweiterten Liste der **E/A-Module** angezeigt.
3. Klicken Sie auf das EAM, das Sie in der Liste der **E/A-Module** in der Systemstruktur anzeigen möchten.
4. Klicken Sie auf das Unterregister **Status**. Die Seite **E/A-Module-Status** wird angezeigt.

Tabelle 11-2. E/A-Modul-Funktionszustand-Statusinformationen

Element	Beschreibung	
Standort	Zeigt den Standort des EAMs im Gehäuse nach Gruppennummer (A, B oder C) und Steckplatznummer (1 oder 2) an. Steckplatznamen: **A1**, **A2**, **B1**, **B2**, **C1** oder **C2**.	
Name	Zeigt den Namen des EAMs an.	
Präsentation	Zeigt an, ob das E/A-Modul **Vorhanden** oder **Nicht vorhanden** ist.	
Seite „Funktionszustand“	 OK	Zeigt an, dass das EAM vorhanden ist und mit dem CMC kommuniziert. Im Falle eines Fehlers bei der Datenübertragung zwischen dem CMC und dem Server kann der CMC den Funktionszustand für das EAM nicht abrufen bzw. anzeigen.
	 Informativ	Zeigt Informationen zum EAM an, wenn keine Änderung im Funktionszustand (OK, Warnung, Schwerwiegend) aufgetreten ist. Beispiele von Zuständen, die den Status „Zur Information“ erzeugen: EAM erkannt; ein Benutzer hat das Aus- und Einschalten des EAMs angefordert.

Tabelle 11-2. E/A-Modul-Funktionszustand-Statusinformationen *(fortgesetzt)*

Element	Beschreibung	
	Warnung	Zeigt an, dass Warnungen ausgestellt wurden und **Korrekturmaßnahmen ergriffen werden müssen.** Wenn keine Korrektur-maßnahmen ergriffen werden, kann dies zu kritischen oder schwerwiegenden Fehlern führen, die Auswirkungen auf die Integrität des EAMs haben können. Beispiele von Zuständen, die Warnungen verursachen: Nichtübereinstimmung der EAM-Struktur mit der Struktur der Mezzanine-Karte des Servers; ungültige EAM-Konfiguration, wobei das neu installierte EAM nicht mit dem existierenden EAM auf derselben Gruppe übereinstimmt.
	Schwerwiegend	Zeigt an, dass mindestens eine Fehlerwarnung ausgegeben wurde. Ein schwerwiegender Zustand weist auf einen Systemfehler im EAM hin; es müssen **sofort Korrekturmaßnahmen ergriffen werden**. Beispiele von Zuständen, die einen schwerwiegenden Zustand verursachen: Fehler im EAM erkannt; EAM wurde entfernt.
	ANMERKUNG: Alle Änderungen des Funktionszustands werden sowohl im Hardware- als auch im CMC-Protokoll aufgezeichnet. Informationen zum Anzeigen der Protokolle finden Sie unter „Hardwareprotokoll anzeigen“ auf Seite 497 und „CMC-Protokoll anzeigen“ auf Seite 500.	
Stromstatus	Zeigt den Stromstatus des EAMs an: **Ein**, **Aus** oder **-** (Nicht vorhanden).	
Service-Tag-Nummer	Zeigt die Service-Tag-Nummer für das EAM an. Die Service-Tag-Nummer ist eine eindeutige Kennung von Dell für Support- und Wartungsbelange.	

Tabelle 11-2. E/A-Modul-Funktionszustand-Statusinformationen *(fortgesetzt)*

Element	Beschreibung
Fabric	Zeigt den Strukturtyp für das EAM an: Gigabit Ethernet, 10GE XAUI, 10GE KR, 10GE XAUI KR, FC 4 GBit/s, FC 8 GBit/s, SAS 3 GBit/s, SAS 6 GBit/s, Infiniband SDR, Infiniband DDR, Infiniband QDR, PCIe Bypass Generation 1, PCIe Bypass Generation 2. **ANMERKUNG:** Um EAM-Nichtübereinstimmungen innerhalb derselben Gruppe zu verhindern, ist es äußerst wichtig, dass Sie die Strukturtypen der EAMs im Gerät kennen. Informationen zur E/A-Struktur finden Sie unter „Verwaltung der E/A-Struktur“ auf Seite 453.
MAC-Adresse	Zeigt die MAC-Adresse für das EAM an. Die MAC-Adresse ist eine eindeutige Adresse, die einem Gerät vom Hardwarehersteller zu Identifikationszwecken zugewiesen ist. **ANMERKUNG:** Passthrough-Module haben keine MAC-Adressen. Nur Switch-Module haben MAC-Adressen.
Rolle	Zeigt die Stack-Zugehörigkeit eines EAMs an, wenn Module miteinander verbunden sind: • **Mitglied** - das Modul ist Teil eines Stack-Satzes. • **Master** - das Modul ist ein primärer Zugangspunkt.

Konfigurieren der Netzwerkeinstellungen für ein einzelnes EAM

Auf der Seite „E/A-Module-Setup“ können die Netzwerkeinstellungen für die Schnittstelle angegeben werden, die zur Verwaltung des EAMs verwendet wird. Für Ethernet-Switches wird die bandexterne Verwaltungsschnittstelle (IP-Adresse) konfiguriert. Die bandinterne Verwaltungsschnittstelle (das heißt VLAN1) wird nicht mittels dieser Schnittstelle konfiguriert.

ANMERKUNG: Um Einstellungen auf der Seite „E/A-Module-Konfiguration“ zu ändern, müssen Sie zur Konfiguration der EAMs der Gruppe A Struktur-A-Administratorrechte besitzen; Struktur-B-Administratorrechte für die Konfiguration von EAMs in Gruppe B; bzw. Struktur-C-Administratorrechte zum Konfigurieren von EAMs in Gruppe C.

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: Lediglich die EAMs, die im Gehäuse vorhanden sind, werden angezeigt.

ANMERKUNG: Versuchen Sie nicht, E/A-Modul-Netzwerkeinstellungen für Ethernet-Passthrough-Module oder Infiniband-Switches zu konfigurieren.

Um die Netzwerkeinstellungen für ein einzelnes EAM zu konfigurieren:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Erweitern Sie in der Systemstruktur das Verzeichnis **E/A-Module**. Klicken Sie auf das Unterregister **Setup**. Es wird die Seite **Konfiguration der E/A-Module-Netzwerkeinstellungen** angezeigt.
3. Um die Netzwerkeinstellungen für E/A-Module zu konfigurieren, tippen/wählen Sie Werte für die folgenden Eigenschaften und klicken dann auf **Anwenden**.

ANMERKUNG: Es können nur EAMs konfiguriert werden, die eingeschaltet sind.

ANMERKUNG: Die auf den EAMs festgelegte IP-Adresse vom CMC wird nicht in die permanente Startkonfiguration des Switch übertragen. Um die konfigurierte IP-Adresse permanent zu speichern, müssen Sie den Befehl `connect switch -n` oder den RACADM-Befehl `racadm connect switch -n` eingeben oder eine direkte Schnittstelle zum GUI des EAMs verwenden, um diese Adresse in der Startkonfiguration zu speichern.

Tabelle 11-3. Konfiguration der E/A-Modul-Netzwerkeinstellungen

Element	Beschreibung
Steckplatz	Zeigt den Standort des EAMs im Gehäuse nach Gruppennummer (A, B oder C) und Steckplatznummer (1 oder 2) an. Steckplatznamen: A1, A2, B1, B2, C1 oder C2. (Der Wert für den Steckplatz kann nicht geändert werden.)
Name	Zeigt den EAM-Produktnamen an. (Der EAM-Name kann nicht geändert werden.)
Stromzustand	Zeig den Stromzustand des EAMs an. (Der Stromzustand kann auf dieser Seite nicht geändert werden.)

Tabelle 11-3. Konfiguration der E/A-Modul-Netzwerkeinstellungen *(fortgesetzt)*

Element	Beschreibung
DHCP aktiviert	Hierdurch kann das EAM automatisch vom Server des dynamischen Host-Konfigurationsprotokolls (DHCP) eine IP-Adresse anfordern und abrufen. Standardeinstellung: Markiert (aktiviert).Wenn diese Option ausgewählt ist, ruft das EAM die IP-Konfiguration (IP-Adresse, Subnetzmaske, und Gateway) automatisch von einem DHCP-Server in Ihrem Netzwerk ab. **ANMERKUNG:** Wenn diese Funktion aktiviert ist, werden IP-Adresse, das Gateway und die Subnetzmasken-Eigenschaftsfelder (direkt an diese Option angrenzend) deaktiviert und sämtliche kürzlich für diese Eigenschaften eingegebenen Werte werden ignoriert. Ist diese Option ausgewählt, müssen Sie eine gültige IP-Adresse, das Gateway und die Subnetzmaske in die entsprechenden Textfelder eingeben, die direkt an diese Option angrenzen.
IP-Adresse	Gibt die IP-Adresse für die EAM-Netzwerkschnittstelle an.
Subnetzmaske	Gibt die Subnetzmaske für die EAM-Netzwerkschnittstelle an.
Gateway	Gibt das Gateway für die EAM-Netzwerkschnittstelle an.

Fehlerbehebung der EAM-Netzwerkeinstellungen

Die folgende Liste enthält Elemente zur Fehlerbehebung für die EAM-Netzwerkeinstellungen.

- Der CMC kann die IP-Adresseinstellung zu schnell nach einer Konfigurationsänderung auslesen; er in diesem Fall wird **0.0.0.0** anzeigen nach Klicken auf **Anwenden.** Sie müssen die Aktualisierungsschaltfläche 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, das direkt mit dem Switch verbunden ist.

Weitere Informationen zu EAM-Netzwerkeinstellungen finden Sie in den Dokumenten *Dell PowerConnect M6220 Switch - Wichtige Informationen* und *Weißbuch zum Dell PowerConnect 6220 Series Port Aggregator.*

12

Fehlerbehebung und Wiederherstellung

Übersicht

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.

- Konfigurationsinformationen sammeln, Fehlerstatus und Fehlerprotokolle
- Strom auf einem Remote-System verwalten
- Lifecycle Controller-Aufträge auf einem Remote-System verwalten
- Gehäuseinformationen anzeigen
- Ereignisprotokolle anzeigen
- Diagnosekonsole verwenden
- 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

Hilfsprogramme zur Gehäuseüberwachung

Konfigurationsinformationen und Gehäusestatus und Protokolle sammeln

Der Unterbefehl **racdump** bietet die Möglichkeit, mit einem einzigen Befehl umfassende Informationen zu Gehäusestatus, Konfigurationsstatus und den historischen Ereignisprotokollen abzufragen.

Seite „Verwendung"

```
racadm racdump
```

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

RACADM-Befehle können im Remote-Zugriff von der Eingabeaufforderung der seriellen, Telnet- oder SSH-Konsole aus oder über eine normale Befehlseingabeaufforderung ausgeführt werden.

Um eine Liste mit Syntax- und Befehlszeilenoptionen zu einzelnen RACDUMP-Unterbefehlen anzuzeigen, geben Sie Folgendes ein:

```
racadm help <racdump>
```

CLI-RACDUMP

Racdump beinhaltet die folgenden Untersysteme und verbindet die folgenden RACADM-Befehle:

Tabelle 12-1. Untersysteme und RACADM-Befehle

Untersystem	RACADM-Befehl
Allgemeine System-/RAC-Informationen	getsysinfo
Sitzungsinformationen	getssinfo
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	gettraclog
Systemereignisprotokoll	getsel

Seite „Verwendung“

```
racadm racdump
```

Remote-RACDUMP

Remote-RACADM ist ein Dienstprogramm auf Client-Seite, das von einer Management Station aus über die bandexterne Netzwerkschnittstelle ausgeführt werden kann. Eine Remote-Option (**-r**) wird zur Verfügung gestellt, mit der eine Verbindung zum verwalteten System hergestellt werden kann und RACADM-Unterbefehle von einer Remote-Konsole oder Management Station aus ausgeführt werden können. Um die Remote-Fähigkeit zu verwenden, sind ein gültiger Benutzername (Option **-u**), ein gültiges Kennwort (Option **-p**) sowie die CMC-IP-Adresse erforderlich.

ANMERKUNG: Wenn Sie die RACADM-Remote-Fähigkeit verwenden, müssen Sie Schreibberechtigungen für die Ordner haben, in denen Sie die RACADM-Unterbefehle für Dateivorgänge verwenden, z. B.:

- `racadm getconfig -f <file name>`
- `racadm sslcertdownload -t <Type>[-f <file name>]`

Verwendung von Remote-RACDUMP

Um den RACDUMP-Unterbefehl im Remote-Zugriff zu verwenden, geben Sie folgende Befehle ein:

```
racadm -r <CMC IP address> -u <username> -p <password>
<subcommand> <subcommand options>
racadm -i -r <CMC IP address> <subcommand> <subcommand
options>
```

ANMERKUNG: Die Option -i weist RACADM an, die Eingabe des Benutzernamens und des Kennworts interaktiv anzufordern. Ohne die Option **-i** müssen der Benutzername und das Kennwort mit dem Befehl unter Verwendung der Optionen **-u** und **-p** angegeben werden.

Beispiel:

```
racadm -r 192,168.0,120 -u root -p calvin racdump
racadm -i -r 192,168.0,120 racdump
```

Wenn die HTTPS-Anschlussnummer des iDRAC6 auf einen vom Standardanschluss (443) abweichenden benutzerdefinierten Anschluss geändert wurde, muss die folgende Syntax verwendet werden:

```
racadm -r <CMC IP address>:<port> -u <username> -p
<password> <subcommand> <subcommand options>
racadm -i -r <CMC IP address>:<port> <subcommand>
<subcommand options>
```

Telnet-RACDUMP

SSH/Telnet-RACADM wird verwendet, um über eine SSH- oder Telnet-Aufforderung einen Bezug zur RACADM-Befehlsanwendung herzustellen.

Weitere Informationen zu RACDUMP-Anweisungen finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC und CMC* auf **support.dell.com/manuals**.

LEDs zum Identifizieren von Komponenten im Gehäuse konfigurieren

Sie können die LEDs von Komponenten für alle oder einzelne Komponenten (Gehäuse, Server und E/A-Module) so einrichten, dass sie zum Identifizieren der Komponente im Gehäuse blinken.

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

Webschnittstelle verwenden

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

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf **Gehäuse**.
3. Klicken Sie auf das Register **Fehlerbehebung**.
4. Klicken Sie auf das Unterregister **Identifizieren**. Die Seite **Identifizieren** wird mit einer Liste aller Komponenten im Gehäuse angezeigt.
5. Zur Aktivierung des Blinkens einer Komponenten-LED, markieren Sie das Kontrollkästchen neben dem Gerätenamen und klicken Sie dann auf **Blinken**.
6. Zur Deaktivierung des Blinkens einer Komponenten-LED, markieren Sie das Kontrollkästchen neben dem Gerätenamen und klicken Sie dann auf **Nicht blinken**.

RACADM verwenden

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 <*Modul*> das Modul bezeichnet, dessen LED Sie konfigurieren möchten. Konfigurationsoptionen:

- `server-`*n*, wobei *n* = 1-16
- `switch-`*n*, wobei *n* = 1–6
- `cmc-activ`

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

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

Konfiguration von SNMP-Alarmen

SNMP (Einfaches Netzwerkverwaltungsprotokoll)-Traps oder *Ereignis-Traps* sind E-Mail-Ereigniswarnungen ähnlich. Sie werden von einer Management Station verwendet, um unangeforderte Daten vom CMC zu empfangen.

Sie können den CMC so konfigurieren, dass Ereignis-Traps erzeugt werden. Tabelle 12-2 gibt einen Überblick zu Ereignissen, die SNMP- und E-Mail-Alarme auslösen. Informationen zu E-Mail-Warnungen finden Sie unter „Konfiguration von E-Mail-Benachrichtigungen“ auf Seite 481.

ANMERKUNG: Beginnend mit CMC Version 2.10 ist SNMP jetzt IPv6-aktiviert. Sie können eine IPv6-Adresse oder einen vollqualifizierten Domänennamen (FQDN) im Ziel für eine Ereigniswarnung einschließen.

Tabelle 12-2. Gehäuseereignisse, die zu SNMP- und E-Mail-Warnungen f ühren können

Ereignis	Beschreibung
Lüftersondenfehler	Ein Lüfter läuft zu langsam oder überhaupt nicht.
Batteriesondenwarnung	Eine Batterie funktioniert nicht mehr.
Temperatursondenwarnung	Die Temperatur geht auf den oberen bzw. unteren Grenzwert zu.
Temperatursondenfehler	Die Temperatur ist für einen ordnungsgemäßen Betrieb zu hoch oder zu niedrig.
Redundanz herabgesetzt	Die Redundanz der Lüfter bzw. Netzteile wurde herabgesetzt.
Redundanz verloren	Es besteht keine Redundanz mehr für die Lüfter und/oder Netzteile.
Netzteilwarnung	Das Netzteil nähert sich einem Fehlerzustand.
Netzteilfehler	Das Netzteil ist fehlerhaft.
Netzteil nicht vorhanden	Ein erwartetes Netzteil ist nicht vorhanden.
Hardwareprotokollfehler	Das Hardwareprotokoll ist nicht funktionsfähig.
Hardwareprotokollwarnung	Das Hardwareprotokoll ist nahezu voll.
Server nicht vorhanden	Ein erwarteter Server ist nicht vorhanden.
Serverfehler	Der Server funktioniert nicht.
KVM nicht vorhanden	Ein erwartetes KVM-Modul ist nicht vorhanden.
KVM-Fehler	Das KVM-Modul funktioniert nicht.

Tabelle 12-2. Gehäuseereignisse, die zu SNMP- und E-Mail-Warnungen f ühren können *(fortgesetzt)*

Ereignis	Beschreibung
E/A-Modul nicht vorhanden	Ein erwartetes E/A-Modul ist nicht vorhanden.
E/A-Modul-Fehler	Das E/A-Modul funktioniert nicht.
Unverträgliche Firmware-Version	Die Firmware passt nicht zu der des Gehäuses oder des Servers.
Gehäusestrom-Schwellenfehler	Die Leistungsaufnahme innerhalb des Gehäuses hat die Eingangsleistungsgrenze des Systems erreicht.
SDKARTE fehlt	Es befindet sich kein Datenträger im SD (Secure Digital)-Kartensteckplatz des CMCs und für eine konfigurierte Funktion des CMCs ist dies erforderlich.
SDKARTEN-Fehler	Beim Zugriff auf den Datenträger im SD (Secure Digital)-Kartensteckplatz des CMCs ist ein Fehler aufgetreten.
Gehäusegruppenfehler	In der Gehäusegruppe liegt ein Konfigurationsfehler vor.

Sie können SNMP-Warnungen über die Webschnittstelle oder RACADM hinzufügen und konfigurieren.

Webschnittstelle verwenden

ANMERKUNG: Zum Hinzufügen oder Konfigurieren von SNMP-Warnungen, müssen Sie **Administratorrechte zur Konfiguration des Gehäuses** besitzen.

ANMERKUNG: Um die Sicherheit zu erhöhen, wird dringend empfohlen, das vorgegebene Kennwort für das Benutzerkonto „root" (Benutzer 1) zu ändern. Das Konto „root" ist das werkseitig voreingestellte Verwaltungskonto des CMC. Sie können das Standardkennwort für das Konto „root" ändern, indem Sie auf Benutzer-ID 1 klicken, um die Seite **Benutzerkonfiguration** zu öffnen. Hilfe zu dieser Seite finden Sie über den Link **Hilfe**, der sich auf dieser Seite oben rechts befindet.

So fügen Sie unter Verwendung der CMC-Webschnittstelle SNMP-Benachrichtigungen hinzu und konfigurieren diese:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur **Gehäuse** aus.
3. Klicken Sie auf das Register **Warnungen.** Die Seite **Gehäuseereignisse** wird angezeigt.
4. Aktivieren Sie Warnmeldungen:
   a. Aktivieren Sie die Kontrollkästchen der Ereignisse, für die Sie Warnmeldungen aktivieren möchten. Um alle Ereignisse für Warnmeldungen zu aktivieren, wählen Sie das Kontrollkästchen **Alle auswählen** aus.
   b. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.
5. Klicken Sie auf das Unterregister **Traps-Einstellungen**. Die Seite **Warnungsziele bei Gehäuseereignissen** wird angezeigt.
6. Geben Sie eine gültige Adresse in ein leeres **Ziel**-Feld ein.

   ANMERKUNG: Eine gültige Adresse ist eine Adresse, die die Trap-Warnungen empfängt. 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

7. Geben Sie die **SNMP-Community-Zeichenkette** ein, zu der die Ziel-Management Station gehört.

   ANMERKUNG: Die Community-Zeichenkette auf der Seite **Warnungsziele bei Gehäuseereignissen** unterscheidet sich von der Community-Zeichenkette auf der Seite **Gehäuse→ Netzwerk→ Dienste**. Die Community-Zeichenkette der SNMP-Traps ist die Community, die der CMC für ausgehende Traps zu Management Stations verwendet. Die Community-Zeichenkette auf der Seite **Gehäuse→ Netzwerk→ Dienste** ist die Community-Zeichenkette, die von Management Stationen zur Abfrage des SNMP-Daemon auf dem CMC verwendet wird.

8. Klicken Sie auf **Apply** (Anwenden), um die Änderungen zu speichern.

So testen Sie einen Ereignis-Trap für ein Warnungsziel:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur **Gehäuse** aus.
3. Klicken Sie auf das Register **Warnungen.** Die Seite **Gehäuseereignisse** wird angezeigt.
4. Klicken Sie auf das Unterregister **Traps-Einstellungen**. Die Seite **Warnungsziele bei Gehäuseereignissen** wird angezeigt.
5. Klicken Sie in der Spalte **Test-Trap** neben dem Ziel auf **Senden**.

ANMERKUNG: Geben Sie Trap-Ziele als korrekt formatierte numerische Adressen (IPv6 oder IPv4) oder vollqualifizierte Domänennamen (FQDNs) an. Wählen Sie ein Format, das mit Ihrer 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).

RACADM verwenden

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. Sie können Schritt 2 überspringen, wenn Sie bereits eine Filtermaske ausgewählt haben.

2. Aktivieren Sie Warnmeldungen, indem Sie Folgendes eingeben:

   ```
   racadm config -g cfgAlerting -o cfgAlertingEnable 1
   ```

3. Geben Sie die Ereignisse an, für die der CMC Warnmeldungen erstellen soll, indem Sie Folgendes eingeben:

   ```
   racadm config -g cfgAlerting -o
   cfgAlertingFilterMask <mask value>
   ```

   wobei *<Maskenwert>* ein Hexadezimalwert zwischen 0x0 und 0x017fffdf ist.

   Um den Maskenwert zu ermitteln, verwenden Sie einen wissenschaftlichen Rechner im Hexadezimalmodus und fügen die zweiten Werte der einzelnen Masken (1, 2, 4 usw.) mit der Taste <ODER> hinzu.

Um z. B. Trap-Warnungen bei Batteriesondenwarnungen (0x2), Netzteilausfällen (0x1000) und KVM-Fehlern (0x80000) zu aktivieren, geben Sie 2 <ODER> 1000 <ODER> 200000 ein, und drücken Sie die Taste <=>.

Der daraus hervorgehende Hexadezimalwert ist 208002, und der Maskenwert für den RACADM-Befehl ist 0x208002.

Tabelle 12-3. Filtermasken für Ereignis-Traps

Ereignis	Filtermaskenwert
Lüftersondenfehler	0x1
Batteriesondenwarnung	0x2
Temperatursondenwarnung	0x8
Temperatursondenfehler	0x10
Redundanz herabgesetzt	0x40
Redundanz verloren	0x80
Netzteilwarnung	0x800
Netzteilfehler	0x1000
Netzteil nicht vorhanden	0x2000
Hardwareprotokollfehler	0x4000
Hardwareprotokollwarnung	0x8000
Server nicht vorhanden	0x10000
Serverfehler	0x20000
KVM nicht vorhanden	0x40000
KVM-Fehler	0x80000
E/A-Modul nicht vorhanden	0x100000
E/A-Modul-Fehler	0x200000
Unverträgliche Firmware-Version	0x400000
Gehäusestrom-Schwellenfehler	0x1000000
SDKARTE fehlt	0x2000000
SDKARTEN-Fehler	0x4000000
Gehäusegruppenfehler	0x8000000

4 Aktivieren Sie Trap-Warnmeldungen, indem Sie Folgendes eingeben:

```
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, indem Sie Folgendes eingeben:

```
racadm config -g cfgTraps -o
cfgTrapsAlertDestIPAddr <IP-Adresse> -i <Index>
```

wobei *<IP Adress>* ein gültiges Ziel ist und *<Index>* der Indexwert, den Sie in Schritt 4 angegeben haben.

6 Geben Sie den Community-Namen an, indem Sie Folgendes eingeben:

```
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, den Sie in Schritt 4 und 5 angegeben haben.

Sie können bis zu vier Ziele für den Empfang von Trap-Warnungen konfigurieren. Um weitere Ziele hinzuzufügen, wiederholen Sie die Schritte 2 bis 6.

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 cfgTraps -i** <*Index*>. Wenn der Index konfiguriert ist, werden für die Objekte **cfgTrapsAlertDestIPAddr** und **cfgTrapsCommunityName** Werte angezeigt.

So testen Sie ein Ereignis-Trap für ein Warnungsziel. Geben Sie zolgendes 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, geben Sie Folgendes ein:

```
racadm getconfig -g cfgTraps -i <Index>
```

Herunterladen der SNMP-MIB-Datei (Management Information Base [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 über die Web-Schnittstelle herunter:

1. Melden Sie sich bei der **CMC-Web-Schnittstelle** an.
2. Klicken Sie in der Systemstruktur auf **Gehäuse.**
3. Klicken Sie auf **Netzwerk→ Dienste→ SNMP**.

   Daraufhin wird der Abschnitt **SNMP-Konfiguration** angezeigt.
4. Klicken Sie zum Herunterladen der CMC-MIB-Datei auf Ihr lokales System auf **Speichern**.

Weitere Informationen zur SNMP-MIB-Datei finden Sie im *Dell OpenManage Server Administrator-SNMP-Referenzhandbuch* unter **support.dell.com/manuals**.

Konfiguration von E-Mail-Benachrichtigungen

Wenn der CMC ein Gehäuseereignis ermittelt, wie z. B. eine Umgebungswarnung oder einen Komponentenfehler, kann er so konfiguriert werden, dass eine E-Mail-Warnung an eine oder mehrere E-Mail-Adressen gesendet wird.

Tabelle 12-2 liefert einen Überblick über die Ereignisse, die einen SNMP- und E-Mail-Alarm auslösen. Informationen zu SNMP-Warnungen finden Sie unter „Konfiguration von SNMP-Alarmen“ auf Seite 474.

Sie können E-Mail-Warnungen über die Webschnittstelle oder RACADM hinzufügen und konfigurieren.

Webschnittstelle verwenden

ANMERKUNG: Zum Hinzufügen oder Konfigurieren von E-Mail-Warnungen müssen Sie die Berechtigung als **Gehäusekonfigurations-Administrator** besitzen.

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur **Gehäuse** aus.
3. Klicken Sie auf das Register **Warnungen.** Die Seite **Gehäuseereignisse** wird angezeigt.
4. Aktivieren Sie Warnmeldungen:
   a. Aktivieren Sie die Kontrollkästchen der Ereignisse, für die Sie Warnmeldungen aktivieren möchten. Um alle Ereignisse für Warnmeldungen zu aktivieren, wählen Sie das Kontrollkästchen **Alle auswählen** aus.
   b. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.
5. Klicken Sie auf das Unterregister **E-Mail-Warnungseinstellungen**. Die Seite **E-Mail-Warnungsziele** wird angezeigt.
6. Geben Sie die IP-Adresse des SMTP-Servers an:
   a. Machen Sie das Feld **SMTP-(E-Mail-)Server** ausfindig, und geben Sie dann die SMTP-Hostnamen oder die IP-Adresse ein.

   ANMERKUNG: Sie müssen den SMTP-E-Mail-Server so konfigurieren, dass von der IP-Adresse des CMC 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.

b Geben Sie den gewünschten E-Mail-Absender für die Warnung ein oder lassen Sie das Feld frei, um den standardmäßigen E-Mail-Absender zu verwenden. Die Voreinstellung ist: cmc@<*IP_address*>, wobei <*IP_address*> die IP-Adresse des CMC ist. Wenn Sie einen Wert eingeben möchten, ist der Syntax für den E-Mail-Namen <*emailname*>[@<*domain*>] und eine E-Mail-Domäne kann optional angegeben werden.

Falls @<*domain*> nicht angegeben ist und es eine aktive CMC-Netzwerkdomäne gibt, dann wird <*emailname*>@<*cmc_domain*> als Quell-E-Mail-Adresse verwendet. Ist @<*domain*> nicht näher spezifiziert und der CMC hat keine aktive Netzwerkdomäne, dann wird die IP-Adresse des CMC verwendet (z. B.: <*emailname*>@<*IP_address*>).

c Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

7 Geben Sie die E-Mail-Adresse(n) an, die die Warnungen empfangen soll(en):

a Geben Sie eine gültige E-Mail-Adresse in ein leeres Feld **Ziel-E-Mail-Adresse** ein.

b Geben Sie optional einen **Namen** ein. Dies ist der Name der Organisation, die die E-Mail erhält. Wird ein Name für eine ungültige E-Mail-Adresse eingegeben, wird er ignoriert.

c Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

So verschicken Sie unter Verwendung der CMC-Webschnittstelle eine Test-E-Mail an ein E-Mail-Warnungsziel:

1 Melden Sie sich bei der CMC-Webschnittstelle an.

2 Wählen Sie in der Systemstruktur **Gehäuse** aus.

3 Klicken Sie auf das Register **Warnungen.** Die Seite **Gehäuseereignisse** wird angezeigt.

4 Klicken Sie auf das Unterregister **E-Mail-Warnungseinstellungen**. Die Seite **E-Mail-Warnungsziele** wird angezeigt.

5 Klicken Sie in der Spalte **Ziel-E-Mail-Adresse** neben dem Ziel auf **Senden**.

RACADM verwenden

Um eine Test-E-Mail unter Verwendung von RACADM an ein E-Mail-Warnungs-Ziel 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 Warnmeldungen, indem Sie Folgendes eingeben:

   ```
   racadm config -g cfgAlerting -o cfgAlertingEnable 1
   ```

   ANMERKUNG: Es kann nur eine Filtermaske für SNMP- und E-Mail-Warnungen festgelegt werden. Sie können Schritt 3 überspringen, wenn Sie bereits eine Filtermaske festgelegt haben.
3. Geben Sie die Ereignisse an, für die der CMC Warnmeldungen erstellen soll, indem Sie Folgendes eingeben:

   ```
   racadm config -g cfgAlerting -o
   cfgAlertingFilterMask <mask value>
   ```

   wobei *<Maskenwert>* ein hexadezimaler Wert zwischen 0x0 und 0x017fffdf ist und mit den vorangestellten Zeichen *0x* ausgedrückt werden muss. Tabelle 12-3 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 „RACADM verwenden“ auf Seite 478.
4. Aktivieren Sie E-Mail-Warnungen, indem Sie Folgendes eingeben:

   ```
   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 eine Ziel-E-Mail-Adresse an, um E-Mail-Warnungen zu erhalten:

   ```
   racadm config -g cfgEmailAlert -o
   cfgEmailAlertAddress <email address> -i <Index>
   ```

   wobei *<E-Mail-Adresse>* eine gültige E-Mail-Adresse und *<Index>* der Indexwert ist, den Sie in Schritt 4 angegeben haben.

6 Geben Sie den Namen des Teilnehmers an, der E-Mail-Warnungen empfangen soll, indem Sie Folgendes eingeben:

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertAddress <email address> -i <Index>
```

wobei *<E-Mail-Name>* der Name der Person oder Gruppe ist, die E-Mail-Warnungen empfängt, und *<Index>* der Indexwert ist, den Sie in Schritt 4 undSchritt 5 angegeben haben. Der E-Mail-Name darf bis zu 32 alphanumerische Zeichen, Bindestriche, Unterstriche und Punkte enthalten. Leerstellen sind nicht gültig.

7 Richten Sie den SMTP-Host ein, indem Sie die Datenbankeigenschaft `cfgRhostsSmtpServerIpAddr` durch folgende Eingabe konfigurieren:

```
racadm config -g cfgRemoteHosts -o
cfgRhostsSmtpServerIpAddr host.domain
```

wobei `host.domain` ein vollständig qualifizierter Domänenname ist.

Sie können bis zu vier Ziel-E-Mail-Adressen für den Empfang von E-Mail-Warnungen konfigurieren. Um weitere E-Mail-Adressen hinzuzufügen, wiederholen SieSchritt 2 bis Schritt 6.

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.

Erste Schritte, um Fehler eines Remote-System zu beheben

Die folgenden Fragen werden häufig für die Fehlerbehebung bei Problemen auf hoher Ebene auf dem verwalteten System gestellt:

1 Ist das System ein- oder ausgeschaltet?

2 Wenn eingeschaltet, funktioniert das Betriebssystem, ist es abgestürzt oder nur blockiert?

3 Wenn ausgeschaltet, wurde der Strom unerwartet ausgeschaltet?

Strom überwachen und Stromsteuerungsbefehle am Gehäuse ausführen

Sie können die Webschnittstelle oder RACADM für Folgendes verwenden:

- Aktuellen Stromstatus des Systems anzeigen.
- Durchführen eines ordentlichen Herunterfahrens durch das Betriebssystem beim Neustart und Ein- oder Ausschalten des Systems.

Informationen zur Stromverwaltung auf dem CMC und zum Konfigurieren des Strombudgets, der Redundanz und der Stromsteuerung finden Sie unter „Stromverwaltung“ auf Seite 363.

Strombudgetstatus anzeigen

Wie Sie über die Webschnittstelle oder RACADM den Strombudgetstatus für das Gehäuse, die Server und die Netzteile anzeigen, erfahren Sie unter „Anzeige des Stromverbrauchsstatus“ auf Seite 389.

Einen Stromsteuerungsvorgang ausführen

Für Anleitungen zum Hochfahren, Herunterfahren, Reset oder Ein- und Ausschalten des Systems, verwenden Sie die CMC-Webschnittstelle oder RACADM und beachten Sie „Durchführen von Energieverwaltungsmaßnahmen am Gehäuse“ auf Seite 409, „Stromsteuerungsvorgänge für ein E/A-Modul ausführen“ auf Seite 411 und „Durchführen von Energieverwaltungsmaßnahmen an einem Server“ auf Seite 412.

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 drei Steckplätze) und ein Netzteil in Seite 2 (die rechten drei 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, um die **Wechselstromredundanz** zu erhalten. (Bei vollständigem Wechselstromredundanz-Betrieb, sollten Sie sicherstellen, dass eine vollständige Netzteileinheitskonfiguration mit sechs 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:** Unzureichender Überschussstrom. 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:** Prüfen Sie auf 110 V Betrieb. Wenn eines der Netzteile an einen 110 V Stromkreis angeschlossen ist, dann müssen Sie dies zunächst als gültige Konfiguration bestätigen, bevor die Server eingeschaltet werden können. Weitere Einzelheiten dazu finden Sie in den Stromkonfigurationseinstellungen.
  - **Lösung C:** Überprüfen Sie die Einstellungen zum maximalen Stromsparmodus. Wenn dieser aktiviert ist, dann dürfen die Server nicht einschalten. Weitere Einzelheiten dazu finden Sie in den Stromkonfigurationseinstellungen.
  - **Lösung D:** 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 1.2 und höhere Versionen verfügen 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:** 2000 W wird als **Überschuss für Systemspitzen** gemeldet.
  - **Lösung:** Das Gehäuse hat in der derzeitigen Konfiguration 2000 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 sechs 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 drei Netzteile auf der linken Seite an ein Wechselstromnetz angeschlossen werden und die drei Netzteile auf der rechten Seite an ein anderes Wechselstromnetz angeschlossen werden. Wenn zwei Netzteileinheiten nicht korrekt angeschlossen sind (z. B. Netzteileinheit 3 und Netzteileinheit 4 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:** Dieses Verhalten wird erwartet, wenn die Gehäusestrom-richtlinie auf **Keine Redundanz** konfiguriert wurde. Um weitere Netzteilfehler und ein nachfolgendes Abschalten der Server zu vermeiden, stellen Sie sicher, dass das Gehäuse mindestens vier Netzteile aufweist und für die **Netzteilredundanz**-Richtlinie konfiguriert ist, sodass ein Ausfall der Netzteileinheit den Serverbetrieb nicht beeinträchtigt.
- **Problem:** Die Gesamtserverleistung verringert sich, wenn Umgebungstemp-eratur 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.

Lifecycle Controller-Aufträge auf einem Remote-System verwalten

Der Lifecycle Controller-Dienst ist auf jedem der Server verfügbar und wird durch iDRAC unterstützt. CMC stellt eine Auflistung aller Lifecycle Controller-Aufträge auf dem/den Server(n) bereit und ermöglicht das Löschen bzw. Bereinigen vorhandener Aufträge unter Verwendung der Web-Schnittstelle. Lesen Sie für Informationen zum Aktivieren des Lifecycle Controllers „Aktualisieren der Serverkomponenten-Firmware unter Verwendung des Lifecycle Controllers“ auf Seite 242.

Die Lifecycle Controller-Auftragsliste ist eine statische Liste mit den auf dem Server vorhandenen Aufträgen und muss neu geladen werden, damit die Liste und der Status der Aufträge auf dem Server auf dem neuesten Stand sind.

Tabelle 12-4 beschreibt die in der Lifecycle Controller-Auftragsliste angezeigten Informationen.

Tabelle 12-4. Status Lifecycle Controller-Aufträge

Ereignis	Filtermaskenwert
Steckplatz	Zeigt den vom Server im Gehäuse besetzten Steckplatz an. Steckplatznummern sind sequenzielle IDs von 1 bis 16 (für die 16 im Gehäuse verfügbaren Steckplätze), mit denen die Position des Servers im Gehäuse identifiziert werden kann. Wenn weniger als 16 Steckplätze mit Servern belegt sind, werden nur die mit Servern bestückten Steckplätzen angezeigt.
Name	Zeigt den Namen des Servers in jedem Steckplatz an.
Modell	Zeigt das Modell des Servers an.
Auftragskennung	Nummer, die vom Lifecycle Controller-Dienst für einen bestimmten Auftrag zugewiesen wird.
Beschreibung	Phrase, die den Typ des Auftrags auf dem Server anzeigt, wie z.B. Aktualisierungsauftrag, Neustartauftrag und so weiter.
Status	Zeigt den Status des Auftrags auf dem Server an.

Die Seite Lifecycle Controller-Aufträge ermöglicht das Löschen, bzw. Bereinigen von auf dem Server vorhandenen Aufträgen.

Löschen von Aufträgen

Der Vorgang **Löschen** ist der Standardvorgang und ermöglicht das Löschen von einzelnen oder von allen Aufträgen auf dem/den Server(n). Der Vorgang „Löschen“entfernt die ausgewählten Aufträge aus der Auftragswarteschlange. Mittels des Kontrollkästchens hinter dem Feld **Modell** ist die Auswahl von allen Aufträgen auf dem Server möglich. Einzelne Aufträge können ausgewählt werden, indem die Kontrollkästchen hinter dem Feld „Auftragsstatus“verwendet werden.

Aufträge bereinigen

Der Vorgang **Bereinigen** kann manchmal erforderlich sein, wenn sich einer oder mehrere vorhandene Aufträge in einem unbestimmten Status befinden und unter Verwendung des Vorgangs „Aufträge löschen“nicht gelöscht werden können. Der Vorgang „Bereinigen“setzt den Datenverwaltungsdienst zurück und entfernt alle Aufträge vom Server. Es kann einige Minuten dauern, bis er abgeschlossen wurde. Mittels des Kontrollkästchens hinter dem Feld „Modell“ ist die Auswahl von allen Aufträgen für den Vorgang „Bereinigen“ möglich.

ANMERKUNG: Verlassen Sie diese Seite nicht, nachdem Sie einen Vorgang für die Planung eingereicht haben.

Gehäusezusammenfassungen anzeigen

Der CMC liefert Rollup-Übersichten zu Gehäuse, aktiven und Standby-CMCs, iKVM, Lüftern, Temperatursensoren und E/A-Modulen (EAMs).

Webschnittstelle verwenden

So zeigen Sie Zusammenfassungen zu Gehäuse, CMCs, iKVM und E/A-Modulen an:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf **Gehäuse.**
3. Klicken Sie auf das Register **Zusammenfassung**. Die Seite **Gehäusezusammenfassung** wird angezeigt.

Tabelle 12-5, Tabelle 12-6, Tabelle 12-7, und Tabelle 12-8 beschreiben die auf der Seite **Gehäusezusammenfassung** angezeigten Informationen.

Tabelle 12-5. Gehäusezusammenfassung

Element	Beschreibung
Name	Zeigt den Namen des Gehäuses an. Der Name identifiziert das Gehäuse im Netzwerk. Für Informationen zur Konfiguration des Gehäusenamens, siehe „Steckplatznamen bearbeiten“ auf Seite 151.
Modell	Zeigt das Gehäusemodell oder den Hersteller an. Z. B. PowerEdge 2900.

Tabelle 12-5. Gehäusezusammenfassung *(fortgesetzt)*

Element	Beschreibung
Service-Tag-Nummer	Zeigt die Service-Tag-Nummer des Gehäuses an. Die Service-Tag-Nummer ist eine vom Hersteller eindeutig identifizierbare Nummer für Support- und Wartungsbelange.
Systemkennnummer	Zeigt die Systemkennnummer des Gehäuses an.
Standort	Zeigt die Position des Gehäuses an.
CMC Failover-bereit	Zeigt an (**Ja**, **Nein**), ob der Standby-CMC (falls vorhanden) im Falle eines Failovers die Funktion übernehmen kann.
Systemstromstatus	Zeigt den Systemstromstatus an.

Tabelle 12-6. CMC-Zusammenfassung

Element	Beschreibung
Informationen zum aktiven CMC	
Name	Zeigt den Namen des CMC an. Z. B. aktiver CMC oder Standby-CMC.
Beschreibung	Enthält eine kurze Beschreibung zum Zweck des CMC.
Uhrzeit/Datum	Zeigt das auf dem aktiven CMC eingestellte Datum und die Uhrzeit an.
Aktive CMC-Position	Zeigt den Steckplatz des aktiven CMC an.
Redundanzmodus	Wird angezeigt, wenn der Standby-CMC im Gehäuse vorhanden ist.
Primäre Firmware-Version	Zeigt die Firmware-Version des aktiven CMC an.
Letzte Aktualisierung der Firmware	Zeigt an, wann die Firmware das letzte Mal aktualisiert wurde. Wenn noch keine Aktualisierungen ausgeführt wurden, wird für diese Eigenschaft **-** (N/A) angezeigt.
Hardwareversion	Zeigt die Hardwareversion des aktiven CMC an.
MAC-Adresse	Zeigt die MAC-Adresse für die CMC-Netzwerkschnittstelle an. Die MAC-Adresse ist eine eindeutig identifizierte Adresse für den CMC über das Netzwerk.
IP-Adresse	Zeigt die IP-Adresse für die CMC-Netzwerkschnittstelle an.

Tabelle 12-6. CMC-Zusammenfassung *(fortgesetzt)*

Element	Beschreibung
Gateway	Zeigt das Gateway für die CMC-Netzwerkschnittstelle an.
Subnetzmaske	Zeigt die Subnetzmaske für die CMC-Netzwerkschnittstelle an.
DHCP verwenden (für die Netzwerkschnittstellen-IP-Adresse)	Zeigt an, ob der CMC aktiviert ist, um automatisch eine IP-Adresse vom DHCP-Server (Dynamisches Host-Konfigurationsprotokoll) anzufordern und zu empfangen (**Ja** oder **Nein**). Die Standardeinstellung für diese Eigenschaft ist **Nein**.
Primärer DNS-Server	Gibt den Namen des primären DNS-Servers an.
Alternativer DNS-Server	Gibt den Namen des alternativen DNS-Servers an.
DHCP für den DNS-Domänennamen verwenden	Zeigt die Verwendung des DHCP an, um den DNS-Domänennamen zu erhalten (**Ja, Nein)**.
DNS-Domänenname	Zeigt den DNS-Domänennamen an.
Informationen zum Standby-CMC	
Präsentation	Zeigt an (**Ja**, **Nein**), ob ein zweiter CMC (Standby-CMC) installiert ist.
Standby-Firmware-Version	Zeigt die auf dem Standby-CMC installierte CMC-Firmware-Version an.

Tabelle 12-7. iKVM-Zusammenfassung

Element	Beschreibung
Präsentation	Zeigt an, ob das iKVM-Modul vorhanden ist (Ja oder Nein).
Name	Zeigt den Namen des iKVM-Moduls an. Der Name identifiziert das iKVM-Modul im Netzwerk.
Hersteller	Zeigt das iKVM-Modell oder den Hersteller an.
Teilenummer	Zeigt die Teilenummer des iKVM an. Die Teilenummer ist eine vom Hersteller eindeutig identifizierbare Nummer. Die Namenskonventionen von Teilenummern sind von Hersteller zu Hersteller unterschiedlich.

Tabelle 12-7. iKVM-Zusammenfassung *(fortgesetzt)*

Element	Beschreibung
Firmware-Version	Zeigt die iKVM-Firmware-Version an.
Hardwareversion	Zeigt die iKVM-Hardwareversion an.
Stromstatus	Zeigt den iKVM-Stromstatus an: **Ein**, **Aus**, **-** (Nicht vorhanden).
Frontblenden-USB/Video aktiviert	Zeigt an, ob die Fronblenden-VGA- und -USB-Anschlüsse aktiviert sind (**Ja** oder **Nein**).
Zugriff auf CMC-CLI über iKVM zulassen	Zeigt an, dass CLI-Zugriff auf dem iKVM aktiviert ist (**Ja** oder **Nein**).

Tabelle 12-8. E/A-Modul-Zusammenfassung

Element	Beschreibung
Standort	Zeigt den von den E/A-Modulen belegten Steckplatz an. Es gibt sechs Steckplätze, die nach Gruppennamen (A, B oder C) und Steckplatznummer (1 oder 2) benannt sind. Steckplatznamen: **A-1**, **A-2**, **B-1**, **B-2**, **C-1** oder **C-2**.
Präsentation	Zeigt an, ob das EAM vorhanden ist (**Ja** oder **Nein**).
Name	Zeigt den Namen des EAM an.
Fabric	Zeigt die Struktur an.
Stromstatus	Zeigt den Stromstatus des EAMs an: **Ein**, **Aus** oder **-** (Nicht vorhanden).
Service-Tag-Nummer	Zeigt die Service-Tag-Nummer des EAMs an. Die Service-Tag-Nummer ist eine vom Hersteller eindeutig identifizierbare Nummer für Support- und Wartungsbelange.

RACADM verwenden

1. Öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC und melden Sie sich an.
2. Um Gehäuse- und CMC-Zusammenfassungen anzuzeigen, geben Sie Folgendes ein:

   ```
   racadm getsysinfo
   ```

3. Um die iKVM-Zusammenfassung anzuzeigen, geben Sie Folgendes ein:

   ```
   racadm getkvminfo
   ```

4. Um die EAM-Zusammenfassung anzuzeigen, geben Sie Folgendes ein:

   ```
   racadm getioinfo
   ```

Gehäuse- und Komponenten-Funktionszustand anzeigen

Webschnittstelle verwenden

So zeigen Sie Zusammenfassungen zum Gehäuse und zum Komponenten-Funktionszustand an:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf **Gehäuse**. Die Seite **Gehäusefunktionszustand** wird angezeigt.

   Der Abschnitt **Gehäuse-Grafiken** bietet eine grafische Darstellung der Gehäusevorder- und -rückseite. Die grafische Darstellung bietet einen visuellen Überblick über die im Gehäuse installierten Komponenten und deren Funktionszustand.

   Jede Grafik zeigt eine Echtzeitdarstellung der installierten Komponenten an. Der Komponentenzustand wird durch die Farbunterlegung der Komponentengrafik angezeigt.

   - Keine Unterlegung - Die Komponente ist vorhanden, wird mit Strom versorgt und kommuniziert mit dem CMC; es gibt keine Anzeichen eines ungünstigen Zustands.
   - Gelbes Vorsichtzeichen - Zeigt an, dass nur Warnungen ausgegeben wurden und dass Korrekturmaßnahmen getroffen werden müssen.

- Rotes X - Zeigt an, dass mindestens ein Fehlerzustand vorliegt. Dies bedeutet, dass der CMC weiterhin mit der Komponente kommunizieren kann und der Funktionszustand als kritisch angegeben ist.
- Grau unterlegt - Zeigt an, dass die Komponente vorhanden ist, aber nicht eingeschaltet. Sie kommuniziert nicht mit dem CMC und es gibt keine Anzeichen eines ungünstigen Zustands.

Alle Komponenten zeigen einen entsprechenden Texthinweis oder Bildschirmtipp, wenn die Maus über die Komponentengrafik bewegt wird. Der Komponentenstatus wird dynamisch aktualisiert und die Farben der Komponentengrafiken und die Texthinweise werden automatisch zur Darstellung des aktuellen Status geändert.

Wenn Sie auf die Komponenten-Untergrafik klicken, werden die Komponenteninformationen und die Quick-Links unter der Gehäusegrafik angezeigt.

Über den Abschnitt „CMC-Hardwareprotokoll“ werden zu Referenzzwecken die letzten 10 Einträge des CMC-Hardwareprotokolls angeboten.

RACADM verwenden

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

```
racadm getmodinfo
```

Ereignisprotokolle anzeigen

Die Seiten **Hardwareprotokoll und CMC-Protokoll** zeigen systemkritische Ereignisse auf dem verwalteten System an.

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 und zum Senden von Warnungen finden Sie unter „Konfiguration von SNMP-Alarmen“ auf Seite 474 und „Konfiguration von E-Mail-Benachrichtigungen“ auf Seite 481.

Beispiele von Hardwareprotokolleinträgen

```
critical System Software event: redundancy lost

Wed May 09 15:26:28 2007 normal System Software
event: log cleared was asserted

Wed May 09 16:06:00 2007 warning System Software
event: predictive failure was asserted

Wed May 09 15:26:31 2007 critical System Software
event: log full was asserted

Wed May 09 15:47:23 2007 unknown System Software
event: unknown event
```

Webschnittstelle verwenden

Sie können das Hardwareprotokoll in der CMC-Webschnittstelle anzeigen oder löschen oder als Textdatei speichern.

Tabelle 12-9enthält Beschreibungen der Informationen, die auf der Seite **Hardwareprotokoll** in der CMC-Webschnittstelle angezeigt werden.

So zeigen Sie das Hardwareprotokoll an:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf **Gehäuse**.
3. Klicken Sie auf das Register **Protokolle**.
4. Klicken Sie auf das Unterregister **Hardwareprotokoll**. Die Seite **Hardwareprotokoll** wird angezeigt.

So speichern Sie eine Kopie des Hardwareprotokolls auf der verwalteten Station oder im Netzwerk:

1 Klicken Sie auf **Protokoll speichern**.

Ein Dialogfeld wird geöffnet.

2 Wählen Sie einen Standort 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 Herunterfahrens oder Starts 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.

Tabelle 12-9. Hardwareprotokollinformationen

Element	Beschreibung	
Schweregrad	OK	Zeigt ein normales Ereignis an, das keine Korrekturmaßnahmen erfordert.
	Informativ	Zeigt einen Informationseintrag über ein Ereignis an, bei dem der Schweregradstatus nicht verändert wurde.
	Unbekannt	Zeigt ein nicht-kritisches Ereignis an, bei dem **möglichst bald Korrekturmaßnahmen vorgenommen werden sollten**, um Systemfehler zu vermeiden.
	Warnung	Zeigt ein kritisches Ereignis an, das umgehend Korrekturmaßnahmen erfordert, um Systemfehler zu vermeiden.
	Schwerwiegend	**Zeigt ein kritisches Ereignis an, das umgehend Korrekturmaßnahmen erfordert, um Systemfehler zu vermeiden.**

Tabelle 12-9. Hardwareprotokollinformationen *(fortgesetzt)*

Element	Beschreibung
Uhrzeit/Datum	Gibt das genaue Datum und die genaue Uhrzeit an, als das Ereignis eingetreten ist (z. B. Wed May 02 16:26:55 2007). Wenn Datum und Uhrzeit nicht angegeben sind, ist das Ereignis zum Zeitpunkt des Systemstarts aufgetreten.
Beschreibung	Liefert eine kurze Ereignisbeschreibung, erstellt vom CMC (zum Beispiel, `Redundanz verloren`, `Server eingesetzt`).

RACADM verwenden

So zeigen Sie das Hardware-Protokoll unter Verwendung von RACADM an:

1. Öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC und melden Sie sich an.
2. Um das Hardwareprotokoll anzuzeigen, geben Sie Folgendes ein:

   ```
   racadm getsel
   ```

   Um das Hardwareprotokoll zu löschen, geben Sie Folgendes ein:

   ```
   racadm clrsel
   ```

CMC-Protokoll anzeigen

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

ANMERKUNG: Um das Hardwareprotokoll zu löschen, müssen Sie die Berechtigung als **Administrator zum Löschen von Protokollen** besitzen.

Webschnittstelle verwenden

Sie können eine Textdateiversion des CMC-Protokolls anzeigen, speichern und über die CMC-Webschnittstelle löschen.

Sie können die Protokolleinträge nach Quelle, Datum/Uhrzeit oder Beschreibung sortieren, indem Sie auf die Spaltenüberschrift klicken. Wenn Sie wiederholt auf eine Spaltenüberschrift klicken, wird die Sortierung rückgängig gemacht.

Tabelle 12-10enthält Beschreibungen der Informationen, die auf der Seite **CMC-Protokoll** in der CMC-Webschnittstelle angezeigt werden.

So zeigen Sie das CMC-Protokoll an:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf **Gehäuse**.
3. Klicken Sie auf das Register **Protokolle**.
4. Klicken Sie auf das Unterregister **CMC-Protokoll**. Die Seite **CMC-Protokoll** wird angezeigt.
5. Um eine Kopie des CMC-Protokolls auf der verwalteten Station oder im Netzwerk zu speichern, klicken Sie auf **Protokoll speichern**.

   Ein Dialogfeld öffnet sich; wählen Sie einen Speicherort für eine Textdatei des Protokolls aus.

Tabelle 12-10. CMC-Protokollinformationen

Befehl	Ergebnis
Quelle	Zeigt die Schnittstelle an (z. B. den CMC), die das Ereignis verursacht hat.
Uhrzeit/Datum	Gibt das genaue Datum und die genaue Uhrzeit an, als das Ereignis eingetreten ist (z. B. Wed May 02 16:26:55 2007).
Beschreibung	Umfasst eine kurze Beschreibung der Maßnahme, wie Anmeldung oder Abmeldung, Fehler bei der Anmeldung oder Löschen der Protokolle. Beschreibungen werden vom CMC erstellt.

RACADM verwenden

So zeigen Sie die CMC-Protokollinformationen unter Verwendung von RACADM an:

1. Öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC und melden Sie sich an.
2. Um das Hardwareprotokoll anzuzeigen, geben Sie Folgendes ein:

   ```
   racadm getraclog
   ```

   Um das Hardwareprotokoll zu löschen, geben Sie Folgendes ein:

   ```
   racadm clrraclog
   ```

Diagnosekonsole verwenden

Über die Seite **Diagnosekonsole** kann ein fortgeschrittener Benutzer oder ein Benutzer unter der Leitung des technischen Supports mithilfe von CLI-Befehlen Gehäusehardware-Probleme diagnostizieren.

ANMERKUNG: Zum Modifizieren dieser Einstellungen müssen Sie die Berechtigung als **Administrator zum Ausführen von Debug-Befehlen** besitzen.

So greifen Sie auf die Seite **Diagnosekonsole** zu:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf **Gehäuse**.
3. Klicken Sie auf das Register **Fehlerbehebung**.
4. Klicken Sie auf das Unterregister **Diagnose**. Die Seite **Diagnosekonsole** wird angezeigt.

Sie führen einen Diagnose-CLI-Befehl aus, indem Sie den Befehl in das Feld **RACADM-Befehl eingeben** tippen und dann auf **Senden** klicken, um den Diagnosebefehl auszuführen. Es wird eine Seite mit Diagnoseergebnissen eingeblendet.

Klicken Sie zum Zurückkehren auf die Seite **Diagnosekonsole** auf **Zurück zur Seite Diagnosekonsole** oder auf **Aktualisieren**.

Die Diagnosekonsole unterstützt die Befehle, die in Tabelle 12-11 aufgelistet sind sowie die RACADM-Befehle.

Tabelle 12-11. Unterstützte Diagnosebefehle

Befehl	Ergebnis
arp	Zeigt den Inhalt der Tabelle des Adressauflösungsprotokolls (ARP) an. ARP-Einträge dürfen nicht hinzugefügt oder gelöscht werden.
ifconfig	Zeigt den Inhalt der Netzwerkschnittstellentabelle an.
netstat	Druckt den Inhalt der Routingtabelle aus.

Tabelle 12-11. Unterstützte Diagnosebefehle *(fortgesetzt)*

Befehl	Ergebnis
ping <*IP-Adresse*>	Überprüft, ob die Ziel-<*IP-Adresse*> unter Verwendung des Inhalts der aktuellen Routingtabelle vom CMC aus erreichbar ist. In das Feld rechts neben dieser Option muss eine Ziel-IP-Adresse eingegeben werden. Ein ICMP-Echo-Paket (Internet-Steuerungsmeldungsprotokoll) wird basierend auf dem aktuellen Inhalt der Routingtabelle zur Ziel-IP-Adresse gesendet.
gettracelog	Zeigt das Ablaufverfolgungsprotokoll an (die Anzeige des Protokolls kann einige Sekunden dauern). Der Befehl **gettracelog -i** gibt die Anzahl der Einträge im Ablaufverfolgungsprotokoll zurück. **ANMERKUNG:** Weitere Informationen zum gettracelog-Befehl finden Sie im Abschnitt zum gettracelog-Befehl im *RACADM-Befehlszeilenreferenzhandbuch für iDRAC7 und CMC*.

Komponenten zurücksetzen

Auf der Seite **Komponenten zurücksetzen** können Benutzer den aktiven CMC zurücksetzen oder Server virtuell neu einsetzen, wodurch ein Entfernen und Wiedereinsetzen der entsprechenden Server simuliert wird. 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 greifen Sie auf die Seite **Diagnosekonsole** zu:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf **Gehäuse**.
3. Klicken Sie auf das Register **Fehlerbehebung**.
4. Klicken Sie auf das Unterregister **Komponenten zurücksetzen**. Die Seite **Komponenten zurücksetzen** wird angezeigt. Der Abschnitt **CMC-Zusammenfassung** auf der Seite **Komponenten zurücksetzen** zeigt die folgenden Informationen an:

Tabelle 12-12. CMC-Zusammenfassung

Attribut	Beschreibung	
Seite „Funktionszustand“	 OK	Der CMC ist vorhanden und kommuniziert mit seinen Komponenten.
	 Informativ	Zeigt Informationen über FlexAddress an, wenn beim Funktionsstatus (OK, Warnung, Schwerwiegend) keine Änderung eingetreten ist.
	 Warnung	Warnungen wurden ausgegeben und **Korrekturmaßnahmen müssen getroffen werden**. Wenn keine Korrekturmaßnahmen vorgenommen werden, können kritische oder schwerwiegende Fehler auftreten, die sich auf die Integrität des CMC auswirken können.
	 Schwerwiegend	Mindestens eine Fehlerwarnung wurde ausgegeben. Ein schwerwiegender Status repräsentiert einen CMC-Systemfehler. **Es müssen umgehend Korrekturmaßnahmen getroffen werden**.
Uhrzeit/Datum		Zeigt das Datum und die Uhrzeit für den CMC unter Verwendung des Formats *MM/TT/JJJJ* an, wobei *MM* der Monat, *DD* der Tag und *JJJJ* das Jahr ist.
Aktive CMC-Position		Zeigt den Standort des aktiven CMC an.
Redundanzmodus	Zeigt **Redundant** an, wenn ein Standby-CMC im Gehäuse vorhanden ist und zeigt **Keine Redundanz** an, wenn kein Standby-CMC im Gehäuse vorhanden ist.	

5 Der Abschnitt **Virtuelles Neueinsetzen von Servern** auf der Seite **Komponenten zurücksetzen** zeigt die folgenden Informationen an:

Tabelle 12-13. Virtuelles Neueinsetzen von Servern

Attribut	Beschreibung	
Steckplatz	Zeigt den vom Server im Gehäuse besetzten Steckplatz an. Steckplatznummern sind sequenzielle IDs von 1 bis 16, die bei der Identifizierung der Position des Servers im Gehäuse hilfreich sind.	
Name	Zeigt den Namen des Servers in jedem Steckplatz an.	
Präsentation	Zeigt an, ob der Server im Steckplatz vorhanden ist (**Ja** oder **Nein**).	
Seite „Funktionszustand“	 OK	Der Server ist vorhanden und kommuniziert mit dem CMC. Im Falle eines Fehlers bei der Datenübertragung zwischen dem CMC und dem Server kann der CMC den Funktionszustand des Servers weder abrufen noch anzeigen.
	 Informativ	Zeigt Informationen über den Server an, wenn beim Funktionszustand (OK, Warnung, Schwerwiegend) keine Änderung eingetreten ist.
	 Warnung	Warnungen wurden ausgegeben und **Korrekturmaßnahmen müssen getroffen werden**. Wenn keine Korrekturmaßnahmen vorgenommen werden, können kritische oder schwerwiegende Fehler auftreten, die sich auf die Integrität des Servers auswirken können.
	 Schwerwiegend	Mindestens eine Fehlerwarnung wurde ausgegeben. Ein schwerwiegender Status repräsentiert einen CMC-Systemfehler. **Es müssen umgehend Korrekturmaßnahmen getroffen werden**.

Tabelle 12-13. Virtuelles Neueinsetzen von Servern *(fortgesetzt)*

Attribut	Beschreibung
iDRAC-Status	Zeigt den Status des durch den Server-iDRAC eingebetteten Verwaltungscontrollers an: • **K. A** - Server ist nicht vorhanden oder das Gehäuse ist nicht eingeschaltet. • **Bereit** - iDRAC ist bereit und funktioniert normal. • **Beschädigt** - iDRAC-Firmware ist beschädigt. Verwenden Sie das iDRAC-Firmware-Aktualisierungsdienstprogramm, um die Firmware zu reparieren. • **Fehlgeschlagen** - Kann nicht mit iDRAC kommunizieren. Verwenden Sie das Kontrollkästchen „Virtuelles Neueinsetzen“, um den Fehler zu beseitigen. Falls dies fehlschlägt, entfernen Sie den Server manuell und setzen Sie ihn wieder ein, um den Fehler zu beseitigen. • **FW-Aktualisierung** - iDRAC-Firmware-Aktualisierung läuft; warten Sie, bis die Aktualisierung beendet ist, bevor Sie eine Maßnahme treffen. • **Initialisierung** - iDRAC-Rücksetzung läuft; warten Sie, bis der Controller den Einschaltvorgang abgeschlossen hat, bevor Sie eine Maßnahme treffen.
Stromzustand	Zeigt den Serverstromstatus an: • **K. A.** - Der CMC hat die Stromversorgung des Servers nicht bestimmt. • **Aus** - Der Server oder das Gehäuse ist ausgeschaltet. • **Ein** - Das Gehäuse und der Server sind eingeschaltet. • **Einschalten** - vorübergehender Zustand zwischen Aus und Ein. Wenn der Einschaltvorgang abgeschlossen ist, ändert sich der Stromzustand zu EIN. • **Ausschalten** - vorübergehender Zustand zwischen Ein und Aus. Wenn der Abschaltvorgang abgeschlossen ist, ändert sich der Stromzustand zu AUS.
Virtuelles Neueinsetzen	Wählen Sie das Kontrollkästchen aus, um diesen Server virtuell neu einzusetzen.

6 Um einen Server virtuell neu einzusetzen, klicken Sie auf das Kontrollkästchen des neu einzusetzenden Servers und wählen Sie dann **Auswahl anwenden**. Dieser Vorgang simuliert das Entfernen und Wiedereinsetzen eines Servers.

7 Wählen Sie **CMC zurücksetzen/Failover** aus, um zu bewirken, dass der aktive CMC zurückgesetzt wird. Wenn ein Standby-CMC vorhanden ist und ein Gehäuse vollständig redundant ist, tritt ein Failover auf und bewirkt, dass der Standby-CMC aktiv wird.

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 verschiedenen 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.

Der CMC umfasst Hilfsprogramme zur Behebung dieser Fehler, wobei das CMC-Ablaufverfolgungsprotokoll die primäre Quelle für Fehlerbehebungsinformationen ist. Dieses Protokoll enthält eine Fehlermeldung für NTP-bezogene Ausfälle. Wenn der CMC sich nicht mit einem konfigurierten Remote-NTP-Server synchronisieren kann, basiert der CMC sein Timing auf der lokalen Systemuhr.

Wenn der CMC anstatt mit einem Remote-Zeitserver mit der lokalen Systemuhr synchronisiert ist, enthält das Ablaufverfolgungsprotokoll 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 kein „*“ bei einem der konfigurierten Server angezeigt wird, ist möglicherweise etwas nicht richtig konfiguriert. Die Ausgabe des obigen Befehls enthält auch 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 starten Sie den ntpd neu, indem Sie NTP deaktivieren, 5-10 Sekunden warten und dann NTP wieder aktivieren.

ANMERKUNG: NTP benötigt 3 zusätzliche Minuten, 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.

Es kann andere NTP-bezogene Ablaufverfolgungsprotokolleinträge geben, die bei der Fehlerbehebung nützlich sein können. Falls es sich eine fehlerhafte Konfiguration einer NTP-Server-IP-Adresse handelt, 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-GUI finden Sie im „Diagnosekonsole verwenden“ auf Seite 502.

LED-Farben und Blinkmuster interpretieren

Die LEDs am Gehäuse liefern Informationen anhand der Farbe und durch Blinken bzw. Nicht-Blinken:

- 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 (siehe „LEDs zum Identifizieren von Komponenten im Gehäuse konfigurieren“ auf Seite 473).

Tabelle 12-14. LED-Farbe und Blinkmuster

Komponente	LED-Farbe, Blinkmuster	Bedeutung
CMC	Grün, beständig leuchtend	Netzstrom eingeschaltet
	Grün, blinkend	Firmware wird hochgeladen
	Grün, dunkel	Ausgeschaltet
	Blau, beständig leuchtend	Aktiv
	Blau, blinkend	Vom Benutzer aktivierte Modulidentifizierung
	Gelb, beständig leuchtend	Nicht verwendet
	Gelb, blinkend	Fehler
	Blau, dunkel	Standby
iKVM	Grün, beständig leuchtend	Netzstrom eingeschaltet
	Grün, blinkend	Firmware wird hochgeladen
	Grün, dunkel	Ausgeschaltet
	Gelb, beständig leuchtend	Nicht verwendet
	Gelb, blinkend	Fehler
	Gelb, dunkel	Kein Fehler
Server	Grün, beständig leuchtend	Netzstrom eingeschaltet
	Grün, blinkend	Firmware wird hochgeladen
	Grün, dunkel	Ausgeschaltet
	Blau, beständig leuchtend	Normal
	Blau, blinkend	Vom Benutzer aktivierte Modulidentifizierung
	Gelb, beständig leuchtend	Nicht verwendet
	Gelb, blinkend	Fehler
	Blau, dunkel	Kein Fehler

Tabelle 12-14. LED-Farbe und Blinkmuster *(fortgesetzt)*

Komponente	LED-Farbe, Blinkmuster	Bedeutung
E/A-Modul (Allgemein)	Grün, beständig leuchtend	Netzstrom 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-Modul (Passthrough)	Grün, beständig leuchtend	Netzstrom 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
Lüfter	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

Tabelle 12-14. LED-Farbe und Blinkmuster *(fortgesetzt)*

Komponente	LED-Farbe, Blinkmuster	Bedeutung
Netzteileinheit	(Oval) Grün, beständig leuchtend	Wechselstrom OK
	(Oval) Grün, blinkend	Nicht verwendet
	(Oval) Grün, dunkel	Wechselstrom nicht OK
	Gelb, beständig leuchtend	Nicht verwendet
	Gelb, blinkend	Fehler
	Gelb, dunkel	Kein Fehler
	(Kreis) Grün, beständig leuchtend	Gleichstrom OK
	(Kreis) Grün, dunkel	Gleichstrom nicht OK

Fehlerbehebung an einem CMC, der nicht mehr reagiert

ANMERKUNG: Es ist nicht möglich, sich über eine serielle Konsole beim Standby-CMC anzumelden.

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.

Problem durch Beobachtung der LEDs erkennen

Wenn Sie den CMC von vorne betrachten, so wie er im Gehäuse installiert ist, sehen Sie auf der linken Seite der Karte zwei LEDs.

Obere LED - Die obere grüne LED zeigt die Stromversorgung an. Wenn Sie NICHT eingeschaltet ist:

1. Überprüfen Sie, dass mindestens ein Netzteil mit Netzstrom versorgt wird.
2. 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.

Untere LED - 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 obere grüne LED auf dem Standby-CMC aktiviert.

Wiederherstellungsinformationen über die serielle DB-9-Schnittstelle abrufen

Wenn die untere LED gelb leuchtet, sollten über die serielle DB-9-Schnittstelle, die sich an der Vorderseite des CMC befindet, Wiederherstellungsinformationen verfügbar sein.

So rufen Sie Wiederherstellungsinformationen ab:

1. Installieren Sie ein NULL-Modemkabel zwischen dem CMC und dem Client-Computer.
2. Öffnen Sie einen Terminalemulator Ihrer Wahl (z. B. HyperTerminal oder Minicom). Stellen Sie Folgendes ein: 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 Folgendes ein:

   ```
   recover
   ```

   Drücken Sie dann die Taste <Eingabe>. Beispiele von Eingabeaufforderungen:

   ```
   recover1[self test] CMC 1 self test failure
   ```

   ```
   recover2[Bad FW images] CMC2 has corrupted images
   ```

   - Wenn die Eingabeaufforderung auf einen Selbsttestfehler hinweist, befinden sich keine betriebsfähigen Komponenten auf dem CMC. Der CMC ist unbrauchbar und muss zu Dell zurückgesendet werden.
   - Wenn die Eingabeaufforderung **Beschädigte Firmware-Images** anzeigt, befolgen Sie die Schritte unter „Firmware-Image wiederherstellen“ auf Seite 515, um das Problem zu beheben.

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 Wiederherstellungs-vorgangs 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 über die CMC-Webschnittstelle (siehe „Diagnosekonsole verwenden“) oder RACADM (siehe „RACADM-Befehlszeilenschnittstelle verwenden“ und Abschnitt **gettracelog**-Befehl im *RACADM-Befehlszeilenreferenzhandbuch für iDRAC6 und CMC* auf das Ablaufverfolgungsprotokoll zugreifen.

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.

Vergessenes Administratorkennwort zurücksetzen

VORSICHTSHINWEIS: Manche Reparaturarbeiten dürfen nur von qualifizierten Servicetechnikern durchgeführt werden. Fehlerbehebungsmaßnahmen oder einfache Reparaturen sollten Sie nur dann selbst durchführen, wenn dies in der Produktdokumentation autorisiert ist, oder wenn Sie vom Team des Online- oder Telefonsupports dazu aufgefordert werden. Schäden durch nicht von Dell genehmigte Wartungsarbeiten werden nicht durch die Garantie abgedeckt. Lesen und befolgen Sie die zusammen mit dem Produkt zur Verfügung gestellten Sicherheitshinweise.

Um Verwaltungsvorgänge auszuführen, benötigt der Benutzer **Administrator**-Rechte. Die CMC-Software hat eine Benutzerkonten-Kennwortschutzfunktion, die deaktiviert werden kann, falls das Administratorkennwort abhanden gekommen ist. Wenn das Administratorkennwort vergessen wurde, kann es mit Hilfe des PASSWORD_RSET-Jumpers auf dem der CMC-Platine wieder-hergestellt werden.

Die CMC-Platine hat einen zweipoligen Reset-Jumper (siehe Abbildung 12-1). Wird ein Jumper auf den Reset-Kontakt gesteckt, werden das Standardadministratorkonto und das Kennwort aktiviert und auf die voreingestellten Werte **Benutzername: root** und **Kennwort: calvin** gesetzt. Das Administratorkonto wird ungeachtet dessen, ob das Konto entfernt wurde oder nicht oder ob das Kennwort geändert wurde, zurückgesetzt.

ANMERKUNG: Stellen Sie sicher, dass sich das CMC-Modul in einem passiven Modus befindet, bevor Sie beginnen.

Um Verwaltungsvorgänge auszuführen, benötigt der Benutzer **Administrator**-Rechte. Wenn das Administratorkennwort vergessen wurde, kann es mit Hilfe des PASSWORD_RST-Jumpers auf der CMC-Platine wiederhergestellt werden.

Der PASSWORD_RST-Jumper nutzt einen zweipoligen Konnektor (siehe Abbildung 12-1).

Während der PASSWORD_RST-Jumper installiert wird, wird das standardmäßige Administratorkonto und Kennwort aktiviert und auf die folgenden Standardwerte eingestellt:

```
username: root

password: calvin
```

Das Administratorkonto wird vorübergehend zurückgesetzt, unabhängig davon, ob das Administratorkonto entfernt worden ist oder das Kennwort geändert wurde.

ANMERKUNG: Wenn der PASSWORD_RST-Jumper installiert wird, wird eine standardmäßige serielle Konsolenkonfiguration (anstelle von Konfigurationseigenschaftswerten) der folgenden Art verwendet:

```
cfgSerialBaudRate=115200

cfgSerialConsoleEnable=1

cfgSerialConsoleQuitKey=^\

cfgSerialConsoleIdleTimeout=0

cfgSerialConsoleNoAuth=0

cfgSerialConsoleCommand=""

cfgSerialConsoleColumns=0
```

1 Drücken Sie die CMC-Freigaberiegel am Handgriff und drehen Sie den Handgriff von der Modulvorderseite weg. Schieben Sie das CMC-Modul aus dem Gehäuse.

ANMERKUNG: Elektrostatische Entladung (ESD) kann den CMC beschädigen. Unter bestimmten Bedingungen baut sich in Ihrem Körper oder in einem Gegenstand elektrostatische Spannung auf, die sich dann am CMC entladen kann. Um Schäden durch elektrostatische Entladung zu vermeiden, müssen Sie Vorsichtsmaßnahmen treffen, um die elektrostatische Spannung von Ihrem Körper abzuleiten, während Sie den CMC handhaben und diesen außenhalb des Gehäuses berühren.

2 Entfernen Sie den Jumper-Stecker von Kennwort-Reset-Kontakt und setzen Sie einen zweipoligen Jumper zur Aktivierung des Standard-Administrator-Kontos ein. Abbildung 12-1 zeigt die Position des Kennwort-Jumpers auf der CMC-Systemplatine.

Abbildung 12-1. Kennwort-Reset-Jumperposition

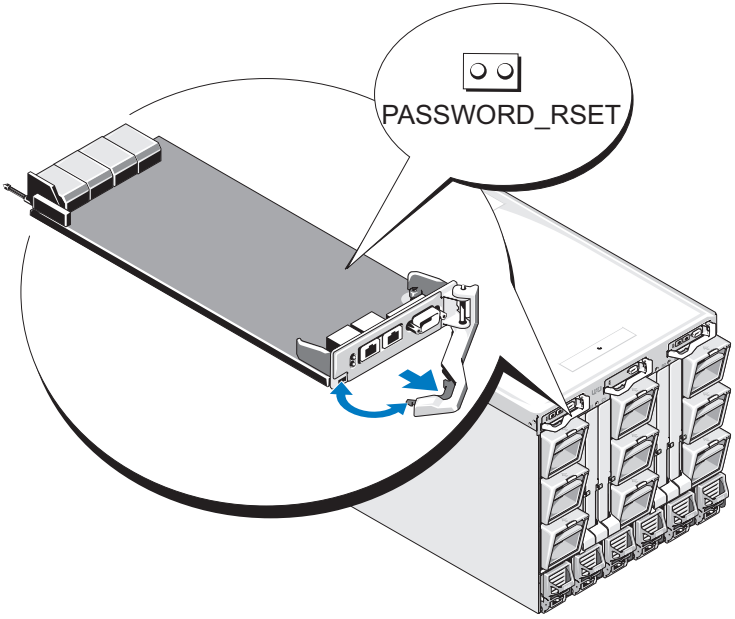


Tabelle 12-15. CMC Kennwort-Jumpereinstellungen

PASSWORD_RSET	(Standardeinstellung)	Die Kennwort-Resetfunktion ist deaktiviert.
		Die Kennwort-Resetfunktion ist deaktiviert.

3 Schieben Sie das CMC-Modul in das Gehäuse. Schließen Sie alle Kabel erneut an, die eventuell abgezogen wurden.

ANMERKUNG: Stellen Sie sicher, dass das CMC-Modul der aktive CMC wird und der aktive CMC bleibt, bis die verbleibenden Schritte vollzogen sind.

4 Wenn das überbrückte CMC-Modul der einzige CMC ist, warten Sie einfach, bis der Neustart abgeschlossen ist. Wenn Sie redundante CMCs in Ihrem Gehäuse haben, dann leiten Sie eine Umschaltung ein, um das überbrückte CMC-Modul zu aktivieren. In der GUI-Schnittstelle:

   a Navigieren Sie zur Seite **Gehäuse**, klicken auf das Unterregister **Strom→ Steuerung**.

   b Wählen Sie die Schaltfläche **Reset CMC (Warmstart)** und klicken Sie auf **Anwenden**.

   Die CMC wird automatisch auf das redundante Modul umgeschaltet und das Modul wird jetzt aktiv.

5 Melden Sie sich beim aktiven CMC mit dem Standard-Administrator-Benutzernamen **root** und dem Kennwort **calvin** an und stellen Sie sämtliche notwendigen Benutzerkonteneinstellungen wieder her. Die vorhandenen Konten und Kennwörter werden nicht deaktiviert und sind noch immer aktiv.

6 Führen Sie alle erforderlichen Verwaltungsmaßnahmen durch, einschließlich der Erstellung eines neuen Administrator-Kennwortes, um das abhanden gekommene Kennwort zu ersetzen.

7 Entfernen Sie den zweipoligen PASSWORD_RST-Jumper und setzen Sie den Jumper-Stecker wieder auf.

   a Drücken Sie die CMC-Freigaberiegel am Handgriff und drehen Sie den Handgriff von der Modulvorderseite weg. Schieben Sie das CMC-Modul aus dem Gehäuse.

   b Entfernen Sie den zweipoligen Jumper und setzen Sie den Jumper-Stecker wieder auf.

   c Schieben Sie das CMC-Modul in das Gehäuse. Schließen Sie alle Kabel wieder an, die eventuell getrennt wurden. Wiederholen Sie Schritt 4, um das überbrückte CMC-Modul zum aktiven CMC zu machen.

Gehäusekonfigurationseinstellungen und Zertifikate speichern und wiederherstellen.

Navigieren Sie im CMC-GUI auf **Gehäuseübersicht→ Setup→ Gehäusesicherung**. Es wird der Bildschirm **Gehäuseübersicht** angezeigt.

So speichern Sie eine Sicherung der Gehäusekonfiguration:

1. Klicken Sie auf dem Bildschirm **Gehäusesicherung** auf **Speichern**.
2. Überschreiben Sie den Standarddateipfad (optional) und klicken Sie auf **OK**, um die Datei zu speichern.

ANMERKUNG: 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.

So stellen Sie die Gehäusekonfiguration wieder her:

1. Klicken Sie auf dem Bildschirm **Gehäusesicherung** auf **Durchsuchen**.
2. Navigieren Sie zur Sicherungsdatei oder geben Sie den Namen der Sicherungsdatei ein und klicken Sie anschließend auf **Öffnen**, um sie auszuwählen.
3. Klicken Sie auf **Wiederherstellen**.

ANMERKUNG: CMC wird beim Wiederherstellen der Konfiguration nicht zurückgesetzt, jedoch kann es einige Zeit dauern, bis jedwede geänderte/neue Konfiguration effektiv durch die CMC-Dienste durchgesetzt wird. Nach der erfolgreichen Fertigstellung werden alle aktuellen Sitzungen beendet.

Warnmeldungen zur Fehlerbehebung

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.

Sie können SNMP-Warnungen über die Webschnittstelle konfigurieren. Weitere Informationen finden Sie unter „Konfiguration von SNMP-Alarmen“ auf Seite 474.

13

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 Symbole 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 oder der Server entfernt wird, das/der die Ursache des Problems ist, oder indem, im Falle von Serverfehlern, die iDRAC Web-Schnittstelle oder Befehlszeilenschnittstelle zum Löschen des Systemereignisprotokolls (SEL/System Event Log) verwendet wird, um die Serverfehler vom LCD-Bedienfeld zu entfernen.

LCD-Schnittstelle verwenden

Über das LCD-Bedienfeld können Sie Konfigurationen und Diagnosen durchführen und Statusinformationen zum Gehäuse und dessen Inhalt abrufen.

LCD-Navigation

Verwenden Sie die Schaltflächen auf der rechten Seite des LCD-Bildschirms, um das LCD-Bedienfeld zu bedienen. 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.

Die mittlere Schaltfläche aktiviert das ausgewählte Element.

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 Tabelle 13-1 beschriebenen Symbole werden zum Wechseln zwischen LCD-Bildschirmen verwendet:

Tabelle 13-1. LCD-Bedienfeld-Navigationssymbole

Symbol Normal	Symbol hervorgehoben	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.
 		**Drehen**. Markieren und drücken Sie die mittlere Schaltfläche, um zwischen der vorderen und hinteren graphischen Ansicht des Gehäuses zu wechseln. **ANMERKUNG:** Der gelbe Hintergrund zeigt an, dass die gegenüberliegende Ansicht Fehler beinhaltet.
		**Komponenten identifizieren** Blinkende, blaue LED an einem Bauteil. **ANMERKUNG:** Um dieses Symbol herum ist ein blinkendes, blaues Rechteck vorhanden, wenn **Komponenten identifizieren** aktiviert ist.

Menü Main (Hauptmenü)

Vom **Hauptmenü** aus können Sie zu den folgenden Bildschirmen wechseln:

- **LCD-Setup-Menü** - wählen Sie die zu verwendende Sprache und den LCD-Bildschirm aus, der angezeigt wird, wenn niemand das LCD verwendet.
- **Server** - zeigt Statusinformationen für Server an.
- **Gehäuse** - zeigt Statusinformationen für das Gehäuse an.

1. Verwenden Sie die Schaltflächen Nach oben bzw. Nach unten, um ein Element zu markieren.
2. Drücken Sie die mittlere Schaltfläche, um die Auswahl zu aktivieren.

Einrichtungsmenü für das LCD-Modul

Im **LCD-Setup**-Menü wird ein Menü mit Elementen angezeigt, die konfiguriert werden können:

- **Spracheinstellung** - wählen Sie die Sprache aus, die für LCD-Bildschirmtexte und Meldungen verwendet werden soll.
- **Standardbildschirm** - wählen Sie den Bildschirm aus, der angezeigt werden soll, wenn keine Aktivität auf dem LCD-Bedienfeld stattfindet.

1. 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 **Hauptmenü** zurückkehren möchten.
2. Drücken Sie die mittlere Schaltfläche, um die Auswahl zu aktivieren.

Spracheinstellungsbildschirm

Auf dem **Spracheinstellungsbildschirm** 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**
- **Serverstatus** (vordere graphische Ansicht des Gehäuses)
- **Modulstatus** (hintere graphische Ansicht des Gehäuses)
- **Benutzerdefiniert** (Dell-Logo mit Gehäusename)

Der derzeit aktive Standardbildschirm ist hellblau hervorgehoben.

1. Markieren Sie mit den Schaltflächen 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.

Graphischer Serverstatusbildschirm

Der **Graphische Serverstatus**-Bildschirm zeigt Symbole für jeden Server an, der im Gehäuse installiert ist, sowie den jeweiligen allgemeinen Funktionszustand. Der Serverfunktionszustand wird durch die Farbe des Serversymbols angegeben:

- Grau - Server ist ausgeschaltet; es liegen keine Fehler vor
- Grün - Server ist eingeschaltet; es liegen keine Fehler vor
- Gelb – Server weist einen oder mehrere nicht-kritische Fehler auf
- Rot – Modul weist einen oder mehrere kritische Fehler auf
- Schwarz - Server ist nicht vorhanden

Ein blinkendes hellblaues Rechteck um ein Serversymbol herum gibt an, dass der Server markiert ist.

So zeigen Sie den Bildschirm für den **Status des graphischen Moduls** an:

1. Markieren Sie das Drehen-Symbol.
2. Drücken Sie die mittlere Schaltfläche.

So zeigen Sie den Statusbildschirm für einen Server an:

1. Markieren Sie den gewünschten Server mit den Pfeilschaltflächen.
2. Drücken Sie die mittlere Schaltfläche. Der **Serverstatus**-Bildschirm wird angezeigt.

So kehren Sie zum Hauptmenü zurück:

1. Markieren Sie das **Zurück-Symbol** mit den Pfeilschaltflächen.
2. Drücken Sie die mittlere Schaltfläche.

Graphischer Modulstatus-Bildschirm

Im Bildschirm des **Status des graphischen Moduls** werden alle Module angezeigt, die auf der Rückseite des Gehäuses installiert sind, und es werden zusammenfassende Informationen zum Funktionszustand für jedes Modul bereitgestellt. Der Modulzustand wird durch die Farbe der einzelnen Modulsymbole wie folgt dargestellt:

- Grau – Modul ist ausgeschaltet oder im Standby-Modus; es liegen keine Fehler vor
- Grün – Modul ist eingeschaltet; es liegen keine Fehler vor
- Gelb – Modul weist einen oder mehrere nicht-kritische Fehler auf
- Rot – Modul weist einen oder mehrere kritische Fehler auf
- Schwarz – Modul ist nicht vorhanden

Ein blinkendes hellblaues Rechteck um ein Modulsymbol herum gibt an, dass das Modul markiert ist.

So zeigen Sie den **Graphischen Serverstatusbildschirm** an:

1. Markieren Sie das Drehen-Symbol.
2. Drücken Sie die mittlere Schaltfläche.

So zeigen Sie den Statusbildschirm für ein Modul an:

1. Verwenden Sie die vier Pfeil-Schaltflächen, um das gewünschte Modul zu markieren.
2. Drücken Sie die mittlere Schaltfläche. Der **Modulstatusbildschirm** wird angezeigt.

So kehren Sie zum **Hauptmenü** zurück:

1. Markieren Sie das **Zurück-Symbol** mit den Pfeilschaltflächen.
2. Drücken Sie die mittlere Schaltfläche. Das **Hauptmenü** wird angezeigt.

Gehäuse-Menübildschirm

Von diesem Bildschirm aus können Sie zu folgenden Bildschirmen wechseln:

- **Modulstatus**-Bildschirm
- **Gehäusestatus**-Bildschirm
- **IP-Zusammenfassungs**-Bildschirm
- **Hauptmenü**

1. Markieren Sie das gewünschte Element mit den Navigationsschaltflächen. (Markieren Sie das **Zurück**-Symbol, um zum **Hauptmenü** zurückzukehren.)
2. Drücken Sie die mittlere Schaltfläche. Der ausgewählte Bildschirm wird angezeigt.

Modulstatusbildschirm

Im **Modulstatus**-Bildschirm werden Informationen und Fehlermeldungen zu einem Modul angezeigt. Informationen zu den Meldungen, die auf diesem Bildschirm angezeigt werden können, finden Sie unter „LCD-Modul- und Serverstatusinformationen“ auf Seite 541 und „LCD-Fehlermeldungen“ auf Seite 532.

Mit den Tasten Nach oben und Nach unten können Sie sich durch die Meldungen bewegen. Mit den Tasten Nach links und Nach rechts können Sie einen Bildlauf in Meldungen ausführen, die nicht auf den Bildschirm passen.

Markieren Sie das **Zurück**-Symbol, und drücken Sie die mittlere Schaltfläche, um zum Bildschirm des **Status des graphischen Moduls** zurückzuwechseln.

Gehäusestatus-Bildschirm

Der Gehäusestatus-Bildschirm zeigt Informationen und Fehlermeldungen bezüglich des Gehäuses an. Siehe „LCD-Fehlermeldungen“ auf Seite 532 und für Meldungen, die auf diesem Bildschirm angezeigt werden können.

Mit den Tasten Nach oben und Nach unten können Sie sich durch die Meldungen bewegen. Mit den Tasten Nach links und Nach rechts können Sie einen Bildlauf in Meldungen ausführen, die nicht auf den Bildschirm passen.

Markieren Sie das **Zurück**-Symbol, und drücken Sie die mittlere Schaltfläche, um zum Bildschirm des **Status des graphischen Moduls** zurückzuwechseln.

IP-Zusammenfassungsbildschirm

Im **IP-Zusammenfassungs**-Bildschirm werden IP-Informationen für den CMC und iDRAC jedes installierten Servers 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 einen Bildlauf ausführen, die nicht auf den Bildschirm passen.

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.

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.

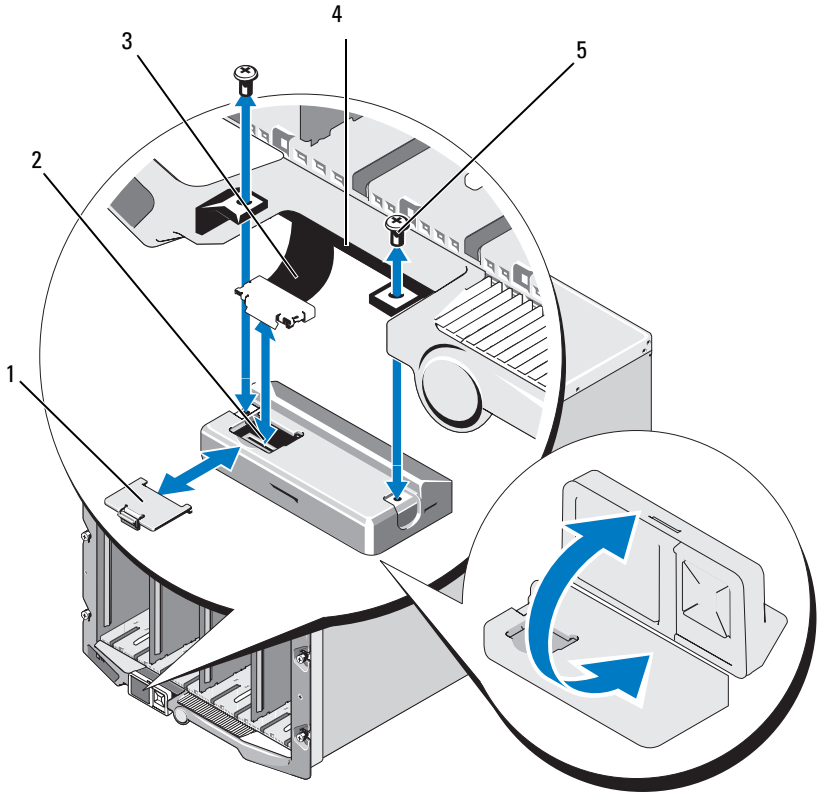
Durch Folgen der blinkenden gelben Symbole durch das LCD-Menüsystem können Sie die Statusbildschirm- und Fehlermeldungen für das Element anzeigen, welches das Problem aufweist.

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. Verwenden Sie für Serverfehler die iDRAC-Webschnittstelle oder die Befehlszeilenschnittstelle, um das Systemereignisprotokoll (SEL) des Servers zu löschen. Verwenden Sie für Gehäusefehler die CMC-Webschnittstelle oder die Befehlszeilenschnittstelle, um das Hardwareprotokoll zu löschen.

LCD Hardware-Fehlerbehebung

Wenn mit dem LCD in Bezug auf Ihre Nutzung des CMC Probleme auftreten, verwenden Sie die folgenden Hardware-seitigen Fehlerbehebungselemente, um festzustellen, ob es sich um einen LCD-Hardwarefehler oder ein Verbindungsproblem handelt.

Abbildung 13-1. LCD-Modul entfernen und installieren



1	Kabelabdeckung	2	LCD-Modul
3	Flachbandkabel	4	Scharniere (2)
5	Schrauben (2)		

Tabelle 13-2. Schritte zur Behebung von LCD-Hardwarefehlern

Symptom	Problem	Wiederherstellungsmaßnahme
Warnmeldung `CMC reagiert nicht` und LED blinkt gelb	Verlust der Kommunikation von CMC zu LCD-Frontblende	Prüfen Sie ob der CMC bootet; danach setzen Sie den CMC mittels GUI oder RACADM-Befehl zurück.
Warnmeldung `CMC reagiert nicht` und LED leuchtet dauerhaft gelb oder ist aus.	Kommunikation mit LCD-Modul hängt während eines CMC-Failovers oder startet neu.	Zeigen Sie das Hardwareprotokoll mittels GUI oder RACADM-Befehlen an. Suchen Sie nach folgender Meldung: `Kommunikation mit LCD-Controller nicht möglich.` Stecken Sie das Flachbandkabel des LCD-Moduls neu ein.
Der Bildschimtext ist durcheinander	Defekter LCD-Bildschirm	Tauschen Sie das LCD-Modul aus.
LED und LCD sind aus.	Das LCD-Kabel ist nicht ordnungsgemäß verbunden oder fehlerhaft; oder das LCD-Modul ist fehlerhaft.	Zeigen Sie das Hardwareprotokoll mittels GUI oder RACADM-Befehlen an. Suchen Sie nach folgenden Meldungen: • `Das LCD-Modulkabel wurde nicht, oder nicht ordnungsgemäß verbunden.` • `Das Bedienfeld für die Systemsteuerung wurde nicht, oder nicht ordnungsgemäß verbunden.` Stecken Sie die Kabel neu ein.
LCD-Meldung `Kein CMC gefunden.`	Kein CMC im Gehäuse vorhanden.	Setzen Sie einen CMC ins Gehäuse ein oder ersetzen Sie den vorhandenen CMC, wenn er nicht funktioniert.

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-Fehlermeldungen

Tabelle 13-3. CMC-Statusbildschirme

Schweregrad	Meldung	Ursache
Kritisch	Die Batterie von CMC <Nummer> ist ausgefallen.	CMC-CMOS-Batterie fehlt oder keine Spannung.
Kritisch	Verlust des CMC <Nummer> LAN -Taktsignals.	Die CMC NIC-Verbindung wurde entfernt oder wurde nicht verbunden.
Warnung	Es wurde eine Firmware- bzw. Software-Inkompatibilität zwischen iDRAC in Steckplatz <Nummer> und dem CMC erkannt.	Die Firmware der beiden Geräte stimmt nicht überein, sodass eine oder mehrere Funktionen nicht unterstützt werden.
Warnung	Es wurde eine Firmware- bzw. Software-Inkompatibilität zwischen dem System-BIOS in Steckplatz <Nummer> und dem CMC erkannt.	Die Firmware der beiden Geräte stimmt nicht überein, sodass eine oder mehrere Funktionen nicht unterstützt werden.

Tabelle 13-3. CMC-Statusbildschirme *(fortgesetzt)*

Schweregrad	Meldung	Ursache
Warnung	Es wurde eine Firmware- bzw. Softwareinkompatibilität zwischen CMC 1 und CMC 2 erkannt.	Die Firmware der beiden Geräte stimmt nicht überein, sodass eine oder mehrere Funktionen nicht unterstützt werden.

Tabelle 13-4. Gehäusestatusbildschirm

Schweregrad	Meldung	Ursache
Kritisch	Lüfter <Nummer> wurde entfernt.	Dieser Lüfter ist für eine ordnungsgemäße Kühlung des Gehäuses erforderlich.
Warnung	Netzteilredundanz wurde herabgesetzt.	Eine oder mehrere Netzteileinheit(en) sind ausgefallen oder wurden entfernt, und das System kann keine vollständige Netzteileinheitredundanz mehr unterstützen.
Kritisch	Verlust der Netzteilredundanz.	Eine oder mehrere Netzteileinheit(en) sind ausgefallen oder wurden entfernt, und das System ist nicht mehr redundant.
Kritisch	Die Netzteile sind nicht redundant. Unzureichende Ressourcen für die Aufrechterhaltung des normalen Betriebs.	Eine oder mehrere Netzteileinheiten sind ausgefallen oder wurden entfernt, und das System verfügt nicht über genügend Strom, um den normalen Betrieb aufrechtzuerhalten. Dies könnte dazu führen, dass Server herunterfahren.
Warnung	Die Umgebungstemperatur des Bedienfelds für die Systemsteuerung ist höher als der obere Warnungsschwellenwert.	Eintrittstemperatur des Gehäuses hat den Warnungsschwellenwert überschritten.

Tabelle 13-4. Gehäusestatusbildschirm *(fortgesetzt)*

Schweregrad	Meldung	Ursache
Kritisch	Die Umgebungstemperatur des Bedienfelds für die Systemsteuerung ist höher als der obere Warnungsschwellenwert.	Eintrittstemperatur des Gehäuses hat den Warnungsschwellenwert überschritten.
Kritisch	Verlust der CMC-Redundanz.	CMC nicht mehr redundant. Dies tritt auf, wenn der Standby-CMC entfernt wurde.
Kritisch	Alle Fehlerprotokollierungen sind deaktiviert.	Das Gehäuse kann in den Protokollen keine Ereignisse speichern. Dies ist in der Regel ein Hinweis darauf, dass ein Problem mit der Systemsteuerung oder dem Systemsteuerungskabel vorliegt.
Warnung	Protokoll ist voll.	Das Gehäuse hat erkannt, dass nur ein weiterer Eintrag zum CEL (Hardwareprotokoll) hinzugefügt werden kann, bis dieses voll ist.
Warnung	Protokoll ist beinahe voll.	Gehäuse-Ereignisprotokoll ist zu 75% voll.

Tabelle 13-5. Lüfterstatusbildschirme

Schweregrad	Meldung	Ursache
Kritisch	Umdrehungszahl des Lüfters <Nummer> liegt unterhalb des unteren kritischen Schwellenwertes.	Die Geschwindigkeit des festgelegten Lüfters ist nicht hoch genug, um das System ausreichend zu kühlen.
Kritisch	Umdrehungszahl des Lüfters <Nummer> liegt oberhalb des oberen kritischen Schwellenwertes.	Die Geschwindigkeit des angegebenen Lüfters ist zu hoch, in der Regel aufgrund eines defekten Lüfterflügels.

Tabelle 13-6. EAM-Statusbildschirme

Schweregrad	Meldung	Ursache
Warnung	Nichtübereinstimmung der Architektur auf E/A-Modul <Nummer> erkannt.	Die Struktur des E/A-Moduls stimmt nicht mit der des Servers bzw. redundanten E/A-Moduls überein.
Warnung	Link-Tuning-Fehler auf E/A-Modul <Nummer> erkannt.	Das E/A-Modul konnte auf einem oder mehreren Servern nicht auf die korrekte Verwendung der NIC eingestellt werden.
Kritisch	Es wurde ein Fehler auf E/A-Modul <Nummer> erkannt.	Das E/A-Module weist einen Fehler auf. Der gleiche Fehler kann auch auftreten, wenn das E/A-Modul einen thermischen Fehler aufweist.

Tabelle 13-7. iKVM Statusbildschirm

Schweregrad	Meldung	Ursache
Warnung	Konsole steht lokalem KVM nicht zur Verfügung.	Minder schwerer Fehler wie z. B. beschädigte Firmware.
Kritisch	Lokales KVM kann keine Hosts erkennen.	USB Host-Auflistungsfehler.
Kritisch	OSCAR, Bildschirmanzeige funktioniert für lokale KVM nicht.	OSCAR-Fehler.
Nicht wiederherstellbar	Lokales KVM funktioniert nicht und wurde ausgeschaltet.	Serieller RIP-Fehler oder USB-Host-Chip-Fehler.

Tabelle 13-8. Netzteileinheit-Statusanzeigen

Schweregrad	Meldung	Ursache
Kritisch	Netzteil <Nummer> fehlerhaft.	Die Netzteileinheit ist fehlerhaft.
Kritisch	Verlust der Stromzufuhr von Netzteil <Nummer>.	Verlust von Netzstrom oder Netzkabel abgezogen.

Tabelle 13-8. Netzteileinheit-Statusanzeigen *(fortgesetzt)*

Schweregrad	Meldung	Ursache
Warnung	Netzteil <Nummer> wird mit 110 Volt betrieben und könnte einen Fehler des Leistungsschutzschalters verursachen.	Netzteil wurde an eine Stromquelle mit 110 Volt angeschlossen.

Tabelle 13-9. Serverstatus-Bildschirm

Schweregrad	Meldung	Ursache
Warnung	Die Umgebungstemperatur der Systemplatine ist niedriger als der untere Warnungsschwellenwert.	Servertemperatur wird kühl.
Kritisch	Die Umgebungstemperatur der Systemplatine ist niedriger als der untere kritische Schwellenwert.	Servertemperatur wird kalt.
Warnung	Die Umgebungstemperatur der Systemplatine ist höher als der obere Warnungsschwellenwert.	Servertemperatur wird warm
Kritisch	Die Umgebungstemperatur der Systemplatine ist höher als der obere kritische Schwellenwert.	Servertemperatur wird zu heiß.
Kritisch	Der Einraststrom der Systemplatine befindet sich außerhalb des zulässigen Bereichs	Strom hat einen Fehlerschwellenwert überschritten.
Kritisch	Ausfall der Systemplatinenbatterie.	CMOS-Batterie ist nicht vorhanden oder weist keine Spannung auf.
Warnung	Niedriger Batteriestand des Speichers.	Niedriger Batteriestand des ROMB.
Kritisch	Ausfall der Batterie des Speichers.	CMOS-Batterie ist nicht vorhanden oder weist keine Spannung auf.

Tabelle 13-9. Serverstatus-Bildschirm *(fortgesetzt)*

Schweregrad	Meldung	Ursache
Kritisch	CPU-Spannung <Nummer> <Spannungssensorname> befindet sich außerhalb des zulässigen Bereichs.	
Kritisch	Systemplatinenspannung <Nummer> <Spannungssensorname> befindet sich außerhalb des zulässigen Bereichs.	
Kritisch	Mezzanine-Kartenspannung <Nummer> <Spannungssensorname> befindet sich außerhalb des zulässigen Bereichs.	
Kritisch	Speicherspannung <Nummer> <Spannungssensorname> befindet sich außerhalb des zulässigen Bereichs.	
Kritisch	CPU <Nummer> weist einen internen Fehler auf (IERR).	CPU-Fehler.
Kritisch	CPU <Nummer> weist ein Übertemperaturereignis (thermischer Auslöser) auf.	CPU überhitzt.
Kritisch	Konfiguration von CPU <Nummer> wird nicht unterstützt.	Falscher Prozessortyp oder an falscher Position.
Kritisch	CPU <Nummer> fehlt.	Erforderliche CPU fehlt oder ist nicht vorhanden.
Kritisch	Mezz B<Steckplatznummer> Status: Add-In-Kartensensor für Mezz B<Steckplatznummer>, Installationsfehler wurde bestätigt	Falsche Mezzanine-Karte für E/A-Architektur installiert

Tabelle 13-9. Serverstatus-Bildschirm *(fortgesetzt)*

Schweregrad	Meldung	Ursache
Kritisch	Mezz C<Steckplatznummer> Status: Add-In-Kartensensor für Mezz C<Steckplatznummer>, Installationsfehler wurde bestätigt	Falsche Mezzanine-Karte für E/A-Architektur installiert
Kritisch	Laufwerk <Nummer> wurde entfernt.	Speicherlaufwerk wurde entfernt.
Kritisch	Fehler auf Laufwerk <Nummer> erkannt.	Speicherlaufwerk fehlerhaft.
Kritisch	Die Spannung der Systemplatinenausfallsicherung befindet sich außerhalb des zulässigen Bereichs.	Dieses Ereignis wird erstellt, wenn sich die Systemplatinenspannungen nicht auf normalen Ebenen befinden.
Kritisch	Der Watchdog-Zeitmesser ist abgelaufen.	Der iDRAC-Watchdog-Zeitmesser läuft ab, und es ist keine Maßnahme eingestellt.
Kritisch	System durch Watchdog-Zeitmesser zurückgesetzt.	Der iDRAC-Watchdog stellte einen Systemabsturz fest (Zeitgeber abgelaufen, da vom Host keine Reaktion eingegangen ist), und die Maßnahme wurde auf Neustart festgelegt.
Kritisch	Der Watchdog-Zeitmesser hat das System ausgeschaltet.	Der iDRAC-Watchdog stellte einen Systemabsturz fest (Zeitgeber abgelaufen, da vom Host keine Reaktion eingegangen ist), und die Maßnahme wurde auf Ausschalten des Stroms festgelegt.
Kritisch	Der Watchdog-Zeitmesser hat das System aus- und wieder eingeschaltet.	Der iDRAC-Watchdog stellte einen Systemabsturz fest (Zeitgeber abgelaufen, da vom Host keine Reaktion eingegangen ist) und die Maßnahme wurde auf Aus- und Einschalten des Stroms festgelegt.

Tabelle 13-9. Serverstatus-Bildschirm *(fortgesetzt)*

Schweregrad	Meldung	Ursache
Kritisch	Protokoll ist voll.	Das SEL-Gerät stellt fest, dass dem SEL nur ein Eintrag hinzugefügt werden kann, bevor es voll ist.
Warnung	Es wurden beständige korrigierbare Speicherfehler auf einem Speichergerät an Standort <Standort> erkannt.	
Warnung	Der Wert für beständige korrigierbare Speicherfehler hat sich für ein Speichergerät an Standort <Standort> erhöht.	Korrigierbare ECC-Fehler erreichen ein kritisches Stadium.
Kritisch	Es wurden Mehrbit-Speicherfehler auf einem Speichergerät an Standort <Standort> erkannt.	Ein nicht korrigierbarer ECC-Fehler wurde festgestellt.
Kritisch	Es wurde ein E/A-Kanalprüfungs-NMI auf einer Komponente auf Bus <Nummer> Gerät <Nummer> Funktion <Nummer> erkannt.	Im E/A-Kanal wird ein kritischer Interrupt erstellt.
Kritisch	Es wurde ein E/A-Kanalprüfungs-NMI auf einer Komponente an Steckplatz <Nummer> erkannt.	Im E/A-Kanal wird ein kritischer Interrupt erstellt.
Kritisch	Es wurde ein PCI-Paritätsfehler an einer Komponente auf Bus <Nummer> Gerät <Nummer> Funktion <Nummer> erkannt.	Auf dem PCI-Bus wurde ein Paritätsfehler festgestellt.
Kritisch	Es wurde ein PCI-Paritätsfehler an einer Komponente auf Steckplatz <Nummer> erkannt.	Auf dem PCI-Bus wurde ein Paritätsfehler festgestellt.
Kritisch	Es wurde ein PCI-Systemfehler an einer Komponente auf Bus <Nummer> Gerät <Nummer> erkannt.	PCI-Fehler wurde von Komponente erkannt.

Tabelle 13-9. Serverstatus-Bildschirm *(fortgesetzt)*

Schweregrad	Meldung	Ursache
Kritisch	Es wurde ein PCI-Systemfehler an einer Komponente auf Steckplatz <Nummer> erkannt.	PCI-Fehler wurde von Komponente erkannt.
Kritisch	Protokollierung beständiger korrigierbarer Speicherfehler wurde für ein Speichergerät an Standort <Standort> deaktiviert.	Einzelbit-Fehlerprotokollierung wird deaktiviert, wenn für ein Speichergerät zu viele SBE (Einzelbitfehler) protokolliert werden.
Kritisch	Alle Fehlerprotokollierungen sind deaktiviert.	
Nicht wiederherstellbar	Prozessorprotokollfehler erkannt.	Das Prozessorprotokoll ist in einen nicht wiederherstellbaren Zustand übergegangen.
Nicht wiederherstellbar	Prozessor-Bus Paritätsfehler.	Der Prozessor-Bus-PERR ist in einen nicht wiederherstellbaren Zustand übergegangen.
Nicht wiederherstellbar	Prozessorinitialisierungsfehler erkannt.	Die Prozessorinitialisierung ist in einen nicht wiederherstellbaren Zustand übergegangen.
Nicht wiederherstellbar	Prozessormaschinenüberprüfung erkannt.	Die Prozessormaschinenüberprüfung ist in einen nicht wiederherstellbaren Zustand übergegangen.
Kritisch	Verlust der Speicherredundanz.	
Kritisch	Es wurde ein schwerwiegender Bus-Fehler an einer Komponente auf Bus <Nummer> Gerät <Nummer> Funktion <Nummer> erkannt.	Schwerwiegender Fehler auf dem PCIE-Bus festgestellt.
Kritisch	Es wurde ein Software-NMI an einer Komponente auf Bus <Nummer> Gerät <Nummer> Funktion <Nummer> erkannt.	Chip-Fehler wurde festgestellt.

Tabelle 13-9. Serverstatus-Bildschirm *(fortgesetzt)*

Schweregrad	Meldung	Ursache
Kritisch	Programmierung virtueller MAC-Adresse einer Komponente auf Bus <Nummer> Gerät <Nummer> Funktion <Nummer> fehlgeschlagen.	Flex-Adresse konnte für dieses Gerät nicht programmiert werden
Kritisch	Unterstützung von Flex-Adresse oder Link-Tuning durch Geräte Options-ROM auf Mezzanine-Karte <Nummer> fehlgeschlagen.	Options-ROM unterstützt Flex-Adresse oder Link-Tuning nicht
Kritisch	Bezug der Link-Tuning oder FlexAddress-Daten von iDRAC fehlgeschlagen.	

ANMERKUNG: Lesen Sie für Informationen zu anderen serverbezogenen LCD-Meldungen das „Server-Benutzerhandbuch".

LCD-Modul- und Serverstatusinformationen

Die Tabellen in diesem Abschnitt beschreiben Statuselemente, die auf dem Frontblenden-LCD für jeden Komponententyp im Gehäuse angezeigt werden.

Tabelle 13-10. 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.

Tabelle 13-10. CMC-Status *(fortgesetzt)*

Element	Beschreibung
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 13-11. 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“
Leistungsbedarf	Aktueller Stromverbrauch in Watt
Spitzenleistung	Spitzenstromverbrauch in Watt
Minimalstrom	Mindeststromverbrauch in Watt
Umgebungstemperatur	Umgebungstemperatur in Grad Celsius
Service-Tag-Nummer	Die vom Werk zugewiesene Service-Tag-Nummer.
CMC-Redundanzmodus	Nicht-redundant oder Redundant
Netzteileinheit-Redundanzmodus	Nicht-redundant, wechselstromredundant oder gleichstromredundant

Tabelle 13-12. Lüfterstatus

Element	Beschreibung
Name/Standort	Beispiel: Lüfter1, Lüfter2 etc.
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 13-13. Netzteileinheitstatus

Element	Beschreibung
Name/Standort	Beispiel: PSU1, PSU2 etc.
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 13-14. EAM-Status

Element	Beschreibung
Name/Standort	Beispiel: EAM A1, EAM B1. etc.
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 ein ist. Dieser Wert ist für ein EAM des Typs „Passthrough“ 0.
Service-Tag-Nummer	Die vom Werk zugewiesene Service-Tag-Nummer.

Tabelle 13-15. iKVM Status

Element	Beschreibung
Name	iKVM
Kein 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“.
Status	Aus oder Ein
Modell/Fabrikation	Eine Beschreibung des iKVM-Modells.
Service-Tag-Nummer	Die vom Werk zugewiesene Service-Tag-Nummer.
Teilenummer	Die Hersteller-Teilenummer.
Firmware-Version	iKVM Firmware-Version.
Hardwareversion	iKVM Hardware-Version.

ANMERKUNG: Diese Informationen werden dynamisch aktualisiert.

Tabelle 13-16. 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“.
Steckplatzname	Gehäuse-Steckplatzname. Zum Beispiel SLOT-01. **ANMERKUNG:** Sie können diese Tabelle über die CMC CLI oder Web GUI einstellen.

Tabelle 13-16. Serverstatus *(fortgesetzt)*

Element	Beschreibung
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-Nummer	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 werden Tabelle 13-16 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-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC*.

Stichwortverzeichnis

L

M

N

P

R

S

T

V

W

Z