Dell Chassis Management Controller Firmware Version 4.3 Benutzerhandbuch

Anmerkungen, Vorsichtshinweise und Warnungen

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

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

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

2012 - 12

Rev. A00

Inhaltsverzeichnis

1

Übersicht

Der Dell Chassis Management Controller (CMC) ist eine Systemverwaltungs-Hardware- und -Software-Lösung zur Verwaltung mehrerer Dell Blade-Gehäuse. Es ist ein hotplug-fähiges Modul, das sich an der Rückseite eines PowerEdge M1000e-Gehäuses befindet. Der CMC verfügt über einen eigenen Mikroprozessor und Speicher und wird vom modularen Gehäuse, an das er angeschlossen ist, mit Strom versorgt.

Der CMC ermöglicht IT-Administratoren das:

- Anzeigen der Bestandsliste
- Durchführen der Konfiguration und Überwachung
- Ein- bzw. ausschalten der Stromversorgung der Blades mit Remote-Zugriff
- Aktivieren von Warnungen für Ereignisse auf Servern und Komponenten im Blade-Gehäuse

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

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

- Automatische Energie- und Temperaturverwaltung in Echtzeit für das gesamte Gehäuse.
  - CMC überwacht den Energiebedarf des Systems und unterstützt den optionalen Betrieb mit „Dynamic Power Supply Engagement“. 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 Obergrenze für den Stromverbrauch
  - E/A-Switches und iDRAC-Netzwerkeinstellungen
  - Das erste Startgerät auf den Serverblades
  - Der CMC überprüft die Konsistenz der E/A-Struktur zwischen den E/A-Modulen und den Blades. Um die Systemhardware zu schützen, werden Komponenten gegebenenfalls deaktiviert
  - 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.

Was ist neu in dieser Version?

Diese Version von CMC unterstützt:

- Cisco FEX-Switch
- FC16 Switch - Brocade M6505
- Zusatzkarten
  - QLogic FC16 2P QME2662
  - Emulex FC16 LPm16002B-D
- 1:n agentenfreie BS-unabhängige Firmwareaktualisierungsfähigkeit für unterstützte 12G Fibre Channel (FC)-Mezzaninkarten
- Aktualisierung der Firmware für Dell PowerEdge M E/A-Aggregator
- Speichern der BIOS-Konfigurationsinformationen auf die Festplatte und Wiederherstellen der Informationen auf denselben oder einen unterschiedlichen Server.
- Konfigurieren des Dell EqualLogic PS-M4110 Blade-Array unter Verwendung von RACADM
- Verwaltung mehrerer Gehäuse:
  - Die Fähigkeit mehrere Gehäusekonfigurationseigenschaften des Führungsgehäuses auszuwählen und auf die Gruppenmitglieder zu übertragen.
  - Die Fähigkeit für die Gruppenmitglieder ihre Gehäuseeinstellungen mit dem Führungsgehäuse synchronisiert zu halten.
- Anzeige, dass das Gehäuse frischlufttauglich ist - Der Begriff „Frischluft“ wird nach dem Modellnamen angezeigt.
- Zurücksetzen des iDRACs, ohne den Neustart des Betriebssystems.

Wichtige Funktionen

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

Verwaltungsfunktionen

Der CMC enthält die folgenden Verwaltungsfunktionen:

- Redundante CMC-Umgebung.
- Registrierung des dynamischen Domänennamensystems (DDNS) für IPv4 und IPv6.
- 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).
- 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.
- Zurücksetzen des iDRACs ohne den Neustart des Betriebssystems.
- Multi-Gehäuseverwaltung, wodurch bis zu acht weitere Gehäuse vom Hauptgehäuse aus sichtbar sind.
- Unterstützung der Speicher-Array-Konfiguration unter Verwendung von RACADM - Ermöglicht Ihnen die Konfiguration von IPs, das Beitreten oder Erstellen von Gruppen und die Auswahl von Strukturen für Speicher-Arrays unter Verwendung von RACADM.
- Verwaltung von mehreren Gehäusen:
  - Die Fähigkeit Gehäusekonfigurationseigenschaften des Führungsgehäuses auszuwählen und auf die Gruppenmitglieder zu übertragen
  - Die Fähigkeit für die Gruppenmitglieder, ihre Gehäuseeinstellungen mit dem Führungsgehäuse synchronisiert zu halten
- Unterstützung zum Speichern von BIOS-Konfigurationsinformationen auf der Festplatte und zum Wiederherstellen auf diese oder einen anderen Server.

Sicherheitsfunktionen

Der CMC bietet die folgenden Sicherheitsfunktionen:

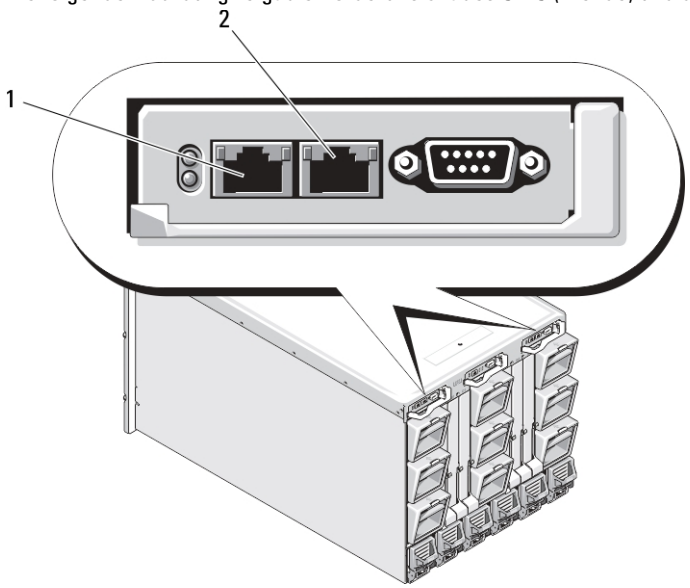
- Sicherheitsverwaltung auf Kennwortebene – Verhindert den unberechtigten Zugriff auf ein Remote-System.
- Zentralisierte Benutzerauthentifizierung durch:
  - Verwendung des Active Directory-Standardschemas oder eines erweiterten Schemas (optional).
  - Hardware-gespeicherte Benutzer-IDs und Kennwörter.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

  ANMERKUNG: Telnet unterstützt keine SSL-Verschlüsselung.
- Konfigurierbare IP-Schnittstellen (falls zutreffend).

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

Gehäuseübersicht

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



1	GB-Schnittstelle
2	STK-Schnittstelle

CMC-Portinformationen

Die folgenden TCP/IP-Schnittstellen werden benötigt, um über Firewalls remote auf CMC zuzugreifen. Hierbei handelt es sich um die Schnittstellen, die CMC für Verbindungen hört.

Tabelle 1. Abhörschnittstellen des CMC-Servers

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

* Konfigurierbare Schnittstelle

Die folgende Tabelle listet die Schnittstellen auf, die CMC als Client verwendet.

Tabelle 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

Minimale CMC-Version

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

Tabelle 3. Minimale CMC-Version für Blade-Server

Server	Minimale Version von CMC
PowerEdge M600	CMC 1.0
PowerEdge M605	CMC 1.0
PowerEdge M805	CMC 1.2
PowerEdge M905	CMC 1.2
PowerEdge M610	CMC 2.0
PowerEdge M610x	CMC 3.0
PowerEdge M710	CMC 2.0
PowerEdge M710HD	CMC 3.0
PowerEdge M910	CMC 2.3
Power Edge M915	CMC 3.2
PowerEdge M420	CMC 4.1
PowerEdge M520	CMC 4.0
PowerEdge M620	CMC 4.0
PowerEdge M820	CMC 4.11
PowerEdge PSM4110	CMC 4.11

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

Tabelle 4. Minimale CMC-Version für EAMs

EAM-Switches	Minimale Version von CMC
PowerConnect M6220	CMC 1.0
PowerConnect M6348	CMC 2.1
PowerConnect M8024	CMC 1.2
PowerConnect M8024-k	CMC 3.2
PowerConnect M8428-k	CMC 3.1
10/100/1000-MBit-Ethernet-Passthrough	CMC 1.0
Dell 4-GBit/s FC Pass-Through-Modul	CMC 1.0
Dell 8/4-GBit/s-FC-SAN-Modul	CMC 1.2
Dell 10Gb Ethernet Passthrough	CMC 2.1
Dell 10-Gb-Ethernet-Passthrough II	CMC 3.0
Dell 10Gb Ethernet Passthrough-K	CMC 3.0
Brocade M4424	CMC 1.0
Brocade M5424	CMC 1.2
Cisco Catalyst CBS 3130X-S	CMC 1.0
Cisco Catalyst CBS 3130G	CMC 1.0
Cisco Catalyst CBS 3032	CMC 1.0
Dell Force10 MXL10/40GbE	CMC 4.11
Dell PowerEdge M E/A-Aggregator	CMC 4.2
Mellanox M2401G DDR-Infiniband-Switch	CMC 1.0
Mellanox M3601Q QDR Infiniband-Switch	CMC 2.0
Mellanox M4001F/M4001Q FDR/QDR Infiniband Switch	CMC 4.0
Mellanox M4001T FDR10 Infiniband-Switch	CMC 4.1
Brocade M6505	CMC 4.3
Cisco Nexus B22DELL	CMC 4.3

Unterstützte Remote-Zugriffsverbindungen

Die folgende Tabelle führt die unterstützten Remote Access Controller auf.

Tabelle 5. 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

Verbindung	Funktionen
	• 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.

Weitere Informationen zu den neusten unterstützten Plattformen finden Sie in der *Infodatei* unter **dell.com/support/manuals**.

Unterstützte Web-Browser

Die neusten Informationen zu unterstützten Web-Browsern finden Sie in der *Infodatei* unter **dell.com/support/manuals**.

Lokalisierte Versionen der CMC-Webschnittstelle anzeigen

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 **dell.com/support/manuals**.

Weitere nützliche Dokumente

Zusätzlich zu diesem Handbuch, können Sie auf die folgenden Handbücher unter **dell.com/support/manuals** zurückgreifen. Wählen Sie **Aus einer Liste von Dell Produkten auswählen** aus und klicken Sie auf **Fortfahren**. Klicken Sie auf**Software → Monitore → Elektronik und Peripherie → Software** :

- Klicken Sie auf **Remote Enterprise System Management** und dann auf **Dell Chassis Management Controller Version 4.3** zur Ansicht von:
  - 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 *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC* enthält Informationen zu den RACADM-Unterbefehlen, den unterstützten Schnittstellen und Eigenschaften-Datenbankgruppen und Objektdefinitionen.
  - Die *Chassis Management Controller Version 4.3 Versionshinweise* geben den letzten Stand der Änderungen am System oder der Dokumentation wieder oder enthalten erweitertes technisches Referenzmaterial für erfahrene Benutzer oder Techniker.
- Klicken Sie auf **Remote Enterprise System Management** und dann auf die erforderliche iDRAC7-Versionsnummer, um das *Integrated Dell Remote Access Controller 7 (iDRAC7) Benutzerhandbuch*, das Informationen über die Installation, Konfiguration und Wartung des iDRACs auf verwalteten Systemen beinhaltet, anzuzeigen.
- Klicken Sie auf **Enterprise System Management** und dann auf den Produktnamen, um die folgenden Dokumente anzuzeigen:
  - 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, die unter **dell.com/support/manuals** verfügbar sind, bieten 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**. Garantieinformationen können möglicherweise als separates Dokument beigelegt sein.
- Das zum Lieferumfang der Rack-Lösung gehörende *Rack-Installationshandbuch* und die *Rack-Installationsanweisungen* beschreiben, wie das System in einem Rack installiert wird.
- Im *Hardware-Benutzerhandbuch* erhalten Sie Informationen über Systemfunktionen, zur Fehlerbehebung am 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.
- Gegebenenfalls sind Versionsinformationen oder Readme-Dateien vorhanden, die den letzten Stand der Änderungen am System oder an der Dokumentation wiedergeben oder fortgeschrittenes technisches Referenzmaterial für erfahrene Benutzer oder IT-Fachleute enthalten.
- 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*.
- Die Dokumentation zu Ihrer Verwaltungskonsolenanwendung von Drittanbietern.

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.
- Aktualisieren der CMC-Firmware

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

Bevor Sie beginnen

Laden Sie die neueste Version der CMC-Firmware 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.

Installieren der CMC-Hardware

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

Verwandte Links

Die redundante CMC-Umgebung verstehen

Prüfliste zur Gehäusegruppen-Einrichtung

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.
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-Webschnittstelle 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 in der CMC-Webschnittstelle 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 in der CMC-Webschnittstelle 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 ist *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.

VORSICHT: Das Verbinden des STK-Ports mit dem Verwaltungsnetzwerk kann zu unvorhersehbaren Ergebnissen führen. Wenn GB und STK an dasselbe Netzwerk angeschlossen werden (Broadcast-Domäne), kann dies zu einer Broadcast-Überlastung führen.

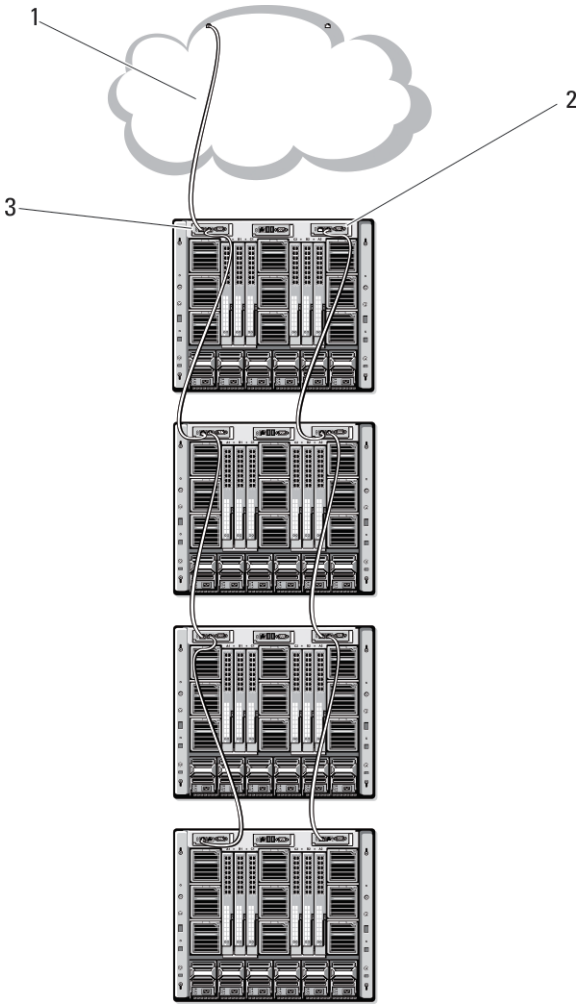
Verkettete CMC-Netzwerkverbindung

Wenn ein Rack mehrere Gehäuse enthält, können Sie die Anzahl der 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 der erforderlichen Verbindungen mit dem Verwaltungsnetzwerk von acht auf zwei reduzieren. Wenn jedes Gehäuse lediglich einen CMC enthält, können Sie die Anzahl der 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.

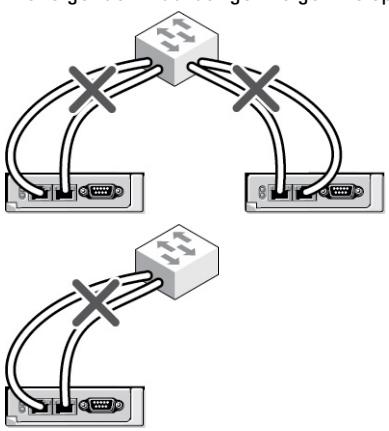
Bilden Sie separate Verkettungen für die CMCs im aktiven CMC-Steckplatz und im sekundären CMC-Steckplatz.

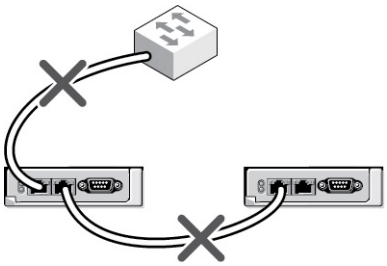
Die folgende Abbildung zeigt die Anordnung der Kabel für vier verkettete Gehäuse, jeweils mit einem aktiven und einem Standby-CMC.



1	Verwaltungsnetzwerk
2	Standby-CMC
3	Aktiver CMC

Die folgenden Abbildungen zeigen Beispiele für die inkorrekte Verkabelung des CMC.





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.

   VORSICHT: 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.
6. Eine Einführung zum CMC finden Sie unter Remote-Zugriffssoftware auf einer Management Station installieren.

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 **dell.com/support/manuals**. Sie können die neueste Version der Dell DRAC Tools unter **dell.com/support** 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. Navigieren Sie zum Verzeichnis **SYSMGMT/ManagementStation/linux/rac**. Geben Sie den folgenden Befehl ein, um die RAC-Software zu installieren:

   ```
   rpm –ivh *.rpm
   ```
5. Um Hilfe zum RACADM-Befehl zu erhalten, geben Sie nach der Eingabe der vorherigen Befehle `racadm help` ein. Weitere Informationen über RACADM finden Sie im *RACADM-Befehlzeilen-Referenzhandbuch für den iDRAC7 und CMC*.

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

RACADM von einer Linux Management Station deinstallieren

1. Melden Sie sich als „root“ beim System an, auf dem die Funktionen der Management Station deinstalliert werden sollen.
2. 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`.

Webbrowser konfigurieren

Sie können CMC, Server und Module, die im Gehäuse installiert sind, durch einen Webbrowser konfigurieren und verwalten. Siehe den Abschnitt *Unterstützte Browser* in der *Infodatei* unter **dell.com/support/manuals**.

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

Verwandte Links

Proxy-Server

Proxy-Server

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

Internet Explorer

So bearbeiten Sie die Ausnahmeliste in Internet Explorer:

1. Starten Sie den Internet Explorer.
2. Klicken Sie auf **Tools** → **Internet-Optionen** → **Verbindungen**.
3. Klicken Sie im Abschnitt **LAN-Einstellungen** auf **LAN-Einstellungen.**
4. 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 **Tools** → **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 **Tools** → **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 **Tools** → **Internetoptionen** und 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 **Tools** → **Internetoptionen** und klicken Sie dann auf **Erweitert**.
3. Gehen Sie mit der Bildlaufleiste zum Abschnitt „Multimedia" und aktivieren Sie **Animationen auf Webseiten wiedergeben**.

Einrichtung des Erstzugriffs auf den CMC

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

ANMERKUNG: Um die M1000e-Lösung zu verwalten, muss sie mit Ihrem Verwaltungsnetzwerk verbunden sein.

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

Der CMC und der iDRAC auf jedem Server und die Netzwerkverwaltungsschnittstellen für alle Switch-E/A-Module sind mit einem gemeinsamen internen Netzwerk im 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.

Es wird empfohlen, dass Sie die Gehäuseverwaltung vom Datennetzwerk isolieren. Dell kann die Laufzeit eines Gehäuses, das nicht richtig in Ihre Umgebung integriert ist, nicht unterstützen oder garantieren. Wegen des möglichen Datenverkehrs auf dem Datennetzwerk können die Verwaltungsschnittstellen auf dem internen Verwaltungsnetzwerk vom für Server bestimmten Datenverkehr überlasten. Dies führt zu Verzögerungen in der CMC- und iDRAC-Kommunikation. Diese Verzögerungen können zu einem unvorhersagbaren Gehäuseverhalten führen, wie etwa die Anzeige von CMC durch iDRAC als offline, obwohl es arbeitet, was wiederum weiteres unerwünschtes Verhalten verursacht. Falls es unmöglich ist, das Verwaltungsnetzwerk physisch zu isolieren, besteht noch die Möglichkeit, den CMC- und iDRAC-Datenverkehr auf ein separates VLAN umzuleiten. Die CMC- und einzelnen iDRAC-Netzwerkschnittstellen können für die Verwendung eines VLAN konfiguriert werden.

Wenn Sie ein Gehäuse haben, verbinden Sie den CMC und 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 Verwaltungsnetzwerkes.

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 Verwaltungsnetzwerk und bietet höhere Redundanz. Der verkettete Verbindungstyp verwendet weniger Schnittstellen im Verwaltungsnetzwerk, schafft jedoch Abhängigkeiten zwischen den CMCs, wodurch sich die Redundanz des Systems verringert.

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

Verwandte Links

CMC-Basisnetzwerkverbindung
Verkettete CMC-Netzwerkverbindung
CMC-Netzwerk anfänglich konfigurieren

CMC-Netzwerk anfänglich konfigurieren

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

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

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

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

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

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

CMC-Netzwerke über die LCD-Bedienfeld-Schnittstelle konfigurieren

ANMERKUNG: Die CMC-Konfiguration über das LCD-Bedienfeld 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.

Das LCD-Bedienfeld befindet sich unten links an der Gehäusevorderseite.

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

1. Drücken Sie den Netzschalter des Gehäuses, um das Gehäuse einzuschalten.

   Der LCD-Bildschirm zeigt beim Einschalten eine Reihe von Initialisierungsseiten 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.

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

   - Klicken Sie auf die mittlere Schaltfläche, um mit dem CMC-Bildschirm **Netzwerkeinstellungen** fortzufahren.
   - Um das Menü **Gehäuse konfigurieren** zu beenden, wählen Sie das Symbol NEIN aus und drücken Sie die mittlere Schaltfläche. Siehe Schritt 9.

3. Klicken Sie auf die mittlere Schaltfläche, um mit dem Bildschirm CMC-**Netzwerkeinstellungen** fortzufahren.
4. Wählen Sie mit der Pfeilschaltfläche nach unten die Netzwerkgeschwindigkeit aus (10 MBit/s, 100 MBit/s, Automatisch (1 GBit/s)).

   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 die 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.

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

5. 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.

   Wenn Automatische Verhandlung für ein Gerät aktiviert ist, jedoch nicht für ein weiteres, kann das Gerät, das 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 Halb-Duplex-Einstellung zurück. Ein derartiger Duplex-Übereinstimmungsfehler führt zu einer langsamen Netzwerkverbindung.

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

6. Wählen Sie das Internet-Protokoll (IPv4, IPv6 oder beide) aus, das Sie für den CMC verwenden möchten und drücken Sie die Schaltfläche in der Mitte, um mit den **CMC-Netzwerkeinstellungen** auf dem nächsten Bildschirm fortzufahren.
7. Wählen Sie den Modus aus, in dem der CMC die NIC-IP-Adressen abrufen soll:

Dynamic Host Configuration Protocol (DHCP)	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 **iDRAC7-Konfigurations**-Bildschirm wird angezeigt. Fahren Sie mit Schritt 9 fort.

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:

- 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 auf die Schaltfläche in der Mitte, um fortzufahren.
- Bestimmen Sie die Subnetzmaske und drücken Sie dann die Schaltfläche in der Mitte.
- 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.
- 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.

8. 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 angezeigt. Fahren Sie mit Schritt 10 fort.

   Bestimmen Sie die **DNS 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 DNS IP-Adresse abgeschlossen ist, drücken Sie auf die Schaltfläche in der Mitte, um fortzufahren.
9. 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.
10. Wählen Sie das Internet-Protokoll (IPv4, IPv6 oder beide) aus, das Sie für die Server verwenden möchten.

Dynamic Host Configuration Protocol (DHCP)	iDRAC ruft die IP-Konfiguration (IP-Adresse, Maske und Gateway) automatisch von einem DHCP-Server im Netzwerk ab. Dem iDRAC im Netzwerk wird eine eindeutige IP-Adresse zugewiesen. Drücken Sie 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: – 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. – Bestimmen Sie die Subnetzmaske und drücken Sie dann die Schaltfläche in der Mitte. – Bestimmen Sie den Gateway und drücken Sie dann die Schaltfläche in der Mitte.

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

11. 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.
12. 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.

Schnittstellen und Protokoll für den Zugriff auf CMC

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

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

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

Tabelle 6. 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 Web-Browser finden Sie in der *Infodatei* unter **dell.com/support/manuals**.
Remote-RACADM-Befehlszeilenschnittstelle	Verwenden Sie dieses Befehlszeilen-Dienstprogramm, um CMC und dessen Komponenten zu verwalten. Sie können Remote- oder Firmware-RACADM verwenden: • Remote-RACADM ist ein Client-Dienstprogramm, das auf einer Management Station ausgeführt wird. Es verwendet die bandexterne Netzwerkschnittstelle, um die RACADM-Befehle auf dem Managed System auszuführen, außerdem wird der HTTPs-Kanal verwendet. Die Option `-r` führt den RACADM-Befehl über ein Netzwerk aus. • Zugriff auf Firmware RACADM ist möglich durch die Anmeldung am CMC mittels SSH oder Telnet. Sie können die Firmware RACADM-Befehle ausführen, ohne die CMC IP, den Benutzernamen oder das Kennwort festzulegen. Sie können nach der RACADM-Eingabeaufforderung die Befehle ohne das racadm-Präfix direkt ausführen.
Gehäuse-LCD-Bedienfeld	Verwenden Sie die LCD auf der Frontblende, um die folgenden Aktivitäten auszuführen: • Warnungen, CMC-IP- oder MAC-Adresse oder benutzerprogrammierbare Zeichenfolgen anzeigen • DHCP festlegen • Statische IP-Einstellungen für CMC konfigurieren Um CMC ohne einen Neustart des Servers neu zu starten, halten Sie die  für 16 Sekunden gedrückt.
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.

Schnittstelle	Beschreibung
	ANMERKUNG: Telnet ist kein sicheres Protokoll und wird standardmäßig angezeigt. Telnet überträgt alle Daten, einschließlich Kennwörter, im Textformat. Bei der Übertragung von vertraulichen Informationen verwenden Sie die SSH-Schnittstelle.
SSH	Verwenden Sie SSH, um RACADM-Befehle auszuführen. Sie bietet dieselben Fähigkeiten wie die Telnet-Konsole und verwendet eine verschlüsselte Transportschicht für höhere Sicherheit. Der SSH-Dienst ist standardmäßig auf CMC aktiviert und kann deaktiviert werden.
WS-MAN	Die LC-Remote Services basieren auf dem WS-Management-Protokoll für 1-zu-n-Verwaltungsaufgaben. Sie müssen einen WS-MAN-Client verwenden, z. B. den WinRM-Client (Windows) oder den OpenWSMAN-Client (Linux), um die LC-Remote Services-Funktion zu verwenden. Sie können außerdem Power Shell und Python verwenden, um auf die WS-MAN-Schnittstelle zu schreiben. Web Services für Management (WS-Management) ist ein SOAP-basiertes (Simple Object Access Protocol) Protokoll, das für Systemverwaltung verwendet wird. CMC verwendet WS–Management zum Übermitteln von DMTF-CIM-basierten Verwaltungsinformationen (Distributed Management Task Force; Common Information Model). Die CIM-Informationen definieren die Semantik- und Informationstypen, die in einem verwalteten System geändert werden können. Die CMC WS-MAN-Implementierung verwendet SSL auf Schnittstelle 443 für Transportsicherheit und unterstützt Standardauthentifizierung. Die durch WS-Management zur Verfügung gestellten Daten werden durch die CMC-Instrumentierungsschnittstelle bereitgestellt, die den DMTF-Profilen und den Erweiterungsprofilen zugeordnet ist. Weitere Informationen stehen zur Verfügung unter: • MOFs und Profile – **delltechcenter.com/page/DCIM.Library** • 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** 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, <**support.microsoft.com/kb/968929**>.

ANMERKUNG: Der CMC-Standardbenutzername ist **root** und das Standardkennwort lautet **calvin**.

Starten von CMC mit anderen Systems Management Tools

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

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

Herunterladen und Aktualisieren der CMC-Firmware

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

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

Einrichten des physischen Standorts und des Namens für das Gehäuse

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

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

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

1. Wählen Sie in der Systemstruktur **Gehäuse-Übersicht** aus und klicken Sie auf **Setup** → **Allgemein**.
   Die Seite **Allgemeine Gehäuseeinstellungen** wird angezeigt.
2. Geben Sie den physischen Standort und den Namen für das Gehäuse ein. Weitere Informationen finden Sie in der *CMC Online-Hilfe*.

   ANMERKUNG: Das Feld „Gehäusestandort" ist optional. Es wird empfohlen, die Felder **Rechenzentrum**, **Gang**, **Rack** und **Rack-Steckplatz** zu verwenden, um den physischen Standort des Gehäuses anzuzeigen.
3. Klicken Sie auf **Anwenden**. Die Einstellungen werden gespeichert.

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

Um den Namen oder den Standort, das Datum und die Uhrzeit für das Gehäuse über die Befehlszeilenschnittstelle einzurichten, gehen Sie zu den Befehlen **setsysinfo** und **setchassisname**. Weitere Informationen finden Sie unter *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC*.

Datum und Uhrzeit auf dem CMC einstellen

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

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

So stellen Sie Datum und Uhrzeit auf dem CMC unter Verwendung der CMC-Webschnittstelle ein:

1. Wählen Sie in der Systemstruktur Gehäuse-Übersicht aus und klicken Sie auf **Setup** → **Datum/Uhrzeit**.
   Die Seite **Datum/Uhrzeit** wird angezeigt.
2. Datum und Uhrzeit können mit einem NTP-Server (Network Time Protocol) synchronisiert werden, indem Sie **NTP aktivieren** auswählen und bis zu drei NTP-Server festlegen.

3. Datum und Uhrzeit können manuell eingestellt werden, indem Sie die Auswahl von **NTP auswählen** aufheben und die Felder **Datum** und **Uhrzeit** bearbeiten, die **Zeitzone** aus dem Drop-Down-Menü auswählen und dann auf **Anwenden** klicken.

Datum und Uhrzeit auf dem CMC mittels RACADM einstellen

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*.

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.

Konfigurieren von LED-Blinken über die CMC-Webschnittstelle

So aktivieren Sie das Blinken von LEDs für eine, mehrere oder alle Komponenten über die CMC-Webschnittstelle:

1. Klicken Sie auf eine der folgenden Seiten:
   - **Gehäuse-Übersicht → Fehlerbehebung → Identifizieren** .
   - **Gehäuse-Übersicht → Gehäuse-Controller → Fehlerbehebung → Identifizieren**.
   - **Gehäuse-Übersicht → Server-Übersicht → Fehlerbehebung → Identifizieren**.

     ANMERKUNG: Auf dieser Seite können nur Server ausgewählt werden.
   - **Gehäuse-Übersicht → E/A-Modulübersicht → Fehlerbehebung → Identifizieren**.

     Die Seite **Identifizieren** wird angezeigt.
2. Wählen Sie zur Aktivierung des Blinkens einer Komponenten-LED die erforderliche Komponente aus und klicken Sie auf **Blinken**.
3. Zur Deaktivierung des Blinkens einer Komponenten-LED, löschen Sie die erforderliche Komponente und klicken Sie auf **Nicht blinken**.

LED-Blinken mittels RACADM konfigurieren

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

```
racadm setled -m <Modul> [-l <led-Status>]
```

wobei *<Modul>* das Modul bezeichnet, dessen LED Sie konfigurieren möchten. Konfigurationsoptionen:

- `server-nx`, wobei *n* = 1-8 und *x* = a, b, c oder d
- `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

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.

Die redundante CMC-Umgebung verstehen

Sie können einen Standby-CMC installieren, der aktiviert wird, wenn der aktive CMC ausfällt. Der redundante CMC kann vorinstalliert sein oder zu einem späteren Zeitpunkt hinzugefügt werden. 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 iDRAC7 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.)*
- Der aktive CMC über die Webschnittstelle zurückgesetzt wird. (Siehe Option **Reset CMC** für **Stromsteuerungsvorgänge,** Beschreibung unter Durchführen von Energieverwaltungsmaßnahmen an einem Server.)
- Das Netzwerkkabel vom aktiven CMC entfernt wird.
- Der aktive CMC vom Gehäuse entfernt wird.
- Ein CMC-Firmware-Flash auf dem aktiven CMC initiiert wird.
- Ein aktiver CMC nicht mehr funktioniert.

  ANMERKUNG: Im Falle eines CMC-Failovers gehen alle iDRAC-Verbindungen und alle aktiven CMC-Sitzungen verloren. Benutzer mit verlorenen Sitzungen müssen sich erneut mit dem aktiven CMC verbinden.

Verwandte Links

Info zum Standby-CMC
Ausfallsicherer CMC-Modus
Aktiver CMC – Auswahlprozess
Funktionszustand eines redundanten CMC abrufen

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 in Aktualisierung der Firmware.

Ausfallsicherer CMC-Modus

Ähnlich wie beim Ausfallschutz, den ein redundanter CMC bietet, aktiviert das M1000e-Gehäuse den ausfallsicheren Modus zum Schutz von Blades und E/A-Modulen vor Ausfällen. Der ausfallsichere Modus wird aktiviert, wenn das Gehäuse nicht von einem CMC kontrolliert wird. Während des CMC-Ausfallzeitraums oder während eines einzelnen Verlusts der CMC-Verwaltung:

- können Sie neu installierte Blades nicht einschalten.
- können Sie nicht per Remote auf vorhandene Blades zugreifen.
- arbeiten die Gehäusekühlungslüfter zum Schutz der Komponenten vor Überhitzung mit voller Leistung.
- wird die Blade-Leistung reduziert, um den Stromverbrauch zu begrenzen, bis die Verwaltung durch den CMC wiederhergestellt wird.

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

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

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

Aktiver CMC – Auswahlprozess

Die beiden CMC-Steckplätze unterscheiden sich nicht; das bedeutet, dass der Steckplatz alleine 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 Anzeigen zu Gehäuseinformationen und Funktionszustandsüberwachung von Gehäuse und Komponenten.

3

Beim CMC anmelden

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

Verwandte Links

- Auf die CMC-Webschnittstelle zugreifen
- Als lokaler Benutzer, Active Directory-Benutzer oder LDAP-Benutzer bei CMC anmelden
- Anmeldung beim CMC mit Smart Card
- Anmelden beim CMC unter Verwendung einfacher Anmeldung
- Anmeldung beim CMC unter Verwendung einer seriellen, Telnet- oder SSH-Konsole
- Auf den CMC über RACADM zugreifen
- Anmeldung beim CMC mit Authentifizierung mit öffentlichem Schlüssel

Auf die CMC-Webschnittstelle zugreifen

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

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

So greifen Sie auf die CMC-Webschnittstelle zu:

1. Öffnen Sie einen unterstützten Webbrowser.
   Die neusten Informationen zu unterstützten Web-Browsern finden Sie in der *Infodatei* unter **dell.com/support/manuals**.
2. Geben Sie in das Feld **Adresse** Folgendes ein, und drücken Sie die Eingabetaste:
   - Um mit einer IPv4-Adresse auf CMC zuzugreifen, geben Sie `https://<CMC IP-Adresse>` ein.
     Wenn die Standard-HTTPS-Anschlussnummer, Anschluss 443, geändert wurde, geben Sie Folgendes ein: `https://[<CMC-IP-Adresse]:<Schnittstellennummer>`
   - Um mit einer IPv6-Adresse auf CMC zuzugreifen, geben Sie `https://[<CMC IP address>]` ein.
     Wenn die Standard-HTTPS-Anschlussnummer, Anschluss 443, geändert wurde, geben Sie Folgendes ein: `https://[<CMC IP address>]:<port number>`

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

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

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

Verwandte Links

Webbrowser konfigurieren
Als lokaler Benutzer, Active Directory-Benutzer oder LDAP-Benutzer bei CMC anmelden
Anmeldung beim CMC mit Smart Card
Anmelden beim CMC unter Verwendung einfacher Anmeldung

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

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

ANMERKUNG: Um die Sicherheit zu erhöhen, empfiehlt Dell dringend, das Standardkennwort des root-Kontos bei der Ersteinrichtung zu ändern.

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

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

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

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

   ANMERKUNG: Dieses Feld ist von Groß-/Kleinschreibung anhängig. Für Active Directory-Benutzer.
2. Geben Sie im Feld **Kennwort** das Benutzerkennwort ein.

   ANMERKUNG: Dieses Feld unterscheidet Groß- und Kleinschreibung.
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.
4. Klicken Sie auf **OK**.

   Sie sind bei CMC mit den erforderlichen Berechtigungen angemeldet.

Verwandte Links

Benutzerkonten und Berechtigungen konfigurieren
Auf die CMC-Webschnittstelle zugreifen

Anmeldung beim CMC mit Smart Card

Sie können sich über eine Smart Card bei CMC anmelden. Smart Cards verfügen über eine Zweifaktor-Authentifizierung (TFA) mit Sicherheit auf zwei Ebenen:

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

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

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

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

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

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

1. Melden Sie sich beim CMC unter Verwendung von `https://<cmcname.domain-name>` an.
   Die **CMC-Anmeldeseite** wird eingeblendet und fordert Sie zum Einlegen der Smart Card auf.

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

2. Legen Sie die Smart Card ein und klicken Sie auf **Anmeldung**.
   Daraufhin wird das Popup-Fenster für die PIN angezeigt.

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

   ANMERKUNG: Wenn der Smart Card-Benutzer in Active Directory vorhanden ist, wird kein Active Directory-Kennwort benötigt.

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

Verwandte Links

CMC SSO oder Smart Card-Anmeldung für Active Directory-Benutzer konfigurieren

Anmelden beim CMC unter Verwendung einfacher Anmeldung

Wenn die einfache Anmeldung (SSO) aktiviert ist, können Sie sich ohne die Eingabe Ihrer Anmeldeinformationen für die Domänen-Benutzerauthentifizierung (also Benutzername und Kennwort) bei CMC anmelden.

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).

Bevor Sie sich über das Verfahren für die einmalige Anmeldung bei CMC anmelden, müssen Sie Folgendes sicherstellen:

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

So melden Sie sich am CMC unter Verwendung einfacher Anmeldung an:

1. Melden Sie sich unter Verwendung Ihres Netzwerkkontos beim Clientsystem an.
2. Greifen Sie auf die CMC-Webschnittstelle über `https://<cmcname.domain-name>` zu.
   Beispiel: **cmc-6G2WXF1.cmcad.lab** wobei **cmc-6G2WXF1** der CMC-Name ist und **cmcad.lab** der Domänenname.

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

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

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

Verwandte Links

CMC SSO oder Smart Card-Anmeldung für Active Directory-Benutzer konfigurieren

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

Sie können sich beim CMC entweder mit einer seriellen oder einer Telnet-/SSH-Verbindung anmelden oder über die Dell-CMC-Konsole auf dem iKVM.

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

1. Stellen Sie mit der Terminalemulationssoftware der Management Station eine Verbindung zum CMC her.
2. Geben Sie Ihren CMC-Benutzernamen und das Kennwort ein und drücken dann <Eingabe>.
   Sie sind am CMC angemeldet.

Verwandte Links

CMC zur Verwendung von Befehlszeilenkonsolen konfigurieren
Aktivieren des iKVM-Zugangs über die Dell CMC-Konsole

Auf den CMC über RACADM zugreifen

RACADM bietet eine Reihe von Befehlen an, mit denen Sie den CMC über eine textbasierte Oberfläche konfigurieren und verwalten können. Auf RACADM kann über eine Telnet-/SSH- oder eine serielle Verbindung zugegriffen werden, unter Verwendung der Dell CMC-Konsole auf dem 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. CMC unterstützt kein Scripting, was bedeutet, dass Sie keine Skripts direkt auf dem CMC ausführen können.

Lesen Sie für weitere Informationen über RACADM das *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC*.

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

Anmeldung beim CMC mit Authentifizierung mit öffentlichem Schlüssel

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

Stellen Sie vor der Anmeldung über SSH beim CMC sicher, dass die öffentlichen Schlüssel hochgeladen wurden.

Beispiel:

- **Anmelden**: `ssh service@<domain>` oder `ssh service@<IP_address>` , wobei IP_address die CMC IP-Adresse ist.
- **Senden von RACADM-Befehlen**: `ssh service@<domain> racadm getversion` und `ssh service@<domain> racadm getsel`

Wenn Sie sich mit den Dienstkonto anmelden, und beim Erstellen des öffentlichen/privaten Schlüsselpaars wurde ein Kennsatz eingerichtet, werden Sie u. U. aufgefordert, diesen Kennsatz erneut einzugeben. Wenn ein Kennsatz mit den Schlüsseln verwendet wird, bieten 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 „sshagent“ verwenden. Informationen über Einrichtung und Verwendung dieser Anwendungen finden Sie in der zur Anwendung gehörenden Dokumentation.

Verwandte Links

Authentifizierung mit öffentlichem Schlüssel über SSH.

CMC-Mehrfachsitzungen

Aus der folgenden Tabelle können Sie eine Liste mit mehreren CMC-Sitzungen entnehmen, die durch die Verwendung der diversen Schnittstellen möglich sind.

Tabelle 7. CMC-Mehrfachsitzungen

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

4

Aktualisieren der Firmware

Sie können die Firmware für folgende Geräte aktualisieren:

- CMC – Aktiv und Standby
- iKVM
- EAMs

Sie können die Firmware für folgende Serverkomponenten aktualisieren:

- iDRAC – Alle iDRACs 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.
- BIOS
- Unified Server Configurator
- 32-Bit Diagnose
- OS-Treiberpaket
- Netzwerkschnittstellen-Controller
- RAID-Controller

Verwandte Links

Herunterladen der CMC-Firmware
Aktuelle Firmware-Versionen anzeigen
Aktualisieren von CMC-Firmware
Aktualisieren der iKVM-Firmware
Server-iDRAC-Firmware aktualisieren
Aktualisieren der Serverkomponenten-Firmware
iDRAC-Firmware mittels CMC wiederherstellen
Aktualisierung der Firmware des EAM-Infrastrukturgeräts

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

Aktuelle Firmware-Versionen anzeigen

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

Anzeige der aktuell installierten Firmwareversionen über die CMC-Webschnittstelle

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

- **Gehäuseübersicht → Aktualisieren**
- **Gehäuseübersicht → Gehäuse-Controller → Aktualisieren**
- **Gehäuseübersicht → Server-Übersicht → Aktualisieren**
- **Gehäuseübersicht → E/A-Modulübersicht → Aktualisieren**
- **Gehäuseübersicht → iKVM → Aktualisierung**

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.

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

Anzeige der aktuell installierten Firmwareversionen über RACADM

Um die derzeit installierte Firmware über RACADM anzuzeigen, benutzen Sie den Unterbefehl **getkvminfo**. Weitere Informationen finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC*.

Aktualisieren von CMC-Firmware

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

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

Wenn eine Benutzersitzung an der Webschnittstelle verwendet wird, um Systemkomponenten-Firmware zu aktualisieren, müssen die Einstellungen für die Inaktivitätszeitüberschreitung 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.

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

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

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

Nachdem der Standby-CMC aktualisiert wurde, tauschen Sie die CMC-Rollen miteinander aus, sodass der neu aktualisierte CMC als aktiver CMC und der CMC mit der früheren Firmware als Standby funktioniert. Hilfe zum Rollentausch finden Sie im Abschnitt zum `cmcchangeover`-Befehl im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 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.

Um zu vermeiden, dass die Verbindung von Benutzern während des Resets unterbrochen wird, benachrichtigen Sie bitte berechtigte Benutzer, die sich am CMC anmelden könnten, und prüfen Sie auf aktive Sitzungen, indem Sie die Seite Sitzungen anzeigen. Um die Seite **Sitzungen** zu öffnen, wählen Sie in der Struktur **Gehäuse** aus, klicken Sie auf das Register **Netzwerk** und dann auf das Unterregister **Sitzungen**.

Wenn Sie Dateien zum und vom CMC übertragen, dreht sich während der Übertragung das Dateiübertragungssymbol. Wenn das Symbol animiert ist, überprüfen Sie, ob der Browser so konfiguriert ist, dass Animationen zugelassen sind. Anleitungen hierzu finden Sie unter Animationen im Internet Explorer erlauben.

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.

Verwandte Links

Herunterladen der CMC-Firmware
Aktuelle Firmware-Versionen anzeigen

CMC-Firmware über die Webschnittstelle aktualisieren

So aktualisieren Sie die CMC-Firmware mit der CMC-Webschnittstelle:

1. Klicken Sie auf eine beliebige der folgenden Seiten:
   - **Gehäuse-Übersicht → Aktualisierung**
   - **Gehäuse-Übersicht → Gehäuse-Controller → Aktualisierung**
   - **Gehäuse-Übersicht → E/A-Modulübersicht → Aktualisierung**
   - **Gehäuse-Übersicht → iKVM → Aktualisierung**

   Die Seite **Firmware-Aktualisierung** wird angezeigt.
2. Wählen Sie im Abschnitt **CMC-Firmware** das/die Kontrollkästchen in der Spalte **Ziele aktualisieren** für den CMC oder die CMC (falls Standby-CMC vorhanden ist), für die Sie die Firmware aktualisieren möchten, und klicken Sie auf **CMC-Aktualisierung anwenden**.
3. Im Feld **Firmware-Image** geben Sie den Pfad zur Firmware-Image-Datei auf der Managementstation oder dem gemeinsam genutzten Netzwerk ein oder klicken Sie auf **Durchsuchen**, um zum Dateispeicherort zu navigieren. Der standardmäßige Firmware-Image-Name lautet `firmimg.cmc`.
4. Klicken Sie auf **Firmware-Aktualisierung beginnen** und 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 Übertragungszeit kann je nach Verbindungsgeschwindigkeit variieren. Wenn der interne Aktualisierungsprozess beginnt, wird die Seite laufend aktualisiert und zeigt den Firmwareaktualisierungszeitgeber an.
5. Zusätzliche Anweisungen:
   - Klicken Sie während der Dateiübertragung nicht auf das Symbol **Aktualisierung** und navigieren Sie nicht zu einer anderen Seite.
   - Um den Prozess abzubrechen, klicken Sie auf **Dateiübertragung und Aktualisierung abbrechen**. Diese Option ist nur während der Dateiübertragung verfügbar.
   - Das Feld **Aktualisierungsstatus** zeigt den Firmware-Aktualisierungsstatus an.

   ANMERKUNG: Die Aktualisierung kann einige Minuten für den CMC dauern.

6. 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. Anweisungen zum Löschen des Browser-Cache finden Sie in der Online-Hilfe zu Ihrem Webbrowser.

Aktualisieren der CMC-Firmware über RACADM

Verwenden Sie den Unterbefehl fwupdate um die CMC-Firmware über RACADM anzuzeigen. Weitere Informationen hierzu finden Sie im *RACADM-Befehlzeilen-Referenzhandbuch für den iDRAC7 und CMC*.

Aktualisieren der iKVM-Firmware

Nach dem erfolgreichen Abschluss der Firmwareaktualisierung wird das iKVM-Modul zurückgesetzt und ist vorübergehend nicht verfügbar.

Verwandte Links

Herunterladen der CMC-Firmware

Aktuelle Firmware-Versionen anzeigen

iKVM-Firmware über die CMC-Web-Schnittstelle aktualisieren

So aktualisieren Sie die iKVM-Firmware mit der CMC-Webschnittstelle:

1. Gehen Sie zu einer der folgenden Seiten:
   - **Gehäuseübersicht → Aktualisieren**
   - **Gehäuseübersicht → Gehäuse-Controller → Aktualisieren**
   - **Gehäuseübersicht → iKVM → Aktualisieren**

   Die Seite **Firmware-Aktualisierung** wird angezeigt.
2. Wählen Sie im Abschnitt **iKVM-Firmware** das Kontrollkästchen in der Spalte **Ziele aktualisieren** für das **iKVM** für das Sie die Firmware aktualisieren wollen und klicken Sie auf **iKVM-Aktualisierung anwenden**.
3. Im Feld **Firmware-Image** geben Sie den Pfad zur Firmware-Image-Datei auf der Managementstation oder dem gemeinsam genutzten Netzwerk ein oder klicken Sie auf **Durchsuchen**, um zum Dateispeicherort zu navigieren. Der Standardname des iKVM-Firmware-Image ist **iKVM.bin**.
4. Klicken Sie auf **Firmware-Aktualisierung beginnen** und dann klicken Sie auf **Ja,** um weiterzufahren.

   Der Abschnitt **Fortschritt der Firmware-Aktualisierung** bietet Statusinformationen zur Firmwareaktualisierung. Ein Statusindikator wird auf der Seite während des Aktualisierungsvorganges angezeigt. Die Übertragungszeit kann je nach Verbindungsgeschwindigkeit variieren. Wenn der interne Aktualisierungsprozess beginnt, wird die Seite laufend aktualisiert und zeigt den Firmwareaktualisierungszeitgeber an.
5. Zusätzliche Anweisungen:
   - Verwenden Sie während der Dateiübertragung nicht die Schaltfläche **Aktualisierung** und navigieren Sie nicht zu einer anderen Seite.
   - Um den Prozess abzubrechen, klicken Sie auf **Dateiübertragung und Aktualisierung abbrechen**. Diese Option ist nur während der Dateiübertragung verfügbar.
   - Das Feld **Aktualisierungsstatus** zeigt den Firmware-Aktualisierungsstatus an.

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.

Aktualisieren der iKVM-Firmware über RACADM

Verwenden Sie den Unterbefehl `fwupdate`, um den Datenverlauf über iKVM-Firmware anzuzeigen. Weitere Informationen hierzu finden Sie im *RACADM-Befehlzeilen-Referenzhandbuch für den iDRAC7 und CMC*.

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-Webschnittstelle angezeigt, wenn die aktuelle Revision auf der Komponente und das Komponenten-Image nicht übereinstimmen.

Bevor Sie die Firmware der EAM-Infrastrukturgeräte aktualisieren, stellen Sie sicher, dass die CMC-Firmware aktualisiert wird.

ANMERKUNG:

Aktualisierungen der Firmware des EAM-Infrastrukturgeräts (IOMINF) werden nur 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 nicht als aktualisierbare Geräte aufgelistet.

Verwandte Links

Herunterladen der CMC-Firmware
Aktuelle Firmware-Versionen anzeigen
EAM-Software über die CMC-Web-Schnittstelle aktualisieren

EAM-Firmware über die CMC-Web-Schnittstelle aktualisieren

So aktualisieren Sie die Firmware des EAM-Infrastruktugerätes in der CMC-Webschnittstelle:

1. Wählen Sie **Gehäuse-Übersicht → E/A-Modul-Übersicht → Aktualisierung**.
   Die Seite **EAM-Firmware und Software** wird angezeigt.
   Sonst gehen Sie zu einer der folgenden Optionen:
   - **Gehäuseübersicht → Aktualisieren**
   - **Gehäuseübersicht → Gehäuse-Controller → Aktualisierung**
   - **Gehäuseübersicht → iKVM → Aktualisieren**

   Die Seite **Firmware-Aktualisierung** mit einem Link, um auf die Seite **EAM-Firmware und Software** zuzugreifen, wird angezeigt.
2. Wählen Sie auf der Seite **EAM-Firmware und Software** im Abschnitt **EAM-Firmware** das Kontrollkästchen für das EAM, für das Sie die Firmware aktualisieren möchten, in der Spalte **Aktualisierung** aus, und klicken Sie auf **Firmwareaktualisierung anwenden**.
   Der Abschnitt **Fortschritt der Aktualisierung** bietet Statusinformationen zur Firmwareaktualisierung. Ein Statusindikator wird auf der Seite während des Aktualisierungsvorganges angezeigt. Die Übertragungszeit kann je

nach Verbindungsgeschwindigkeit variieren. Wenn der interne Aktualisierungsprozess beginnt, wird die Seite laufend aktualisiert und zeigt den Firmwareaktualisierungszeitgeber an.

ANMERKUNG: Verwenden Sie während der Dateiübertragung nicht die Schaltfläche **Aktualisierung** und navigieren Sie nicht zu einer anderen Seite.

ANMERKUNG: Es wird bei der IOMINF-Firmware-Aktualisierung kein Zeitgeber angezeigt.

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

Aktualisieren der EAM-Firmware über RACADM

Um die Firmware des EAM-Infrastrukturgeräts mit RACADM zu aktualisieren, verwenden Sie den fwupdate-Unterbefehl. Weitere Informationen finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC*.

Server-iDRAC-Firmware aktualisieren

Sie können die Firmware für iDRAC6 und iDRAC7 aktualisieren.

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.

Der iDRAC (auf einem Server) wird zurückgesetzt und ist vorübergehend nicht verfügbar, nachdem die Firmware-Aktualisierungen erfolgreich hochgeladen wurden.

Verwandte Links

Herunterladen der CMC-Firmware

Aktuelle Firmware-Versionen anzeigen

Server-iDRAC Firmware über die Webschnittstelle aktualisieren

So aktualisieren Sie die iDRAC-Firmware im Server über die CMC-Webschnittstelle:

1. Gehen Sie zu einer der folgenden Seiten:
   - **Gehäuseübersicht → Aktualisieren**
   - **Gehäuseübersicht → Gehäuse-Controller → Aktualisierung**
   - **Gehäuseübersicht → iKVM → Aktualisieren**

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

   Sie können auch Server-iDRAC-Firmware unter **Gehäuseübersicht → Server-Übersicht → Aktualisierung** aktualisieren. Weitere Informationen finden Sie unter Aktualisieren der Serverkomponenten-Firmware.
2. Um iDRAC6 Firmware zu aktualisieren, wählen Sie im Abschnitt **iDRAC6 Enterprise Firmware** in der Spalte **Ziele aktualisieren** das Kontrollkästchen für die iKVM, für die Sie die Firmware aktualisieren möchten, und klicken Sie auf **iDRAC6 Enterprise-Aktualisierung anwenden** und fahren Sie mit Schritt 4 fort.
3. Um iDRAC7 Firmware zu aktualisieren, klicken Sie im Abschnitt **iDRAC7 Enterprise Firmware** auf den Link **Aktualisierung** für den Server, für den Sie die Firmware aktualisieren möchten.

   Die Seite **Serverkomponentenaktualisierung** wird angezeigt. Um fortzufahren, siehe Abschnitt Aktualisieren der Serverkomponenten-Firmware.

4. Im Feld **Firmware-Image** geben Sie den Pfad zur Firmware-Image-Datei auf Ihrer Managementstation oder dem gemeinsam genutzten Netzwerk ein oder klicken Sie auf **Durchsuchen**, um zum Dateispeicherort zu navigieren. Der Standardname für das iDRAC-Firmware-Image ist **firmimg.imc**.
5. Klicken Sie auf **Firmware-Aktualisierung beginnen** und dann klicken Sie auf **Ja,** um weiterzufahren.

   Der Abschnitt **Fortschritt der Firmware-Aktualisierung** bietet Statusinformationen zur Firmwareaktualisierung. Ein Statusindikator wird auf der Seite während des Aktualisierungsvorganges angezeigt. Die Übertragungszeit kann je nach Verbindungsgeschwindigkeit variieren. Wenn der interne Aktualisierungsprozess beginnt, wird die Seite laufend aktualisiert und zeigt den Firmwareaktualisierungszeitgeber an.
6. Zusätzliche Anweisungen:

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

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

   Wenn die Aktualisierung abgeschlossen ist, wird das iKVM zurückgesetzt und die neue Firmware wird auf der Seite **Firmware-Aktualisierung** angezeigt.

Server-iDRAC-Firmware mittels RACADM aktualisieren

Verwenden Sie den Unterbefehl **fwupdate** um die iDRAC-Firmware über RACADM zu aktualisieren. Weitere Informationen hierzu finden Sie im *RACADM-Befehlzeilen-Referenzhandbuch für den iDRAC7 und CMC*.

Aktualisieren der Serverkomponenten-Firmware

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

Dell Update Packages (DUPs) werden zur Durchführung der Firmware-Aktualisierungen mit dem Lifecycle-Controller verwendet. Die standardmäßige CMC-Konfiguration hat eine Größenbeschränkung von 48 MB für das DUP. Die DUP-Komponente für das BS-Treiberpaket überschreitet diesen Grenzwert und muss separat über die Funktion „Erweiterter Speicher“ aktualisiert werden.

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

Vor der Verwendung der Lifecycle Controller-basierten Aktualisierungsfunktion müssen die Server-Firmwareversionen aktualisiert werden.

Sie müssen die CMC-Firmware vor dem Aktualisieren der Firmware-Module für die Serverkomponente aktualisieren.

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

1. BIOS
2. Lifecycle-Controller
3. iDRAC

Sie können die Firmware-Module der Serverkomponenten über die CMC-Webschnittstelle auf der Seite **Gehäuseübersicht** → **Server-Übersicht** → **Aktualisieren** → **Serverkomponentenaktualisierung** aktualisieren.

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

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

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

Wenn der Dienst Lifecycle Controller des Servers deaktiviert ist, zeigt der Abschnitt **Komponente/Gerät-Firmware-Bestandsaufnahme** *Lifecycle Controller kann nicht aktiviert werden* an.

Verwandte Links

Aktivierung des Lifecycle Controllers
Filtern von Komponenten für Firmware-Aktualisierungen
Anzeigen der Firmware-Bestandsliste
Lifecycle-Controller-Jobvorgänge
Aktualisierung der Firmware des EAM-Infrastrukturgeräts

Aktivierung des Lifecycle Controllers

Sie können den Lifecycle Controller-Dienst während des Server-Startvorgangs aktivieren:

- Drücken Sie bei iDRAC6-Servern auf der Startkonsole, wenn Sie dazu über die Nachricht `Drücken Sie innerhalb von 5 Sekunden 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 **Systemdienste**.
- 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** aus.

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

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

- *Lifecycle Controller Remote Services-Benutzerhandbuch*.
- **delltechcenter.com/page/Lifecycle+Controller**

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-Konfigurations**berechtigung und **iDRAC-Anmeldungs**berechtigung.

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

Filtern von Komponenten für Firmware-Aktualisierungen

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.
- Filtern Sie die ausgewählten Komponenten und Geräte automatisch, 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.

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

So filtern Sie die Geräte

1. Wählen Sie in der Systemstruktur **Server-Übersicht** aus und klicken Sie auf**Aktualisierung** → **Serverkomponentenaktualisierung**.

   Die Seite **Serverkomponentenaktualisierung** wird angezeigt.
2. Wählen Sie im Abschnitt **Komponente/Geräteaktualisierungsfilter** eines oder mehrere der folgenden Werkzeuge aus:

   - BIOS
   - iDRAC
   - Lifecycle-Controller
   - 32-Bit Diagnose
   - BS-Treiberpaket
   - Netzwerkschnittstellencontroller (I/F)
   - RAID-Controller

Im Abschnitt **Firmware-Bestandsaufnahme** zeigt nur die jeweiligen Komponenten oder Geräte über alle im Gehäuse vorhandenen Server hinweg an. 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.

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

Wenn kein Filter ausgewählt wird und im Bestandsaufnahmeabschnitt eine Auswahl zur Aktualisierung einer Komponente oder eines Gerätes vorgenommen wird, dann wird der mit dieser Auswahl verbundene Filter automatisch aktiviert. Es kann eine weitere Filterung auftreten, bei der der Bestandsaufnahmeabschnitt alle Server anzeigt, die eine Übereinstimmung mit der gewählten Komponente hinsichtlich des Modells, Typs oder irgendeiner anderen Identitätsform aufweisen. Wenn z.B. eine BIOS-Komponente auf einem der Server für die Aktualisierung ausgewählt wird, wird der Filter automatisch auf BIOS eingestellt und der Bestandsaufnahmeabschnitt zeigt die Server an, die mit der Modellbezeichnung des ausgewählten Servers übereinstimmen.

Komponenten für die Firmware-Aktualisierung über RACADM filtern

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

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

Weitere Informationen finden Sie im RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC, das unter **dell.com/support/manuals** verfügbar ist.

Anzeigen der Firmware-Bestandsliste

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

Firmwarebestandsaufnahme über die CMC-Webschnittstelle anzeigen

So zeigen Sie die Firmware-Bestandsaufnahme an:

1. Wählen Sie in der Systemstruktur **Server-Übersicht** aus und klicken Sie auf **Aktualisierung** → **Serverkomponentenaktualisierung**.

   Die Seite **Serverkomponentenaktualisierung** wird angezeigt.

2. Zeigen Sie die Firmware-Bestandsaufnahmedetails im Abschnitt **Komponente/Gerät-Firmware-Bestandsaufnahme**. Die Tabelle enthält

   - Server, die derzeit den Lifecycle Controller-Dienst nicht unterstützen, werden als **Nicht unterstützt** aufgeführt. Es steht ein Hyperlink zur Verfügung, der zu einer alternativen Seite führt, auf der es möglich ist, nur die iDRAC-Firmware zu aktualisieren. Diese Seite unterstützt nur iDRAC-Firmware-Aktualisierung und keine Aktualisierung irgendwelcher der Komponenten oder Geräte des Servers. iDRAC-Firmware-Aktualisierung ist nicht von dem Lifecycle-Controller-Dienst abhängig.
   - Wird der Server als **Nicht bereit** aufgeführt, weist es darauf hin, dass sich der iDRAC auf dem Server zum Zeitpunkt des Abrufens der Firmware-Bestandsaufnahme noch in der Initialisierungsphase befand. Warten Sie etwas, bis der iDRAC komplett betriebsbereit ist und aktualisieren Sie dann die Seite, damit die Firmware-Bestandsaufnahme erneut abgerufen werden kann.
   - Wenn die Bestandsaufnahme der Komponenten und Geräte nicht dem entspricht, was physikalisch auf dem Server installiert ist, dann müssen Sie während des Server-Startvorgangs Lifecycle-Controller aufrufen. Dies ist beim Aktualisieren der internen Komponenten- und Geräteinformationen hilfreich und stellt eine Möglichkeit zur Prüfung der derzeit installierten Komponenten und Geräte dar. Dieses Verhalten tritt dann auf, wenn:

* Die Server-iDRAC-Firmware aktualisiert wird, um die Lifecycle Controller-Funktionalität neu bei der Serververwaltung einzuführen.
* Die neuen Geräte in den Server eingesetzt werden.

Um diese Maßnahme zu automatisieren, stellt das iDRAC-Konfigurationshilfsprogramm (für iDRAC6) oder das iDRAC-Einstellungsdienstprogramm (für iDRAC7) 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 `Drücken Sie innerhalb von 5 Sekunden 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-Bestandsaufnahme 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-Bestandsaufnahme beim Neustart erfassen**.

– Es stehen Optionen zum Durchführen der verschiedenen Lifecycle Controller-Vorgänge, wie z.B. Aktualisierung, Rollback, Neuinstallation und Joblöschung zur Verfügung. Es kann immer nur ein Vorgangstyp durchgeführt werden. Nicht unterstützte Komponenten und Server werden möglicherweise als Teil der Bestandsaufnahme aufgeführt, Lifecycle Controller-Vorgänge sind jedoch zulässig.

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

Tabelle 8. 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 Steckplätze angezeigt.
Name	Zeigt den Namen des Servers in den einzelnen Steckplätzen an.
Modell	Zeigt das Modell des Servers an.
Komponente/Gerät	Zeigt eine Beschreibung der Komponente oder des Geräts auf dem Server an. Wenn die Spaltenbreite zu schmal ist, stellt das Mouse-Over-Hilfswerkzeug eine Ansicht mit der Beschreibung bereit.
Aktuelle Version	Zeigt die aktuelle Version der Komponente oder des Geräts auf dem Server an.
Rollback-Version	Zeigt die Rollback-Version der Komponente oder des Geräts auf dem Server an.
Jobstatus	Zeigt den Jobstatus von jeglichen Vorgängen an, die auf dem Server geplant sind. Der Jobstatus wird kontinuierlich dynamisch aktualisiert. Wenn ein Jobabschluss über den Status als abgeschlossen erkannt wird, werden für den Fall, dass sich bei einer der Komponenten oder Geräte die Firmwareversion geändert hat, die Firmwareversionen der Komponenten und Geräte auf dem Server automatisch aktualisiert. Neben dem aktuellen Status ist auch ein Info-Symbol vorhanden, das zusätzliche Informationen über den aktuellen Jobstatus bereitstellt. Diese Informationen können angezeigt werden, indem auf das Symbol geklickt wird oder der Mauszeiger über das Symbol bewegt wird.

Feld	Beschreibung
Aktualisierung	Wählt die Komponente oder das Gerät für die Firmware-Aktualisierung auf dem Server aus.

Anzeigen der Firmware-Bestandsliste über RACADM

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

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

Weitere Informationen finden Sie im RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC, das unter **dell.com/support/manuals** verfügbar ist.

Lifecycle-Controller-Jobvorgänge

Sie können Lifecycle-Controller-Vorgänge wie diese durchführen:

- Neuinstallation
- Zurücksetzen
- Aktualisierung
- Jobs löschen

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

Zum Durchführen der verschiedenen Lifecycle Controller-Vorgänge brauchen Sie:

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

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

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

Verlassen Sie die Seite nicht, wenn ein Vorgang für die Planung unterbreitet 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.

Verwandte Links

Neuinstallation der Serverkomponenten-Firmware
Zurücksetzen der Serverkomponenten-Firmware
Aktualisieren der Serverkomponenten-Firmware
Geplante Serverkomponenten-Firmware-Jobs löschen

Neuinstallation der Serverkomponenten-Firmware

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

Neuinstallation der Serverkomponenten-Firmware über die Webschnittstelle

So führen Sie eine Neuinstallation der Serverkomponenten-Firmware aus:

1. Wählen Sie in der Systemstruktur **Server-Übersicht** aus und klicken Sie auf **Klicken → Aktualisierung → Serverkomponentenaktualisierung**.

   Die Seite **Serverkomponentenaktualisierung** wird angezeigt.
2. Filtern Sie die Komponente oder das Gerät (optional).
3. Wählen Sie in der Spalte **Aktuelle Version** das Kontrollkästchen für die Komponente oder das Gerät, für die oder das Sie die Firmware neu istallieren möchten.
4. Wählen Sie eine der folgenden Optionen:

   - **Jetzt neu starten** - Sofort neu starten.
   - **Bei nächstem Neustart** - Manuell zu einem späteren Zeitpunkt neu starten.
5. Klicken Sie auf **Neu installieren**. Die Firmware-Version für die ausgewählten Komponenten oder Geräte wird neuinstalliert.

Zurücksetzen der Serverkomponenten-Firmware

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

Zurücksetzen der Serverkomponenten-Firmware über die CMC-Webschnittstelle

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

1. Erweitern Sie in der CMC-Webschnittstelle die Systemstruktur, wählen Sie **Server-Übersicht** und klicken Sie anschließend auf **Aktualisieren → Server-Komponentenaktualisierung**.

   Die Seite **Serverkomponentenaktualisierung** wird angezeigt.
2. Filtern Sie die Komponente oder das Gerät (optional).
3. Wählen Sie in der Spalte **Version zurücksetzen** das Kontrollkästchen für die Komponente oder das Gerät, für die oder das Sie die Firmware zurücksetzen möchten.
4. Wählen Sie eine der folgenden Optionen:

   - **Jetzt neu starten** - Sofort neu starten.
   - **Bei nächstem Neustart** - Manuell zu einem späteren Zeitpunkt neu starten.
5. Klicken Sie auf **Zurücksetzen**. Die vorher installierte Firmware-Version für die ausgewählten Komponenten oder Geräte wird neuinstalliert.

Aktualisieren der Serverkomponenten-Firmware

Sie können die nächste Version des Firmware-Image für die ausgewählten Komponenten oder Geräte über einen oder mehrere Server hinweg installieren. Das Firmware-Image steht innerhalb des Lifecycle Controllers für einen Rollback-Vorgang zur Verfügung.

ANMERKUNG: Stellen Sie für Firmware-Aktualisierung der iDRAC- und BS-Treiber-Pakete sicher, dass die Erweiterte Speicherfunktion aktiviert ist.

Es wird empfohlen, die Jobswarteschlange zu löschen, bevor Sie die Aktualisierung einer Serverkomponentenfirmware initialisieren. Auf der Seite Lifecycle Controller-Jobs ist eine Liste mit allen Jobs auf den/dem Server(n) vorhanden. Diese Seite ermöglicht die Löschung einzelner/mehrerer Jobs oder die Bereinigung aller Jobs auf dem Server. Weitere Informationen finden Sie im Abschnitt „Fehlerbehebung“ unter „Lifecycle Controller-Jobs auf einem Remote-System verwalten“.

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 Jobsstatus 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. Zum Aktualisieren mehrerer Komponenten auf einem Server wird empfohlen, zuerst die Lifecycle-Controller- und 32-Bit-Diagnose-Komponenten zusammen zu aktualisieren. Diese benötigen keinen Neustart des Servers und können relativ schnell abgeschlossen werden. Die anderen Komponenten können anschließend zusammen aktualisiert werden.

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

Aktualisieren der Serverkomponenten-Firmware über die CMC-Webschnittstelle

So aktualisieren Sie Firmware zu der nächsten Version:

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

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

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

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

   ANMERKUNG: Die Größenbeschränkung für die Aktualisierung von entweder einzelnen DUPs oder kombinierten DUPs kann ignoriert werden, wenn die Funktion "Erweiterter Speicher" installiert und aktiviert wurde. Weitere Informationen zum Aktivieren des erweiterten Speichers finden Sie unter CMC Erweiterte Speicherkarte konfigurieren.
4. Geben Sie die Firmware-Image-Datei für die ausgewählte(n) Komponente(n) bzw. das/die ausgewählte(n) Gerät(e) an. Das ist eine Microsoft Windows Dell Update Package (DUP)-Datei.
5. Wählen Sie eine der folgenden Optionen:

   – **Jetzt neu starten** - Sofort neu starten.

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

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

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

Geplante Serverkomponenten-Firmware-Jobs löschen

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

Geplante Serverkomponenten-Firmware-Jobs über die Webschnittstelle löschen

So löschen Sie geplante Serverkomponenten-Firmware-Jobs:

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

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

iDRAC-Firmware mittels CMC wiederherstellen

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

Für 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. Führen Sie die beschriebenen Schritte für das Aktualisieren der Firmware durch.

5

Gehäuseinformationen anzeigen und Funktionszustandsüberwachung von Gehäuse und individuellen Komponenten

Sie können Informationen anzeigen und den Funktionszustand für Folgendes überwachen:

- Aktive und Standby-CMC
- Alle Server und einzelne Server
- Speicher-Arrays
- Alle E/A-Module (EAMs) und einzelne EAMs
- Lüfter
- iKVM
- Netzteile (PSUs)
- Temperatursensoren
- LCD-Baugruppe

Gehäuse-Komponenten-Zusammenfassungen anzeigen

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

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

Um den Gehäusefunktionszustand anzuzeigen, klicken Sie auf **Gehäuseübersicht** → **Eigenschaften** → **Funktionszustand** . 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. Außerdem werden die neuesten Ereignisse im CMC-Hardwareprotokoll angezeigt. Weitere Informationen finden Sie in *CMC-Online-Hilfe*.

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

Gehäuse-Grafiken

Das Gehäuse wird in Vorder- und Rückansichten dargestellt (jeweils die oberen und unteren Bilder). 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. 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 9. : Serversymbolzustände

Symbol	Beschreibung
	Der Server ist eingeschaltet und arbeitet normal.
	Der Server ist ausgeschaltet.
	Der Server meldet einen nicht-kritischen Fehler.
	Der Server meldet einen kritischen Fehler.

Symbol	Beschreibung
	Es ist kein Server vorhanden.

Ausgewählte Komponenteninformationen

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

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

Servermodellnamen und Service-Tag-Nummer anzeigen

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

1. 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.
2. Positionieren Sie den Cursor auf dem Steckplatznamen oder der Steckplatznummer eines Servers; falls verfügbar, wird eine Quickinfo mit dem Modellnamen und der Service-Tag-Nummer des Servers angezeigt.

Gehäusezusammenfassung anzeigen

Sie können eine Zusammenfassung über zu den in dem Gehäuse installierten Komponenten anzeigen.

Um die Zusammenfassung der Gehäuseinformationen in the CMC -Webschnittstelle anzuzeigen, klicken Sie auf **Gehäuse-Übersicht → Eigenschaften → Zusammenfassung** .

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

Gehäuse-Controllerinformationen und Status anzeigen

Um Gehäuse-Controllerinformationen und Status anzuzeigen, gehen Sie in der CMC Webschnittstelle zu **Gehäuseübersicht → Gehäuse-Controller → Eigenschaften → Status**.

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

Informationen und Funktionszustand von allen Servern anzeigen

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

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

Die Seite **Gehäusefunktionszustand** bietet einen grafischen Überblick über alle Server, die im Gehäuse installiert sind. Der Serverfunktionszustand wird durch die Farbe der Server-Untergrafik angegeben. Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.

2. Gehen Sie zu **Gehäuse-Übersicht** → **Server-Übersicht** → **Eigenschaften** → **Status**.
   Die Seite **Status der Server** enthält Übersichten zu den Servern im Gehäuse. Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.

Anzeigen des Funktionszustands eines einzelnen Servers

So zeigen Sie den Funktionszustand von einzelnen Servern an:

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

2. Klicken Sie in der Systemstruktur auf **Gehäuseübersicht** und erweitern Sie **Server-Übersicht**. Es werden alle Server (1 - 16) in der erweiterten Liste angezeigt. Klicken Sie auf den Steckplatz, in dem sich das Speicher-Array befindet.
   Die Seite **Serverstatus** (nicht zu verwechseln mit der Seite **Status der Server** bietet den Funktionszustand des Servers im Gehäuse und eine Start-URL zur iDRAC-Webschnittstelle, die die Firmware darstellt, die zur Verwaltung des Servers verwendet wird. Weitere Informationen finden Sie in der *CMC Online-Hilfe*.

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

Anzeigen des Speicher-Array-Status

So zeigen Sie den Funktionszustand von allen Servern an:

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

2. Klicken Sie in der Systemstruktur auf **Gehäuseübersicht**und erweitern Sie **Server-Übersicht**. Es werden alle Server (1 - 16) in der erweiterten Liste angezeigt. Klicken Sie auf den Steckplatz, in dem sich das Speicher-Array befindet.
   Die Seite „Speicher-Array-Status“ bietet eine Übersicht über den Funktionszustand sowie den Eigenschaften der Speicherarrays. Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.

Informationen und Funktionszustand von allen EAMs anzeigen

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

1. Gehen Sie zu **Gehäuse-Übersicht** → **Eigenschaften** → **Funktionszustand**.

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. Positionieren Sie den Cursor auf die einzelne Server-Untergrafik. Der Texthinweis liefert zusätzliche Informationen zu diesem EAM. Klicken Sie auf die EAM-Untergrafik, um die EAM-Informationen rechts anzuzeigen.

2. Wählen Sie **Gehäuse-Übersicht** → **E/A-Modul-Übersicht** → **Eigenschaften** → **Status**.

   Die Seite **E/A-Modul-Status** enthält Übersichten zu allen mit dem Gehäuse verbundenen E/A-Modulen. Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.

Anzeigen der Informationen und des Funktionszustands eines einzelnen EAMs

Um den Funktionszustand des einzelnen EAMs in der CMC-Webschnittstelle anzuzeigen, führen Sie einen der folgenden Schritte aus:

1. Gehen Sie zu **Gehäuseübersicht** → **Eigenschaften** → **Funktionszustand** .

   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. Positionieren Sie den Cursor auf der einzelnen EAM-Untergrafik. Der Texthinweis liefert zusätzliche Informationen zu diesem EAM. Klicken Sie auf die EAM-Untergrafik, um die EAM-Informationen rechts anzuzeigen.

2. Gehen Sie zu **Gehäuseübersicht** und erweitern Sie die **E/A-Modulübersicht** in der Systemstruktur. Es werden alle EAMs (1–6) in der erweiterten Liste angezeigt. Klicken Sie auf das EAM (Steckplatz), das Sie anzeigen möchten.

   Die Seite **E/A-Modulstatus** (zu unterscheiden von der generellen Seite **E/A-Module-Status**), die für den EAM-Steckplatz spezifisch ist, wird angezeigt. Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.

Informationen und Funktionszustand der Lüfter anzeigen

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.

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

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

1. Klicken Sie auf **Gehäuseübersicht** → **Eigenschaften** → **Funktionszustand** .

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

2. Gehen Sie zu **Gehäuse-Übersicht** → **Lüfter** → **Eigenschaften** .

   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.

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

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

iKVM-Informationen und Funktionszustand anzeigen

Der Name des Lokalzugriffs-KVM-Modul für das Dell M1000e-Servergehäuse lautet Avocent Integrated KVM Switch-Modul (iKVM).

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

1. Wählen Sie **Gehäuse-Übersicht → Eigenschaften → Funktionszustand** .

   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. Bewegen Sie den Cursor über die iKVM-Untergrafik und ein entsprechender Texthinweis oder Bildschirmtipp wird angezeigt. Der Texthinweis liefert zusätzliche Informationen zu dem iKVM. Klicken Sie auf die iKVM-Untergrafik, um die Informationen über den iKVM auf der rechten Seite anzuzeigen.
2. Wählen Sie **Gehäuse-Übersicht → iKVM → Eigenschaften** .

   Die Seite **iKVM-Status** zeigt den Status und die Messwerte der iKVM an, die dem Gehäuse zugeordnet sind. Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.

Funktionszustand und Informationen der Netzteileinheit anzeigen

Um den Funktionszustand der Netzteileinheiten (PSUs), die dem Gehäuse zugeordnet sind, anzuzeigen, führen Sie einen der folgenden Schritte aus:

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

   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. 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. Klicken Sie auf die Netzteileinheit-Untergrafik, um die Netzteileinheit-Zusammenfassung rechts auf der Seite anzuzeigen.
2. Klicken Sie auf **Gehäuse-Übersicht → Netzteile**.

   Die Seite **Netzteilstatus** zeigt den Status und die Messwerte der Netzteileinheiten an, die dem Gehäuse zugeordnet sind. Sie stellt den allgemeinen Stromzustand, Systemstromstatus, und den Netzteilredundanzstatus bereit. Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.

Informationen und Funktionszustand der Temperatursensoren anzeigen

So zeigen Sie den Funktionszustand der Temperatursensoren an:

Gehen Sie zu **Gehäuse-Übersicht → Temperatursensoren**.

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

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

Anzeigen von Informationen und Funktionszustand für die LCD

So zeigen Sie den Funktionszustand der LCD an:

1. Gehen Sie in der CMC-Webschnittstelle in der Systemstruktur zu **Gehäuse-Übersicht** und klicken Sie anschließend auf **Eigenschaften** → **Funktionszustand**.

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

6

Den CMC konfigurieren

Mit CMC können Sie CMC-Eigenschaften konfigurieren, Benutzer einrichten und Warnungen für die Ausführung von Remote-Verwaltungsaufgaben einrichten.

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

Sie können CMC über die Webschnittstelle or RACADM konfigurieren.

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

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

- Ändern der Netzwerkeinstellungen falls erforderlich.
- Schnittstellen für den Zugriff auf CMC Konfigurieren.
- LED-Anzeige konfigurieren.
- Einrichten der Gehäusegruppe falls erforderlich.
- Server, IOMs, or iKVM konfigurieren.
- VLAN-Einstellungen konfigurieren.
- Erforderliche Zertifikate abrufen.
- Hinzufügen und Konfiguration von CMC-Benutzern mit Berechtigungen.
- Konfiguration und Aktivierung von E-Mail-Warnmeldungen and SNMP-Traps.
- Einrichten der Strombegrenzungsrichtlinie falls erforderlich.

Verwandte Links

Beim CMC anmelden
Anzeigen und Ändern von CMC-Netzwerk-LAN-Einstellungen
Netzwerksicherheitseinstellungen konfigurieren
Konfigurieren der virtuellen LAN-Tag-Einstellungen für CMC
Dienste konfigurieren
LEDs zum Identifizieren von Komponenten im Gehäuse konfigurieren
Einrichten einer Gehäusegruppe
Konfigurieren eines Servers
Verwaltung der E/A-Struktur
iKVM konfigurieren und verwenden
Zertifikate abrufen
Benutzerkonten und Berechtigungen konfigurieren
CMC für das Versenden von Warnungen konfigurieren
Energieverwaltung und -überwachung
Mehrere CMCs über RACADM konfigurieren

Anzeigen und Ändern von CMC-Netzwerk-LAN-Einstellungen

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

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

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

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

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

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

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

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

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

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

- `getniccfg`
- `getconfig`
- cfgCurrentLanNetworking

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

- `getconfig`
- cfgIPv6LanNetworking

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

Lesen Sie für weitere Informationen über die Unterbefehle und Objekte das *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC*.

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 4cfgNicIPv4Enable 0
```

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

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

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

ANMERKUNG: Die CMC-IPv6-Adressierung ist standardmäßig deaktiviert.

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

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

```
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0 racadm config -g
cfgLanNetworking -o cfgNicIpAddress <statische IP-Adresse> racadm config -g
cfgLanNetworking -o cfgNicGateway <statisches Gateway> racadm config -g racadm
config -g cfgLanNetworking -o cfgNicNetmask <statische Subnetzmaske>
```

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

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

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

Aktivieren oder Deaktivieren von DHCP für die CMC-Netzwerkschnittstellenadresse

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

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

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

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

Um die Funktion DHCP für DNS-Server-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-Adresse> racadm config -
g cfgLanNetworking -o cfgDNSServer2 <IPv4-Adresse>
```

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

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

Konfigurieren der DNS-Einstellungen (IPv4 und IPv6)

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

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

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

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

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

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

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

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

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

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

Konfigurieren von „Automatische Verhandlung", „Duplexmodus" und „Netzwerkgeschwindigkeit" (IPv4 und IPv6)

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

wobei:

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

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

wobei:

<Geschwindigkeit> ist 10 oder 100 (Standard)

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

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

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

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

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

Netzwerksicherheitseinstellungen konfigurieren

Sie können die Netzwerksicherheitseinstellungen nur für IPv4 konfigurieren.

Netzwerksicherheitseinstellungen über die CMC-Webschnittstelle konfigurieren

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

So konfigurieren Sie die Netzwerksicherheitseinstellungen über die CMC-Webschnittstelle:

1. Wählen Sie in der Systemstruktur **Gehäuse-Übersicht?** aus und klicken Sie auf **Netzwerk** → **Netzwerk**. Die Seite **Netzwerkkonfiguration** wird angezeigt.
2. Im Abschnitt IPv4-Einstellungen, klicken Sie auf **Erweiterte Einstellungen**. Die Seite **Netzwerksicherheit** wird angezeigt.
3. Geben Sie den IP-Bereich und die IP-Blockierungswerte ein. Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.
4. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

CMC-Netzwerksicherheitseinstellungen über RACADM konfigurieren

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

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

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

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

Konfigurieren der virtuellen LAN-Tag-Einstellungen für CMC

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

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

So konfigurieren Sie VLAN für CMC mithilfe der CMC-Webschnittstelle:

1. Gehen Sie zu einer der folgenden Seiten:
   - Wählen Sie in der Systemstruktur **Gehäuse-Übersicht** und klicken Sie auf **Netzwerk** → **VLAN**?.
   - Wählen Sie in der Systemstruktur **Gehäuse-Übersicht** → **Server-Übersicht** und klicken Sie auf **Netzwerk** → **VLAN**?.

   Die Seite **VLAN-Tag-Einstellungen** wird angezeigt. VLAN-Tags sind Gehäuseeigenschaften. Sie bleiben mit dem Gehäuse verbunden, selbst wenn eine Komponente entfernt wird.
2. Aktivieren Sie im Abschnitt **CMC** VLAN für CMC, legen Sie die Priorität fest und weisen Sie die ID zu. Weitere Informationen über die Felder finden Sie in der *CMC Online-Hilfe*.
3. Klicken Sie auf Anwenden. Die VLAN-Tag-Einstellungen werden gespeichert.
   Sie können auch über das Unterregister **Gehäuse-Übersicht** → **Server** → **Setup** → **VLAN** auf diese Seite zugreifen.

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

1. Aktivieren Sie die VLAN-Funktionen des externen Gehäuseverwaltungsnetzwerks:
   ```
   racadm config -g cfgLanNetworking -o cfgNicVLanEnable 1
   ```
2. Geben Sie die VLAN-Kennung für das externe Gehäuseverwaltungsnetzwerk an:
   ```
   racadm config -g cfgLanNetworking -o cfgNicVlanID <VLAN id>
   ```
   Gültige Werte für <VLAN-ID> sind 1– 4000 und 4021– 4094. Der Standardwert ist 1.
   Beispiel:
   ```
   racadm config -g cfgLanNetworking -o cfgNicVlanID 1
   ```
3. Dann geben Sie die VLAN-Priorität für das externe Gehäuseverwaltungsnetzwerk an:
   ```
   racadm config -g cfgLanNetworking -o cfgNicVLanPriority <VLAN-Priorität>
   ```
   Gültige Werte für <VLAN-Priorität> sind 0–7. Der Standardwert ist 0.
   Beispiel:
   ```
   racadm config -g cfgLanNetworking -o cfgNicVLanPriority 7
   ```
   Sie können auch sowohl VLAN-Kennung als auch VLAN-Priorität in einem einzigen Befehl eingeben:
   ```
   racadm setniccfg -v <VLAN-ID> <VLAN-Priorität>
   ```
   Beispiel:
   ```
   racadm setniccfg -v 1 7
   ```
4. Zum Entfernen des CMC-VLAN deaktivieren Sie die VLAN-Funktionen des externen Gehäuseverwaltungsnetzwerks:
   ```
   racadm config -g cfgLanNetworking -o cfgNicVLanEnable 0
   ```

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

```
racadm setniccfg -v
```

Dienste konfigurieren

Sie können die folgenden Dienste auf CMC konfigurieren und aktivieren:

- CMC Serielle Konsole – Aktivieren Sie den Zugriff auf CMC mithilfe der seriellen Konsole.
- Web Server – Zugang zur CMC-Webschnittstelle aktivieren. Wenn Sie die Option deaktivieren, aktivieren Sie den Web Server wieder über den lokalen RACADM, da die Deaktivierung des Web Servers auch den Remote-RACADM deaktiviert.
- SSH – Aktivieren Sie den Zugriff auf CMC über Firmware RACADM.
- Telnet – Aktivieren Sie den Zugriff auf CMC über Firmware RACADM
- RACADM – Aktivieren Sie den Zugriff auf CMC mittels RACADM.
- SNMP – Aktivieren Sie CMC zum Versenden von SNMP-Traps für Ereignisse.
- Remote-Syslog – Aktivieren Sie CMC, um Ereignisse auf einem Remote-Server zu protokollieren.

Der CMC enthält einen Web Server, der dazu konfiguriert ist, das SSL-Sicherheitsprotokoll des Industriestandards zu verwenden, um verschlüsselte Daten über das Internet von Clients zu empfangen bzw. sie an sie zu übermitteln. Der Web Server enthält ein von Dell™ selbstsigniertes, digitales SSL- Zertifikat (Server-ID) und ist dafür verantwortlich, sichere HTTP-Aufforderung von Clienten zu empfangen bzw. auf diese zu antworten. Dieser Dienst ist für die webbasierte Schnittstelle und das Remote-RACADM-CLI-Hilfsprogramm erforderlich, damit mit den CMC kommuniziert werden kann.

Im Falle eines Web Server-Resets warten Sie mindestens eine Minute, bis die Dienste wieder verfügbar werden. Ein Web Server-Reset tritt meist als Resultat eines der folgenden Ereignisse auf:

- Eigenschaften der Netzwerkkonfiguration oder der Netzwerksicherheit werden über die CMC-Web-Benutzeroberfläche oder über RACADM geändert.
- Web Server-Schnittstellenkonfiguration wird über die Web-Benutzeroberfläche oder über RACADM geändert.
- CMC wird zurückgesetzt.
- Ein neues SSL-Serverzertifikat wird hochgeladen.

ANMERKUNG: Zum Modifizieren von Diensteinstellungen müssen Sie die Berechtigung als **Gehäusekonfigurations-Administrator** besitzen.

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.

Dienste unter Verwendung der CMC-Webschnittstelle konfigurieren

So konfigurieren Sie CMC-Dienste über die CMC-Webschnittstellle:

1. Wählen Sie in der Systemstruktur **Gehäuse-Übersicht** aus und klicken Sie auf **Netzwerk → Sicherheit**. Die Seite **Services** wird angezeigt.
2. Konfigurieren Sie die folgenden Dienste nach Bedarf:
   - Serielle-CMC-Konsole
   - Webserver

- SSH
- Telnet
- Remote-RACADM
- SNMP
- Remote-Syslog

Weitere Informationen zu den Feldern finden Sie unter *CMC-Online-Hilfe*.

3. Klicken Sie auf **Anwenden**; dies aktualisiert alle Standard-Zeitüberschreitungen und alle maximalen Zeitüberschreitungsgrenzwerte.

Dienste über RACADM konfigurieren

Verwenden Sie für die Aktivierung und Konfiguration der verschiedenen Dienste die folgenden RACADM-Objekte:

- `cfgRacTuning`
- `cfgRacTuneRemoteRacadmEnable`

Weitere Informationen zu diesen Objekten finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC* unter **dell.com/support/manuals**.

Wenn die Firmware auf dem Server eine Funktion nicht unterstützt, bewirkt das Konfigurieren einer Eigenschaft zu dieser Funktion, dass ein Fehler angezeigt wird. Wenn zum Beispiel RACADM verwendet wird, um Remote-Syslog auf einem nicht unterstützten iDRAC zu aktivieren, wird eine Fehlermeldung angezeigt.

Wenn, in gleicher Weise, mit dem RACADM-getconfig-Befehl die iDRAC-Eigenschaften angezeigt werden, werden die Eigenschaftswerte einer Funktion, die auf dem Server nicht unterstützt wird, als N/A angezeigt.

Beispiel:

```
$ racadm getconfig -g cfgSessionManagement -m server-1 #
cfgSsnMgtWebServerMaxSessions=N/A # cfgSsnMgtWebServerActiveSessions=N/A #
cfgSsnMgtWebServerTimeout=N/A # cfgSsnMgtSSHMaxSessions=N/A #
cfgSsnMgtSSHActiveSessions=N/A # cfgSsnMgtSSHTimeout=N/A #
cfgSsnMgtTelnetMaxSessions=N/A # cfgSsnMgtTelnetActiveSessions=N/A #
cfgSsnMgtTelnetTimeout=N/A
```

Erweiterte CMC-Speicherkarte konfigurieren

Sie können die optionalen wechselbaren Flash-Datenträger für die Verwendung als erweiterten nicht-flüchtigen Speicher aktivieren oder reparieren. Der Betrieb einiger CMC-Funktionen ist von erweitertem nicht-flüchtigem Speicher abhängig.

So aktivieren oder reparieren Sie den wechselbaren Flash-Datenträger mithilfe der CMC-Webschnittstelle:

1. Wählen Sie in der Systemstruktur **Gehäuse-Übersicht**aus und klicken Sie auf **Gehäuse-Controller → Flash Media**. Die Seite Wechselbarer Flash-Datenträger wird angezeigt.
2. Wählen Sie im Drop-Down-Menü nach Bedarf eine der folgenden Optionen aus:
   - Flash-Datenträger zum Speichern von Gehäusedaten verwenden
   - Datenträger des aktiven Controllers reparieren
   - Mit Replikation von Daten zwischen Datenträgern beginnen
   - Mit Replikation von Daten zwischen Datenträgern beginnen
   - Verwendung des Flash-Datenträgers zum Speichern von Gehäusedaten abbrechen

   Weitere Informationen zu diesen Optionen finden Sie in der *CMC-Online-Hilfe*.
3. Klicken Sie auf **Anwenden**, um die ausgewählten Optionen anzuwenden.

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.

Einrichten einer Gehäusegruppe

CMC ermöglicht Ihnen die Überwachung mehrerer Gehäuse von einem einzigen Führungsgehäuse aus. Bei aktivierter Gehäusegruppe erzeugt der CMC des Führungsgehäuses eine grafische Darstellung des Status des Führungsgehäuses und von allen in der Gehäusegruppe enthaltenen Gehäusen.

Im Folgenden werden die Gehäusegruppenfunktionen dargestellt:

- Die **Gehäusegruppen**-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 **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.

Eine Gehäuseguppe kann maximal acht Mitglieder enthalten. Des Weiteren kann ein Führungs- bzw. ein Mitgliedgehäuse nur Teil einer Gruppe sein. Wenn diese bereits Teil einer Gruppe sind, können weder Führungs- noch Mitgliedsgehäuse einer weiteren Gruppe beitreten. Gehäuse können aus einer Gruppe gelöscht werden und später zu einer anderen Gruppe hinzugefügt werden.

So legen Sie eine Gehäusgruppe unter Verwendung der CMC-Webschnittstelle fest:

1. Melden Sie sich an dem als Führungsserver eingeplanten Gehäuse mit Administratorrechten an.
2. Klicken Sie auf **Setup** → **Gruppenverwaltung**. Die Seite **Gehäusgruppe** wird angezeigt.
3. Wählen Sie auf der **Gehäusegruppen**seite unter **Rolle Führung**. Es wird ein Feld zum Hinzufügen des Gruppennamens angezeigt.
4. Geben Sie den Gruppennamen im Feld **Gruppenname** ein und klicken Sie anschließend auf **Anwenden.**

   ANMERKUNG: Für einen Domänennamen gelten die gleichen Regeln wie für den Gruppennamen.

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

Verwandte Links

Hinzufügen von Mitgliedern zu einer Gehäusegruppe
Entfernen eines Mitglieds aus der Führung
Auflösen einer Gehäusgruppe
Deaktivieren eines einzelnen Mitglieds am Mitgliedsgehäuse
Starten der Webseite eines Mitgliedsgehäuses oder Servers
Propagieren der Führungsgehäuseeigenschaften auf ein Mitgliedsgehäuse

Hinzufügen von Mitgliedern zu einer Gehäusegruppe

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 **Benutzername** einen Benutzernamen mit Gehäuseadministratorrechten an.
6. Geben Sie im Feld **Kennwort** das zugehörige Kennwort an.
7. Klicken Sie auf **Anwenden**.
8. Wiederholen Sie Schritt 4 bis 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.

   Weitere Informationen zum Propagieren der Eigenschaften des Führungsgehäuses auf ein Mitgliedsgehäuse finden Sie unter Propagieren der Eigenschaften des Führungsgehäuses auf ein Mitgliedsgehäuse.

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.

Verwandte Links

Deaktivieren eines einzelnen Mitglieds am Mitgliedsgehäuse

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 Seite **Gehäusegruppen** unter **Rolle**, **Keine** aus und klicken Sie anschließend auf **Anwenden**.

Das Führungsgehäuse benachrichtigt anschließend alle Mitglieder, dass sie aus der Gruppe entfernt wurden. 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 der Führung und dem Mitglied aufgrund eines Netzwerkproblems verhindert wird. Deaktivieren Sie in diesem Falle das Mitglied des Mitgliedsgehäuses, um das Entfernen abzuschließen.

Deaktivieren eines einzelnen Mitglieds am Mitgliedsgehäuse

Gelegentlich kann ein Mitglied durch das Führungsgehäuse nicht aus einer Gruppe entfernt werden. Dies kann bei einem Verlust der Netzwerkverbindung zum Mitglied vorkommen. So entfernen Sie ein Mitglied aus einer Gruppe im Mitgliedsgehäuse:

1. Melden Sie sich mit Gehäuseadministratorrechten am Mitgliedsgehäuse an.
2. Klicken Sie 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 für das gewünschte Gehäuse **CMC starten** aus.

   Wenn ein Server in einem Gehäuse das benötigte Ziel ist, verfahren Sie folgendermaßen:
   a) Wählen Sie das Bild des Zielgehäuses aus.
   b) Wählen Sie im 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.

Propagieren der Führungsgehäuseeigenschaften auf ein Mitgliedsgehäuse

Sie können die Eigenschaften eines Führungsgehäuses auf ein Mitgliedsgehäuse einer Gruppe anwenden. Um ein Mitglied mit den Führungseigenschaften zu synchronisieren:

1. Melden Sie sich mit Administratorrechten am Führungsgehäuse an.
2. Wählen Sie in der Struktur das Führungsgehäuse aus.
3. Klicken Sie auf **Setup** → **Gruppenverwaltung**.
4. Wählen Sie im Abschnitt **Gehäuseeigenschaften propagieren** eine der Propagierungstypen aus:

   – Propagierung bei Änderung - Wählen Sie diese Option zur automatischen Propagierung der ausgewählten Gehäuseeigenschaften-Einstellungen aus. Die Änderungen der Eigenschaften werden bei jeder Änderung der Führungseigenschaften an alle aktuellen Gruppenmitglieder propagiert.

– Manuelle Propagierung - Wählen Sie diese Option zur manuellen Propagierung der Führungseigenschaften der Gehäusegruppe zu seinen Mitgliedern. Die Einstellungen für die Führungsgehäuseeigenschaften werden nur zu den Gruppenmitgliedern propagiert, wenn der Führungsgehäuse-Administrator auf **Propagieren** klickt.

5. Wählen Sie im Abschnitt **Propagierungseigenschaften** die Kategorien der Führungskonfigurationseigenschaften aus, die an die Gehäusemitglieder propagiert werden sollen.

   Wählen Sie ausschließlich die Einstellungskategorien aus, die Sie übergreifend auf allen Mitgliedern der Gehäusegruppe identisch konfigurieren möchten. Wählen Sie zum Beispiel die Kategorie **Protokollierungs- und Warnmeldungseigenschaften** aus, um zu aktivieren, dass alle Gehäuse in der Gruppe die Protokollierungs- und Warnmeldungskonfigurationseinstellungen des Führungsgehäuses teilen.

6. Klicken Sie auf **Speichern**.

   Wurde **Propagierung bei Änderung** ausgewählt, übernehmen die Gehäusemitglieder die Eigenschaften des Führungsgehäuses. Wenn **Manuelle Propagierung** ausgewählt wurde, klicken Sie auf **Propagieren**, wann immer Sie die ausgewählten Einstellungen zu den Mitgliedsgehäusen propagieren möchten. Weitere Informationen zur Propagierung von Führungsgehäuseeigenschaften auf ein Mitgliedsgehäuse finden Sie in der *CMC-Online-Hilfe*.

Blade-Bestandsaufnahme für MCM-Gruppe

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

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

Speichern des Berichts zur Serverbestandsaufnahme

So speichern Sie den Bericht zur Serverbestandsaufnahme über die CMC-Webschnittstelle:

1. Klicken Sie in der Systemstruktur auf **Gruppe**. Die Seite **Funktionszustand der Gehäusegruppe** wird angezeigt.
2. Klicken Sie auf **Bericht zur Bestandsaufnahme speichern**. Im Dialogfeld **Datei herunterladen** 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-Bestandsaufnahme 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-Bestandsaufnahme in der Position Ein befinden.

Exportierte Daten

Der Bericht zur Server-Bestandsaufnahme 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 Server-Bestandsaufnahme:

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

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

- **Gehäusegruppe ist ausgeschaltet**

- Ausgeschaltet

  ANMERKUNG: Wenn ein Server eingesetzt wird, während das Gehäuse ausgeschaltet ist, wird die Modellnummer in der Webschnittstelle erst angezeigt, wenn das Gehäuse wieder eingeschaltet wird.

Die folgende Tabelle listet die spezifischen Datenfelder und Anforderungen für Felder auf, die für jeden Server gemeldet werden müssen:

Tabelle 10. Blade-Bestandsaufnahme – Feldbeschreibungen

Datenfeld	Beispiel
Gehäusename	Rechenzentrum für Führungsgehäuse
Gehäuse-IP-Adresse	192.168.0.1
Einschubposition	1
Steckplatzname	SLOT-01
Host-Name	Unternehmens-Webserver **ANMERKUNG:** Es wird ein Server-Administrator-Agent benötigt, der auf dem Server ausgeführt wird. Ansonsten wird er leer angezeigt.
Betriebssystem	Windows Server 2008 **ANMERKUNG:** Es wird ein Server-Administrator-Agent benötigt, der auf dem Server ausgeführt wird. Ansonsten wird er leer angezeigt.
Modell	PowerEdgeM610
Service Tag (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.
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 mit 1,87 GHzn **ANMERKUNG:** Es wird ein CMC ab Version 4.0 auf dem Mitglied benötigt. Ansonsten wird er leer angezeigt.

Datenformat

Der Bestandsaufnahmebericht wird in einem **.CSV** -Dateiformat generiert, damit er in verschiedene Tools importiert werden kann, z. B. Microsoft Excel. Die **.CSV** -Datei für den Bestandsaufnahmebericht kann in die Vorlage importiert werden, indem Sie in MS Excel **Date** → **Aus Text** auswählen. Nachdem der Bestandsaufnahmebericht nach MS Excel importiert wurde und falls eine Nachricht angezeigt wird, in der zusätzliche Informationen angefordert werden, wählen Sie „Trennzeichen-getrennt“ aus, um die Datei nach MS Excel zu importieren.

Zertifikate abrufen

In der folgenden Tabelle werden die Zertifikattypen auf der Basis des Anmeldetyps aufgelistet.

Tabelle 11. : Anmelde- und Zertifikattypen

Anmeldetyp	Zertifikattyp	Abrufmöglichkeit
Einmalige Anmeldung über Active Directory	Vertrauenswürdiges Zertifizierungsstellenzertifikat	Zertifikatsignierungsanforderung (CSR) generieren und diese von einer Zertifizierungsstelle signieren lassen
Smart Card-Anmeldung als Active Directory-Benutzer	• Benutzerzertifikat • Vertrauenswürdiges Zertifizierungsstellenzertifikat	• Benutzerzertifikat – Smart Card-Benutzerzertifikat als Base64-kodierte Datei unter Verwendung der Kartenverwaltungssoftware exportieren, die durch den Smart Card-Anbieter bereitgestellt wird. • Vertrauenswürdiges Zertifizierungsstellenzertifikat – Dieses Zertifikat wird von einer Zertifizierungsstelle ausgegeben.
Active Directory-Benutzeranmeldung	Vertrauenswürdiges Zertifizierungsstellenzertifikat	Dieses Zertifikat wird durch eine Zertifizierungsstelle ausgegeben.
Lokale Benutzeranmeldung	SSL-Zertifikat	Zertifikatsignierungsanforderung (CSR) generieren und diese von einer vertrauenswürdigen Zertifizierungsstelle signieren lassen **ANMERKUNG:** Der CMC wird mit einem standardmäßigen selbstsignierten SSL-Server-Zertifikat geliefert. Der CMC Web-Server und Virtual Console verwenden dieses Zertifikat.

Verwandte Links

Secure Sockets Layer (SSL) Server-Zertifikate

Secure Sockets Layer (SSL) Server-Zertifikate

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.

Der Verschlüsselungsprozess bietet ein hohes Maß an Datenschutz. CMC wendet den 128-Bit-SSL-Verschlüsselungsstandard an. Hierbei handelt es sich um die sicherste Form der Verschlüsselung, die allgemein für Internet-Browser in Nordamerika 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 Unternehmen, das in der IT-Branche dafür anerkannt ist, hohe Ansprüche bezüglich der zuverlässigen Abschirmung, Identifizierung und anderer wichtiger Sicherheitskriterien zu erfüllen. 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.

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.

Verwandte Links

Neue Zertifikatsignierungsanforderung erstellen
Serverzertifikat hochladen
Serverzertifikat anzeigen

Neue Zertifikatsignierungsanforderung erstellen

Um Sicherheit zu gewährleisten, wird dringend empfohlen, 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 angezeigt oder geändert werden können. Ohne ein sicheres Serverzertifikat ist der CMC durch Zugriff von unberechtigten Benutzern gefährdet.

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.

Nach dem Erstellen des CSR werden Sie zum Speichern einer Kopie auf Ihre Management Station oder Ihr geteiltes Netzwerk aufgefordert, und die eindeutigen Informationen, die für die Erstellung der CSR verwendet wurden, werden auf dem CMC gespeichert. 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.

VORSICHT: 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.

Neue Zertifikatsignierungsanforderung über die Webschnittstelle erstellen

So erstellen Sie ein CSR über die CMC-Webschnittstelle:

1. Klicken Sie in der Systemstruktur auf **Gehäuse-Übersicht**, und dann auf **Netzwerk → SSL**. Das **SSL-Hauptmenü** wird angezeigt.
2. Wählen Sie **Neue Zertifikatsignierungsanforderung (CSR) erstellen** aus und klicken Sie auf **Weiter**. Die Seite **Zertifikatsignierungsanforderung (CSR) erstellen** wird angezeigt.
3. Geben Sie für jedes CSR-Attribut einen Wert ein.
4. Klicken Sie auf **Erstellen**. Das Dialogfeld **Dateien herunterladen** wird angezeigt.
5. 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.

CSR über RACADM generieren

Um eine CSR zu generieren, verwenden Sie die Objekte in der Gruppe `cfgRacSecurityData`, um die Werte und die Verwendung des Befehls `sslcsrgen` für die Generierung der CSR anzugeben. Weitere Informationen finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC* unter **dell.com/support/manuals**.

Serverzertifikat hochladen

Nach der Generierung einer Zertifikatsignierungsanforderung (CSR) können Sie das signierte SSL-Serverzertifikat auf die CMC-Firmware hochladen. CMC wird zurückgesetzt, nachdem Sie das Zertifikat hochgeladen haben. CMC akzeptiert nur X509, Base 64-kodierte Web Server-Zertifikate.

VORSICHT: Während das Zertifikat hochgeladen wird, ist CMC nicht verfügbar.

Serverzertifikat über die CMC-Web-Schnittstelle hochladen

So laden Sie ein Serverzertifikat unter Verwendung der CMC-Firmware hoch:

1. Klicken Sie in der Systemstruktur auf **Gehäuse-Übersicht** und dann auf **Netzwerk → SSL**. Das **SSL-Hauptmenü** wird angezeigt.
2. Wählen Sie **Server-Zertifikat auf Basis von erstellter CSR hochladen** und klicken Sie dann auf **Weiter**.
3. Klicken Sie auf **Datei auswählen** und geben Sie die Zertifikatsdatei an.
4. 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 absoluten Dateipfad eingeben, der den vollständigen Pfad und den vollständigen Dateinamen sowie die Dateierweiterung enthält.

Serverzertifikat über RACADM hochladen

Um das SSL-Serverzertifikat hochzuladen, verwenden Sie den Befehl `sslcertupload`. Weitere Informationen finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC* unter **dell.com/support/manuals**.

Web Server-Schlüssel und Zertifikat hochladen

Sie können einen Webserver-Schlüssel und ein Serverzertifikat für den Webserver-Schlüssel hochladen. Das Serverzertifikat wird von einer Zertifizierungsstelle ausgestellt.

Das Web-Server-Zertifikat ist ein wesentlicher Bestandteil des SSL-Verschlüsselungsvorgangs. Es authentifiziert sich selbst an einem SSL-aktivierten Client und ermöglicht dem Client, sich am Server selbst zu authentifizieren, wodurch beiden Systemen gestattet wird, eine verschlüsselte Verbindung herzustellen.

ANMERKUNG: Zum Hochladen eines Webserver-Schlüssels und Serverzertifikats müssen Sie Berechtigungen als **Gehäusekonfiguration-Administrator** haben.

Web Server-Schlüssel und Zertifikat über die CMC-Webschnittstelle hochladen

So laden Sie einen Web-Server-Schlüssel und Zertifikat über die CMC-Webschnittstelle hoch:

1. Wählen Sie in der Systemstruktur **Gehäuse-Übersicht?** aus und klicken Sie auf **Netzwerk** → **SSL**. Das **SSL-Hauptmenü** wird angezeigt.
2. Wählen Sie **Web-Schlüssel und Zertifikat hochladen** und klicken dann auf **Weiter**.
3. Klicken Sie auf **Datei auswählen** und geben Sie die Private Schlüsseldatei und Zertifikatdatei 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.

   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.

Webserver-Schlüssel und Zertifikat über RACADM hochladen

Um den SSL-Schlüssel vom Client zum iDRAC hochzuladen, geben Sie den folgenden Befehl ein:

```
racadm sslkeyupload -t <Typ> -f <Dateiname>
```

Weitere Informationen finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC*, das unter **dell.com/support/manuals** verfügbar ist.

Serverzertifikat anzeigen

Sie können das SSL-Serverzertifikat anzeigen, das derzeit in CMC verwendet wird.

Serverzertifikat über die Web-Schnittstelle anzeigen

In der der CMC-Webschnittstelle, wählen Sie **Gehäuseübersicht** → **Netzwerk** → **SSL** und dann **Serverzertifikat anzeigen** und klicken Sie auf Weiter. Auf der Seite Serverzertifikat anzeigen wird das neueste SSL-Serverzertifikat angezeigt. Weitere Informationen finden Sie in den Online-Hilfe-Themen.

Serverzertifikat über RACADM anzeigen

Um das SSL-Serverzertifikat anzuzeigen, verwenden Sie den Befehl `sslcertview`. Weitere Informationen finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC* unter **dell.com/support/manuals**.

Mehrere CMCs über RACADM konfigurieren

Mit RACADM können Sie einen oder mehrere CMCs mit identischen Eigenschaften konfigurieren.

Wenn Sie eine spezifische CMC-Karte mit deren Gruppen-ID und Objekt-ID abfragen, erstellt RACADM die racadm.cfg-Konfigurationsdatei aus den abgerufenen Informationen. Wenn Sie die Datei zu einem oder mehreren CMCs exportieren, können Sie in kürzester Zeit Ihre Controller mit identischen Eigenschaften konfigurieren.

ANMERKUNG: Einige Konfigurationsdateien enthalten eindeutige CMC-Informationen (wie die statische IP-Adresse), die vor dem Exportieren der Datei zu anderen CMCs geändert werden müssen.

1. Verwenden Sie RACADM, um den Ziel-CMC abzufragen, der die gewünschte Konfiguration enthält.

   ANMERKUNG: Die erstellte Konfigurationsdatei ist **myfile.cfg**. Sie können die Datei umbenennen. Die erstellte **.cfg**-Datei enthält keine Benutzerkennwörter. Wenn die **.cfg**-Datei auf den neuen CMC hochgeladen wurde, müssen Sie alle Kennwörter erneut hinzufügen.
2. Öffnen Sie eine Telnet/SSH-Textkonsole für den CMC, melden Sie sich an und geben Sie Folgendes ein:

   ```
   racadm getconfig-f myfile.cfg
   ```

   ANMERKUNG: Das Umleiten der CMC-Konfiguration zu einer Datei mit `getconfig-f` wird nur mit der Remote-RACADM-Schnittstelle unterstützt.
3. Modifizieren Sie die Konfigurationsdatei mit einem Klartext-Editor (optional). Formatierungen in der Konfigurationsdatei können die RACADM-Datenbank beschädigen.
4. Verwenden Sie die neu erstellte Konfigurationsdatei, um einen Ziel-CMC zu modifizieren. Geben Sie in der Befehlszeile Folgendes ein:

   ```
   racadm config -f myfile.cfg
   ```
5. Setzen Sie den konfigurierten Ziel-CMC zurück. Geben Sie in der Befehlszeile Folgendes ein:

   ```
   racadm reset
   ```

   Der Unterbefehl `getconfig -f myfile.cfg` (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.

Verwandte Links

CMC-Konfigurationsdatei erstellen

CMC-Konfigurationsdatei erstellen

Die CMC-Konfigurationsdatei, **<Dateiname>.cfg**, wird mit dem Befehl `racadm config -f <Dateiname>.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 *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Befehlszeilen-Referenzhandbuch für iDRAC7 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. Eine vollständige Liste der Objekte und Gruppen finden Sie im Kapitel zu den Datenbankeigenschaften des *RACADM-Befehlszeilen-Referenzhandbuchs für iDRAC6 und CMC*.

  VORSICHT: Verwenden Sie den Unterbefehl `racresetcfg`, um die Datenbank und die CMC-Netzwerkschnittstellen-Einstellungen auf die ursprünglichen Standardeinstellungen zurückzusetzen und alle Benutzer und Benutzerkonfigurationen zu entfernen. Während der Stammbenutzer verfügbar ist, werden die Einstellungen anderer Benutzer ebenfalls auf die Standardeinstellungen zurückgesetzt.
- Wenn Sie `racadm getconfig -f <Dateiname>.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.

Verwandte Links

Parsing-Regeln

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 <Dateiname>.cfg`-Befehl erstellen und dann einen `racadm config -f <Dateiname>.cfg`-Befehl auf einem anderen CMC ausführen, ohne dass Sie Escape-Zeichen hinzufügen müssen.

Beispiel:

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

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

  Das Anfangszeichen [, das einen Gruppennamen anzeigt, muss in Spalte Eins stehen. Der Gruppenname muss vor allen anderen Objekten in dieser Gruppe angegeben werden. Objekte, die keinen zugewiesenen Gruppennamen enthalten, erzeugen Fehler. Die Konfigurationsdaten sind in Gruppen zusammengefasst, wie im Kapitel Datenbankeigenschaften des *RACADM-Befehlszeilen-Referenzhandbuchs für iDRAC6 und CMC* definiert. Das folgende Beispiel zeigt einen Gruppennamen, ein Objekt und den Eigenschaftswert des Objekts an.

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

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

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

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

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

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

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

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

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

  Benutzer müssen ein indiziertes Objekt manuell mit folgendem Befehl entfernen:

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

  ANMERKUNG: Eine NULL-Zeichenkette (durch zwei "-Zeichen gekennzeichnet) weist iDRAC an, den Index für die angegebene Gruppe zu löschen.

  Um den Inhalt einer indizierten Gruppe anzuzeigen, verwenden Sie den folgenden Befehl:

  ```
  racadm getconfig -g <Gruppenname> -i <Index 1-16>
  ```

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

  ```
  [cfgUserAdmin] cfgUserAdminUserName= <BENUTZERNAME>
  ```

- Wenn bei Verwendung von Remote-RACADM zur Erfassung der Konfigurationsgruppen in eine Datei eine Schlüsseleigenschaft innerhalb einer Gruppe nicht festgelegt ist, wird die Konfigurationsgruppe nicht als Teil der Konfigurationsdatei gespeichert. Falls diese Konfigurationsgruppen auf andere CMCs geklont werden müssen, muss die Schlüsseleigenschaft vor Ausführung des Befehls `getconfig -f` festgelegt werden.

Oder Sie können die fehlenden Eigenschaften nach Ausführung des Befehls `getconfig -f` manuell in die Konfigurationsdatei eingeben. Dies gilt für alle racadm-indizierten Gruppen.

Dies ist die Liste der indizierten Gruppen, die dieses Verhalten und die entsprechenden Schlüsseleigenschaften aufweisen:

- cfgUserAdmin – cfgUserAdminUserName
- cfgEmailAlert – cfgEmailAlertAddress
- cfgTraps – cfgTrapsAlertDestIPAddr
- cfgStandardSchema – cfgSSADRoleGroupName
- cfgServerInfo – cfgServerBmcMacAddress

CMC-IP-Adresse modifizieren

Wenn Sie die CMC-IP-Adresse in der Konfigurationsdatei ändern, entfernen Sie alle unnötigen `<Variable> = <Wert>`-Einträge. Es verbleibt lediglich die tatsächliche Bezeichnung der variablen Gruppe mit "[" und "]" zusammen mit den beiden `<Variable> = <Wert>`-Einträgen, die sich auf die IP-Adressenänderung beziehen.

Beispiel:

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

Die Datei wird aktualisiert wie folgt:

```
# # Object Gruppe "cfgLanNetworking" # [cfgLanNetworking]
cfgNicIpAddress=10.35.9.143 # Kommentar, der Rest dieser Zeile wird ignoriert
cfgNicGateway=10.35.9.1
```

Mit dem Befehl `racadm config -f <myfile>.cfg` wird die Datei geparst, und Fehler werden nach Zeilennummer identifiziert. Eine korrekte Datei aktualisiert die richtigen Einträge. Außerdem kann derselbe `getconfig`-Befehl (siehe vorheriges Beispiel) zur Bestätigung der Aktualisierung verwendet werden.

Verwenden Sie diese Datei, um unternehmensweite Änderungen herunterzuladen, oder um neue Systeme mit dem Befehl `racadm getconfig -f <meineDatei>.cfg` über das Netzwerk zu konfigurieren.

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

Anzeigen und Beenden der CMC-Sitzungen

Sie können die Anzahl der Benutzer anzeigen, die derzeit bei iDRAC7 angemeldet sind, und die Benutzersitzungen beenden.

ANMERKUNG: Um eine Sitzung zu beenden, müssen Sie die Berechtigung als **Gehäusekonfiguration-Administrator** besitzen.

Anzeigen und Beenden der CMC-Sitzungen über die Webschnittstelle

So verwalten oder beenden Sie eine Sitzung über die Webschnittstelle:

1. Wählen Sie in der Systemstruktur **Gehäuseübersicht** aus und klicken Sie auf **Netzwerk** → **Sitzungen**.
   Daraufhin werden auf der Seite **Sitzungen** die Sitzungs-ID, der Benutzername, die IP-Adresse und der Sitzungstyp angezeigt. Weitere Informationen zu diesen Eigenschaften finden Sie in der *CMC-Online-Hilfe*.
2. Um die Sitzung zu beenden, klicken Sie auf **Beenden** für die Sitzung.

Anzeigen und Beenden der CMC-Sitzungen über RACADM

Sie benötigen Administratorberechtigungen, um CMC-Sitzungen über RACADM beenden zu können.

Verwenden Sie zum Anzeigen der aktuellen Benutzersitzungen den Befehl `getssninfo`.

Verwenden Sie zum Beenden einer Benutzersitzung den Befehl `closessn`.

Weitere Informationen zu diesen Befehlen finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC* unter **dell.com/support/manuals**.

7

Konfigurieren eines Servers

Sie können das Folgende für den Server ausführen:

- Steckplatznamen konfigurieren
- iDRAC Netzwerkeinstellungen konfigurieren
- iDRAC-VLAN-TagEinstellungen konfigurieren
- Erstes Startlaufwerk einstellen
- Server-FlexAddress konfigurieren
- Remote-Dateifreigabe konfigurieren
- BIOS-Einstellungen mithilfe der Funktion zum Klonen von Servern konfigurieren

Steckplatznamen konfigurieren

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

- Namen dürfen **maximal 15** nicht erweiterte ASCII-Zeichen (ASCII-Codes 32 bis 126) enthalten.
- Steckplatznamen müssen innerhalb des Gehäuses eindeutig sein. Derselbe Name darf nicht für einen zweiten Steckplatz verwendet werden.
- Für Zeichenketten wird nicht zwischen Groß- und Kleinschreibung unterschieden. `Server-1, server-1, und SERVER-1` gelten als gleiche Namen.
- Steckplatznamen dürfen nicht mit einer der folgenden Zeichenketten beginnen:
  - `Switch-`
  - `Lüfter-`
  - `PS-`
  - `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.

Die Einstellung des Steckplatznamens in der Webschnittstelle befindet sich nur auf dem CMC. Wird ein Server vom Gehäuse entfernt, verbleibt die Einstellung des Steckplatznamens nicht beim Server.

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

Die Einstellung des Steckplatznamens in der CMC-Webschnittstelle setzt immer die Änderungen außer Kraft, die auf der iDRAC-Schnittstelle am Anzeigenamen vorgenommen wurden.

So bearbeiten Sie einen Steckplatznamen über die CMC-Webschnittstelle:

1. Wählen Sie in der Systemstruktur **Gehäuse-Übersicht** → **Server-Übersicht** aus und klicken Sie auf **Setup** → **Steckplatznamen**. Die Seite **Steckplatznamen** wird angezeigt.
2. Im Feld **Steckplatzname** können Sie den Steckplatzname bearbeiten. Wiederholen Sie diese Maßnahme für jeden Steckplatz, den Sie umbenennen möchten.
3. Um einen Serverhostnamen als Steckplatzname zu verwenden, wählen Sie **Hostname verwenden** für die Option **Steckplatzname** aus. Dadurch werden die statischen Steckplatznamen mit dem Host-Namen des Servers (oder dem Systemnamen) überschrieben, falls verfügbar. Dazu muss der OMSA-Agent auf dem Server installiert sein. Weitere Informationen zu dem OMSA-Agent finden Sie im *OpenManage Server Administrator-Benutzerhandbuch*.
4. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.
5. Um den Standardsteckplatznamen (**STECKPLATZ-01** bis **STECKPLATZ-16**, basierend auf der Position des Serversteckplatzes) zum Server, wiederherzustellen, verwenden Sie **Standardwert wiederherstellen**.

iDRAC Netzwerkeinstellungen konfigurieren

Sie können installierte und neu eingefügte iDRAC-Netzwerkkonfigurationseinstellungen des Servers konfigurieren. Ein Benutzer kann ein oder mehrere installierte iDRAC-Geräte 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 zu iDRAC finden Sie im *iDRAC7-Benutzerhandbuch* unter **dell.com/support/manuals**.

Verwandte Links

[iDRAC QuickDeploy-Netzwerkeinstellungen (iDRAC Netzwerkeinstellungen zur schnellen Bereitstellung) konfigurieren]

[iDRAC-Netzwerkeinstellungen für individuelle Server-iDRAC ändern]

[iDRAC-Netzwerkeinstellungen über RACADM ändern]

iDRAC QuickDeploy-Netzwerkeinstellungen (iDRAC Netzwerkeinstellungen zur schnellen Bereitstellung) konfigurieren

Verwenden Sie die QuickDeploy-Einstellungen, um die Netzwerkeinstellungen für neu eingefügte Server zu konfigurieren. Nach der Aktivierung von QuickDeploy werden die QuickDeploy-Einstellungen auf Server angewandt, wenn dieser Server installiert ist.

So aktivieren Sie die iDRAC-Einstellungen für die QuickDeploy und stellen sie unter Verwendung der CMC-Webschnittstelle ein:

1. Wählen Sie in der Systemstruktur **Server-Übersicht** aus und klicken Sie auf **Setup** → **iDRAC**. Die Seite **iDRAC bereitstellen** wird angezeigt.
2. Legen Sie im Abschnitt **QuickDeploy-Einstellungen** die Einstellungen fest, die in der folgenden Tabelle erwähnt wurden.

Tabelle 12. : QuickDeploy-Einstellungen

Einstellung	Beschreibung
QuickDeploy aktiviert	Aktiviert/deaktiviert die Funktion **QuickDeploy** (Schnelle Bereitstellung), welche die iDRAC-Einstellungen, die auf

Einstellung	Beschreibung
	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 Stammbenutzerkennwort ein, wenn das Kontrollkästchen **iDRAC-Stammkennwort bei Servereinfügung einstellen** markiert ist. Standardmäßig ist diese Funktion deaktiviert.
iDRAC-Stammkennwort nach Einsetzen des Servers 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 **QuickDeploy aktiviert** gewählt wird, 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 oder deaktiviert den iDRAC-LAN-Kanal. Diese Option ist standardmäßig deaktiviert.
iDRAC IPv4 aktivieren	Aktiviert oder deaktiviert IPv4 auf dem iDRAC. Diese Option ist standardmäßig aktiviert.
iDRAC-IPMI-über-LAN aktivieren	Aktiviert oder deaktiviert den IPMI-über-LAN-Kanal für jeden iDRAC, der sich in dem Gehäuse befindet. Standardmäßig ist dieser deaktiviert.
iDRAC-DHCP aktivieren	Aktiviert oder deaktiviert DHCP für jeden iDRAC, der sich in dem Gehäuse befindet. Wenn diese Option aktiviert ist, sind die Felder **QuickDeploy-IP**, **QuickDeploy-Subnetzmaske** und **QuickDeploy-Gateway** deaktiviert und können nicht geändert werden, da DHCP verwendet wird, um diese Einstellungen automatisch für jeden iDRAC zuzuweisen. Diese Option ist standardmäßig deaktiviert.
iDRAC-IPv4-Adresse starten (Steckplatz 1)	Gibt die statische IP-Adresse des iDRAC des Servers in Steckplatz 1 des Gehäuses an. Die IP-Adresse jedes nachfolgenden iDRAC wird für jeden Steckplatz jeweils um 1 erhöht, angefangen mit der statischen IP-Adresse von Steckplatz 1. Falls die IP-Adresse plus die Steckplatznummer größer als die Subnetzmaske ist, wird eine Fehlermeldung angezeigt.

Einstellung	Beschreibung
	ANMERKUNG: Die Subnetzmaske und das Gateway werden nicht wie die IP-Adresse erhöht. Wenn zum Beispiel die ursprüngliche IP-Adresse `192.168.0.250` und die Subnetzmaske `255.255.0.0` ist, dann ist die IP-Adresse für QuickDeploy für Steckplatz 15: `192.168.0.265`. Wenn die Subnetzmaske `255.255.255.0` wäre, würde die Fehlermeldung `IP-Adressenbereich für QuickDeploy befindet sich nicht vollständig innerhalb des Subnetzes für QuickDeploy` angezeigt, wenn Sie entweder auf **QuickDeploy-Einstellungen speichern** oder **Automatische Bestückung mit QuickDeploy-Einstellungen** klicken.
iDRAC IPv4-Netzmaske	Gibt die QuickDeploy-Subnetzmaske an, die allen neu eingefügten Servern zugewiesen ist.
iDRAC IPv4-Gateway	Gibt das Standard-Gateway für schnelle Bereitstellung an, das allen iDRACs, die sich im Gehäuse befinden, zugewiesen wird.
iDRAC IPv6 aktivieren	Aktiviert die IPv6-Adressierung für jedes im Gehäuse vorhandenen iDRAC, das IPv6 fähig ist.
iDRAC IPv6-Autokonfiguration aktivieren	Aktiviert den iDRAC zur Beschaffung von IPv6-Einstellungen (Adresse und Präfixlänge) von einem DHCPv6-Server und aktiviert auch statuslose automatische Adresskonfiguration. Diese Option ist standardmäßig aktiviert.
iDRAC IPv6-Gateway	Gibt das Standard-IPv6-Gateway an, das den iDRACs zugewiesen wird. Der Standardwert ist "::".
iDRAC IPv6-Präfixlänge	Gibt die Präfixlänge an, die den IPv6-Adressen auf dem iDRAC zugewiesen wird. Der Standardwert ist 64.

3. Klicken Sie auf **QuickDeploy-Einstellungen speichern**, um die Auswahl zu speichern. Wenn Sie die Änderungen an den Einstellungen des iDRAC-Netzwerkes vorgenommen haben, klicken Sie auf **iDRAC-Netzwerkeinstellungen anwenden**, um die Einstellungen zur iDRAC bereitzustellen.

   Die QuickDeploy-Funktion wird nur ausgeführt, wenn sie aktiviert ist und ein Server im Gehäuse eingefügt ist. Wenn **iDRAC-Stammkennwort bei Servereinfügung einstellen** und **QuickDeploy aktiviert** aktiviert sind, wird der Benutzer aufgefordert, die LCD-Schnittstelle zu verwenden, um die Kennwortänderung zu erlauben oder nicht zu erlauben. Wenn Netzwerkeinstellungen vorhanden sind, die sich von den aktuellen iDRAC-Einstellungen unterscheiden, wird der Benutzer aufgefordert, die Änderungen entweder anzunehmen oder abzulehnen.

   ANMERKUNG: Wenn eine LAN- oder IPMI-über-LAN-Abweichung vorhanden ist, wird der Benutzer aufgefordert, die IP-Adresseinstellungen für QuickDeploy anzunehmen. Wenn der Unterschied in der DHCP-Einstellung liegt, wird der Benutzer aufgefordert, die DHPC-QuickDeploy-Einstellung anzunehmen.

   Um die QuickDeploy-Einstellungen in den Abschnitt **iDRAC-Netzwerkeinstellungen** zu kopieren, klicken Sie auf **Mit QuickDeploy-Einstellungen automatisch bestücken**. Die Netzwerkkonfigurationseinstellungen zur schnellen Bereitstellung werden in die entsprechenden Felder der Tabelle **iDRAC-Netzwerkkonfigurationseinstellungen** kopiert.

ANMERKUNG: An den QuickDeploy-Feldern vorgenommene Änderungen sind sofort wirksam, aber Änderungen, die an einer oder mehreren der iDRAC-Servernetzwerkkonfigurationseinstellungen vorgenommen wurden, nehmen unter Umständen ein paar Minuten in Anspruch, um von der CMC zu einem iDRAC zu propagieren. Wenn **Aktualisieren** zu früh betätigt wird, werden eventuell nur teilweise richtige Daten für einen oder mehrere iDRAC-Server angezeigt.

iDRAC-Netzwerkeinstellungen für individuelle Server-iDRAC ändern

Mithilfe dieser 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.

So ändern Sie die iDRAC-Netzwerkeinstellungen über die CMC-Webschnittstelle:

1. Wählen Sie in der Systemstruktur **Server-Übersicht** aus und klicken Sie auf **Setup** → **iDRAC**. Die Seite **iDRAC bereitstellen** wird angezeigt. Der Abschnitt **iDRAC-Netzwerkeinstellungen** führt die iDRAC IPv4- und IPv6-Netzwerkkonfigurationseinstellungen aller installierten Server auf.
2. Ändern Sie entsprechend den Serveranforderungen die iDRAC-Netzwerkeinstellungen.

   ANMERKUNG: Sie müssen die Option **LAN aktivieren** auswählen, um die IPv4- oder IPv6-Einstellungen festzulegen. Weitere Informationen über die Felder finden Sie in der CMC-Online-Hilfe.
3. Um die Einstellung auf dem iDRAC bereitzustellen, klicken Sie auf **iDRAC-Netzwerkeinstellungen anwenden**. Wenn Sie Änderungen an den Einstellungen zur schnellen Bereitstellung vorgenommen haben, werden diese ebenfalls gespeichert.

   Die Tabelle **iDRAC-Netzwerkeinstellungen** zeigt zukünftige Netzwerkkonfigurationseinstellungen; die für installierte Server angezeigten Werte können die gleichen sein wie die Werte der zurzeit installierten iDRAC-Netzwerkkonfigurationseinstellungen (müssen es aber nicht). Klicken Sie auf **Aktualisierung**, um die Seite **iDRAC-Bereitstellung** mit jeder installierten iDRAC-Netzwerkkonfigurationseinstellung zu aktualisieren, nachdem Äderungen vorgenommen wurden.

   ANMERKUNG: An den Feldern der schnellen Bereitstellung vorgenommene Änderungen sind sofort wirksam, aber Änderungen, die an einer oder mehreren der iDRAC-Servernetzwerkkonfigurationseinstellungen vorgenommen wurden, nehmen unter Umständen ein paar Minuten in Anspruch, um von der CMC zu einem iDRAC zu propagieren. Wenn **Aktualisierung** zu früh gedrückt wird, werden eventuell nur teilweise richtige Daten für einen oder mehrere iDRAC-Server angezeigt.

iDRAC-Netzwerkeinstellungen über RACADM ändern

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

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

Weitere Informationen über die Standardwerte und Bereiche der einzelnen Eigenschaften finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC*.

Konfigurieren der iDRAC-VLAN-Einstellungen

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

iDRAC-VLAN-Tag-Einstellungen mittels der Webschnittstelle konfigurieren

So konfigurieren Sie VLAN für Server mittels der CMC-Webschnittstelle:

1. Gehen Sie zu einer der folgenden Seiten:
   - Klicken Sie in der Systemstruktur auf **Gehäuse-Übersicht?** und dann auf **Netzwerk** → **VLAN**?.
   - Klicken Sie in der Systemstruktur auf **Gehäuse-Übersicht?** → **Server-Übersicht** und dann auf **Netzwerk** → **VLAN**?. Die Seite **VLAN-Tag-Einstellungen** wird angezeigt.
2. Aktivieren Sie im Abschnitt **iDRAC** VLAN für den/die Server, legen Sie die Priorität fest und geben Sie die ID ein. Weitere Informationen über die Felder finden Sie in der *CMC Online-Hilfe*.
3. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

iDRAC-VLAN-Tag-Einstellungen über RACADM einstellen

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

  Gültige Werte für `<n>` sind 1 – 16.

  Gültige Werte für `<VLAN-ID>` sind 1– 4000 und 4021– 4094. Die Standardeinstellung ist 1.

  Gültige Werte für `<VLAN-Priorität>` sind 0 – 7. Die Standardeinstellung ist 0.

  Beispiel:

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

  Beispiel:

- Um ein Server-VLAN zu entfernen, deaktivieren Sie die VLAN-Funktionen des angegebenen Servernetzwerks:
  `racadm setniccfg -m server-<n> -v`

  Gültige Werte für `<n>` sind 1 – 16.

  Beispiel:

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

Erstes Startlaufwerk einstellen

Sie können das CMC-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.

Sie können das erste Startgerät nur für den nächsten Start oder für alle nachfolgenden Neustarts einstellen. Aufgrund dieser Auswahl können Sie das erste Startgerät für den Server einstellen. Beim nächsten und allen nachfolgenden

Neustarts startet das System von dem ausgewählten Gerät, das in der BIOS-Startreihenfolge an erster Stelle bleibt, bis eine erneute Änderung entweder von der CMC-Webschnittstelle oder von der BIOS-Startreihenfolge aus erfolgt.

ANMERKUNG: Die Einstellungen für das erste Startgerät in der CMC-Web-Schnittstelle überschreiben die Starteinstellungen im System-BIOS.

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

Sie können die folgenden Geräte für ersten Start einstellen.

Tabelle 13. : Startlaufwerke

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

Verwandte Links

Festlegen des ersten Startlaufwerks für mehrere Server über die CMC-Webschnittstelle
Festlegen des ersten Startgeräts für individuellen Server mit der CMC-Webschnittstelle
Erstes Startgerät über RACADM festlegen

Festlegen des ersten Startlaufwerks für mehrere Server über die CMC-Webschnittstelle

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

So legen Sie das erste Startlaufwerk für mehrere Server über die CMC-Webschnittstelle fest:

1. Wählen Sie in der Systemstruktur **Server-Übersicht** aus und klicken Sie auf **Setup** → **Erstes Startgerät**. Eine Serverliste wird angezeigt.
2. In der Spalte **Erstes Startgerät** im Drop-Down-Menü, wählen Sie für jeden Server das zu verwendende Startlaufwerk aus.

3. Wenn der Server bei jedem Hochfahren von dem ausgewählten Gerät starten soll, deaktivieren Sie die Option **Einmalig starten** für den betreffenden Server. Wenn der Server beim nächsten Hochfahren einmalig von dem ausgewählten Laufwerk starten soll, aktivieren Sie die Option **Einmalig starten** für den betreffenden Server.
4. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

Festlegen des ersten Startgeräts für individuellen Server mit der CMC-Webschnittstelle

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

So legen Sie das erste Startgerät für individuellen Server über die CMC-Webschnittstelle fest:

1. Wählen Sie in der Systemstruktur **Server-Übersicht** und klicken Sie dann auf den Server, für den Sie das erste Startgerät einstellen wollen.
2. Wählen Sie **Setup** → **Erstes Startgerät**. Die Seite **Erstes Startgerät** wird angezeigt.
3. Wählen Sie im Dropdown-Menü **Erstes Startgerät** für jeden Server das zu verwendende Startgerät.
4. Wenn der Server bei jedem Hochfahren von dem ausgewählten Gerät starten soll, löschen Sie die Option **Einmaliger Start** für den betreffenden Server. Wenn der Server beim nächsten Hochfahren einmalig von dem ausgewählten Laufwerk starten soll, wählen Sie die Option **Einmalig starten** für den Server.
5. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

Erstes Startgerät über RACADM festlegen

Um das erste Startgerät festzulegen, verwenden Sie das Objekt `cfgServerFirstBootDevice`.

Um den einmaligen Start für ein Gerät einzurichten, verwenden Sie das Objekt `cfgServerBootOnce`.

Weitere Informationen zu diesen Objekten finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC und CMC* unter **dell.com/support/manuals**.

Konfigurieren der Server-FlexAddress

Informationen über das Konfigurieren der FlexAddresses für Server finden Sie unter FlexAddress für Server-Level-Steckplätze konfigurieren.

Remote-Dateifreigabe konfigurieren

Die Remote-Dateifreigabe für virtuelle Datenträger ordnet ein Freigabelaufwerk im Netzwerk über den CMC einem oder mehreren Servern zu, um ein Betriebssystem bereitzustellen oder zu aktualisieren. Wenn das Laufwerk angeschlossen ist, kann auf die Remote-Datei zugegriffen werden, wie wenn sie sich auf dem lokalen System befinden würde. Es werden zwei Arten von Datenträgern unterstützt: Diskettenlaufwerke und CD/DVD-Laufwerke.

Zur Ausführung eines Remote-Dateifreigabevorgangs (verbinden, trennen oder bereitstellen) müssen Sie über die Berechtigung als Gehäusekonfiguration-Administrator oder Server Administrator verfügen.

So konfigurieren Sie die Remote-Dateifreigabe über die CMC-Webschnittstelle:

1. Wählen Sie in der Systemstruktur **Server-Übersicht** aus und klicken Sie auf **Setup** → **Remote-Dateifreigabe**. Die Seite **Remote-Dateifreigabe bereitstellen** wird angezeigt.

   Tragen Sie das Ergebnis Ihrer Maßnahme hier ein (optional).
2. Nehmen Sie die gewünschten Einstellungen vor. Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.

3. Klicken Sie auf **Verbinden,** um eine Verbindung zu einer Remote-Dateifreigabe herzustellen. Um eine Verbindung zu einer Remote-Dateifreigabe herzustellen, müssen Sie den Pfad, den Benutzernamen und das Kennwort angeben. Ein erfolgreicher Vorgang ermöglicht den Zugriff auf den Datenträger.

   Klicken Sie auf **Trennen**, um eine zuvor verbundene Remote-Dateifreigabe zu trennen.

   Klicken Sie auf **Bereitstellen**, um das Datenträgergerät bereitzustellen.

   ANMERKUNG: 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 ist verbunden.
   - Die Datei ist als erstes Startgerät für die Server ausgewählt.
   - Der Server wird neu gestartet.
   - Strom wird an den Server angelegt, falls der Server ausgeschaltet ist.

BIOS-Einstellungen mithilfe der Funktion zum Klonen konfigurieren

Mit der Funktion zum Erstellen von Server-Klonen können Sie alle BIOS-Einstellungen von einem spezifizierten Server auf einen oder mehrere Server anwenden. Klonbare BIOS-Einstellungen are 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 RAC-Servern aufgelistet, sie sind auf der Hauptseite jedoch ausgegraut und für die Verwendung mit dieser Funktion nicht aktiviert.

So verwenden Sie die Funktion zum Klonen von Servern:

- iDRAC muss in der erforderlichen Mindestversion vorliegen.iDRAC6-Server müssen mindestens in Version 3.2 und iDRAC7-Server in der Version 1.00.00 vorliegen.
- Auf dem Server muss die Generierung von iDRAC unterstützt werden.
- Der Server muss eingeschaltet sein.

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

Sie können Folgendes durchführen:

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

Verwandte Links

Zugreifen auf die Seite Bios-Profil
Hinzufügen oder Speichern eines Profils
Verwalten von gespeicherten Profilen
Profil anwenden
BIOS-Einstellungen anzeigen
Profilprotokoll anzeigen
Fertigstellungsstatus und Fehlerbehebung

Zugreifen auf die Seite Bios-Profil

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

Um auf die BIOS-Profil-Seite über die CMC-Webschnittstelle zuzugreifen, navigieren Sie in der Systemansicht zu **Geräuse-Übersicht** → **Server-Übersicht** und klicken Sie auf **Setup** → **Profile**. Die Seite **BIOS-Profile** wird angezeigt.

Verwandte Links

Hinzufügen oder Speichern eines Profils
Verwalten von gespeicherten Profilen
Profil anwenden
BIOS-Einstellungen anzeigen
Profilprotokoll anzeigen
Fertigstellungsstatus und Fehlerbehebung

Hinzufügen oder Speichern eines Profils

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

Wenn Sie ein gespeichertes Profil erstellen, 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“.

So fügen Sie ein Profil hinzu oder speichern Sie es:

1. Wählen Sie auf der Seite **BIOS-Profil** im Abschnitt **Speichern und Anwenden von Profilen** den Server aus, von dem die Einstellungen generiert werden sollen und klicken Sie auf **Profil speichern**.

   Der Abschnitt **BIOS-Profil speichern** wird angezeigt.
2. Geben Sie in den Feldern **Profilname** und **Beschreibung** den Profilnamen und eine Beschreibung (optional) ein und klicken Sie auf **Profil speichern**.

   CMC kommuniziert mit dem LC, um die verfügbaren BIOS-Einstellungen abzurufen und diese als ein benanntes Profil zu speichern.

   Eine Fortschrittsanzeige zeigt an, dass der Speichervorgang durchgeführt wird. Nachdem der Vorgang abgeschlossen wurde, wird die Meldung „Vorgang erfolgreich“ angezeigt.

Verwandte Links

Zugreifen auf die Seite Bios-Profil

Verwalten von gespeicherten Profilen

Sie können BIOS-Profile bearbeiten, anzeigen oder löschen.

So verwalten Sie die gespeicherten Profile im CMC:

1. Klicken Sie auf der Seite **BIOS-Profil** im Abschnitt **Profil anwenden** auf **Profile verwalten**. Die Seite **BIOS-Profile verwalten** wird angezeigt.
2. Um ein Profil zu bearbeiten, klicken Sie auf **Bearbeiten**.
3. Um BIOS-Einstellungen anzuzeigen, klicken Sie auf **Anzeigen**.

4. Um ein Profil zu entfernen, klicken Sie auf **Entfernen.**
   Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.

Profil anwenden

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

ANMERKUNG: Wenn ein Server Lifecycle Controller nicht unterstützt oder das Gehäuse ausgeschaltet ist, können Sie kein Profil auf den Server anwenden.

So wenden Sie ein Profil auf einen oder mehrere Server an:

1. Wählen Sie auf der Seite **BIOS-Profile** im Abschnitt **Profile speichern und anwenden** die Server aus, für die Sie das ausgewählte Profil anwenden möchten.
   Das Drop-Down-Menü **Profil auswählen** wird aktiviert.
2. Wählen Sie das erforderliche Profil aus dem Drop-Down-Menü **Profil auswählen** aus.
   Die Option **Profil anwenden** wird aktiviert.
3. Klicken Sie auf **Profil anwenden**.
   Eine Warnmeldung wird ausgegeben, dass das Anwenden des neuen BIOS-Profils die aktuellen Einstellungen überschreibt und ebenfalls die ausgewählten Server neustartet. Sie werden dazu aufgefordert, dies zu bestätigen, falls Sie mit dem Vorgang fortfahren möchten.

   ANMERKUNG: Ist die Option „CSIOR" deaktiviert, wird eine Warnmeldung ausgegeben, dass CSIOR nicht für die Server, auf die der Blade-Klonvorgang zielt, aktiviert ist. Sie müssen zuerst CSIOR aktivieren, um den Blade-Klonvorgang abzuschließen.
4. Klicken Sie auf **OK**, um das Profil auf den ausgewählten Server anzuwenden.
   Das ausgewählte Profil wird auf den/die Server angewendet und der/die Server wird/werden sofort neu gestartet. Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.

Verwandte Links

Zugreifen auf die Seite Bios-Profil

Importieren eines Profils

Sie können ein BIOS-Profil, das vormals auf einem Server gespeichert war, in CMC importieren.

So importieren Sie ein auf einem Server gespeichertes Profil in CMC:

1. Auf der Seite **BIOS-Profil** im Abschnitt **Verwalten von Profilen auf SD-Karte** klicken Sie auf **Profil importieren**.
   Der Abschnitt **BIOS-Profil importieren** wird angezeigt.
2. Klicken Sie auf **Durchsuchen**, um auf das Profil an dem erforderlichen Standort zuzugreifen und klicken Sie dann auf **Profil importieren**.
   Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.

Exportieren eines Profils

Sie können ein BIOS-Profil, das auf einem nichtflüchtigen CMC-Datenträger (SD-Karte) gespeichert ist, zu einem angegebenen Pfad auf einem anderen Server exportieren.

Zum Exportieren eines gespeicherten Profils:

1. Wählen Sie das erforderliche Profil auf der Seite **BIOS-Profil** im Abschnitt **Profile auf der SD-Karte verwalten** aus und klicken Sie dann auf **Profil exportieren**.

   Ein Dialogfeld **Datei-Download** wird angezeigt und Sie werden dazu aufgefordert, die Datei zu öffnen oder zu speichern.
2. Klicken Sie auf **Speichern** oder **Öffnen**, um das Profil auf den erforderlichen Standort zu exportieren.

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

Bearbeiten des Profils

Sie können den Namen und die Beschreibung des BIOS-Profils, das auf dem nichtflüchtigen Datenträger (SD-Karte) gespeichert ist, bearbeiten.

So bearbeiten Sie ein gespeichertes Profil:

1. Wählen Sie auf der Seite **BIOS-Profil** im Abschnitt **Verwalten von Profilen auf SD-Karte** das erforderliche Profil aus und klicken Sie dann auf **Profil bearbeiten**.

   Der Abschnitt **BIOS-Profil bearbeiten - <Profilname>** wird angezeigt.
2. Bearbeiten Sie den Profilnamen und die Beschreibung des BIOS-Profils wie erforderlich und klicken Sie auf **Profil bearbeiten**.

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

Löschen eines Profils

Sie können ein BIOS-Profil löschen, das auf dem CMC nichtflüchtigen Datenträger (SD-Karte) gespeichert ist.

So löschen Sie ein gespeichertes Profil:

1. Wählen Sie auf der Seite **BIOS-Profil** im Abschnitt **Verwalten von Profilen auf SD-Karte** das erforderliche Profil aus und klicken Sie auf **Profil löschen**.

   Es wird eine Warnmeldung angezeigt, dass der Profillöschvorgang das ausgewählte Profil dauerhaft löschen wird.
2. Klicken Sie auf **OK**, um das ausgewählte Profil zu löschen.

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

BIOS-Einstellungen anzeigen

Klicken Sie zum Anzeigen der **BIOS-Einstellungen** für einen ausgewählten Server auf der Seite **BIOS-Profil** im Abschnitt **Profile speichern und anwenden**, klicken Sie auf **Anzeigen** in der Spalte der BIOS-Einstellungen für den Server, für das Sie die Informationen zu den BIOS-Einstellungen anzeigen möchten. Die Seite **Einstellungen anzeigen** wird angezeigt.

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

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

So aktivieren Sie CSIOR auf:

- Server der 11. Generation – Wählen Sie nach dem Neustart des Servers aus dem **Ctrl-E**-Setup **System-Dienste** aus, aktivieren Sie **CSIOR** und speichern Sie die Änderungen.
- Server der 12. Generation – Wählen Sie nach dem Neustart des Servers aus dem **F2**Setup, wählen Sie **iDRAC-Einstellungen → Lifecycle Controller** aus, aktivieren Sie **CSIOR** und speichern Sie die Änderungen.

Verwandte Links

Zugreifen auf die Seite Bios-Profil

Anzeigen der Profileinstellungen

Zum Anzeigen der Profileinstellungen der gespeicherten BIOS-Profile gehen Sie zur Seite **BIOS-Profil**. Klicken Sie im Abschnitt **Verwalten von Profilen auf SD-Karte** in der Spalte „Profileinstellungen“ auf **Ansicht**, um die BIOS-Profile, für die Sie die Profileinstellungen anzeigen möchten, anzuzeigen. Die Seite **Einstellungen anzeigen** wird angezeigt.

Profilprotokoll anzeigen

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

Fertigstellungsstatus und Fehlerbehebung

So überprüfen Sie den Fertigstellungsstatus für ein angewendetes BIOS-Profil:

1. Notieren Sie sich auf der Seite **BIOS-Profile** die Job ID (JID) des übermittelten Jobs aus dem Abschnitt **Neu erstelltes Profilprotokoll**.
2. Wählen Sie in der Systemstruktur **Server-Übersicht?** aus und klicken Sie auf **Fehlerbehebung → Lifecycle Controller-Aufträge**. Suchen Sie die gleiche JID in der Tabelle **Jobs**.

iDRAC mit einfacher Anmeldung starten

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

Ein Benutzer kann die iDRAC-Webschnittstelle eventuell starten, ohne sich ein zweites Mal anmelden zu müssen, da diese Funktion die einfache Anmeldung verwendet. Richtlinien zur einfachen Anmeldung werden unten beschrieben.

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

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

  ANMERKUNG: Benutzer werden eventuell aufgefordert, sich bei iDRAC anzumelden (siehe den dritten Aufzählungspunkt unter den Richtlinien zur einfachen Anmeldung).

ANMERKUNG: Wenn iDRAC-Netzwerk-LAN deaktiviert ist (LAN aktiviert = Nein), ist einfache Anmeldung nicht verfügbar.

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

Verwandte Links

iDRAC über die Seite Serverstatus starten
iDRAC von der Seite Serverstatus starten

iDRAC über die Seite Serverstatus starten

Start der iDRAC-Verwaltungskonsole von der Seite **Server-Status** aus:

1. Klicken Sie in der Systemstruktur auf **Server-Übersicht**. Die Seite **Serverstatus** wird angezeigt.
2. Klicken Sie auf **iDRAC starten** für den Server, für den Sie die iDRAC-Webschnittstelle starten wollen.

iDRAC von der Seite Serverstatus starten

So starten Sie die iDRAC-Verwaltungskonsole für einen individuellen Server:

1. Erweitern Sie den Eintrag **Server-Übersicht** in der Systemstruktur. Es werden alle Server (1 - 16) in der erweiterten Liste der **Server** angezeigt.
2. Klicken Sie auf den Server, für den Sie die iDRAC-Webschnittstelle starten möchten. Die Seite **Server-Status** wird angezeigt.
3. Klicken Sie auf **iDRAC-GUI starten**. Die iDRAC-Webschnittstelle wird angezeigt.

Remote-Konsole über die CMC-Webschnittstelle starten

Sie können eine Keyboard-Video-Mouse (KVM)-Sitzung direkt auf dem Server starten. Die Remote-Konsolen-Funktion wird nur unterstützt, wenn alle folgenden Bedingungen erfüllt sind:

- Der Gehäusestrom ist eingeschaltet.
- Server, die 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).

Die Remote-Konsole kann auch von der iDRAC-WEbschnittstelle gestartet werden. Weitere Informationen finden Sie im *iDRAC-Benutzerhandbuch*.

Verwandte Links

Remote-Konsole von der Seite Gehäusefunktionszustand starten
Remote-Konsole von der Seite „Status der Server“ starten
Remote-Konsole von der Seite Status der Server starten

Remote-Konsole von der Seite Gehäusefunktionszustand starten

So starten Sie eine Remote-Konsole von der CMC-Webschnittstelle:

1. Wählen Sie in der Systemstruktur **Gehäuse-Übersicht** aus und klicken Sie auf **Eigenschaften** → **Funktionszustand**. Die Seite **Gehäusefunktionszustand** wird angezeigt.
2. Klicken Sie auf den angegebenen Server in der Gehäuse-Grafik.
3. Klicken Sie im Abschnitt **Quicklinks** auf den Link **Remote-Konsole starten**, um die Remote-Konsole zu starten.

Remote-Konsole von der Seite „Status der Server“ starten

So starten Sie eine Remote-Konsole für einen individuellen Server:

1. Erweitern Sie in der Systemstruktur **Server-Übersicht**. Es werden alle Server (1 - 16) in der erweiterten Liste der Server angezeigt.
2. Klicken Sie auf den Server, für den Sie die Remote-Konsole starten wollen. Die Seite **Serverstatus** wird angezeigt.
3. Klicken Sie auf **Remote-Konsole starten**.

Remote-Konsole von der Seite Status der Server starten

So starten Sie eine Remote-Konsole von der Seite **Status der Server**:

1. Wählen Sie in der Systemstruktur **Server-Übersicht** aus und klicken Sie auf **Eigenschaften** → **Status**. Die Seite **Serverstatus** wird angezeigt.
2. Klicken Sie für den erforderlichen Server auf **Remote-Konsole starten**.

8

CMC für das Versenden von Warnungen konfigurieren

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

So konfigurieren Sie CMC zum Versenden von Warnungen:

1. Aktivieren Sie die globalen Gehäuseereigniswarnungen.
2. Optional können Sie die Ereignisse auswählen, für die Warnungen erstellt werden müssen.
3. Konfigurieren Sie die Einstellungen für die E-Mail-Warnung oder die SNMP-Trap-Einstellungen.

Verwandte Links

Warnungen aktivieren und deaktivieren
Konfiguration von Warnungszielen

Warnungen aktivieren und deaktivieren

Um Warnungen an konfigurierte Ziele zu senden, müssen Sie die globale Warnungsoption aktivieren. Diese Eigenschaft überschreibt die individuellen Warnungseinstellungen.

Stellen Sie sicher, dass die SNMP- oder E-Mail-Warnungsziele konfiguriert werden, um Warnungen empfangen zu können.

Warnungen über die CMC-Web-Schnittstelle aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie die Generierung von Warnungen:

1. Wählen Sie in der Systemstruktur **Gehäuse-Übersicht** aus und klicken Sie auf **Warnungen** → **Gehäuseereignisse**.
   Die Seite **Gehäuseereignisse** wird angezeigt.
2. Wählen Sie im Abschnitt **Gehäuseereignisfilter-Konfiguration** die Option **Gehäuseereigniswarnungen** um die Erzeugung von Warnungen zu aktivieren. Andernfalls löschen Sie diese Option.
3. Führen Sie im Abschnitt **Gehäuseereignisliste** einen der folgenden Vorgänge aus:
   - Wählen Sie die Ereignisse aus, für die Warnungen erstellt werden müssen.
   - Wählen Sie die Option **Warnungen aktivieren** in der Spaltenüberschrift aus, um Warnungen für alle Ereignisse zu erstellen. Andernfalls löschen Sie diese Option.
4. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

Warnungen über RACADM aktivieren oder deaktivieren

Um die Erstellung von Warnungen zu aktivieren oder zu deaktivieren, verwenden Sie das **cfgIpmiLanAlertEnable** RACAM-Objekt. Weitere Informationen finden Sie im *RACADM-Befehlzeilen-Referenzhandbuch für den iDRAC7 und CMC*.

Konfiguration von Warnungszielen

Die Management Station verwendet Simple Network Management Protocol (SNMP), um Daten vom CMC zu erhalten.

Sie können die IPv4- und IPv6-Warnungsziele, die E-Mail-Einstellungen und die SMTP-Server-Einstellungen konfigurieren und diese Einstellungen testen.

Stellen Sie vor der Konfiguration der Enstellungen für E-Mail-Warnungen oder SNMP-Trap sicher, dass Sie über die Berechtigung **Gehäusekonfigurations-Administrator** verfügen.

Verwandte Links

SNMP-Trap-Warnungsziele konfigurieren
Einstellungen für E-Mail-Warnungen konfigurieren

SNMP-Trap-Warnungsziele konfigurieren

Sie können die IPv6- oder IPv4-Adressen für den Empfang von SNMP-Traps konfigurieren.

SNMP-Trap-Warnungsziele über die CMC-Webschnittstelle konfigurieren

So konfigurieren Sie IPv4- oder IPv6-Warnzieleinstellungen über die CMC-Webschnittstelle:

1. Wählen Sie in der Systemstruktur **Gehäuse-Übersicht** aus und klicken Sie auf **Warnungen → Trap-Einstellungen**.
   Die Seite **Warnungsziele bei Gehäuseereignissen** wird angezeigt.
2. Geben Sie Folgendes ein:
   - Geben Sie im Feld **Ziel** eine gültige IP-Adresse ein. Verwenden Sie das 4-Punkt-IPv4-Format, Standard-IPv6-Adressnotation oder FQDN. Zum Beispiel: **123.123.123.123** oder **2001:db8:85a3::8a2e:370:7334** oder **dell.com**.
     Wählen Sie ein Format, das mit der Netzwerk-Technologie/Infrastruktur in Einklang steht. Die Testtrap-Funktionalität kann keine inkorrekten Einstellungen aufgrund der aktuellen Netzwerkkonfiguration erkennen (z. B. die Verwendung eines IPv6-Ziels in einer reinen IPv4-Umgebung).
   - Geben Sie im Feld **Community-Zeichenkette** eine gültige Community-Zeichenkette ein, zu der die Ziel-Management Station gehört.
     Diese Community-Zeichenkette 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.
   - Wählen Sie unter **Aktiviert** das Kontrollkästchen der entsprechenden Ziel-IP aus, um die IP-Adresse zum Empfangen der Traps zu aktivieren. Sie können bis zu vier IP-Adressen festlegen.
3. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.
4. Um zu überprüfen, ob die IP-Adressen die SNMP-Traps empfangen, klicken Sie auf **Senden** in der Spalte **SNMP Trap testen**.
   Die IP-Warnziele sind damit konfiguriert.

SNMP-Trap-Warnungsziele über RACADM konfigurieren

So konfigurieren Sie IP-Warnungsziel über RACADM:

1. Öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC und melden Sie sich an.

   ANMERKUNG: Es kann nur eine Filtermaske für SNMP- und E-Mail-Warnungen festgelegt werden. Sie können Schritt 2 überspringen, wenn Sie bereits eine Filtermaske ausgewählt haben.

2. Aktivieren Sie die Erstellung von Warnungen:

   ```
   racadm config -g cfgAlerting -o cfgAlertingEnable 1
   ```

3. Geben Sie die Ereignisse an, für die Warnungen erstellt werden müssen:

   ```
   racadm config -g cfgAlerting -o cfgAlertingFilterMask <Maskenwert>
   ```

   wobei `<Maskenwert>` ein Hexadezimalwert zwischen 0x0 and 0xffffffff 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 14. Filtermasken für Ereignis-Traps

Ereignis	Filtermaskenwert
Lüftersonden-Fehler	0x1
Batteriesondenwarnung	0x2
Temperatursondenwarnung	0x8
Temperatursonden-Fehler	0x10
Redundanz herabgesetzt	0x40
Redundanzverlust	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
EAM nicht vorhanden	0x100000
EAM-Fehler	0x200000
Firmware-Versionen stimmen nicht überein	0x400000
Gehäusestrom-Schwellenwert-Fehler	0x1000000

Ereignis	Filtermaskenwert
SD-Karte nicht vorhanden	0x2000000
SDKARTEN-Fehler	0x4000000
Gehäusegruppenfehler	0x8000000
Server-Sleeve fehlt	0x10000000
Struktur-Nichtübereinstimmung	0x20000000

4. Trap-Warnungen aktivieren:
   ```
   racadm config -g cfgTraps -o cfgTrapsEnable 1 -i <Index>
   ```
   wobei `<Index>` ein Wert von 1 - 4 ist. Die Indexnummer wird vom CMC verwendet, um bis zu vier konfigurierbare Ziele für Trap-Warnungen zu unterscheiden. Geben Sie Trap-Ziele als korrekt formatierte numerische Adressen (IPv6 oder IPv4) oder vollqualifizierte Domänennamen (FQDNs) an.
5. Bestimmen Sie eine Ziel-IP-Adresse, um Trap-Warnungen zu erhalten:
   ```
   racadm config -g cfgTraps -o cfgTrapsAlertDestIPAddr <IP-Adresse> -i <Index>
   ```
   wobei `<IP-Adresse>` ein gültiges Ziel ist und `<Index>` der Indexwert, der in Schritt 4 angegeben wurde.
6. Geben Sie den Community-Namen an:
   ```
   racadm config -g cfgTraps -o cfgTrapsCommunityName <Community-Name> -i
   <Index>
   ```
   wobei `<Community-Name>` die SNMP-Community ist, zu der das Gehäuse gehört, und `<Index>` der Indexwert, der Sie in Schritt 4 und 5 angegeben wurde.

   Sie können bis zu vier Ziele für den Empfang von Trap-Warnungen konfigurieren. Um weitere Ziele hinzuzufügen, wiederholen Sie die Schritte 2 bis 6.

   ANMERKUNG: Die Befehle in Schritten 2 bis 6 überschreiben alle vorhandenen Einstellungen, die für den angegebenen Index konfiguriert wurden (1-4). Um festzustellen, ob ein Index über zuvor konfigurierte Werte verfügt, geben Sie Folgendes ein: `racadm get config -g cfgTraps -i <Index>`. Wenn der Index konfiguriert ist, werden für die Objekte **cfgTrapsAlertDestIPAddr** und **cfgTrapsCommunityName** Werte angezeigt.
7. So testen Sie ein Ereignis-Trap für ein Warnungsziel. Geben Sie Folgendes ein:
   ```
   racadm testtrap -i <Index>
   ```
   wobei `<Index>` ein Wert von 1-4 ist und das Warnungsziel darstellt, das Sie testen möchten.

   Wenn Sie sich über die Indexnummer nicht sicher sind, geben Sie Folgendes ein:
   ```
   racadm getconfig -g cfgTraps -i <Index>
   ```

Einstellungen für E-Mail-Warnungen konfigurieren

Wenn der CMC ein Gehäuseereignis ermittelt, wie z. B. eine Umgebungswarnung oder einen Komponentenfehler, kann er so konfiguriert werden, dass eine E-Mail-Warnung an eine oder mehrere E-Mail-Adressen gesendet wird.

Sie müssen den SMTP-E-Mail-Server so konfigurieren, dass von der CMC-IP-Adresse weitergeleitete E-Mails angenommen werden können; eine Funktion, die bei den meisten Mail-Servern aus Sicherheitsgründen normalerweise deaktiviert ist. Wie Sie dies auf sichere Art und Weise einrichten können, können Sie in der mit dem SMTP-Server mitgelieferten Dokumentation nachlesen.

ANMERKUNG: Wenn Ihr Mail-Server Microsoft Exchange Server 2007 ist, ist sicherzustellen, dass der iDRAC7-Domänenname so konfiguriert ist, dass der Mail-Server die E-Mail-Warnungen des iDRAC7 empfängt.

ANMERKUNG: E-Mail-Warnungen unterstützen sowohl IPv4- als auch IPv6-Adressen. Der DRAC DNS-Domänenname muss beim Nutzen von IPv6 festgelegt werden.

Wenn Ihr Netzwerk über einen SMTP-Server verfügt, der periodisch IP-Adressen ausgibt und erneuert, und die Adressen unterschiedlich sind, ergibt sich eine Zeitspanne, während der diese Einstellung der Eigenschaften aufgrund einer Änderung in der festgelegten SMTP-Server-IP-Adresse nicht funktioniert. Verwenden Sie in solchen Fällen den DNS-Namen.

E-Mail-Warnungseinstellungen über die Web-Schnittstelle konfigurieren

So konfigurieren Sie die E-Mail-Warnungseinstellungen über die Web-Schnittstelle:

1. Wählen Sie in der Systemstruktur **Gehäuse-Übersicht** aus und klicken Sie auf **Warnungen** → **E-Mail-Warnungseinstellungen**.
2. Geben Sie die SMTP-E-Mail-Servereinstellungen und die E-Mail-Adresse(n) an, um die Warnungen zu erhalten. Weitere Informationen über die Felder finden Sie in der *CMC Online-Hilfe*.
3. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.
4. Klicken Sie auf **Senden** unter **Test-E-Mail**, um eine Test-E-Mail an ein angegebenes E-Mail-Warnungsziel zu senden.

E-Mail-Warnungseinstellungen über RACADM konfigurieren

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 die Erstellung von Warnungen:
   ```
   racadm config -g cfgAlerting -o cfgAlertingEnable 1
   ```
   ANMERKUNG: Es kann nur eine Filtermaske für SNMP- und E-Mail-Warnungen festgelegt werden. Sie können Schritt 3 überspringen, wenn Sie bereits eine Filtermaske festgelegt haben.
3. Geben Sie die Ereignisse an, für die Warnungen erstellt werden müssen:
   ```
   racadm config -g cfgAlerting -o cfgAlertingFilterMask <Maskenwert>
   ```
   wobei `<Maskenwert>` ein hexadezimaler Wert zwischen 0x0 and 0xffffffff ist und mit den vorangestellten Zeichen 0x ausgedrückt werden muss. Die Tabelle Filtermasken für Ereignis-Traps liefert die Filtermasken für jeden Ereignistyp. Eine Anleitung zum Berechnen des Hexadezimalwerts für die Filtermaske, die Sie aktivieren möchten, finden Sie in Schritt 3 in Konfigurieren von SNMP-Trap-Zielen über RACADM.
4. So aktivieren Sie die E-Mail-Warnung:
   ```
   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 <E-Mail-Adresse> -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:
   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertAddress <E-Mail-Name> -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 und 5 angegeben haben. Der E-Mail-Name darf bis zu 32 alphanumerische Zeichen, Bindestriche, Unterstriche und Punkte enthalten. Leerstellen sind nicht gültig.

7. Einrichten des SMTP-Hosts:

   ```
   racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr host.domain
   ```

   Dabei ist `host.domain` die FQDN.

   Sie können bis zu vier Ziel-E-Mail-Adressen für den Empfang von E-Mail-Warnungen konfigurieren. Um weitere E-Mail-Adressen hinzuzufügen, wiederholen Sie die Schritte 2-6.

   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: x`racadm get config -g cfgEmailAlert -i <Index>`. Wenn der Index konfiguriert ist, werden für die Objekte **cfgEmailAlertAddress** und **cfgEmailAlertEmailName** Werte angezeigt.

   Weitere Informationen finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC*, das unter **dell.com/support/manuals** verfügbar ist.

9

Benutzerkonten und Berechtigungen konfigurieren

Sie können Benutzerkonten mit spezifischen Berechtigungen (*rollenbasierten Berechtigungen*) einrichten, um Ihr System über CMC zu verwalten und um die Systemsicherheit zu gewährleisten. Standardmäßig ist CMC mit einem lokalen Administratorkonto konfiguriert. Der Standardbenutzername lautet *root*, und das Kennwort lautet *calvin*. Als Administrator können Sie Benutzerkonten einrichten, damit andere Benutzer auf CMC zugreifen können.

Sie können bis zu 16 lokale Benutzer einrichten oder Verzeichnisdienste benutzen, wie z. B. Microsoft Active Directory oder LDAP, um weitere Benutzerkonten einzurichten. Durch die Verwendung eines Verzeichnisdienstes verfügen Sie über einen zentralen Standort für die Verwaltung berechtigter Benutzerkonten.

CMC unterstützt den rollenbasierten Zugriff auf Benutzer mit einem Satz aus zugewiesenen Berechtigungen. Die folgenden Rollen sind verfügbar: Administrator, Operator, Schreibgeschützt oder Kein/e/r. Die Rolle definiert den Umfang der zugewiesenen Berechtigungen.

Verwandte Links

Typen von Benutzern
Lokale Benutzer konfigurieren
Konfigurieren von Active Directory-Benutzern
Generische LDAP-Benutzer konfigurieren
Ändern der Einstellungen für Stammbenutzer-Administratorkonto

Typen von Benutzern

Es gibt zwei Typen von Benutzern:

- CMC-Benutzer oder Gehäuse-Benutzer
- iDRAC-Benutzer oder Server-Benutzer (da iDRAC auf einem Server resident ist)

CMC- und iDrac-Benutzer können lokale Benutzer oder Verzeichnisdienstbenutzer sein.

Mit Ausnahme des Falls, dass der CMC-Benutzer die Berechtigung als **Server-Administrator** besitzt, werden die einem CMC-Benutzer gewährten Berechtigungen nicht automatisch auf denselben Benutzer auf einem Server übertragen, da Serverbenutzer unabhängig von CMC-Benutzern erstellt werden. Mit anderen Worten, CMC Active Directory-Benutzer und iDRAC Active Directory-Benutzer befinden sich in zwei unterschiedlichen Zweigen der Active Directory-Struktur. Um einen lokalen Serverbenutzer zu erstellen, muss sich der Administrator für Benutzerkonfiguration direkt am Server anmelden. Der Benutzerkonfiguration-Administrator kann keinen Serverbenutzer aus einem CMC-Benutzer erstellen oder umgekehrt. Diese Regel schützt die Sicherheit und Integrität der Server.

Tabelle 15. : Typen von Benutzern

Berechtigung	Beschreibung
CMC-Anmeldung, Benutzer	Der Benutzer kann sich am CMC anmelden und alle CMC-Daten anzeigen. Er kann aber keine Daten hinzufügen oder ändern oder Befehle ausführen. Es ist möglich, dass ein Benutzer andere Berechtigungen ohne CMC-Anmeldebenutzerberechtigung besitzt. Diese Funktion ist sinnvoll, wenn sich

Berechtigung	Beschreibung
	ein Benutzer vorübergehend nicht anmelden darf. Wenn die CMC-Anmeldeberechtigung dieses Benutzers wiederhergestellt ist, erhält der Benutzer alle zuvor gewährten Berechtigungen zurück.
Gehäusekonfiguration-Administrator	Benutzer können Daten hinzufügen oder ändern, die: • das Gehäuse identifizieren, z. B. den Gehäusenamen und die Gehäuseposition. • dem Gehäuse speziell zugewiesen sind, z. B. der IP-Modus (statisch oder DHCP), statische IP-Adresse, statischer Gateway und statische Subnetzmaske. • Dienste für das Gehäuse bereitstellen, z. B. Datum und Uhrzeit, Firmware-Aktualisierung und CMC-Reset. • dem Gehäuse zugeordnet sind, wie z. B. der Name des Steckplatzes und die Steckplatzpriorität. Obwohl sich diese Eigenschaften auf die Server beziehen, handelt es sich bei ihnen ausschließlich um Gehäuseeigenschaften, die sich auf die Steckplätze und nicht auf die Server selbst beziehen. Aus diesem Grund können Steckplatznamen und Steckplatzprioritäten hinzugefügt oder geändert werden, ungeachtet, ob sich Server in den Steckplätzen befinden oder nicht. Wenn ein Server auf ein anderes Gehäuse verschoben wird, werden der Steckplatzname und die Priorität, die dem im neuen Gehäuse belegten Steckplatz zugewiesen werden, übertragen. Der vorherige Steckplatzname und die vorherige Priorität verbleiben beim vorherigen Gehäuse. **ANMERKUNG:** CMC-Benutzer mit einer Berechtigung als **Administrator für die Gehäusekonfiguration** können die Energieversorgungseinstellungen konfigurieren. Es sind jedoch Benutzer mit einer Berechtigung als **Administrator für die Gehäusesteuerung** erforderlich, um Energieversorgungsvorgänge auf dem Gehäuse auszuführen, darunter Strom einschalten und Strom ausschalten sowie Strom ein- und ausschalten.
Benutzerkonfigurations-Administrator	Ein Benutzer kann: • Hinzufügen eines neuen Benutzers. • Ändern des Kennworts eines Benutzers. • Ändern der Berechtigungen eines Benutzers. • Aktivieren oder Deaktivieren der Anmeldungsberechtigung eines Benutzers unter Beibehaltung des Namens des Benutzers und anderer Berechtigungen in der Datenbank.
Administrator zum Löschen von Protokollen	Ein Benutzer kann das Hardwareprotokoll und das CMC-Protokoll löschen.
Gehäusesteuerungs-Administrator (Strombefehle)	CMC-Benutzer mit einer Berechtigung als Administrator für die **Gehäusestromversorgung** können alle Vorgänge im Zusammenhang mit der Stromversorgung ausführen. Sie können Gehäusestromvorgänge steuern, einschließlich Strom einschalten, Strom ausschalten und Strom aus- und einschalten. **ANMERKUNG:** Für die Konfiguration von Stromversorgungseinstellungen ist eine Berechtigung als **Administrator für die Gehäusekonfiguration** erforderlich.

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 eine **Server Administrator**-Berechtigung eine Maßnahme zum Ausführen auf einem Server ausgibt, sendet die CMC-Firmware den Befehl zum Zielserver, ohne die Berechtigungen des Benutzers auf dem Server zu überprüfen. Mit anderen Worten: die **Server Administrator**-Berechtigung setzt alle fehlenden Administratorrechte auf dem Server außer Kraft. Ohne die **Server Administrator**-Berechtigung kann ein auf dem Gehäuse erstellter Benutzer nur dann einen Befehl auf einem Server ausführen, wenn alle folgenden Bedingungen erfüllt werden: • Derselbe Benutzername ist auf dem Server vorhanden. • Derselbe Benutzername muss auf dem Server das identische Kennwort besitzen. • Der Benutzer muss die Berechtigung zum Ausführen des Befehls aufweisen. Wenn ein CMC-Benutzer, der nicht über die **Server Administrator**-Berechtigung verfügt, eine Maßnahme ausgibt, die auf einem Server ausgeführt werden soll, sendet der CMC mit dem Benutzernamen und dem Kennwort des Benutzers einen Befehl an den Zielserver. Wenn der Benutzer auf dem Server nicht vorhanden ist oder das Kennwort nicht übereinstimmt, wird dem Benutzer das Ausführen der Maßnahme verweigert. Wenn der Benutzer auf dem Zielserver vorhanden ist und das Kennwort übereinstimmt, reagiert der Server mit den Berechtigungen, die dem Benutzer auf dem Server gewährt wurden. Basierend auf den Berechtigungen, mit denen der Server reagiert, wird über die CMC-Firmware entschieden, ob dem Benutzer das Recht zum Ausführen der Maßnahme zusteht. Im Folgenden werden die Berechtigungen und Maßnahmen auf dem Server aufgeführt, auf die der Server Administrator Anspruch hat. Diese Rechte werden nur dann angewendet, wenn der Gehäusebenutzer nicht über die Server Administrator-Berechtigung auf dem Gehäuse verfügt. Serverkonfiguration-Administrator: • IP-Adresse einstellen • Gateway einstellen • Subnetzmaske einstellen • Erstes Startgerät einstellen Benutzer konfigurieren: • iDRAC-Stammkennwort einstellen • iDRAC-Reset Serversteuerung-Administrator: • Einschalten • Ausschalten • Aus- und einschalten • Ordentliches Herunterfahren • Serverneustart

Berechtigung	Beschreibung
Warnungstests für Benutzer	Benutzer kann Testwarnungsmeldungen senden.
Administrator für Debug-Befehle	Benutzer kann Systemdiagnosebefehle ausführen.
Struktur A-Administrator	Benutzer kann die Struktur A-EAM festlegen und konfigurieren, 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.

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

ANMERKUNG: Wenn Sie Administrator, Hauptbenutzer oder Gastbenutzer auswählen und dann eine Berechtigung aus dem vordefinierten Satz hinzufügen oder daraus entfernen, wird die CMC-Gruppe automatisch zu Benutzerdefiniert geändert.

Tabelle 16. : CMC-Gruppenberechtigungen

Benutzergruppe	Gewährte Berechtigungen
Administrator	• CMC-Anmeldung, Benutzer • Gehäusekonfiguration-Administrator • Benutzerkonfigurations-Administrator • Administrator zum Löschen von Protokollen • Server Administrator • Warnungstests für Benutzer • Administrator für Debug-Befehle • Struktur A-Administrator • Struktur B-Administrator • Struktur C-Administrator
Hauptbenutzer	• Anmelden • Administrator zum Löschen von Protokollen • Gehäusesteuerungs-Administrator (Strombefehle) • Server Administrator • Warnungstests für Benutzer • Struktur A-Administrator • Struktur B-Administrator • Struktur C-Administrator
Gastbenutzer	Anmelden
Benutzerdefiniert	Wählen Sie eine beliebige Kombination der folgenden Berechtigungen aus: • CMC-Anmeldung, Benutzer • Gehäusekonfiguration-Administrator • Benutzerkonfigurations-Administrator • Administrator zum Löschen von Protokollen

Benutzergruppe	Gewährte Berechtigungen
	• Gehäusesteuerungs-Administrator (Strombefehle) • Server Administrator • Warnungstests für Benutzer • Administrator für Debug-Befehle • Struktur A-Administrator • Struktur B-Administrator • Struktur C-Administrator
Keine	Keine zugewiesenen Berechtigungen

Tabelle 17. Vergleich der Berechtigungen zwischen CMC-Administrator, Hauptbenutzer und Gastbenutzer

Berechtigungssatz	Administratorrechte	Hauptbenutzer-Berechtigungen	Gastbenutzer-Berechtigungen
CMC-Anmeldung, Benutzer	Ja	Ja	Ja
Gehäusekonfiguration-Administrator	Ja	Nein	Nein
Benutzerkonfigurations-Administrator	Ja	Nein	Nein
Administrator zum Löschen von Protokollen	Ja	Ja	Nein
Gehäusesteuerungs-Administrator (Strombefehle)	Ja	Ja	Nein
Server Administrator	Ja	Ja	Nein
Warnungstests für Benutzer	Ja	Ja	Nein
Administrator für Debug-Befehle	Ja	Nein	Nein
Struktur A-Administrator	Ja	Ja	Nein
Struktur B-Administrator	Ja	Ja	Nein
Struktur C-Administrator	Ja	Ja	Nein

Ändern der Einstellungen für Stammbenutzer-Administratorkonto

Zum Zweck der zusätzlichen Sicherheit wird dringend empfohlen, das Standardkennwort des Stammkontos (Benutzer 1) zu ändern. Das Root-Konto ist das Standard-Administrationskonto, das mit CMC geliefert wird.

So ändern Sie das Standardkennwort für das Stammkonto über die CMC-Webschnittstelle:

1. Wählen Sie in der Systemstruktur **Gehäuse-Übersicht** aus und klicken Sie auf **Benutzerauthentifizierung** → **Lokale Benutzer**?. Die Seite **Benutzer** wird angezeigt.
2. Klicken Sie in der Spalte **Benutzer-ID** auf Benutzer-ID 1.

   ANMERKUNG: Benutzer-ID1 ist das Stammbenutzerkonto, das mit CMC geliefert wird. Es kann nicht geändert werden.

   Die Seite **Benutzerkonfiguration** wird angezeigt.

3. Wählen Sie das Kontrollkästchen **Kennwort ändern** aus.
4. Geben Sie das neue Kennwort in die Felder **Kennwort** und **Kennwort bestätigen** ein.
5. Klicken Sie auf **Anwenden**. Das Kennwort für Benutzer-ID1 wurde geändert.

Lokale Benutzer konfigurieren

Sie können in CMC bis zu 16 lokale Benutzer mit spezifischen Zugriffsberechtigungen konfigurieren. Bevor Sie einen CMC-Benutzer erstellen, müssen Sie überprüfen, ob etwaige aktuellen Benutzer vorhanden sind. Sie können Benutzernamen, Kennwörter und Rollen mit den Berechtigungen für diese Benutzer definieren. Die Benutzernamen und Kennwörter können über sichere CMC-Schnittstellen geändert werden (z. B. über die Web-Schnittstelle, RACADM oder WS-MAN).

Lokale Benutzer über die CMC-Webschnittstelle konfigurieren

So fügen Sie lokale CMC-Benutzer hinzu und konfigurieren sie:

ANMERKUNG: Sie müssen die Berechtigung **Benutzer konfigurieren** besitzen, um einen CMC-Benutzer zu erstellen.

1. Wählen Sie in der Systemstruktur **Gehäuse-Übersicht** aus und klicken Sie auf? **Benutzerauthentifizierung** → **Lokale Benutzer**?. Die Seite **Benutzer** wird angezeigt.
2. In der Spalte **Benutzer-ID** klicken Sie auf eine Benutzer-ID-Nummer. Die Seite **Benutzerkonfiguration** wird angezeigt.

   ANMERKUNG: Benutzer-ID 1 ist das Stammbenutzerkonto, das standardmäßig mit CMC geliefert wird. Das lässt sich nicht ändern.
3. Aktivieren Sie die Benutzer-ID, legen Sie den Benutzernamen und das Kennwort fest, und greifen Sie dann auf die Berechtigungen für den Benutzer zu. Weitere Informationen zu diesen Optionen finden Sie in der *CMC-Online-Hilfe*.
4. Klicken Sie auf **Anwenden**. Der Benutzer wird mit den erforderlichen Berechtigungen erstellt.

Lokale Benutzer über RACADM konfigurieren

ANMERKUNG: Sie müssen als Benutzer **root** angemeldet sein, um RACADM-Befehle auf einem Remote-Linux-System ausführen zu können.

Sie können bis zu 16 Benutzer in der CMC-Eigenschaftsdatenbank konfigurieren. Bevor Sie einen CMC-Benutzer manuell aktivieren, prüfen Sie, ob aktuelle Benutzer vorhanden sind.

Wenn Sie einen neuen CMC konfigurieren oder den Befehl racadm `racresetcfg` verwendet haben, ist der einzige aktuelle Benutzer `root` mit dem Kennwort `calvin`. Der `racresetcfg` Unterbefehl setzt alle Konfigurationsparameter auf die ursprünglichen Standardeinstellungen zurück. Alle vorherigen Änderungen gehen verloren.

ANMERKUNG: Benutzer können zu einem beliebigen Zeitpunkt aktiviert und deaktiviert werden, wobei die Deaktivierung eines Benutzers diesen nicht aus der Datenbank löscht.

Um zu überprüfen, ob ein Benutzer existiert, öffnen Sie eine Telnet/SSH-Textkonsole auf dem CMC, melden Sie sich an und geben Sie den folgenden Befehl einmal für jeden Index von 1–16 ein:

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

ANMERKUNG: Sie können auch `racadm getconfig -f <myfile.cfg>` eingeben, und die Datei **myfile.cfg**, in der alle CMC-Konfigurationsparameter enthalten sind, anzeigen oder bearbeiten.

Mehrere Parameter und Objekt-IDs werden mit ihren aktuellen Werten angezeigt. Zwei Objekte von Bedeutung sind:

```
# cfgUserAdminIndex=XX cfgUserAdminUserName=
```

Wenn das Objekt `cfgUserAdminUserName` keinen Wert besitzt, steht diese Indexnummer, die durch das Objekt `cfgUserAdminIndex` angezeigt wird, zur Verfügung. Wenn hinter dem "=" ein Name steht, wird dieser Index von diesem Benutzernamen verwendet.

Wenn Sie einen Benutzer mit dem Unterbefehl racadm `config` manuell aktivieren oder deaktivieren, **muss** der Index mit der Option `–i` angegeben werden.

Beobachten Sie, ob das im vorausgehenden Beispiel angezeigte Objekt `cfgUserAdminIndex` das Zeichen # enthält. It indicates that it is a read-only object. Ebenso: Wenn der Befehl `racadm config –f racadm.cfg` zur Angabe einer beliebigen Anzahl von zu schreibenden Gruppen/Objekten verwendet wird, kann der Index nicht angegeben werden. Ein neuer Benutzer wird zum ersten verfügbaren Index hinzugefügt. Dieses Verhalten bietet größere Flexibilität bei der Konfiguration eines zweiten CMC mit denselben Einstellungen wie der Haupt-CMC.

CMC-Benutzer über RACADM hinzufügen

Führen Sie zum Hinzufügen eines neuen Benutzers zur CMC-Konfiguration folgende Schritte aus:

1. Legen Sie den Benutzernamen fest.
2. Legen Sie das Kennwort fest.
3. Legen Sie die Benutzerberechtigungen fest. Weitere Information über Benutzerberechtigungen finden Sie unter Typen von Benutzern.
4. Aktivieren Sie den Benutzer.

Beispiel:

Im folgenden Beispiel wird beschrieben, wie man einen neuen Benutzer namens "John" mit dem Kennwort "123456" und Anmeldeberechtigungen zum CMC hinzufügt.

ANMERKUNG: 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
```

Weitere Informationen zu RACADM-Befehlen finden Sie im *RACADM Command Line Reference Guide for iDRAC7 and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC), das unter **dell.com/support/manuals** verfügbar ist.

Einen CMC-Benutzer deaktivieren

Bei der Verwendung von RACADM müssen Benutzer manuell und individuell deaktiviert werden. Benutzer können nicht über eine Konfigurationsdatei gelöscht werden.

Für das Löschen eines CMC-Benutzers lautet die Syntax wie folgt:

```
racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i <index>"" racadm
config -g cfgUserAdmin -i 2 -o cfgUserAdminPrivilege 0x0
```

Eine Null-Kette doppelter Anführungszeichen ("") weist den CMC an, die Benutzerkonfiguration am angegebenen Index zu entfernen und auf die ursprünglichen Werkseinstellungen zurückzusetzen.

CMC-Benutzer mit Berechtigungen aktivieren

Um einen Benutzer mit spezifischen administrativen Berechtigungen (rollenbasierte Autorität) zu aktivieren:

1. Machen Sie zuerst einen verfügbaren Benutzer-Index mithilfe der Befehlssyntax ausfindig:
   ```
   racadm getconfig -g cfgUserAdmin -i <Index>
   ```
2. Geben Sie die folgenden Befehle mit dem neuen Benutzernamen und dem neuen Kennwort ein.
   ```
   racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <Index>
   <Benutzerberechtigungs-Bitmaskenwert>
   ```

   ANMERKUNG: Eine Liste gültiger Bit-Maskenwerte für spezifische Benutzerberechtigungen ist im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC* enthalten, das unter **dell.com/support/manuals** verfügbar ist. Der Standard-Berechtigungswert ist 0, was darauf hinweist, dass der Benutzer über keine aktivierten Berechtigungen verfügt.

Konfigurieren von Active Directory-Benutzern

Wenn Ihre Firma die Microsoft Active Directory-Software verwendet, kann die Software so konfiguriert werden, dass sie Zugriff auf CMC bietet. Sie können dann bestehenden Benutzern im Verzeichnisdienst CMC-Benutzerberechtigungen erteilen und diese steuern. Das ist eine lizenzierte Funktion.

ANMERKUNG: 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.

Sie können die Benutzerauthentifizierung über Active Directory konfigurieren, um sich am CMC anzumelden. Rollenbasierte Autorität kann bereitgestellt werden, die es einem Administrator ermöglicht, spezifische Berechtigungen für jeden Benutzer zu konfigurieren.

Unterstützte Active Directory-Authentifizierungsmechanismen

Sie können mit Active Directory den Benutzerzugriff auf CMC mittels zweier Methoden definieren:

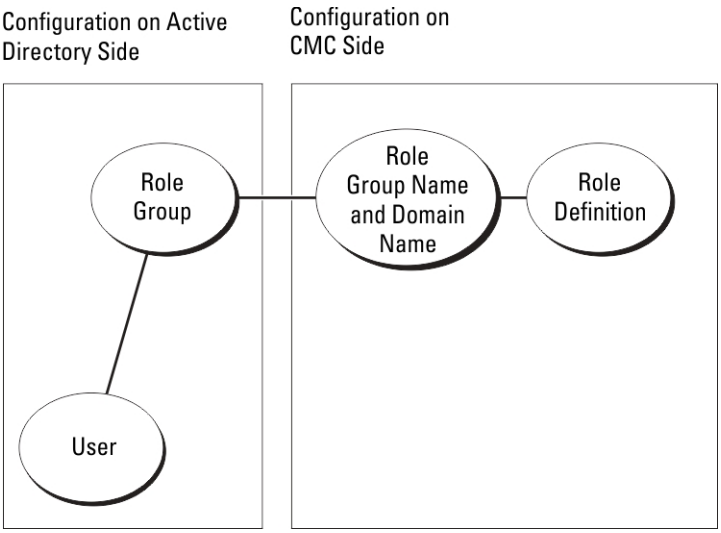
- Die *Standardschemalösung*, die nur Microsoft-Standard-Active Directory-Gruppenobjekte verwendet.
- Lösung *Erweitertes Schema*, die über benutzerdefinierte Active Directory-Objekte verfügt. Alle Zugriffssteuerungsobjekte werden im Active Directory verwahrt. Bei der Konfiguration des Benutzerzugangs auf verschiedenen CMCs mit unterschiedlichen Ebenen der Benutzerberechtigung besteht maximale Flexibilität.

Verwandte Links

Übersicht des Standardschema-Active Directory
Übersicht über Active Directory mit erweitertem Schema

Übersicht des Standardschema-Active Directory

Wie in der folgenden Abbildung dargestellt, erfordert die Verwendung des Standardschemas für die Active Directory-Integration die Konfiguration unter Active Directory und unter CMC.



In Active Directory wird ein Standardgruppenobjekt als Rollengruppe verwendet. Ein Benutzer, der Zugang zum CMC hat, ist ein Mitglied der Rollengruppe. Um diesem Benutzer Zugriff auf einen bestimmten CMC zu gewähren, muss der Rollengruppenname und dessen Domänenname auf der jeweiligen CMC Karte konfiguriert werden. Die Rolle und die Berechtigungsebene wird auf jeder CMC Karte und nicht im Active Directory definiert. Sie können bis zu fünf Rollengruppen für jeden CMC konfigurieren. Tabellen-Referenznummer zeigt die Standard-Rollengruppen-Berechtigungen.

Tabelle 18. Standardeinstellungsberechtigungen der Rollengruppe

Rollengruppe	Standard-Berechtigungsebene	Gewährte Berechtigungen	Bitmaske
1	Keine	• CMC-Anmeldung, Benutzer • Gehäusekonfiguration-Administrator • Benutzerkonfigurations-Administrator • Administrator zum Löschen von Protokollen • Gehäusesteuerungs-Administrator (Strombefehle) • Server Administrator • Warnungstests für Benutzer • Administrator für Debug-Befehle • Struktur A-Administrator • Struktur B-Administrator • Struktur C-Administrator	0x00000fff
2	Keine	• CMC-Anmeldung, Benutzer • Administrator zum Löschen von Protokollen • Gehäusesteuerungs-Administrator (Strombefehle) • Server Administrator • Warnungstests für Benutzer • Struktur A-Administrator • Struktur B-Administrator • Struktur C-Administrator	0x00000ed9
3	Keine	CMC-Anmeldung, Benutzer	0x00000001
4	Keine	Keine zugewiesenen Berechtigungen	0x00000000
5	Keine	Keine zugewiesenen Berechtigungen	0x00000000

ANMERKUNG: Die Bitmasken-Werte werden nur verwendet, wenn das Standardschema mit RACADM eingerichtet wird.

ANMERKUNG: Weitere Informationen über Benutzerberechtigungen finden Sie unter Typen von Benutzern.

Active Directory-Standardschema konfigurieren

So konfigurieren Sie CMC für den Zugriff auf eine Active Directory-Anmeldung:

1. Öffnen Sie auf einem Active Directory-Server (Domänen-Controller) das **Active Directory-Benutzer- und -Computer-Snap-In**.
2. CMC-Webschnittstelle oder RACADM verwenden:
   a) Erstellen Sie eine Gruppe oder wählen Sie eine bestehende Gruppe aus.
   b) Konfigurieren Sie die Rollenberechtigung.
3. Fügen Sie den Active Directory-Benutzer als ein Mitglied der Active Directory-Gruppe hinzu, um auf den CMC zuzugreifen.

Active Directory mit Standardschema unter Verwendung der CMC-Webschnittstelle konfigurieren

ANMERKUNG: Weitere Informationen zu den verschiedenen Feldern finden Sie in der *CMC-Online-Hilfe*.

1. Wählen Sie in der Systemstruktur **Gehäuse-Übersicht** aus und klicken Sie auf **Benutzer-Authentifizierung → Verzeichnisdienste**. Die Seite **Verzeichnisdienste** wird angezeigt.
2. Wählen Sie **Microsoft Active Directory (Standardschema)** aus. Die für Standardschema zu konfigurierenden Einstellungen werden auf der gleichen Seite angezeigt.
3. Geben Sie folgendes an:
   - Aktivieren Sie Active Directory, geben Sie den Root-Domänennamen und den Zeitüberschreitungswert ein.
   - Wenn der gezielte Aufruf den Domänen-Controller und den globalen Katalog durchsuchen soll, wählen Sie **AD-Server für Suche durchsuchen (optional)** aus.
4. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

   ANMERKUNG: Sie müssen die Einstellungen anwenden, bevor Sie fortfahren. Wenn Sie die Einstellungen nicht anwenden, verlieren Sie die eingegebenen Einstellungen, wenn Sie zur nächsten Seite wechseln.
5. Klicken Sie im Abschnitt **Standardschemaeinstellungen** auf eine **Rollengruppe**. Die Seite **Rollengruppe konfigurieren** wird angezeigt.
6. Geben Sie den Gruppenname, die Domäne und Berechtigungen für eine Rollengruppe ein.
7. Klicken Sie auf **Anwenden**, um die Einstellungen der Rollengruppe zu speichern und dann auf die Seite **Zurück zur Konfiguration**.
8. Falls Sie die Zertifikatsvalidierung aktiviert haben, müssen Sie das von der Zertifizierungsstelle signierte Root-Zertifikat der Domänengesamtstruktur auf den CMC hochladen. Geben Sie im Abschnitt **Zertifikate verwalten** den Dateipfad des Zertifikats ein oder suchen Sie nach der Zertifikatsdatei. Klicken Sie auf **Hochladen**, um die Datei auf den CMC hochzuladen.

   ANMERKUNG: Der Wert **Dateipfad** zeigt den relativen Dateipfad des Zertifikats an, das Sie hochladen. Sie müssen den vollständigen Dateipfad eintippen, der den vollständigen Pfad und den kompletten Dateinamen und die Dateierweiterung umfasst.

   Die SSL-Zertifikate für die Domänen-Controller müssen von dem von der Root-Zertifizierungsstelle signierten Zertifikat signiert werden. Das von der Root-Zertifizierungsstelle signierte Zertifikat muss auf der Management Station verfügbar sein, die auf den CMC zugreift.
9. Falls Sie die Option „Einmalige Anmeldung" (Single Sign-On, SSO) aktiviert haben, klicken Sie im Abschnitt „**Kerberos-Keytab**" auf **Durchsuchen**, geben Sie die Keytab-Datei an, und klicken Sie auf **Hochladen**. Wenn der

Vorgang beendet ist, wird ein Meldungsfenster eingeblendet, das anzeigt, ob der Upload erfolgreich oder fehlerhaft war.

10. Klicken Sie auf **Anwenden**. Der CMC-Webserver startet automatisch neu, wenn Sie auf **Anwenden** klicken.
11. Melden Sie sich ab und dann beim CMC an, um die CMC Active Directory-Konfiguration abzuschließen.
12. Wählen Sie in der Systemstruktur **Gehäuse** aus und navigieren Sie zur Registerkarte **Netzwerk**. Die Seite **Netzwerkkonfiguration** wird angezeigt.
13. Unter **Netzwerkeinstellungen** , wenn **DHCP verwenden (für Netzwerkschnittstellen-IP-Adresse)** ausgewählt ist, wählen Sie **DHCP zum Abrufen der DNS-Serveradresse verwenden** aus.

    Um die IP-Adresse eines DNS-Servers manuell einzugeben, wählen Sie **DHCP zum Abrufen der DNS-Serveradressen verwenden** ab und geben Sie die primäre und die alternative IP-Adresse des DNS-Servers ein.
14. Klicken Sie auf **Änderungen anwenden**.

    Die Funktionskonfiguration CMC-Standardschema von Active Directory ist abgeschlossen.

Konfiguration des Active Directory mit Standardschema unter Verwendung von RACADM

So konfigurieren Sie CMC Active Directory mit Standardschema unter Verwendung von RACADM:

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 <vollständig qualifizierter root-Domänenname> racadm config
   -g cfgStandardSchema -i <Index> -o cfgSSADRoleGroupName <allgemeiner Name
   der Rollengruppe> racadm config -g cfgStandardSchema -i <Index> -o
   cfgSSADRoleGroupDomain <vollständig qualifizierter Domänenname> racadm
   config -g cfgStandardSchema -i <Index> -o cfgSSADRoleGroupPrivilege
   <Bitmaskennummer für bestimmte Benutzerberechtigungen> racadm sslcertupload
   -t 0x2 -f <ADS-root-CA-Zertifikat> racadm sslcertdownload -t 0x1 -f < RAC-
   SSL-Zertifikat >
   ```

   ANMERKUNG: Lesen Sie für Bitmaskennummerwerte das Kapitel 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 <primäre DNS-IP-Adresse>
     racadm config -g cfgLanNetworking -o cfgDNSServer2 <sekundäre DNS-IP-
     Adresse>
     ```

Übersicht über Active Directory mit erweitertem Schema

Für die Verwendung der Lösung mit dem erweiterten Schema benötigen Sie die Active Directory-Schema-Erweiterung.

Active Directory-Schemaerweiterungen

Bei den Active Directory-Daten handelt es sich um eine verteilte Datenbank von *Attributen* und *Klassen.* Das Active Directory-Schema enthält die Regeln, die den Typ der Daten bestimmen, die der Datenbank hinzugefügt werden können bzw. darin gespeichert werden. Ein Beispiel einer Klasse, die in der Datenbank gespeichert wird, ist die Benutzerklasse. Beispielhafte Attribute der Benutzerklasse sind der Vorname, der Nachname bzw. die Telefonnummer des Benutzers.

Sie können die Active Directory-Datenbank erweitern, indem Sie Ihre eigenen einzigartigen *Attribute* und *Klassen* für besondere Anforderungen hinzufügen. Dell hat das Schema um die erforderlichen Änderungen zur Unterstützung von Remote-Management-Authentifizierung und -Autorisierung erweitert.

Jedes *Attribut* bzw. jede *Klasse*, das/die zu einem vorhandenen Active Directory-Schema hinzugefügt wird, muss mit einer eindeutigen ID definiert werden. Um branchenweit eindeutige IDs zu gewährleisten, unterhält Microsoft eine Datenbank von Active Directory-Objektbezeichnern (OIDs). Wenn also Unternehmen das Schema erweitern, sind diese Erweiterungen eindeutig und ergeben keine Konflikte. Um das Schema im Active Directory von Microsoft zu erweitern, hat Dell eindeutige OIDs (Namenserweiterungen) und eindeutig verlinkte Attribut-IDs für die Attribute und Klassen erhalten, die dem Verzeichnisdienst hinzugefügt werden.

- Dell-Erweiterung: `dell`
- Grund-OID von Dell: `1.2.840.113556.1.8000.1280`
- RACLinkID-Bereich:`12070` to `12079`

Übersicht über die Schemaerweiterungen

Dell hat das Schema um *Zuordnungs-*, *Geräte-* und *Berechtigungs*eigenschaften erweitert. Die *Zuordnungs*eigenschaft wird zur Verknüpfung der Benutzer oder Gruppen mit einem spezifischen Satz an Berechtigungen für ein oder mehrere RAC-Geräte verwendet. Dieses Modell ist unkompliziert und gibt dem Administrator höchste Flexibilität bei der Verwaltung verschiedener Benutzergruppen, RAC-Berechtigungen und RAC-Geräten im Netzwerk.

Wenn zwei CMCs im Netzwerk vorhanden sind, die Sie mit Active Directory für die Authentifizierung und Autorisierung integrieren wollen, müssen Sie mindestens ein Zuordnungsobjekt und ein RAC-Geräteobjekt für jeden CMC erstellen. Sie können verschiedene Zuordnungsobjekte erstellen, wobei jedes Zuordnungsobjekt nach Bedarf mit beliebig vielen Benutzern, Benutzergruppen oder RAC-Geräteobjekten verbunden werden kann. Die Benutzer und RAC-Geräteobjekte können Mitglieder beliebiger Domänen im Unternehmen sein.

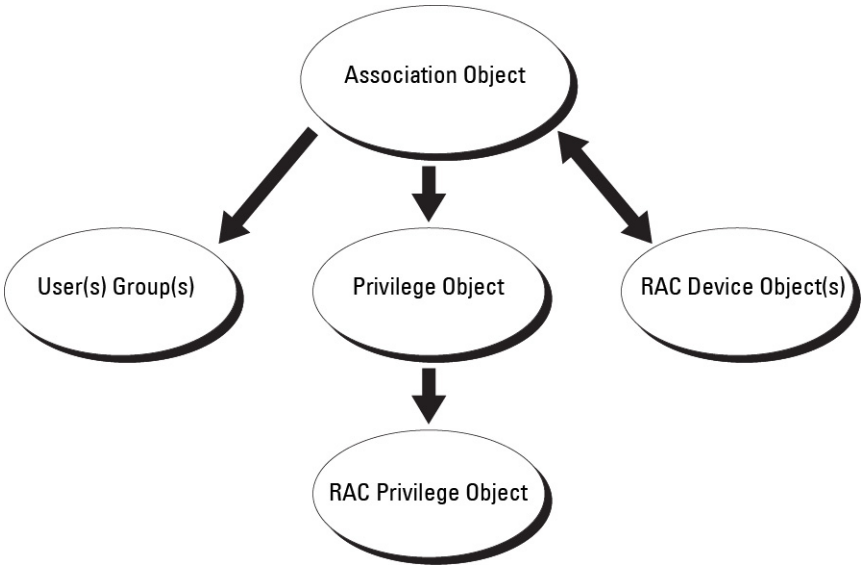
Jedes Zuordnungsobjekt darf jedoch nur mit einem Berechtigungsobjekt verbunden werden (bzw. jedes Zuordnungsobjekt kann Benutzer, Benutzergruppen oder RAC-Geräteobjekte verbinden). Dieses Beispiel ermöglicht es dem Administrator, die Berechtigungen jedes Benutzers über spezielle CMCs zu steuern.

Das RAC-Geräteobjekt ist die Verknüpfung zur RAC-Firmware für die Active Directory-Abfrage zur Authentifizierung und Autorisierung. Wenn ein RAC dem Netzwerk hinzugefügt wird, muss der Administrator den RAC und sein Geräteobjekt mit seinem Active Directory-Namen so konfigurieren, dass Benutzer Authentifizierung und Genehmigung bei Active Directory ausführen können. Der Administrator muss außerdem auch mindestens einen RAC zum Zuordnungsobjekt hinzufügen, damit Benutzer Authentifizierungen vornehmen können.

Die folgende Abbildung zeigt, dass das Zuordnungsobjekt die Verbindung bereitstellt, die für die gesamte Authentifizierung und Genehmigung erforderlich ist.

ANMERKUNG: Das RAC-Berechtigungsobjekt gilt für DRAC 4, DRAC 5 und CMC.

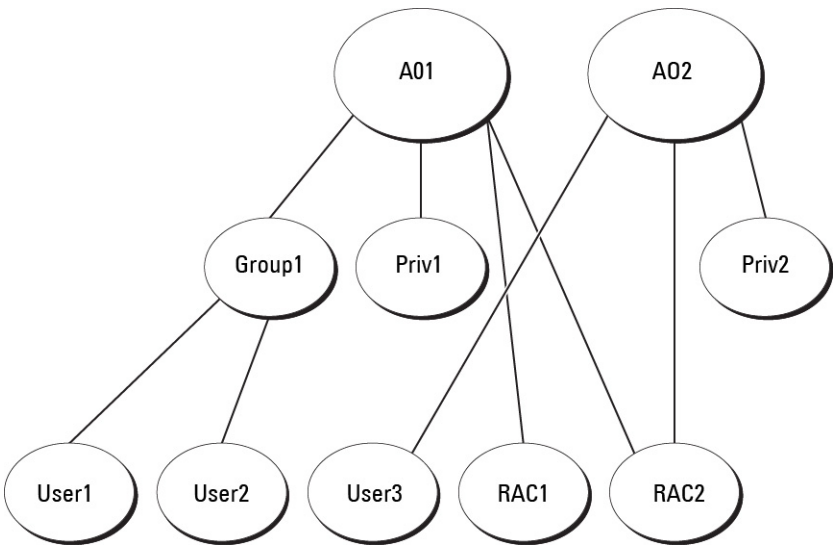
Sie können eine beliebige Anzahl an Zuordnungsobjekten erstellen. Es ist jedoch erforderlich, dass Sie mindestens ein Zuordnungsobjekt erstellen, und Sie müssen ein RAC-Geräteobjekt für jedes RAC (CMC) auf dem Netzwerk haben, das mit dem Active Directory integriert werden soll.



Das Zuordnungsobjekt lässt ebenso viele oder wenige Benutzer bzw. Gruppen und auch RAC-Geräteobjekte zu. Das Zuordnungsobjekt enthält jedoch nur ein Berechtigungsobjekt pro Zuordnungsobjekt. Das Zuordnungsobjekt verbindet die *Benutzer,* die *Berechtigungen* auf RAC- (CMC) Geräten haben.

Außerdem können Sie Active Directory-Objekte für eine einzelne Domäne oder in mehreren Domänen konfigurieren. Sie haben zum Beispiel zwei CMCs (RAC1 und RAC2) und drei vorhandene Active Directory-Benutzer (Benutzer1, Benutzer2 und Benutzer3). Sie wollen Benutzer1 und Benutzer2 eine Administratorberechtigung für beide CMCs geben und Benutzer3 eine Anmeldungsberechtigung für die RAC2-Karte. Die folgende Abbildung 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.

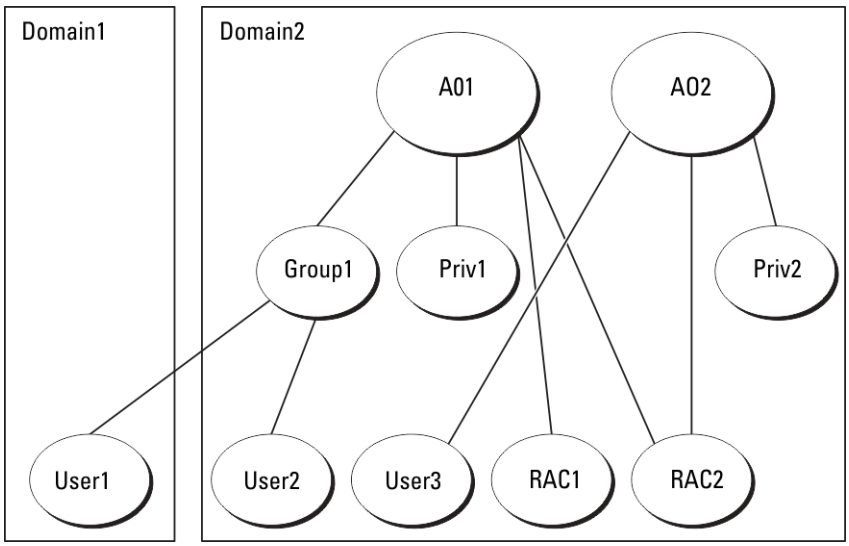


So konfigurieren Sie die Objekte für das Einzeldomänen-Szenario:

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.

Die folgende Abbildung 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 Administratorrechten für beide CMCs und Benutzer3 mit Anmeldungsberechtigungen für die RAC2-Karte.



So konfigurieren Sie die Objekte für das Mehrdomänen-Szenario:

1. Stellen Sie sicher, dass sich die Gesamtstrukturfunktion der Domäne im systemeigenen oder im Windows 2003-Modus befindet.
2. Erstellen Sie zwei Zuordnungsobjekte, A01 (mit universellem Bereich) und A02 in jeder Domäne. Die Abbildung „Active Directory-Objekte in mehreren Domänen einrichten“ zeigt die Objekte in Domäne2.
3. Erstellen Sie zwei RAC-Geräteobjekte, RAC1 und RAC2, die die zwei CMCs repräsentieren.
4. Erstellen Sie zwei Berechtigungsobjekte, Ber1 und Ber2, wobei Ber1 alle Berechtigungen (Administrator) und Ber2 Anmeldungsberechtigung hat.
5. Ordnen Sie Benutzer1 und Benutzer2 in Gruppe1 ein. Die Gruppenreichweite von Gruppe 1 muss universell sein.
6. Fügen Sie Gruppe1 als Mitglieder im Zuordnungsobjekt 1 (A01), Ber1 als Berechtigungsobjekte in A01 und RAC1, RAC2 als RAC-Geräte in A01 hinzu.
7. Fügen Sie Benutzer3 als Mitglied im Zuordnungsobjekt 2 (A02), Ber2 als Berechtigungsobjekte in A02 und RAC2 als RAC-Geräte in A02 hinzu.

Active Directory mit erweitertem Schema konfigurieren

So konfigurieren Sie Active Directory für den Zugriff auf CMC:

1. Erweitern des Active Directory-Schemas.
2. Active Directory-Benutzer und Computer-Snap-In erweitern.

3. CMC-Benutzer mit Berechtigungen zum Active Directory hinzufügen.
4. Aktivieren Sie SSL auf allen Domänen-Controllern.
5. Konfigurieren Sie die CMC Active Directory-Eigenschaften über die CMC-Web-Schnittstelle oder RACADM.

Verwandte Links

Erweitern des Active Directory-Schemas
Dell-Erweiterung zu Active Directory Benutzer- und Computer-Snap-In installieren
CMC-Benutzer und -Berechtigungen zum Active Directory hinzufügen
Active Directory mit erweitertem Schema unter Verwendung der CMC-Webschnittstelle konfigurieren
Konfiguration des Active Directory mit erweitertem Schema unter Verwendung von RACADM

Erweitern des Active Directory-Schemas

Mit der Erweiterung des Active Directory-Schemas werden eine Dell-Organisationseinheit, Schemaklassen und -attribute sowie Beispielberechtigungen und Zuordnungsobjekte zum Active Directory-Schema hinzugefügt. Bevor Sie das Schema erweitern, müssen Sie sicherstellen, dass Sie Schema-Admin-Berechtigungen auf dem Schema Master-FSMO-Rollenbesitzer (Flexible Single Master Operation) der Domänenstruktur besitzen.

Sie können das Schema mit einer der folgenden Methoden erweitern:

- Dell Schema Extender-Dienstprogramm
- LDIF-Script-Datei

Die Dell-Organisationseinheit wird dem Schema nicht hinzugefügt, wenn Sie die LDIF-Skriptdatei verwenden.

Die LDIF-Dateien und Dell Schema Extender befinden sich auf der DVD *Dell Systems Management Tools and Documentation* in den folgenden jeweiligen Verzeichnissen:

- **DVD-Laufwerk:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools \Remote_Management_Advanced\LDIF_Files**
- **<DVDdrive>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools \Remote_Management_Advanced\Schema Extender**

Lesen Sie zur Verwendung der LDIF-Dateien die Anleitungen in der Infodatei im Verzeichnis **LDIF_Files**.

Sie können Schema Extender oder die LDIF-Dateien an einem beliebigen Standort kopieren und ausführen.

Dell Schema Extender verwenden

VORSICHT: Das Dienstprogramm Dell Schema Extender verwendet die Datei SchemaExtenderOem.ini. Um sicherzustellen, dass das Dell Schema Extender-Dienstprogramm richtig funktioniert, modifizieren Sie den Namen dieser Datei nicht.

1. Klicken Sie im **Begrüßungsbildschirm** auf **Weiter**.
2. Lesen Sie die Warnung und vergewissern Sie sich, dass Sie sie verstehen und klicken Sie dann auf **Weiter**.
3. Wählen Sie **Aktuelle Anmeldeinformationen verwenden** aus, oder geben Sie einen Benutzernamen und ein Kennwort mit Schema-Administratorrechten ein.
4. Klicken Sie auf **Weiter,** um Dell Schema Extender auszuführen.
5. Klicken Sie auf **Fertig stellen**.

   Das Schema wird erweitert. Um die Schema-Erweiterung zu überprüfen, verwenden Sie die Microsoft-Verwaltungskonsole (MMC) und das Active Directory-Schema-Snap-In, um zu prüfen, ob Klassen und Attribute vorhanden sind. Weitere Informationen zu Klassen und Attribute finden Sie in Klassen und Attribute. Näheres zur Benutzung der Verwaltungskonsole (MMC) und des Active Directory-Schema-Snap-In finden Sie in der Microsoft-Dokumentation.

Klassen und Attribute

Tabelle 19. : Klassendefinitionen für Klassen, die zum Active Directory-Schema hinzugefügt wurden

Klassenname	Zugewiesene Objekt-Identifikationsnummer (OID)
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Tabelle 20. : dellRacDevice Class

OID	1.2.840.113556.1.8000.1280.1.7.1.1
Beschreibung	Repräsentiert das Dell RAC-Gerät. Das RAC muss im Active Directory als delliDRACDevice konfiguriert sein. Mit dieser Konfiguration kann der CMC Lightweight Directory Access Protocol (LDAP)-Abfragen an das Active Directory senden.
Klassentyp	Strukturklasse
SuperClasses	dellProduct
Attribute	dellSchemaVersion dellRacType

Tabelle 21. : delliDRACAssociationObject Class

OID	1.2.840.113556.1.8000.1280.1.7.1.2
Beschreibung	Repräsentiert das Dell-Zuordnungsobjekt. Das Zuordnungsobjekt ist die Verbindung zwischen Benutzern und Geräten.
Klassentyp	Strukturklasse
SuperClasses	Gruppe
Attribute	dellProductMembers dellPrivilegeMember

Tabelle 22. : dellRAC4Privileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Beschreibung	Definiert die Berechtigungen (Autorisierungsrechte) für das CMC-Gerät.
Klassentyp	Erweiterungsklasse
SuperClasses	Keine
Attribute	dellIsLoginUser dellIsCardConfigAdmin

OID	1.2.840.113556.1.8000.1280.1.1.1.3
	dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsTestAlertUser dellIsDebugCommandAdmin dellPermissionMask1 dellPermissionMask2

Tabelle 23. : dellPrivileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Beschreibung	Wird als Container-Klasse für die Dell-Berechtigungen (Autorisierungsrechte) verwendet.
Klassentyp	Strukturklasse
SuperClasses	Benutzer
Attribute	dellRAC4Privileges

Tabelle 24. : 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 25. : Liste von Attributen, die dem Active Directory-Schema hinzugefügt wurden

Zugewiesener OID/Syntax-Objektkennzeichner	Einzelbewertung
Attribut: `dellPrivilegeMember` **Beschreibung:** Liste mit `dellPrivilege`-Objekten, die zu diesem Attribut gehören. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.1 **Eindeutiger Name**: (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
Attribut: `dellProductMembers` **Beschreibung**: Die Liste von `dellRacDevices`-Objekten, die zu dieser Funktion gehören. Dieses Attribut ist die Vorwärtsverbindung zur `dellAssociationMembers`-Rückwärtsverbindung. **Link-ID**: 12070 **OID:** 1.2.840.113556.1.8000.1280.1.1.2.2 **Eindeutiger Name**: (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

Zugewiesener OID/Syntax-Objektkennzeichner	Einzelbewertung
Attribut: `dellIsCardConfigAdmin` **Beschreibung**: TRUE, wenn der Benutzer Kartenkonfigurationsrechte auf dem Gerät hat. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.4 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut: `dellIsLoginUser` **Beschreibung**: TRUE, wenn der Benutzer Anmeldungsrechte auf dem Gerät hat. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.3 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut: `dellIsUserConfigAdmin` **Beschreibung**: TRUE, wenn der Benutzer Benutzerkonfigurationsrechte auf dem Gerät hat. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.5 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
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 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut: `dellIsServerResetUser` **Beschreibung**: TRUE, wenn der Benutzer Server-Reset-Rechte auf dem Gerät hat. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.7 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut: `dellIsTestAlertUser` **Beschreibung**: TRUE, wenn der Benutzerrechte für Warnungstests für Benutzer auf dem Gerät hat. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.10 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut: `dellIsDebugCommandAdmin` **Beschreibung**: TRUE, wenn der Benutzer Debug-Befehlsadministratorenrechte auf dem Gerät hat. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.11 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut: `dellSchemaVersion` **Beschreibung**: Die aktuelle Schemaversion wird verwendet, um das Schema zu aktualisieren.	TRUE

Zugewiesener OID/Syntax-Objektkennzeichner	Einzelbewertung
OID: 1.2.840.113556.1.8000.1280.1.1.2.12 Zeichenfolge zum Ignorieren von Groß-/Kleinschreibung (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	
Attribut: `dellRacType` **Beschreibung**: Dieses Attribut ist der aktuelle RAC-Typ für das DellRacDevice-Objekt und die Rückwärtsverknüpfung zur Vorwärtsverknüpfung von dellAssociationObjectMembers. **OID**: 1.2.840.113556.1.8000.1280.1.1.2.13 Zeichenfolge zum Ignorieren von Groß-/Kleinschreibung (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
Attribut: `dellAssociationMembers` **Beschreibung**: Liste der dellAssociationObjectMembers, die zu diesem Produkt gehören. Dieses Attribut ist die Rückwärtsverbindung zum Attribut dellProductMembers. **Link-ID**: 12071 **OID**: 1.2.840.113556.1.8000.1280.1.1.2.14 Eindeutiger Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
Attribut: `dellPermissionsMask1` **OID**: 1.2.840.113556.1.8000.1280.1.6.2.1 Integer (LDAPTYPE_INTEGER)	
Attribut: `dellPermissionsMask2` **OID**: 1.2.840.113556.1.8000.1280.1.6.2.2 Integer (LDAPTYPE_INTEGER)	

Dell-Erweiterung zu Active Directory Benutzer- und Computer-Snap-In installieren

Wenn Sie das Schema im Active Directory erweitern, müssen Sie auch die Active Directory-Benutzer und das Computer-Snap-In erweitern, sodass der Administrator RAC-Geräte (CMC), Benutzer und Benutzergruppen, RAC-Zuordnungen und RAC-Berechtigungen verwalten kann.

Wenn Sie die Systems Management Software mit der DVD *Dell Systems Management Tools and Documentation* installieren, können Sie das Snap-In erweitern, indem Sie während des Installationsverfahrens die Option **Snap-In von Active Directory-Benutzern und -Computern** auswählen. Das *Schnellinstallationshandbuch zu Dell OpenManage-Software* enthält zusätzliche Anleitungen zur Installation von Systemverwaltungssoftware. Die Snap-In-Installation für 64-Bit-Versionen von Windows-Betriebssystemen finden Sie unter: **<DVLaufwerk>:\SYSMGMT\ManagementStation \support\OMActiveDirectory_SnapIn64**

Weitere Informationen über Active Directory-Benutzer- und -Computer-Snap-In finden Sie in der Microsoft-Dokumentation.

CMC-Benutzer und -Berechtigungen zum Active Directory hinzufügen

Mit dem von Dell erweiterten Active Directory-Benutzer- und -Computer-Snap-In können Sie CMC-Benutzer und -Berechtigungen hinzuzufügen, indem Sie RAC-Gerät-, Zuordnungs- und Berechtigungsobjekte erstellen. Um die einzelnen Objekte hinzuzufügen, führen Sie folgende Verfahren durch:

- RAC-Geräteobjekt erstellen
- Erstellen eines Berechtigungsobjekts
- Erstellen eines Zuordnungsobjekts
- Einem Zuordnungsobjekt Objekte hinzufügen

Verwandte Links

RAC-Geräteobjekt erstellen

So erstellen Sie ein RAC-Geräteobjekt:

1. Klicken Sie im Fenster **Console Root (MCC)** mit der rechten Maustaste auf einen Container.
2. Wählen Sie **Neu** → **?Dell Remote Management Object Advanced**. Das Fenster **Neues Objekt** wird angezeigt.
3. Geben Sie einen Namen für das neue Objekt ein. Der Name muss mit dem CMC-Namen übereinstimmen, den Sie in „Active Directory mit erweitertem Schema unter Verwendung der iDRAC6-Webschnittstelle“ eingeben.
4. Wählen Sie **RAC-Geräteobjekt** und klicken Sie auf **OK**.

Berechtigungsobjekt erstellen

So erstellen Sie ein Berechtigungsobjekt:

ANMERKUNG: Sie müssen ein Berechtigungsobjekt in der gleichen Domäne erstellen, in der auch das verknüpfte Zuordnungsobjekt vorhanden ist.

1. Klicken Sie im Fenster **Console Root (MMC)** mit der rechten Maustaste auf einen Container.
2. Wählen Sie **Neu** → **Dell Remote Management Object Advanced**. 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 die Registerkarte **RAC-Berechtigungen** um einem Benutzer oder einer Gruppe Berechtigungen zuzuweisen. Weitere Informationen über CMC-Benutzerberechtigungen finden Sie unter Typen von Benutzern.

Zuordnungsobjekt erstellen

Das Zuordnungsobjekt wird von einer Gruppe abgeleitet und muss einen Gruppentyp enthalten. Die Zuordnungsreichweite legt den Sicherheitsgruppentyp für das Zuordnungsobjekt fest. Wenn Sie ein Zuordnungsobjekt erstellen, müssen Sie die Zuordnungsreichweite wählen, die auf den Typ von Objekten zutrifft, die Sie hinzufügen wollen. Wird z. B. Universal ausgewählt, bedeutet dies, dass Zuordnungsobjekte nur verfügbar sind, wenn die Active Directory-Domäne im systemspezifischen Modus oder einem höheren Modus funktioniert.

So erstellen Sie ein Zuordnungsobjekt:

1. Klicken Sie im Fenster **Console Root (MMC)** mit der rechten Maustaste auf einen Container.
2. Wählen Sie **Neu** → **Dell Remote Management Object Advanced**. Hierdurch wird das Fenster **Neues Objekt** geöffnet.
3. Geben Sie einen Namen für das neue Objekt ein, und wählen Sie **Zuordnungsobjekt** aus.
4. Wählen Sie den Bereich für das **Zuordnungsobjekt** und klicken Sie auf **OK**.

Objekte zu einem Zuordnungsobjekt hinzufügen

Durch die Verwendung des Fensters **Zuordnungsobjekt-Eigenschaften** können Sie Benutzer oder Benutzergruppen, Berechtigungsobjekte und RAC-Geräte oder RAC-Gerätegruppen zuordnen. Wenn 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.

Verwandte Links

Benutzer oder Benutzergruppen hinzufügen
Berechtigungen hinzufügen
RAC-Geräte oder RAC-Gerätegruppen hinzufügen

Benutzer oder Benutzergruppen hinzufügen

So fügen Sie Benutzer oder Benutzergruppen hinzu:

1. Klicken Sie mit der rechten Maustaste auf das **Zuordnungsobjekt** und wählen Sie **Eigenschaften** aus.
2. Wählen Sie das Register **Benutzer** und klicken Sie auf **Hinzufügen.**
3. Geben Sie den Namen des Benutzers oder der Benutzergruppe ein und klicken Sie auf **OK**.

Berechtigungen hinzufügen

So fügen Sie Berechtigungen hinzu:

1. Wählen Sie das Register **Berechtigungsobjekt** und klicken Sie auf **Hinzufügen.**
2. Geben Sie den Namen des Berechtigungsobjekts ein und klicken Sie auf **OK**.
   Klicken Sie auf das Register **Berechtigungsobjekt**, um das Berechtigungsobjekt der Zuordnung hinzuzufügen, welche die Berechtigungen des Benutzers bzw. der Benutzergruppe bei Authentifizierung eines RAC-Geräts definiert. Einem Zuordnungsobjekt kann nur ein Berechtigungsobjekt hinzugefügt werden.

RAC-Geräte oder RAC-Gerätegruppen hinzufügen

Um RAC-Geräte oder RAC-Gerätegruppen hinzufügen:

1. Wählen Sie die Registerkarte **Produkte** und klicken Sie auf **Hinzufügen**.
2. Geben Sie die Namen der RAC-Geräte oder RAC-Gerätegruppen ein und klicken Sie auf **OK**.
3. Im Fenster **Eigenschaften** klicken Sie auf **Anwenden** und dann auf **OK**.
   Klicken Sie auf das Register **Produkte**, um der Zuordnung ein oder mehrere RAC-Geräte hinzuzufügen. Die zugeordneten Geräte geben die an das Netzwerk angeschlossenen RAC-Geräte an, die für die festgelegten Benutzer oder Benutzergruppen verfügbar sind. Einem Zuordnungsobjekt können mehrere RAC-Geräte hinzugefügt werden.

Active Directory mit erweitertem Schema unter Verwendung der CMC-Webschnittstelle konfigurieren

So konfigurieren Sie Active Directory mit erweitertem Schema über die Web-Schnittstelle:

ANMERKUNG: Weitere Informationen zu den verschiedenen Feldern finden Sie in der *CMC-Online-Hilfe*.

1. Wählen Sie in der Systemstruktur **Gehäuse-Übersicht** aus und klicken Sie auf **Benutzerauthentifizierung** → **Verzeichnisdienste**?.
2. Wählen Sie **Microsoft Active Directory (Erweitertes Schema)** aus. Die für erweitertes Schema zu konfigurierenden Einstellungen werden auf der gleichen Seite angezeigt.
3. Geben Sie Folgendes an:
   - Aktivieren Sie Active Directory, geben Sie den Root-Domänennamen und den Zeitüberschreitungswert ein.
   - Wenn der gezielte Aufruf den Domänen-Controller und den globalen Katalog durchsuchen soll, wählen Sie die Option **AD-Server für Suche durchsuchen (optional)** aus und legen Sie die Details für den Domänen-Controller und den globalen Katalog fest.

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

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

ANMERKUNG: Domänen-Controller und Server des globalen Katalogs, die nicht korrekt für alle Domänen und Anwendungen konfiguriert sind, können zu unerwarteten Ergebnissen bei der Funktionsweise der vorhandenen Anwendungen/Domänen führen.

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

   ANMERKUNG: Sie müssen Ihre Einstellungen anwenden, bevor Sie fortfahren. Wenn Sie die Einstellungen nicht anwenden, verlieren Sie die eingegebenen Einstellungen, wenn Sie zur nächsten Seite wechseln.

5. Im Abschnitt **Erweiterte Schemaeinstellungen** geben Sie den CMC-Gerätenamen und den Domänennamen ein.
6. Falls Sie die Zertifikatsvalidierung aktiviert haben, müssen Sie das von der Zertifizierungsstelle signierte Root-Zertifikat der Domänengesamtstruktur auf den CMC hochladen. Geben Sie im Abschnitt **Zertifikate verwalten** den Dateipfad des Zertifikats ein oder suchen Sie nach der Zertifikatsdatei. Klicken Sie auf **Hochladen**, um die Datei auf den CMC hochzuladen.

   ANMERKUNG: Der Wert `Dateipfad` zeigt den relativen Dateipfad des Zertifikats an, das Sie hochladen. Sie müssen den absoluten Dateipfad eingeben, der den vollständigen Pfad und den vollständigen Dateinamen sowie die Dateierweiterung enthält.

   Die SSL-Zertifikate für die Domänen-Controller müssen von dem von der root-Zertifizierungsstelle signierten Zertifikat signiert werden. Das von der Root-Zertifizierungsstelle signierte Zertifikat muss auf der Management Station verfügbar sein, die auf den CMC zugreift.

   VORSICHT: Die SSL-Zertifikatüberprüfung ist standardmäßig erforderlich. Das Deaktivieren dieses Zertifikats ist mit Risiken verbunden.

7. Falls Sie die Option „Einmalige Anmeldung" (Single Sign-On, SSO) aktiviert haben, klicken Sie im Abschnitt „Kerberos-Keytab" auf **Durchsuchen**, geben Sie die Keytab-Datei an, und klicken Sie auf **Hochladen**. Wenn der Vorgang beendet ist, wird ein Meldungsfenster eingeblendet, das anzeigt, ob der Upload erfolgreich oder fehlerhaft war.
8. Klicken Sie auf **Anwenden**. Der CMC-Webserver startet automatisch neu, wenn Sie auf **Anwenden** klicken.
9. Melden Sie sich bei der CMC-Web-Schnittstelle an.
10. Wählen Sie in der Systemstruktur **Gehäuse** aus, klicken Sie auf das Register **Netzwerk** und klicken Sie anschließend auf die Unterregisterkarte **Netzwerk**. Die Seite **Netzwerkkonfiguration** wird angezeigt.
11. Wenn **DHCP verwenden** für Netzwerkschnittstellen-IP-Adresse aktiviert ist, wählen Sie eine der folgenden Vorgehensweisen aus:

    – Wählen Sie **DHCP zum Abrufen von DNS-Serveradressen verwenden** aus, um die DNS-Server-Adressen zu aktivieren, die automatisch vom DHCP-Server abgerufen werden sollen.

    – Konfigurieren Sie manuell eine DNS-Server-IP-Adresse, indem Sie das Kontrollkästchen **DHCP zum Abrufen von DNS-Serveradressen verwenden** frei lassen und dann die IP-Adresse des primären und des alternativen DNS-Servers in die entsprechenden Felder eingeben.

12. Klicken Sie auf **Änderungen anwenden**. Die Active Directory-Einstellungen für das erweiterte Schema sind konfiguriert.

Konfiguration des Active Directory mit erweitertem Schema unter Verwendung von RACADM

So konfigurieren Sie das CMC Active Directory mit erweitertem Schema unter Verwendung von RACADM:

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  <vollständig qualifizierter CMC-Domänenname> racadm config -
   g cfgActiveDirectory -o cfgADRootDomain <vollständig qualifizierter root-
   ```

```
Domänenname> racadm config -g cfgActiveDirectory -o cfgADRacName <CMC
allgemeiner Name> racadm sslcertupload -t 0x2 -f <ADS-root-CA-Zertifikat> -
r racadm sslcertdownload -t 0x1 -f <CMC-SSL-Zertifikat>
```

ANMERKUNG: Sie können diesen Befehl nur über Remote-RACADM verwenden. Weitere Informationen zum Remote-RACADM finden Sie unter *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC*.

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 cfgADDomainController <AD-Domänen-
Controller-IP-Adresse>
```

Um einen Server anzugeben, der den globalen Katalog enthält, geben Sie Folgendes ein:

```
racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog <AD-IP-Adresse
des globalen Katalogs>
```

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 <primäre DNS-IP-Adresse>
     racadm config -g cfgLanNetworking -o cfgDNSServer2 <sekundäre DNS-IP-
     Adresse>
     ```

   Die Funktionskonfiguration des erweiterten Schemas ist abgeschlossen.

Generische LDAP-Benutzer konfigurieren

CMC bietet eine allgemeine Lösung zur Unterstützung LDAP-basierter Authentifizierung (Lightweight Directory Access Protocol). Für diese Funktion ist auf Ihren Verzeichnisdiensten keine Schemaeweiterung erforderlich.

Ein CMC-Administrator kann nun die LDAP-Server-Benutzeranmeldungen in den CMC integrieren. Diese Integration erfordert die Konfiguration sowohl des LDAP-Servers wie auch des CMC. Auf der Seite des LDAP-Servers wird ein

Standardgruppenobjekt als Rollengruppe verwendet. Ein Benutzer, der Zugang zum CMC hat, wird ein Mitglied der Rollengruppe. Berechtigungen sind weiterhin auf dem CMC für die Authentifizierung gespeichert, ähnlich wie bei der Standardschema-Einrichtung mit Active Directory-Unterstützung.

Damit der LDAP-Benutzer auf eine bestimmte CMC-Karte zugreifen kann, müssen der Rollengruppenname und dessen Domänenname auf der spezifischen CMC-Karte konfiguriert werden. Sie können maximal fünf Rollengruppen für jeden CMC konfigurieren. Ein Benutzer hat die Möglichkeit, zu mehreren Gruppen innerhalb des Verzeichnisdienstes hinzugefügt zu werden. Wenn der Benutzer ein Mitglied mehrerer Gruppen ist, dann erhält der Benutzer die Berechtigungen aller dieser Gruppen.

Für Informationen über Zugriffsebene der Rollengruppen und die standardmäßigen Einstellungen der Rollengruppen, gehen Sie zu Typen von Benutzern.

Die folgende Abbildung zeigt die CMC-Konfiguration bei allgemeinem LDAP.

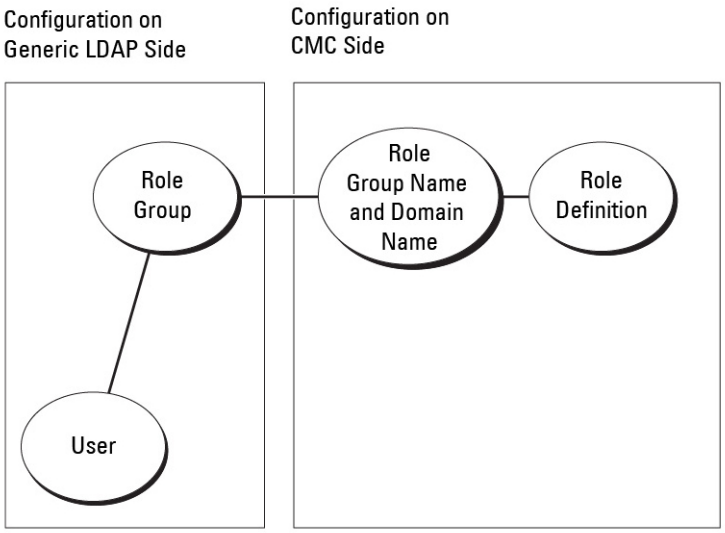


Abbildung 2. CMC-Konfiguration bei allgemeinem LDAP

Allgemeines LDAP-Verzeichnis für Zugriff auf CMC konfigurieren

Die allgemeine LDAP-Implementierung des CMC verwendet zwei Phasen, um einem Benutzer Zugriff zu gewähren – Benutzerauthentifizierung und dann Benutzerautorisierung.

Authentifizierung von LDAP-Benutzern

Manche Verzeichnisserver erfordern eine Bindung, bevor eine Suche auf einem spezifischen LDAP-Server durchgeführt werden kann.

So authentifizieren Sie einen Benutzer:

1. Optionale Bindung zum Verzeichnisdienst. Standard ist die anonyme Bindung.
2. Suche nach dem Benutzer auf Basis von dessen Benutzeranmeldung. Das Standardattribut ist `uid`.
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, ist der Benutzer authentifiziert.

Autorisierung von LDAP-Benutzern

So autorisieren Sie einen Benutzer:

1. Durchsuchen Sie alle konfigurierten Gruppen nach dem Domänenname des Benutzers und zwar innerhalb der Attribute `member bzw. uniqueMember`. Ein Administrator kann dieses Feld konfigurieren.
2. Hinzufügen der Berechtigungen für jede Gruppe, der der Benutzer als Mitglied angehört.

Konfiguration des allgemeinen LDAP-Verzeichnisdienstes mit der CMC-Webschnittstelle

So konfigurieren Sie den generischen LDAP-Verzeichnisdienst über die Web-Schnittstelle:

ANMERKUNG: Sie müssen die Berechtigung als **Gehäusekonfiguration-Administrator** besitzen.

1. Klicken Sie in der Systemstruktur auf **Gehäuse-Übersicht**, und dann auf **Benutzerauthentifizierung** → **Verzeichnisdienste**?.
2. Wählen Sie generisches **LDAP** aus. Die Einstellungen, die für Standardschema konfiguriert werden sollen, werden auf derselben Seite angezeigt.
3. Geben Sie Folgendes an:

   ANMERKUNG: Weitere Informationen zu den verschiedenen Feldern finden Sie in der *CMC-Online-Hilfe*.

   - Allgemeine Einstellungen
   - Für LDAP zu verwendenden Server:
     * Statischer Server – Geben Sie den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse und die LDAP-Schnittstellennummer ein.
     * DNS-Server – Geben Sie den DNS-Server an, um eine Liste von LDAP-Servern durch Suchen nach deren SRV-Einträgen im DNS abzurufen.

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

       `_[Dienstname]._tcp.[Suchdomäne]`

       wobei `<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.
4. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

   ANMERKUNG: Sie müssen die 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.
5. Klicken Sie im Abschnitt **Gruppeneinstellungen** auf eine **Rollengruppe.** Die Seite **LDAP-Rollengruppe konfigurieren** wird angezeigt.
6. Geben Sie den Gruppendomänenname und die Rollengruppen-Berechtigungen ein.
7. Klicken Sie auf **Anwenden**, um die Einstellungen der Rollengruppe zu speichern, Klicken Sie auf **Zurück zur Seite Konfiguration**, und dann wählen Sie **Generisches LDAP**.
8. Wenn Sie **Überprüfung des Zertifikats aktiviert** gewählt haben, geben Sie das CA-Zertifikat im Abschnitt **Zertifikate verwalten** an, um das LDAP-Serverzertifikat während des Secure Socket Layer (SSL)-Handshake zu validieren. Klicken Sie auf **Hochladen**. Das Zertifikat wird auf den CMC heraufgeladen und weitere Details werden angezeigt.
9. Klicken Sie auf **Anwenden**. Der generische LDAP-Verzeichnisdienst ist damit konfiguriert.

Konfiguration des allgemeinen LDAP-Verzeichnisdienstes mittels RACADM

Um den LDAP-Verzeichnisdienst zu konfigurieren, verwenden Sie die Objekte in `cfgLdap` und `cfgLdapRoleGroup` RACADM-Gruppen.

Es gibt viele Möglichkeiten zur Konfiguration von LDAP-Anmeldungen. Meistens können einige Optionen in der Standardeinstellung verwendet werden.

ANMERKUNG: Wir empfehlen dringend die Verwendung des Befehls racadm `testfeature -f LDAP`, um die LDAP-Einstellungen bei Ersteinrichtungen zu testen. Diese Funktion unterstützt sowohl IPv4 wie auch IPv6.

Die erforderlichen Eigenschaftenänderungen sind zum Beispiel die Aktivierung von LDAP-Anmeldungen, die Einstellung des Server-FQDN oder der -IP und die Konfiguration der Base-DN des LDAP-Servers.

- `$ racadm config -g cfgLDAP -o cfgLDAPEnable 1`
- `$ racadm config -g cfgLDAP -o cfgLDAPServer 192,168.0,1`
- `$ racadm config -g cfgLDAP -o cfgLDAPBaseDN dc= company,dc=com`

Der CMC kann so konfiguriert werden, dass er optional einen DNS-Server auf SRV-Einträge abfragt. Falls die Eigenschaft `cfgLDAPSRVLookupEnable` aktiviert ist, wird die Eigenschaft `cfgLDAPServer` ignoriert. Die folgende Abfrage wird für die Suche nach SRV-Einträgen im DNS verwendet:

`_ldap._tcp.domainname.com`

`ldap` in der obigen Abfrage ist die Eigenschaft `cfgLDAPSRVLookupServiceName`.

`cfgLDAPSRVLookupDomainName` ist als **domainname.com** konfiguriert.

Weitere Informationen zu RACADM-Objekten finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC*, das unter **dell.com/support/manuals** verfügbar ist.

10

CMC für die einfache Anmeldung oder Smart Card-Anmeldung konfigurieren

Dieser Abschnitt enthält Informationen zum Konfigurieren von CMC für die Smart Card-Anmeldung sowie für die einfache Anmeldung (Single Sign-On, SSO) von Active Directory-Benutzern.

Beginnend mit CMC Version 2.10 unterstützt CMC Kerberos-basierte Active Directory-Authentifizierung zum Unterstützen von Smart Card- und -SSO-Anmeldungen.

SSO verwendet Kerberos als Authentifizierungsmethode, die Benutzern, die sich bei der Domäne angemeldet haben, automatische oder einfache Anmeldung für nachfolgende Anwendungen wie Exchange ermöglicht. Bei der einfachen Anmeldung verwendet der CMC die Anmeldeinformationen des Clientsystems, die im Betriebssystem zwischengespeichert werden, nachdem Sie sich mit einem gültigen Active Directory-Konto angemeldet haben.

Die Zweifaktor-Authentifizierung bietet eine höhere Sicherheitsstufe, indem Benutzer aufgefordert werden, ein Kennwort oder eine PIN sowie eine physische Karte mit einem privaten Schlüssel oder einem digitalen Zertifikat bereitzustellen. Kerberos verwendet diesen Zweifaktor-Authentifizierungsmechanismus und ermöglicht es Systemen, ihre Authentizität zu beweisen.

ANMERKUNG: Die Auswahl einer Anmeldemethode legt keine Richtlinienattribute hinsichtlich anderer Anmeldeschnittstellen, z. B. SSH, fest. Sie müssen auch sonstige Richtlinienattribute für andere Anmeldeschnittstellen festlegen. Falls Sie alle anderen Anmeldeschnittstellen deaktivieren möchten, navigieren Sie zur Seite **Dienste** und deaktivieren Sie alle (oder bestimmte) Anmeldeschnittstellen.

Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7 und Windows Server 2008 können Kerberos als Authentifizierungsmethode für SSO- und Smart Card-Anmeldung verwenden.

Weitere Informationen über Kerberos finden Sie auf der Microsoft-Website.

Verwandte Links

Systemanforderungen
Vorbedingungen für die einfache Anmeldung oder Smart Card-Anmeldung
CMC SSO oder Smart Card-Anmeldung für Active Directory-Benutzer konfigurieren

Systemanforderungen

Zur 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 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 Dienstprogramm fehlerhafte Keytab-Dateien.

  Windows6.0-KB957072-x86.msu für Verwendung von GSS_API- und SSL-Transaktionen während einer LDAP-Bindung.
- Kerberos-Schlüsselverteilungscenter – KDC (mit der Active Directory-Serversoftware)

- DHCP-Server (empfohlen).
- Die DNS-Server-Reverse-Zone muss einen Eintrag für den Active Directory-Server und den CMC enthalten.

Client-Systeme

- Für reine Smart Card-Anmeldung muss das Clientsystem die verteilbare Komponente von Microsoft Visual C++ 2005 enthalten. Weitere Informationen finden Sie unter **www.microsoft.com/downloads/details.aspx?FamilyID=32BC1BEEA3F9-4C13-9C99-220B62A191EE&displaylang=en**
- Für einfache Anmeldung oder Smart Card-Anmeldung muss das Clientsystem ein Teil der Active Directory-Domäne und des Kerberos-Bereichs sein.

CMC

- 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.

Vorbedingungen für die einfache Anmeldung oder Smart Card-Anmeldung

Die Voraussetzungen für die Konfiguration der SSO- oder Smart Card-Anmeldungen lauten wie folgt:

- Einrichtung des Kerberos-Bereichs und Key Distribution Centers (KDC)) für Active Directory (ksetup).
- Gewährleisten Sie eine robuste NTP- und DNS-Infrastruktur zur Vermeidung von Problemen mit Clock-Drift und Reverse-Lookup.
- Konfiguration des CMC mit der Standardschema-Rollengruppe mit autorisierten Mitgliedern.
- Erstellen Sie für Smart Card „Active Directory-Benutzer" für jeden CMC und konfigurieren Sie Kerberos-DES-Verschlüsselung, jedoch nicht Vorauthentifizierung.
- Browser für SSO oder Smart Card-Anmeldung konfigurieren
- Registrieren Sie die CMC-Benutzer mit Ktpass beim Schlüsselverteilungscenter (dies erzeugt auch einen Schlüssel zum Hochladen auf den CMC).

Verwandte Links

Active Directory-Standardschema konfigurieren
Active Directory mit erweitertem Schema konfigurieren
Browser für SSO-Anmeldung konfigurieren
Kerberos Keytab-Datei generieren
Browser für Smart Card-Anmeldung konfigurieren

Kerberos Keytab-Datei generieren

Zur Unterstützung der SSO- und Smart Card-Anmeldungs-Authentifizierung unterstützt CMC das Windows-Kerberos-Netzwerk. Mit dem ktpass-Hilfsprogramm (wird von Microsoft als Teil der Server-Installations-CD/DVD bereitgestellt) werden die Bindungen des Dienstprinzipalnamens (SPN =Service Principal Name) zu einem Benutzerkonto erstellt und die Vertrauensinformationen in eine MIT-artige Kerberos-Keytab-Datei exportiert. Weitere Informationen zum Dienstprogramm ktpass finden Sie auf der Microsoft-Website.

Sie müssen vor dem Erstellen einer Keytab-Datei ein Active Directory-Benutzerkonto zur Benutzung mit der Option **-mapuser** des Befehls ktpass einrichten. Außerdem müssen Sie denselben Namen verwenden wie den CMC-DNS-Namen, zu dem Sie die erstellte Keytab-Datei hochladen.

So generieren Sie eine Keytab-Datei mithilfe des ktpass-Tools:

1. Führen Sie das Dienstprogramm *ktpass* auf dem Domänen-Controller (Active Directory-Server) aus, auf dem Sie den CMC einem Benutzerkonto in Active Directory zuordnen möchten.
2. Verwenden Sie den folgenden `ktpass`-Befehl, um die Kerberos-Keytab-Datei zu erstellen:

   ```
   C:\>ktpass -princ HTTP/cmcname.domain_name.com@REALM_NAME.COM - mapuser
   dracname -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -pass * -out c:
   \krbkeytab
   ```

   ANMERKUNG: Der `cmcname.domainname.com` muss gemäß RFC in Kleinbuchstaben und der `@REALM_NAME` muss in Großbuchstaben angegeben werden. Darüber hinaus unterstützt der CMC den DES-CBC-MD5-Typ von Kryptographie für Kerberos-Authentifizierung.

   Dieses Verfahren erstellt eine Keytab-Datei, die Sie zum CMC hochladen müssen.

   ANMERKUNG: Das Keytab enthält einen Verschlüsselungsschlüssel und muss an einem sicheren Ort aufbewahrt werden. Weitere Informationen zum Dienstprogramm *ktpass* finden Sie auf der **Microsoft**-Website.

Konfigurieren des CMC für das Active Directory-Schema

Weitere Informationen über die Konfiguration des CMC für das Active Directory-Standardschema finden Sie unter Active Directory-Standardschema konfigurieren.

Weitere Informationen über die Konfiguration des CMC für Erweitertes Schema für Active Directory, finden Sie unter Übersicht des Active Directory mit erweitertem Schema.

Browser für SSO-Anmeldung konfigurieren

Einfache Anmeldung (SSO) wird von Internet Explorer Version 6.0 und 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 **Das kann Ihre Garantie ungültig machen** anzeigt, klicken Sie auf **I'll be careful. I promise.**
2. Im Textfeld **Filter** geben Sie **negotiate** (verhandeln) ein.

   Der Browser zeigt eine Liste bevorzugter Namen an, die alle das Wort „negotiate“ enthalten.
3. Doppelklicken Sie in der Liste auf **network.negotiate-auth.trusted-uris**.
4. Geben Sie im Dialogfeld **Enter string value** (Zeichenfolgewert eingeben) den Domänennamen des CMC ein und klicken Sie auf **OK**.

Browser für Smart Card-Anmeldung konfigurieren

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.

CMC SSO oder Smart Card-Anmeldung für Active Directory-Benutzer konfigurieren

Sie können die CMC-Webschnittstelle oder RACADM zum konfigurieren von CMC SSO oder Smart Card-Anmeldung benutzen.

Verwandte Links

[Vorbedingungen für die einfache Anmeldung oder Smart Card-Anmeldung]
[Keytab-Datei hochladen]

Konfiguration der CMC SSO- oder Smart Card-Anmeldung für Active Directory-Benutzer über die Webschnittstelle

So konfigurieren Sie Active Directory SSO- oder Smart Card-Anmeldung für CMC:

ANMERKUNG: Weitere Informationen zu den verfügbaren Optionen finden Sie in der *CMC-Online-Hilfe*.

1. Führen Sie beim Konfigurieren von Active Directory zum Einstellen des Benutzerkontos die folgenden zusätzlichen Schritte aus:
   - Laden Sie die Keytab-Datei hoch
   - Um SSO (Single Sign-On) zu aktivieren, wählen Sie die Option **Einfache Anmeldung aktivieren** aus.
   - Um Smart Card-Anmeldung zu aktivieren, wählen Sie die Option **Smart-Card-Anmeldung aktivieren** aus.

     ANMERKUNG: Alle bandexternen Befehlszeilenschnittstellen, einschließlich Secure Shell (SSH), Telnet, Seriell und Remote-RACADM, bleiben für diese Option unverändert.
2. Klicken Sie auf **Anwenden**.

   Die Einstellungen werden gespeichert.

   Sie können das Active Directory mit Kerberos-Authentifizierung testen, indem Sie den RACADM-Befehl verwenden:

   ```
   testfeature -f adkrb -u <Benutzer>@<Domäne>
   ```

   wobei `<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 erneut ausführen. Weitere Informationen finden Sie unter *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC* auf **dell.com/support/manuals**.

Keytab-Datei hochladen

Die Kerberos-Keytab-Datei liefert die CMC-Benutzername-Kennwort-Anmeldeinformationen für das KDC (Kerberos Data Center), das wiederum Zugriff auf das Active Directory ermöglicht. Jeder CMC im Kerberos-Bereich muss beim Active Directory registriert sein und eine eindeutige Keytab-Datei aufweisen.

Sie können einen Kerberos-Keytab hochladen, der auf dem zugeordneten Active Directory-Server erstellt wurde. Sie können die Kerberos-Keytab-Datei vom Active Directory-Server aus erzeugen, indem Sie das Dienstprogramm **ktpass.exe** ausführen. Diese Keytab-Datei stellt eine Vertrauensstellung zwischen dem Active Directory-Server und dem CMC her.

So laden Sie die Keytab-Datei hoch:

1. Wählen Sie in der Systemstruktur **Gehäuse-Übersicht** aus und klicken Sie auf **Benutzerauthentifizierung** → **Verzeichnisdienste**.
2. Wählen Sie **Microsoft Active Directory (Standardschema)** aus.
3. Klicken Sie im **Kerberos-Keytab** Abschnitt auf **Durchsuchen**, wählen Sie Keytab-Datei aus, und klicken Sie auf **hochladen**.

   Wenn der Vorgang beendet ist, wird eine Meldung angezeigt, die anzeigt ob die Keytab-Datei erfolgreich hochgeladen wurde.

Konfiguration der CMC SSO- oder Smart Card-Anmeldung für Active Directory-Benutzer über RACADM

Neben den im Rahmen der Konfiguration von Active Directory ausgeführten Schritten führen Sie zum Aktivieren von SSO den folgenden Befehl aus:

```
racadm -g cfgActiveDirectory -o cfgADSSOEnable 1
```

Neben den im Rahmen der Konfiguration von Active Directory ausgeführten Schritten verwenden Sie zum Aktivieren der Smart Card-Anmeldung die folgenden Objekte:

- `cfgSmartCardLogonEnable`
- `cfgSmartCardCRLEnable`

11

CMC zur Verwendung von Befehlszeilenkonsolen konfigurieren

Dieser Abschnitt enthält Informationen über die Funktionen der CMC-Befehlszeilenkonsole (bzw. der serielle/Telnet-/Secure Shell-Konsole) und erklärt, wie das System eingerichtet wird, sodass Systemverwaltungsmaßnahmen über die Konsole ausgeführt werden können. Informationen zur Verwendung der RACADM-Befehle im CMC über die Befehlszeilenkonsole finden Sie unter *RACADM -Befehlszeilen-Referenzhandbuchs für iDRAC6 und CMC*.

Verwandte Links

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

Funktionen der CMC-Befehlszeilenkonsolenverbindung

Der CMC unterstützt die folgenden Funktionen von seriellen, Telnet- und SSH-Konsolen:

- Eine serielle Client-Verbindung und bis zu vier gleichzeitige Telnet-Client-Verbindungen.
- Bis zu vier gleichzeitige Secure Shell- (SSH-) Client-Verbindungen.
- RACADM-Befehlsunterstützung.
- Integrierter connect-Befehl zum Anschließen an die serielle Konsole von Servern und E/A-Modulen; auch als `racadm connect`-Befehl verfügbar.
- Befehlszeilenbearbeitung und Protokoll.
- Steuerung der Sitzungszeitüberschreitung auf allen Konsolen-Schnittstellen.

CMC-Befehlszeilenbefehle

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

Tabelle 26. CMC-Befehlszeilenbefehle

Befehl	Beschreibung
`racadm`	RACADM-Befehle beginnen mit dem Stichwort `racadm` und werden von einem Unterbefehl gefolgt. Weitere Informationen finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC*.
`connect`	Verbindet sich mit der seriellen Konsole eines Servers oder eines E/A-Moduls. Weitere Informationen finden Sie unter Verbindung zu Servern oder Modulen mit dem connect-Befehl . **ANMERKUNG:** Sie können auch den Befehl racadm `connect` verwenden.

Befehl	Beschreibung
`exit`, `logout` und `quit`	Alle diese Befehle führen die gleiche Maßnahme aus. Sie beenden die aktuelle Sitzung und kehren zu einer Anmeldungseingabeaufforderung zurück.

Telnet-Konsole mit dem CMC verwenden

Mit CMC können Sie bis zu vier Telnet-Sitzungen gleichzeiting durchführen.

Wenn Ihre Management Station Windows XP oder Windows 2003 ausführt, kann ein Problem mit den Zeichen in einer CMC-Telnet-Sitzung auftreten. Dieses Problem kann sich als eingefrorene Anmeldung äußern, bei der die Eingabetaste nicht reagiert und keine Kennwort-Eingabeaufforderung eingeblendet wird.

Um dieses Problem zu beheben, laden Sie Hotfix 824810 von 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` muss unter Windows von einem VT100 oder ANSI-Terminalemulator ausgeführt werden. Sie können `OpenSSH` auch mithilfe von **Putty.exe** ausführen. Das Ausführen von `OpenSSH` an der Windows-Eingabeaufforderung ergibt keine vollständige Funktionalität (d. h. einige Tasten reagieren nicht und es werden keine Grafiken angezeigt). Führen Sie für Linux SSH-Client-Dienste aus, um über beliebige Shells eine Verbindung zum CMC herzustellen.

Vier gleichzeitige SSH-Sitzungen werden jeweils zu einem gegebenen Zeitpunkt unterstützt. Die Sitzungszeitüberschreitung wird durch die Eigenschaft `cfgSsnMgtSshIdleTimeout` gesteuert. Lesen Sie für weitere Informationen das Kapitel Datenbankeigenschaften des *RACADM Befehlszeilen-Referenzhandbuchs für iDRAC7 und CMC*, die Seite **Diensteverwaltung** in der Webschnittstelle, oder lesen Sie Dienste konfigurieren.

Der CMC unterstützt auch Authentifizierung mit öffentlichem Schlüssel (PKA) über SSH. Diese Authentifizierungsmethode verbessert SSH-Scripting-Automatisierung durch Beseitigung des Bedarfs, Benutzer-ID/Kennwort einzubetten bzw. anzufordern. Weitere Informationen finden Sie unter Konfigurieren der Authentifizierung mit öffentlichem Schlüssel über SSH.

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

Zur Konfiguration von SSH gehen Sie zu Dienste konfigurieren.

Verwandte Links

Dienste konfigurieren

Unterstützte SSH-Verschlüsselungssysteme

Um mit CMC über das SSH-Protokoll zu kommunizieren, unterstützt es verschiedene Verschlüsselungsschemas, die in der folgenden Tabelle aufgelistet sind.

Tabelle 27. Verschlüsselungsschemata

Schematyp	Schema
Asymmetrische Verschlüsselung	Diffie-Hellman DSA/DSS 512-1024 (zufallsbestimmt) Bits gemäß NIST-Spezifikation
Symmetrische Verschlüsselung	• AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
Meldungsintegrität	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
Authentifizierung	Kennwort

Authentifizierung mit öffentlichem Schlüssel über SSH.

Sie können bis zu 6 öffentliche Schlüssel konfigurieren, die mit dem Dienst-Benutzernamen über 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.

ANMERKUNG: Es gibt keine GUI-Unterstützung zur Verwaltung dieser Funktionen; Sie können nur RACADM verwenden.

Beim Hinzufügen neuer öffentlicher Schlüssel müssen Sie sicherstellen, dass bestehende Schlüssel nicht bereits den Index belegen, zu dem der neue Schlüssel hinzugefügt werden soll. Der CMC führt vor dem Hinzufügen eines Schlüssels keine Prüfungen durch, um sicherzustellen, dass keine vorherigen Schlüssel gelöscht werden. Sobald ein neuer Schlüssel hinzugefügt wurde, tritt er automatisch in Kraft, solange die SSH-Schnittstelle aktiviert ist.

Beachten Sie bei Verwendung des Anmerkungsabschnitts des öffentlichen Schlüssels, dass nur die ersten 16 Zeichen vom CMC verwendet werden. Die Anmerkung des öffentlichen Schlüssels wird vom CMC verwendet, um SSH-Benutzer bei Verwendung des RACADM-Befehls `getssninfo` zu unterscheiden, 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 Typ Benutzer IP-Adresse Anmeldung Datum/Zeit SSH PC1 x.x.x.x
16.06.09 09:00:00 SSH PC2 x.x.x.x 16.06.09 09:00:00
```

Lesen Sie für weitere Informationen zu `sshpkauth` das *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC*.

Verwandte Links

- Generieren öffentlicher Schlüssel für Windows
- Generieren öffentlicher Schlüssel für Linux
- Hinweise zur RACADM-Syntax für CMC
- Öffentliche Schlüssel anzeigen
- Öffentliche Schlüssel hinzufügen
- Öffentliche Schlüssel löschen

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 <Dateiname des öffentlichen Schlüssels>
```

ANMERKUNG: Sie können die Datei-Hochladen-Option nur mit Remote-RACADM verwenden. Lesen Sie für weitere Informationen das *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 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 "<Text des öffentlichen Schlüssels>"
```

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
```

Frontblende für iKVM-Verbindung aktivieren

Für Informationen und Anleitungen zur Verwendung des iKVM-Frontblendenanschlusses, siehe Aktivierung oder Deaktivierung des Zugriffs auf das iKVM von der Frontblende aus

Terminalemulationssoftware konfigurieren

Der 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 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-Konfigurationsdateiname>` ein und fahren Sie mit Schritt 12 fort.
2. Geben Sie bei der Linux-Eingabeaufforderung `minicom -s` ein.
3. Wählen Sie die Option **Seriellen Anschluss einrichten** aus und drücken Sie die Taste <Eingabe>.
4. Drücken Sie <a> und wählen Sie dann das entsprechende serielle Gerät aus (Beispiel: `/dev/ttyS0`).
5. Drücken Sie <e> und stellen Sie dann die Option **Bps/Par/Bits** auf **115200 8N1** ein.
6. Drücken Sie <f> und stellen Sie dann die **Hardware-Datenflusssteuerung** auf **Ja** und die **Software-Datenflusssteuerung** auf **Nein** ein. Um das Menü **Seriellen Anschluss einrichten** zu beenden, drücken Sie die Taste <Eingabe>.
7. Wählen Sie **Modem und Wählen** aus und drücken Sie die Taste <Eingabe>.
8. Im Menü **Modem-Wählen und Parameter-Setup** drücken Sie die <Rücktaste>, um die Einstellungen bei **init**, **reset**, **connect** und **hangup** zu löschen, damit diese leer sind, und drücken dann die Taste <Eingabe>, um den jeweiligen Leerwert zu speichern.
9. Wenn alle angegebenen Felder gelöscht sind, drücken Sie die Taste <Eingabe>, um das Menü **Modem-Wählen und Parameter-Setup** zu beenden.
10. Wählen Sie **Minicom beenden** aus und drücken Sie die Taste <Eingabe>.
11. An der Befehls-Shell-Eingabeaufforderung geben Sie `minicom <Minicom-Konfigurationsdateiname>` ein.
12. 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 die folgende Tabelle zum Konfigurieren einer beliebigen Minicom-Version.

Tabelle 28. Minicom-Einstellungen

Beschreibung der Einstellung	Erforderliche Einstellung
Bit/s/Par/Bit	115200 8N1
Hardware-Datenflusssteuerung	Ja
Software-Datenflusssteuerung	Nein

Beschreibung der Einstellung	Erforderliche Einstellung
Terminalemulation	ANSI
Einwahl per Modem und Parameter-Einstellungen	Löschen Sie die Einstellungen **init**, **reset**, **connect** und **hangup**, sodass sie leer sind

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

Der CMC kann eine Verbindung herstellen, um die serielle Konsole von Servern oder E/A-Modulen umzuleiten.

Für Server kann die serielle Konsolenumleitung so erreicht werden:

- Über die CMC-Befehlszeile mit dem connect- oder racadm connect-Befehl. Lesen Sie für weitere Informationen das *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC*.
- Serielle Konsolenumleitungsfunktion der iDRAC-Webschnittstelle.
- iDRAC-Seriell-über-LAN (SOL)-Funktionalität.

Bei einer seriellen, Telnet- oder SSH-Konsole unterstützt der CMC den Befehl connect, um eine serielle Verbindung zu einem Server oder 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.

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

ANMERKUNG: Der Befehl `connect` stellt die Option `-b` (binär) bereit. Bei der Option `-b` werden reine Binärdaten übergegeben und `cfgSerialConsoleQuitKey` wird nicht verwendet. Zudem verursachen Übergänge beim DTR-Signal (z. B. wenn das serielle Kabel entfernt wird, um eine Verbindung eines Debuggers herzustellen) keine 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 13-1 für eine Veranschaulichung der Positionierung der EAMs im Gehäuse.) Wenn Sie sich beim connect-Befehl auf die EAMs beziehen, werden die EAMs Switches zugewiesen wie in der folgenden Tabelle dargestellt.

Tabelle 29. 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

Bezeichnung des E/A-Moduls	Switch
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 verwalteten seriellen Serverkonsole herzustellen, verwenden Sie den Befehl `connect server-nx`, wobei `n` 1-8 ist und `x` a, b, c oder d 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.

Verwandte Links

BIOS des verwalteten Servers für die serielle Konsolenumleitung konfigurieren
Windows für serielle Konsolenumleitung konfigurieren
Linux während des Starts für die Umleitung der seriellen Konsole konfigurieren
Linux für die Umleitung der seriellen Konsole nach Start konfigurieren

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) oder über die iDRAC7-Web-GUI eine Remote-Konsolen-Sitzung aufzubauen (siehe *iDRAC7-Benutzerhandbuch* unter **dell.com/support/manuals**).

Die serielle Kommunikation ist im BIOS standardmäßig ausgeschaltet. Um die Daten der Hosttextkonsole zu „Seriell über LAN“ umzuleiten, müssen Sie die Konsolenumleitung über COM1 aktivieren. So ändern Sie die BIOS-Einstellung:

1. 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:
   - 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.

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 sind erforderlich, um einen anderen Bootloader zu verwenden.

ANMERKUNG: Beim Konfigurieren des Client-VT100-Emulationsfensters stellen Sie das Fenster bzw. die Anwendung, die die umgeleitete 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, erstellt durch anaconda # # Beachten Sie, dass grub nicht
   erneut ausgeführt werden muss, nachdem Sie Änderungen an # dieser Datei #
   vorgenommen haben. HINWEIS: Sie haben keine /boot-Partition. Dies bedeutet,
   dass # alle Kernel und initrd-Pfade relativ zu / sind, z. B. # root (hd0,0)
   # kernel /boot/vmlinuz-version ro root=/dev/sda1 # initrd /boot/initrd-
   version.img #boot=/dev/sda default=0 timeout=10 #splashimage=(hd0,2)/grub/
   splash.xpm.gz serial --unit=1 --speed=57600 terminal --timeout=10 serial
   title Red Hat Linux Advanced Server (2.4.9-e.3smp) root (hd0,0) kernel /
   boot/vmlinuz-2.4.9-e.3smp ro root=/dev/sda1 hda=ide-scsi console=ttyS0
   console=ttyS1,115200n8r initrd /boot/initrd-2.4.9-e.3smp.img title Red Hat
   Linux Advanced Server-up (2.4.9-e.3) root (hd0,00) kernel /boot/
   vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s initrd /boot/initrd-2.4.9-e.3.im
   ```

   Folgen Sie beim Bearbeiten der Datei **/etc/grub.conf** diesen Richtlinien:

   - Deaktivieren Sie die GRUB-Grafikschnittstelle und verwenden Sie die textbasierte Schnittstelle; ansonsten wird der GRUB-Bildschirm nicht in der Konsolenumleitung angezeigt. Zum Deaktivieren der grafischen Schnittstelle kommentieren Sie die Zeile aus, die mit `splashimage` beginnt.
   - Zum Starten mehrerer GRUB-Optionen, um Konsolensitzungen über die serielle Verbindung zu beginnen, fügen Sie allen Optionen die folgende Zeile hinzu:

     ```
     console=ttyS1,57600
     ```

     Das Beispiel zeigt, dass `console=ttyS1,57600` nur zur ersten Option hinzugefügt wurde.

Linux für die Umleitung der seriellen Konsole nach Start konfigurieren

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

Fügen Sie eine neue Zeile hinzu, um `agetty` auf der seriellen COM2-Schnittstelle zu konfigurieren:

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

Das folgende Beispiel zeigt die Datei mit der neuen Zeile.

```
# # inittab This file describes how the INIT process # should set up the system
in a certain # run-level. # # Author: Miquel van Smoorenburg # Modified for RHS
Linux by Marc Ewing and # Donnie Barnes # # Default runlevel. The runlevels
used by RHS are: # 0 - halt (Do NOT set initdefault to this) # 1 - Single user
mode # 2 - Multiuser, without NFS (The same as 3, if you # do not have
networking) # 3 - Full multiuser mode # 4 - unused # 5 - X11 # 6 - reboot (Do
NOT set initdefault to this) # id:3:initdefault: # System initialization.
si::sysinit:/etc/rc.d/rc.sysinit l0:0:wait:/etc/rc.d/rc 0 l1:1:wait:/etc/
rc.d/rc 1 l2:2:wait:/etc/rc.d/rc 2 l3:3:wait:/etc/rc.d/rc 3 l4:4:wait:/etc/
rc.d/rc 4 l5:5:wait:/etc/rc.d/rc 5 l6:6:wait:/etc/rc.d/rc 6 # Things to run in
every runlevel. ud::once:/sbin/update # Trap CTRL-ALT-DELETE ca::ctrlaltdel:/
sbin/shutdown -t3 -r now # When our UPS tells us power has failed, assume we
have a few # minutes of power left. Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have power installed and your # UPS is
connected and working correctly. pf::powerfail:/sbin/shutdown -f -h +2 "Power
Failure; System Shutting Down" # If power was restored before the shutdown
kicked in, cancel it. pr:12345:powerokwait:/sbin/shutdown -c "Power Restored;
Shutdown Cancelled" # Run gettys in standard runlevels co:2345:respawn:/sbin/
agetty -h -L 57600 ttyS1 ansi 1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2 3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4 5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6 # Run xdm in runlevel 5 # xdm is now a
separate service x:5:respawn:/etc/X11/prefdm -nodaemon
```

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
```

12

FlexAddress- und FlexAdress Plus-Karten verwenden

Dieser Abschnitt enthält Informationen über FlexAddress- und FlexAddress Plus-Karten, wie sie sie konfigurieren und verwenden.

Verwandte Links

Über FlexAddress
Über FlexAddress Plus
FlexAddress im Vergleich mit FlexAddress Plus

Über FlexAddress

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

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

FlexAddress ermöglicht es dem CMC, WWN/MAC-IDs einem bestimmten Steckplatz zuzuweisen und die werkseitigen IDs außer Kraft zu setzen. Wird das Servermodul ausgetauscht, bleiben die steckplatzbasierten WWN/MAC-IDs erhalten. Dank dieser Funktion ist es nicht mehr notwendig, die Ethernet-Netzwerkverwaltungsinstrumente und die SAN-Ressourcen für ein neues Servermodul neu zu konfigurieren.

Außerdem erfolgt das *Überschreiben* nur, wenn ein Servermodul in ein FlexAddress-aktiviertes Gehäuse eingesetzt wird. Es werden keine permanenten Änderungen am Servermodul vorgenommen. Wird ein Servermodul in ein Gehäuse eingesetzt, das FlexAddress nicht unterstützt, werden die werkseitig zugewiesenen WWN/MAC-IDs verwendet.

Die FlexAddress-Funktionskarte enthält einen Bereich von MAC-Adressen. Vor der Installation von FlexAddress können Sie den MAC-Adressenbereich, der auf einer FlexAddress-Funktionskarte enthalten ist, feststellen, indem Sie die SD-Karte in einen USB-Speicherkartenleser einsetzen und die Datei **pwwn_mac.xml** anzeigen. Diese Klartext-XML-Datei auf der SD-Karte beinhaltet die XML-Kennung *mac_start*. Diese Kennung ist die hexadezimale MAC-Start-Adresse für diesen eindeutigen MAC-Adressbereich. Das Tag *mac_count* ist die Gesamtzahl der MAC-Adressen, die die SD-Karte zuweist. Der gesamte zugewiesen MAC-Bereich kann wie folgt bestimmt werden:

```
<mac_start> + 0xCF (208 - 1) = mac_end
```

wobei 208 *mac_count* ist und die Formel lautet:

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

Beispiel:

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

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

Über FlexAddress Plus

FlexAddress Plus ist eine neue Funktion bei der Kartenversion 2.0. Es ist eine Erweiterung der FlexAddress-Funktionskarte Version 1.0. FlexAddress Plus enthält mehr MAC-Adressen als die FlexAddress-Funktion. Beide Funktionen ermöglichen es dem Gehäuse, WWN/MAC-Adressen (World Wide Name/Media Access Control) für Fibre Channel- und Ethernet-Geräte zuzuweisen. Gehäusezugewiesene WWN/MAC-Adressen sind global eindeutig und für jeden Serversteckplatz spezifisch.

FlexAddress im Vergleich mit FlexAddress Plus

FlexAddress verfügt über 208 Adressen, die auf 16 Serversteckplätze aufgeteilt sind, so dass jedem Steckplatz 13 MACs zugewiesen sind.

FlexAddress verfügt über 2928 Adressen, die auf 16 Serversteckplätze 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
FlexAddress	4	4	4	1	13
FlexAddress Plus	60	60	60	3	183

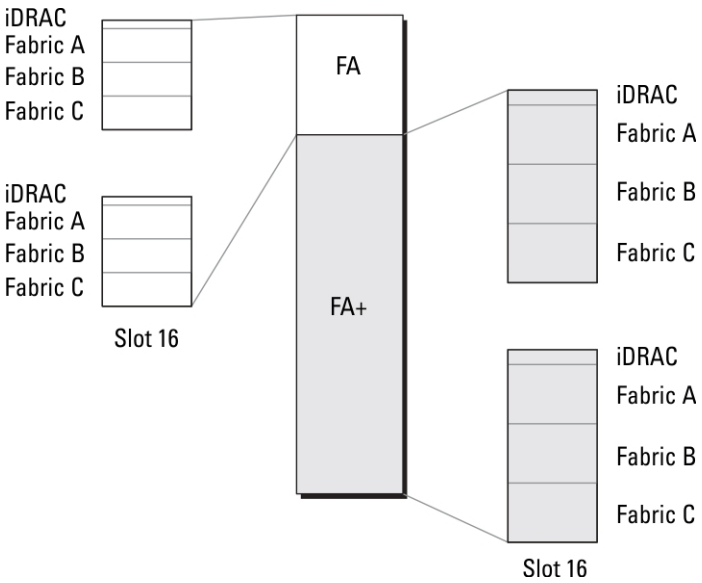


Abbildung 3. Funktionsvergleich FlexAddress (FA) gegenüber FlexPlusAddress (FA+)

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 Updates, die in der untenstehenden Tabelle aufgeführt sind, umfassen: Servermodul-BIOS, E/A-Zusatzkarten-BIOS oder -Firmware und 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
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 xx0x Systeme • Version 2.10 oder höher für PowerEdge xx1x 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. Weitere Informationen finden Sie unter Bestätigung von FlexAddress Aktivierung.

Aktivieren von FlexAddress Plus

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

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

Einige Server 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 der *Infodatei* unter **dell.com/support/manuals**.

Bestätigung FlexAddress-Aktivierung

Verwenden Sie den folgenden RACADM-Befehl, um die SD-Funktionskarte und ihren Status zu bestätigen:

```
racadm featurecard -s
```

Tabelle 30. 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 Funktionskarte ist ungültig und enthält die folgenden Funktionen FlexAddress: Die Funktionskarte ist an ein anderes Gehäuse gebunden, svctag = ABC1234, SD card SN = 01122334455	Entfernen Sie die SD-Karte; bestimmen und installieren Sie die SD-Karte für das aktuelle Gehäuse.

Statusmeldung	Maßnahmen
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 dieses Gehäuses anzuzeigen:

```
racadm feature -s
```

Der Befehl gibt die folgende Statusmeldung aus:

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

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

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

Dell-Funktionskarten können mehr als eine Funktion enthalten. Sobald eine auf einer Dell-Funktionskarte enthaltene Funktion auf einem Gehäuse aktiviert ist, können keine anderen Funktionen, die möglicherweise auf der Dell-Funktionskarte enthalten sind, auf einem anderen Gehäuse aktiviert werden. In diesem Fall zeigt der Befehl „racadm feature -s“ die folgende Meldung für die betroffenen Funktionen an:

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

Weitere Informationen zu der **Funktion** und den **featurecard** Befehlen finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 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. Der Begriff FlexAddress bedeutet in diesem Kontext sowohl FlexAddress als auch FlexAddressPlus.

ANMERKUNG: Die SD-Karte muss physisch im CMC installiert sein und das Gehäuse muss 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 der FlexAddress-Funktion und Wiederherstellung der SD-Karte:

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

Der Befehl gibt die folgende Statusmeldung bei erfolgreicher Ausführung zurück:

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

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

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

Lesen Sie für weitere Informationen zu diesem Befehl den Abschnitte zum **feature-Befehl** des *RACADM-Befehlszeilen-Referenzhandbuchs für iDRAC7 und CMC*.

Anzeige von FlexAddress-Informationen

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

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

Verwandte Links

Anzeigen der FlexAddress-Gehäuseinformationen
Anzeigen von FlexAddress-Informationen für alle Server
Anzeige der FlexAddress Informationen für einzelne Server

Anzeigen der FlexAddress-Gehäuseinformationen

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

Um den FlexAddress-Status für das Gehäuse mithilfe der CMC Webschnittstelle anzuzeigen, gehen Sie zu **Gehäuseübersicht** → **Setup** → **Allgemein**.

Die Seite **Allgemeine Gehäuseeinstellungen** wird angezeigt.

Der Eintrag für **FlexAddress** weist den Wert **Aktiv** oder **Nicht Aktiv** auf. Der Eintrag **Aktiv** bedeutet, dass die Funktion für das Gehäuse installiert wurde und **Nicht aktiv** bedeutet, dass die Funktion nicht für das Gehäuse installiert wurde und nicht verfügbar ist.

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 <Steckplatz-Nr.>]
```

wobei *<Steckplatz-Nr.>* ein Wert von 1– 16 ist.

Weitere Informationen zu **getflexaddr** finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC.*

Anzeigen von FlexAddress-Informationen für alle Server

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

Die Seite **WWN/MAC-Zusammenfassung** wird angezeigt, die die WWN-Konfiguration und MAC-Adressen für alle Steckplätze im Gehäuse zur Verfügung stellt.

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 ist aktiv oder nicht aktiv. • Strukturtyp. • Serverzugewiesene und gehäusezugewiesene verwendete WWN/MAC-Adressen. Ein grünes Häkchen zeigt den aktiven Adresstyp, entweder serverzugewiesen oder gehäusezugewiesen.

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

Anzeige der FlexAddress Informationen für einzelne Server

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

1. Erweitern Sie **Server-Übersicht** in der Systemstruktur.
   Es werden alle Server (1 - 16) in der erweiterten Liste der **Server** angezeigt.
2. Klicken Sie auf den Server, den Sie anzeigen möchten.
   Die Seite **Serverstatus** wird angezeigt.
3. Klicken Sie auf das Register **Setup** und dann das Unterregister **FlexAddress**.
   Die Seite **FlexAddress**, die WWN-Konfiguration und die MAC-Adressen für ausgewählten Server bietet, wird angezeigt. Weitere Informationen finden Sie in der *CMC-Online-Hilfe.*

FlexAddress konfigurieren

FlexAddress ist eine optionale Erweiterung, die es ermöglicht, die werkseitig zugewiesenen WWN/MAC-IDs der Servermodule mit einer WWN/MAC-ID des Gehäuses zu ersetzen.

ANMERKUNG: In diesem Bereich bedeutet der Begriff FlexAddress auch FlexAddress Plus.

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

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

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

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

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: Stellen Sie sicher, dass Sie die Blade-Server ausschalten, bevor Sie die Flex-Adresse für die Struktur-Ebene (A, B, C oder DRAC) ändern.

Verwandte Links

Wake-On-LAN mit FlexAddress
Konfiguration der FlexAddress Struktur und Steckplatz auf Gehäuseebene
Serverseitige FlexAddress-Steckplatzkonfiguration
Zusätzliche Konfiguration von FlexAddress für Linux

Wake-On-LAN mit FlexAddress

Wenn die FlexAddress-Funktion zum ersten Mal auf einem Servermodul bereitgestellt wird, erfordert dies ein Herunterfahren und erneutes Hochfahren, damit FlexAddress wirksam wird. FlexAddress auf Ethernet-Geräten wird vom BIOS des Systemmoduls programmiert. Damit das BIOS des Servermoduls die Adresse programmieren kann, muss es in Betrieb sein, was erfordert, dass das Servermodul eingeschaltet ist. Ist das Herunter-/Hochfahren abgeschlossen, sind die gehäusezugewiesenen MAC-IDs für die Wake-On-LAN (WOL)-Funktion verfügbar.

Konfiguration der FlexAddress Struktur und Steckplatz auf Gehäuseebene

Auf Gehäuseebene können Sie FlexAddress für Strukturen und Steckplätze aktivieren oder deaktivieren. FlexAddress ist jeweils für eine Struktur 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.

FlexAddress für Struktur und Steckplatz auf Gehäuseebene über die CMC-Webschnittstelle konfigurieren

So aktivieren oder deaktivieren Sie Strukturen und Steckplätze für die Verwendung mit der FlexAddress-Funktion mithilfe der CMC-Webschnittstelle:

1. Gehen Sie in der Systemstruktur zu **Server-Übersicht** und klicken Sie dann auf **Setup → FlexAddress.** .
   Die Seite **FlexAddress bereitstellen** wird angezeigt.
2. Wählen Sie im Abschnitt **Struktur für gehäusezugewiesene WWN/MACs auswählen** den Strukturtyp, für den Sie FlexAddress aktivieren möchten. Zum Deaktivieren heben Sie die Auswahl der Option auf.

   ANMERKUNG: Sind keine Strukturen ausgewählt, wird FlexAddress für die ausgewählten Steckplätze nicht aktiviert.

   Die Seite **Steckplatz auswählen für gehäusezugewiesene WWN/MACs** wird angezeigt.
3. Wählen Sie die Option **Aktiviert** für den Steckplatz aus, für den Sie FlexAddress aktivieren möchten. Zum Deaktivieren heben Sie die Auswahl der Option auf.

   ANMERKUNG: Ist ein Server im Steckplatz vorhanden, schalten Sie ihn aus, bevor Sie die Funktion FlexAddress für diesen Steckplatz aktivieren.

ANMERKUNG: Sind keine Steckplätze ausgewählt, wird FlexAddress für die ausgewählten Strukturen nicht aktiviert.

4. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.
   Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.

FlexAddress für Struktur und Steckplatz auf Gehäuseebene über RADACM konfigurieren

Verwenden Sie zum Aktivieren oder Deaktivieren von Strukturen die folgenden RACADM-Befehle:

```
racadm setflexaddr [-f <Strukturname> <Status>]
```

wobei, `<Strukturname> = A, B, C oder iDRAC` und `<Status> = 0 oder 1`

0 deaktiviert und 1 aktiviert bedeuten.

Verwenden Sie zum Aktivieren oder Deaktivieren von Steckplätzen die folgenden RACADM-Befehle:

```
racadm setflexaddr [-i <Steckplatz-Nr.> <Status>
```

wobei, `<Steckplatz-Nr.> = 1 oder 16` und `<Status> = 0 oder 1`

0 deaktiviert und 1 aktiviert bedeuten.

Weitere Informationen zum **setflexaddr** -Befehl finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC*.

Serverseitige FlexAddress-Steckplatzkonfiguration

Auf Serverebene können Sie FlexAddress für einzelne Steckplätze aktivieren oder deaktivieren.

FlexAddress über Server-Level-Steckplätze unter Verwendung der CMC-Webschnittstelle konfigurieren

Aktivieren oder Deaktivieren eines einzelnen Steckplatzes für die Verwendung mit der FlexAddress-Funktion mithilfe der CMC-Webschnittstelle:

1. Erweitern Sie **Server-Übersicht** in der Systemstruktur.
   Es werden alle Server (1 - 16) in der erweiterten Liste der **Server** angezeigt.
2. Klicken Sie auf den Server, den Sie anzeigen möchten.
   Die Seite **Serverstatus** wird angezeigt.
3. Klicken Sie auf das Register **Setup** und dann das Unterregister **FlexAddress**.
   Die Seite **FlexAddress** wird angezeigt.
4. Im Dropdown-Menü **FlexAddress aktiviert** wählen Sie **Ja** aus, um FlexAddress zu aktivieren, oder wählen Sie **Nein**, um FlexAddress zu deaktivieren.
5. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.
   Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.

FlexAddress über Server-Level-Steckplätze unter Verwendung von RACADM konfigurieren

So konfigurieren Sie die flexaddress für Server-Level-Steckplätze unter Verwendung von RACADM:

```
racadm setflexaddr [-i <Steckplatz-Nr.> <Status>] [-f <Strukturname> <Status>]
```

wobei `<slot#> = 1 to 16` (<Steckplatz-Nr.> = 1 bis 16)

`<Strukturname> = A, B, C`

`<Status> = 0 oder 1`

0 bedeutet deaktiviert und 1 bedeutet aktiviert.

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 zeigt das Hardware Discovery-Menü (Hardwareerkennung) an und erkennt die MAC-Adressänderung, wenn Hardware entfernt und durch neue Hardware ersetzt wird.

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 FlexAddress-Funktion finden Sie unter CMCNoble_Über FlexAddress.

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.

Befehlsmeldungen

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

Tabelle 31. FlexAddress-Befehle und -Ausgaben

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

Situation	Befehl	Ausgang
eine Struktur, während die Servermodule eingeschaltet sind.		`sie einen eingeschalteten Server betrifft`

FlexAddress DELL SOFTWARE-LIZENZVEREINBARUNG

Dies ist ein rechtlich bindender Vertrag zwischen Ihnen, dem Benutzer, und Dell Products L.P oder Dell Global B.V. ("Dell"). Diese Vereinbarung erstreckt sich auf jede Software (zusammenfassend als „Software“ bezeichnet), die mit dem Dell-Produkt geliefert wird und für die keine separate Lizenzvereinbarung zwischen Ihnen und dem Hersteller bzw. dem Eigentümer der Software besteht. Diese Vereinbarung ist nicht für den Verkauf von Software oder von anderem geistigen Eigentum bestimmt. Alle Eigentumsrechte und Rechte an geistigem Eigentum sind im Besitz des Herstellers oder Eigentümers der Software. Alle Rechte, die in dieser Vereinbarung nicht ausdrücklich übertragen werden, sind im Besitz des Herstellers oder Eigentümers der Software. Durch Öffnen bzw. Aufbrechen des Siegels am bzw. an den Softwarepaket(en), Installieren oder Herunterladen der Software oder Verwenden der Software, die bereits im Computer geladen oder im Produkt integriert ist, erkennen Sie die Bestimmungen dieser Vereinbarung an. Wenn Sie diesen Bestimmungen nicht zustimmen, geben Sie bitte die gesamte Software inklusive Begleitmaterial (Disketten, CDs, gedrucktes Material und Verpackungen) unverzüglich zurück, und löschen Sie die bereits geladene oder integrierte Software.

Sie sind berechtigt, eine Kopie der Software auf einem einzigen Computer zu installieren und zu verwenden. Wenn Sie über mehrere Lizenzen der Software verfügen, ist es Ihnen gestattet, so viele Kopien der Software gleichzeitig zu verwenden, wie Sie Lizenzen haben. Die Software wird auf einem Computer „verwendet“, wenn sie in einen temporären Speicher geladen oder auf einem permanenten Speicher des Computers installiert ist. Die Installation auf einem Netzwerkserver nur zum Zweck der internen Verteilung stellt jedoch keine „Verwendung“ dar, wenn (und nur wenn) Sie für jeden Computer, an den die Software verteilt wird, über eine gesonderte Lizenz verfügen. Sie müssen sicherstellen, dass die Anzahl der Personen, die die auf einem Netzwerkserver installierte Software verwenden, nicht die Anzahl der vorhandenen Lizenzen übersteigt. Wenn mehr Personen die Software verwenden, die auf einem Netzwerkserver installiert ist, als Lizenzen vorhanden sind, müssen Sie erst so viele zusätzliche Lizenzen erwerben, bis die Anzahl der Lizenzen der Anzahl der Benutzer entspricht, bevor Sie weiteren Benutzern die Verwendung der Software gestatten dürfen. Als gewerblicher Kunde oder als Dell-Tochtergesellschaft gewähren Sie hiermit Dell oder einem von Dell bestimmten Vertreter das Recht, während der normalen Geschäftszeiten ein Audit der Softwareverwendung durchzuführen; außerdem erklären Sie sich damit einverstanden, Dell bei einem solchen Audit zu unterstützen und Dell alle Aufzeichnungen zur Verfügung zu stellen, die billigerweise mit der Verwendung der Software in Beziehung stehen. Das Audit beschränkt sich auf die Überprüfung der Einhaltung der Bestimmungen dieser Vereinbarung.

Die Software ist durch US-amerikanische Urheberrechtsgesetze und Bestimmungen internationaler Verträge geschützt. Sie sind berechtigt, eine Kopie der Software ausschließlich zu Sicherungs- oder Archivierungszwecken zu erstellen oder die Software auf eine einzige Festplatte zu übertragen, wenn Sie das Original ausschließlich zu Sicherungs- und Archivierungszwecken aufbewahren. Sie sind nicht berechtigt, die Software 240 bei Benutzung von FlexAddress and FlexAdress Plus Karten durch Vermietung oder Leasing zu veräußern oder die schriftlichen Begleitmaterialien zu kopieren; Sie sind jedoch berechtigt, die Software mit sämtlichen Begleitmaterialien dauerhaft als Teil eines Verkaufs des Dell-Produkts zu übertragen, vorausgesetzt, Sie behalten keine Kopien zurück, und der Empfänger stimmt den Bestimmungen dieser Vereinbarung zu. Jede Übertragung muss die neueste Aktualisierung und alle früheren Versionen enthalten. Sie sind nicht berechtigt, die Software zurückzuentwickeln, zu dekompilieren oder zu disassemblieren. Wenn das Paket, das mit dem Computer geliefert wird, CDs, 3,5-Zoll- und/oder 5,25-Zoll-Disketten enthält, dürfen Sie nur die Datenträger verwenden, die für Ihren Computer geeignet sind. Sie sind nicht berechtigt, die Datenträger auf einem anderen Computer oder auf einem anderen Netzwerk zu verwenden oder sie zu verleihen, zu vermieten, zu verleasen oder an andere Benutzer zu übertragen, außer innerhalb der Grenzen dieses Vertrages.

BESCHRÄNKTE GARANTIE

Dell garantiert, dass die Software für einen Zeitraum von 90 Tagen ab Erhalt bei normalem Gebrauch frei von Material- und Verarbeitungsfehlern sein wird. Diese Garantie ist auf Ihre Person beschränkt und nicht übertragbar. Jegliche

konkludente Garantie ist ab dem Erhalt der Software auf neunzig (90) Tage beschränkt. Da einige Staaten oder Rechtsordnungen die Begrenzung der Gültigkeitsdauer von konkludenten Garantien nicht gestatten, gilt die vorstehende Einschränkung für Sie möglicherweise nicht. Die gesamte Haftung von Dell und seinen Lieferanten und Ihr ausschließlicher Anspruch beschränkt sich auf (a) Rückerstattung des Kaufpreises der Software oder (b) den Ersatz von Datenträgern, die der vorstehenden Garantie nicht genügen, sofern diese unter Angabe einer Rücksendegenehmigungsnummer an Dell geschickt werden, wobei Sie das Risiko und die Kosten tragen. Diese eingeschränkte Garantie gilt nicht, wenn Disketten durch einen Unfall oder durch falsche und unsachgemäße Anwendung beschädigt wurden oder an ihnen von anderen Parteien als Dell Reparaturen oder Veränderungen vorgenommen wurden. Der Garantiezeitraum für Ersatzdisketten ist auf die verbleibende ursprüngliche Garantiedauer oder dreißig (30) Tage beschränkt, je nachdem welcher der beiden Zeiträume länger ist.

Dell kann NICHT garantieren, dass die Software Ihren Anforderungen entspricht oder die Software ohne Unterbrechung bzw. fehlerfrei funktioniert. Sie übernehmen selbst die Verantwortung für die Auswahl der Software, um die von Ihnen gewünschten Ergebnisse zu erzielen, und für die Verwendung sowie die Ergebnisse, die durch den Gebrauch der Software erzielt werden.

DELL LEHNT AUCH IM NAMEN SEINER LIEFERANTEN ALLE ANDEREN AUSDRÜCKLICHEN ODER KONKLUDENTEN GARANTIEN FÜR DIE SOFTWARE SOWIE DIE GESAMTEN BEILIEGENDEN GEDRUCKTEN MATERIALIEN AB, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF JEGLICHE KONKLUDENTEN GARANTIEN FÜR MARKTGÄNGIGE QUALITÄT UND TAUGLICHKEIT FÜR EINEN BESTIMMTEN ZWECK. Diese beschränkte Garantie verleiht Ihnen bestimmte Rechte; möglicherweise haben Sie weitere Rechte, die je nach Staat, Land oder Rechtsordnung unterschiedlich sein können.

DELL HAFTET NICHT FÜR DIREKTE ODER INDIREKTE SCHÄDEN (DIES GILT UNTER ANDEREM AUCH OHNE BESCHRÄNKUNG FÜR FOLGESCHÄDEN JEGLICHER ART, FÜR SCHÄDEN DURCH ENTGANGENE GEWINNE, BETRIEBSUNTERBRECHUNGEN, VERLUST VON GESCHÄFTSDATEN ODER SONSTIGE PEKUNIÄRE VERLUSTE), DIE AUS DER VERWENDUNG ODER DER FEHLENDEN MÖGLICHKEIT, DIE SOFTWARE ZU VERWENDEN, ENTSTEHEN, AUCH WENN AUF DIE MÖGLICHKEIT DES ENTSTEHENS SOLCHER SCHÄDEN HINGEWIESEN WURDE. In einigen Staaten oder Gerichtsbarkeiten ist ein Ausschluss oder eine Beschränkung der Haftung für Folgeschäden oder beiläufig entstandene Schäden nicht zulässig, deshalb gilt die oben aufgeführte Beschränkung für Sie möglicherweise nicht.

OPEN-SOURCE-SOFTWARE

Ein Teil dieser CD enthält eventuell Open-Source-Software, die Sie gemäß den Bedingungen der spezifischen Lizenz verwenden können, unter der die Open-Source-Software veröffentlicht wird.

Die Veröffentlichung dieser Open-Source-Software erfolgt in der Hoffnung, dass sie Ihnen von Nutzen sein wird, WIRD JEDOCH „OHNE MÄNGELGEWÄHR“ ZUR VERFÜGUNG GESTELLT, OHNE IRGENDEINE AUSDRÜCKLICHE ODER IMPLIZITE GARANTIE, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE IMPLIZITE GARANTIE FÜR MARKTREIFE ODER DIE VERWENDBARKEIT FÜR EINEN BESTIMMTEN ZWECK. DELL, DIE URHEBERRECHTSINHABER ODER BETEILIGTE HAFTEN IN KEINER WEISE FÜR DIREKTE, INDIREKTE, BESONDERE, VERSCHÄRFTE, ZUFALLS- ODER FOLGESCHÄDEN (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZGÜTERN ODER -DIENSTEN, ENTGANGENE NUTZUNG ODER GEWINNE, DATENVERLUSTE BZW. BETRIEBSUNTERBRECHUNG), DIE SICH AUS DER VERWENDUNG DIESER SOFTWARE ERGEBEN, UND ZWAR UNABHÄNGIG DAVON, WIE DIESE VERURSACHT WERDEN BZW. AUF WELCHER HAFTUNGSTHEORIE SIE BASIEREN UND OB SIE AUF VERTRAG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER UNERLAUBTER HANDLUNG (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF FAHRLÄSSIGKEIT) BERUHEN. DIES GILT SELBST DANN, WENN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE.

.U.S. STAATLICH BESCHRÄNKTE RECHTE

Die Software und die Dokumentation verstehen sich als Handelswaren ("commercial items") im Sinne von 48 C.F.R. 2,101 (Code of Federal Regulations), bestehend aus "kommerzieller Computersoftware" und "kommerzieller Computersoftwaredokumentation" gemäß 48 C.F.R. 12,212. Im Einklang mit 48 C.F.R. 12,212 und 48 C.F.R. 227,7202-1 bis 227,7202-4 beziehen sämtliche U.S. Regierungs-Endnutzer die Software und die Dokumentation ausschließlich mit den hierin festgelegten Rechten.

Vertragsnehmer bzw. Hersteller ist Dell Products, L.P., One Dell Way, Round Rock, Texas 78682.

ALLGEMEIN

Diese Lizenzvereinbarung gilt bis zu einer Kündigung. Sie gilt gemäß oben genannten Bedingungen oder wenn Sie gegen irgendeine der Bestimmungen verstoßen, als gekündigt. Im Fall der Kündigung sind Sie verpflichtet, die Software und das Begleitmaterial sowie sämtliche Kopien davon zu vernichten. Diese Vereinbarung unterliegt den Gesetzen des US-Bundesstaates Texas. Jede Bestimmung dieser Vereinbarung ist unabhängig von den anderen Bestimmungen gültig. Wenn es sich herausstellt, dass eine Bestimmung der vorliegenden Vereinbarung nicht durchsetzbar ist, so wird die Gültigkeit und Durchsetzbarkeit der übrigen Bestimmungen und Bedingungen davon nicht berührt. Diese Vereinbarung ist für Rechtsnachfolger und Abtretungsempfänger bindend. Dell und Sie selbst erklären sich einverstanden, in dem höchstmöglichen rechtlich erlaubten Maße auf alle Rechte auf ein Gerichtsverfahren im Hinblick auf die Software und diese Vereinbarung zu verzichten. Da in einigen Rechtsordnungen diese Verzichtserklärung nicht rechtsgültig ist, gilt die Verzichtserklärung für Sie möglicherweise nicht. Sie bestätigen hiermit, dass Sie diese Vereinbarung gelesen und verstanden haben, dass Sie sich an die vorgenannten Bestimmungen halten und dass diese Vereinbarung hinsichtlich der Software die vollständige und exklusive Vereinbarung zwischen Ihnen und Dell darstellt.

13

Verwaltung der E/A-Struktur

Das Gehäuse kann bis zu sechs E/A-Module (EAMs) enthalten, 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 drei diskrete Datenpfade aufgeteilt: A, B und C. Diese Pfade werden als STRUKTUREN bezeichnet und unterstützen Ethernet, Fibre Channel und InfiniBand. Diese diskreten Strukturpfade sind in zwei E/A-Banken unterteilt: Bank eins und zwei. Jeder Server-E/A-Adapter (Mezzanine-Karte oder LOM) kann entweder zwei oder vier Schnittstellen haben, je nach Kapazität. Diese Schnittstellen sind gleichmäßig auf die E/A-Modulbänke eins und zwei aufgeteilt, um Redundanz zu ermöglichen. Wenn Sie die Ethernet-, iSCSI- oder FibreChannel-Netzwerke bereitstellen, sollten Sie deren redundante Links über die Bänke eins und zwei spannen, um maximale Verfügbarkeit zu erzielen. Das diskrete E/A-Modul ist mit der Strukturkennung und der Banknummer gekennzeichnet.

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-Steckplatz in jedem Servermodul verbunden.
- Für Gruppe C sind die EAM-Steckplätze permanent mit dem zweiten MC-Steckplatz in jedem Servermodul verbunden.

ANMERKUNG: In der CMC-Befehlszeilenschnittstelle werden die EAMs mit der Konvention Schalter-n bezeichnet: A1=Schalter-1, A2=Schalter-2, B1=Schalter-3, B2=Schalter-4, C1=Schalter-5 und C2=Schalter-6.

Verwandte Links

Struktur-Verwaltungsübersicht
Ungültige Konfigurationen
Neues Einschaltszenario
EAM-Funktionszustand überwachen
Netzwerkeinstellungen für EAM(s) konfigurieren
VLAN für EAM verwalten
Energiesteuerungsvorgang für EAMs verwalten
Aktivieren oder Deaktivieren von LED-Blinken für EAMs
EAM auf Werkseinstellungen zurücksetzen

Struktur-Verwaltungsübersicht

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.

Die folgende Abbildung zeigt die Position der EAMs im Gehäuse. Der Standort der einzelnen EAMs im Gehäuse wird durch die Gruppennummer (A, B oder C) und die Steckplatznummer (1 oder 2) angezeigt. 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.

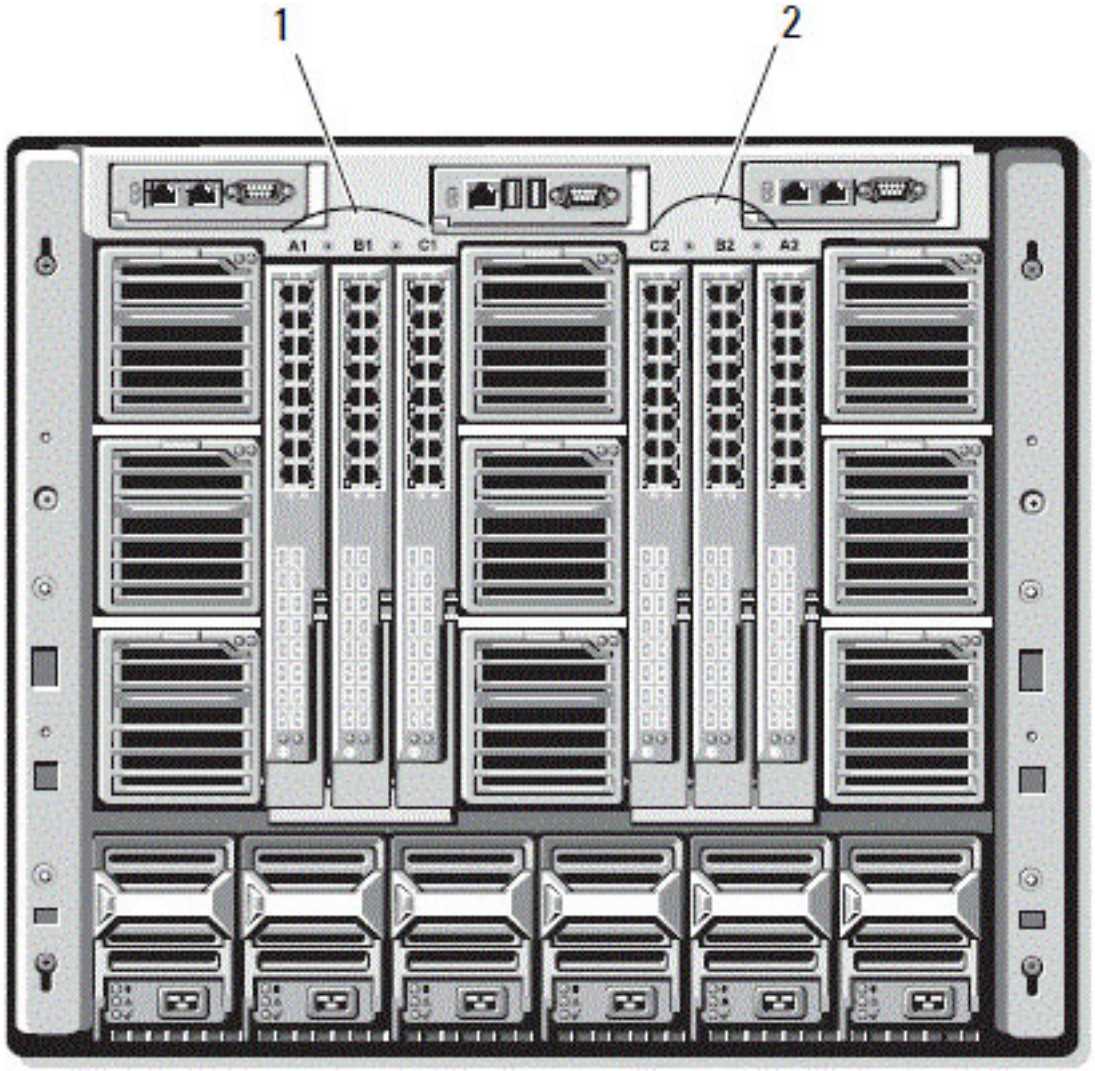


Abbildung 4. Rückansicht eines Gehäuses mit ausgewiesenen EAM-Standorten

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.

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

Neues Einschaltszenario

Wenn 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

Weitere Informationen zur Überwachung des EAM-Funktionszustands finden Sie unter Informationen und Funktionszustand von allen EAMs anzeigen und Informationen und Funktionszustand eines einzelnen EAM anzeigen.

Netzwerkeinstellungen für EAM(s) konfigurieren

Sie können die Netzwerkeinstellungen der zur Verwaltung der EAM verwendeten Schnittstelle angeben. Für Ethernet-Switches wird die bandexterne Verwaltungsschnittstelle (IP-Adresse) konfiguriert. Die bandinterne Verwaltungsschnittstelle (das heißt VLAN1) wird nicht mittels dieser Schnittstelle konfiguriert.

Stellen Sie vor der Konfiguration der Netzwerkeinstellungen für EAM(s) sicher, dass das IOM eingeschaltet ist.

Um die Netzwerkeinstellungen zu konfigurieren, müssen Sie Folgendes aufweisen:

- Struktur A-Administrator-Berechtigungen, um EAMs in Gruppe A zu konfigurieren.
- Struktur B-Administrator-Berechtigungen, um EAMs in Gruppe B zu konfigurieren.
- Struktur C-Administrator-Berechtigungen, um EAMs in Gruppe C zu konfigurieren.

ANMERKUNG: Für Ethernet-Switches können weder die bandinternen (VLAN1) noch die bandexterne Verwaltungs-IP-Adressen gleich sein bzw. sich im gleichen Netzwerk befinden; dies führt dazu, dass die bandexterne IP-Adresse nicht vergeben wird. Beachten Sie die EAM-Dokumentation für die standardmäßige bandinterne Verwaltungs-IP-Adresse.

ANMERKUNG: Die Netzwerkeinstellungen des E/A-Moduls für Ethernet-Passthrough und Infiniband-Schalter dürfen nicht konfiguriert werden.

Konfigurieren der Netzwerkeinstellungen für EAMs über die CMC-Webschnittstelle

ANMERKUNG: Diese Funktion wird nur auf dem PowerEdge M E/A-Aggregator EAM unterstützt. Andere EAMs einschließlich MXL 10/40GbE werden nicht unterstützt.

Um die Netzwerkeinstellungen für EAMs über die CMC-Webschnittstelle zu konfigurieren:

1. Gehen Sie in der Systemstruktur zu **E/A-Modul-Übersicht** und klicken Sie auf **Setup**, oder erweitern Sie **E/A-Modul-Übersicht**, wählen Sie das EAM aus und klicken Sie auf **Setup**.

   Auf der Seite **E/A-Module bereitstellen** werden die eingeschalteten IOMs angezeigt.
2. Aktivieren Sie DHCP für die erforderlichen IOMs, geben Sie die IP-Adresse ein, Subnetzmaske und Gateway-Adresse.
3. Geben Sie für verwaltbare IOMs Stammkennwort, SNMP RO Community-Zeichenkette und Syslog-Server-IP-Adresse ein. Weitere Informationen über die Felder finden Sie in der *CMC-Online-Hilfe*.

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

   Die Netzwerkeinstellungen sind für das/die IOM(s) konfiguriert.

   ANMERKUNG: Für IOMs, die verwaltbar sind, können Sie die VLANs, Netzwerkeigenschaften und EA-Ports auf Standardeinstellungen zurücksetzen.

Konfigurieren von Netzwerkeinstellungen für EAMs mit RACADM

Um die Netzwerkeinstellungen für EAMs mit RACADM zu konfigurieren, stellen Sie das Datum und die Uhrzeit ein. Siehe den Abschnitt **bereitstellen** Befehl im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC*.

Sie können den Benutzernamen, das Kennwort und die SNMP-Zeichenkette für ein EAM mithilfe des Befehls RACADM **bereitstellen** einstellen:

```
racadm deploy -m switch-<n> -u root -p <Kennwort>

racadm deploy -m switch-<n> -u root -p <Kennwort> -v SNMPv2
<snmpCommunityString> ro

racadm deploy -a [server|switch] -u root -p <Kennwort>
```

EAM auf Werkseinstellungen zurücksetzen

Sie können EAM auf die Werkseinstellungen mithilfe der Seite **E/A-Module bereitstellen** zurücksetzen.

ANMERKUNG: Die Funktion wird nur auf dem PowerEdge M E/A-Aggregator EAM unterstützt. Andere EAMs einschließlich MXL 10/40GbE werden nicht unterstützt.

So setzen Sie die ausgewählten EAMs auf die Werkseinstellungen mithilfe der CMC-Webschnittstelle zurück:

1. Wählen Sie in der Systemstruktur **E/A-Modul-Übersicht** aus und klicken Sie auf **Setup** oder erweitern Sie in der Systemstruktur **E/A-Modul-Übersicht**, wählen Sie das EAM aus und klicken Sie auf **Setup**.
   Auf der Seite **E/A-Module bereitstellen** werden die eingeschalteten IOMs angezeigt.
2. Klicken Sie für die erforderlichen IOMs auf **Zurücksetzen**.
   Es wird eine Bestätigungsmeldung angezeigt.
3. Klicken Sie auf **OK**, um fortzufahren.

Verwandte Links

Struktur-Verwaltungsübersicht
Ungültige Konfigurationen
Neues Einschaltszenario
EAM-Funktionszustand überwachen
Netzwerkeinstellungen für EAM(s) konfigurieren
VLAN für EAM verwalten
Energiesteuerungsvorgang für EAMs verwalten
Aktivieren oder Deaktivieren von LED-Blinken für EAMs

EAM-Software über die CMC-Web-Schnittstelle aktualisieren

Sie können die EAM-Software durch die Auswahl des erforderlichen Software-Images von einem bestimmten Standort aus aktualisieren. Sie können ebenfalls die Software auf eine frühere Version zurücksetzen.

ANMERKUNG: Die Funktion wird nur auf dem PowerEdge M E/A-Aggregator EAM unterstützt. Andere EAMs einschließlich MXL 10/40GbE werden nicht unterstützt.

So aktualisieren Sie die Software des EAM-Infrastrukturgerätes in der CMC-Webschnittstelle:

1. Wählen Sie **Gehäuse-Übersicht → E/A-Modul-Übersicht → Aktualisierung** .
   Die Seite **EAM-Firmware und Software** wird angezeigt.
   Sonst gehen Sie zu einer der folgenden Optionen:
   - **Gehäuseübersicht → Aktualisieren**
   - **Gehäuseübersicht → Gehäuse-Controller → Aktualisierung**
   - **Gehäuseübersicht → iKVM → Aktualisieren**

Die Seite **Firmware-Aktualisierung** mit einem Link für den Zugriff auf die Seite **EAM-Firmware und Software**, wird angezeigt.

2. Wählen Sie auf der Seite **EAM-Firmware und -Software** im Abschnitt **EAM-Software** das Kontrollkästchen für das EAM, das Sie aktualisieren möchten, in der Spalte **Aktualisierung** aus und klicken Sie auf **Softwareaktualisierung anwenden**.

   Alternativ können Sie, um die Software auf eine frühere Version zurückzusetzen, das Kontrollkästchen in der Spalte **Zurücksetzen** auswählen.

3. Wählen Sie das Software-Image für die Softwareaktualisierung durch Verwendung der Option **Durchsuchen** aus. Der Name des Software-Images wird im Feld **EAM-Softwarestandort** angezeigt.

   Der Abschnitt **Fortschritt der Aktualisierung** bietet Softwareaktualisierungs- oder Rollback-Statusinformationen. Ein Statusindikator wird auf der Seite während des Aktualisierungsvorganges angezeigt. Die Übertragungszeit kann je nach Verbindungsgeschwindigkeit variieren. Wenn der interne Aktualisierungsprozess beginnt, wird die Seite laufend aktualisiert und zeigt den Firmwareaktualisierungszeitgeber an.

   ANMERKUNG: Verwenden Sie während der Dateiübertragung nicht die Schaltfläche **Aktualisierung** und navigieren Sie nicht zu einer anderen Seite.

   ANMERKUNG: Es wird bei der IOMINF-Firmware-Aktualisierung kein Zeitgeber angezeigt.

   Wenn die Aktualisierung oder Rollback abgeschlossen ist, gibt es einen kurzzeitigen Verlust der Konnektivität zum EAM-Gerät, da es zurückgesetzt wird, und die neue Firmware wird auf der Seite **EAM-Firmware und Software** angezeigt.

VLAN für EAM verwalten

Virtuelle LANs (VLANs) für EAMs ermöglichen Ihnen, Benutzer in verschiedene individuelle Netzwerksegmente aus Sicherheits- und anderen Gründen aufzuteilen. Durch die Verwendung von VLANs können Sie die Netzwerke für individuelle Benutzer auf einen Switch mit 32 Ports isolieren. Sie können ausgewählte Ports auf einem Switch dem ausgewählten VLAN zuordnen und diese Ports als einen separaten Switch behandeln.

CMC-Webschnittstelle ermöglicht das Konfigurieren der bandinternen Verwaltungsports (VLAN) auf den EAMs.

Verwandte Links

VLAN-Einstellungen für EAMs über die CMC-Webschnittstelle konfigurieren
VLAN-Einstellungen für EAMs über die CMC-Webschnittstelle anzeigen
Aktuelle VLAN-Einstellungen für EAMs über die CMC-Webschnittstelle anzeigen
Gekennzeichnete VLANs für EAMs über die CMC-Webschnittstelle hinzufügen
VLANs für EAMs über die CMC-Webschnittstelle entfernen
Nicht gekennzeichnete VLANs für EAMs über die CMC-Webschnittstelle aktualisieren
VLANs für EAMs über die CMC-Webschnittstelle zurücksetzen

VLAN-Einstellungen für EAMs über die CMC-Webschnittstelle konfigurieren

ANMERKUNG: Sie können VLAN-Einstellungen nur auf PowerEdge M E/A-Aggregator-EAM konfigurieren. Andere EAMs einschließlich MXL 10/40GbE werden nicht unterstützt.

So werden die VLAN-Einstellungen auf IOM(s) über die CMC-Webschnittstelle konfiguriert:

1. Wählen Sie in der Systemstruktur **E/A-Modul-Übersicht** aus und klicken Sie auf **Setup VLAN-Manager**.

   Auf der Seite VLAN Manager werden die eingeschalteten EAMs sowie die verfügbaren Ports angezeigt.

2. Wählen Sie im Abschnitt **E/A-Modul auswählen** den Konfigurationstyp aus der Dropdown-Liste aus und wählen Sie anschließend die erforderlichen EAMs.

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

3. Wählen Sie im Abschnitt **Port-Bereich angeben** den Bereich von Strukturports aus, die dem/den ausgewählten EAM(s) zugewiesen werden sollen.

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

4. Wählen Sie die Option **Alle auswählen** oder **Alle abwählen** aus, um die Änderungen an allen oder keinem EAM(s) vorzunehmen.

   oder

   Markieren Sie das Kontrollkästchen für die entsprechenden Steckplätze, um die erforderlichen EAMs auszuwählen.

5. Geben Sie im Abschnitt **VLANs bearbeiten** die VLAN-IDs für die EAMs ein. Geben Sie VLAN-IDs im Bereich von 1 bis 4094 ein. VLAN-IDs können als Bereich oder getrennt durch Komma eingetragen werden. Beispiel: 1,5,10,100-200.
6. Wählen Sie ggf. eine der nachfolgenden Optionen aus dem Drop-Down-Menü aus:

   - Gekennzeichnete VLANs hinzufügen
   - VLANs entfernen
   - Nicht gekennzeichnete VLANs aktualisieren
   - Auf alle VLANs zurücksetzen
   - VLANs anzeigen

7. Klicken Sie auf **Speichern**, um die neuen Einstellungen auf der Seite **VLAN Manager** zu speichern.

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

   ANMERKUNG: Im Abschnitt „Zusammenfassung, VLANs von allen Ports“ werden Informationen zu den im Gehäuse vorhandenen EAMs sowie den zugewiesenen VLANs angezeigt. Klicken Sie auf Speichern, um eine csv-Datei der Zusammenfassung der aktuellen VLAN-Einstellungen zu speichern.

   ANMERKUNG: Im Abschnitt „CMC-verwaltete VLANs“ wird die Zusammenfassung aller den EAMs zugewiesenen VLANs angezeigt.

8. Klicken Sie auf **Anwenden**.

   Die Netzwerkeinstellungen sind für das/die EAM(s) konfiguriert.

VLAN-Einstellungen für EAMs über die CMC-Webschnittstelle anzeigen

So werden die VLAN-Einstellungen auf IOM(s) über die CMC-Webschnittstelle angezeigt:

1. Wählen Sie in der Systemstruktur **E/A-Modulübersicht** aus und klicken Sie auf **Setup → VLAN-Manager**.

   Die Seite **VLAN-Manager** wird angezeigt.

   Im Abschnitt **Zusammenfassung, VLANs von allen Ports** werden Informationen zu den aktuellen VLAN-Einstellungen für die IOMs angezeigt.

2. Klicken Sie auf **Speichern**, um die VLAN-Einstellungen als Datei zu speichern.

Aktuelle VLAN-Einstellungen für EAMs über die CMC-Webschnittstelle anzeigen

So werden die aktuellen VLAN-Einstellungen auf IOMs über die CMC-Webschnittstelle angezeigt:

1. Wählen Sie in der Systemstruktur **E/A-Modul-Übersicht** aus und klicken Sie auf **Setup → VLAN-Manager**.

   Die Seite **VLAN-Manager** wird angezeigt.

2. Im Abschnitt **VLANs bearbeiten** wählen Sie **VLANs anzeigen** aus der Dropdown-Liste aus und klicken Sie auf **Anwenden**.

   Die Meldung „Vorgang erfolgreich“ wird angezeigt. Die aktuellen den EAMs zugewiesenen VLAN-Einstellungen werden im Feld VLAN-Zuweisung, Zusammenfassung angezeigt.

Gekennzeichnete VLANs für EAMs über die CMC-Webschnittstelle hinzufügen

So fügen Sie gekennzeichnete VLANs für EAM(s) über die CMC-Webschnittstelle hinzu:

1. Wählen Sie in der Systemstruktur **E/A-Modul-Übersicht** aus und klicken Sie auf **Setup → VLAN-Manager**.
   Die Seite VLAN-Manager wird angezeigt.
2. Wählen Sie im Abschnitt **E/A Modül wählen** die erforderlichen EAMs.
3. Wählen Sie im Abschnitt **Port-Bereich angeben** den Bereich von Strukturports aus, die dem/den ausgewählten IOM(s) zugewiesen werden sollen.
   Weitere Informationen zu den Feldern finden Sie unter *CMC Online-Hilfe*.
4. Wählen Sie die Option **Alle auswählen** oder **Alle abwählen** aus, um die Änderungen an allen oder keinem EAM(s) vorzunehmen.
   oder
   Markieren Sie das Kontrollkästchen neben den entsprechenden Steckplätzen, um die erforderlichen EAMs auszuwählen.
5. Im Abschnitt **VLANs bearbeiten** wählen Sie **Gekennzeichnete VLANs hinzufügen** aus der Dropdown-Liste aus und klicken Sie auf **Anwenden**.
   Die gekennzeichneten VLANs werden den ausgewählten IOMs zugewiesen.
   Die Meldung „Vorgang erfolgreich" wird angezeigt. Die aktuellen den IOMs zugewiesenen VLAN-Einstellungen werden im Feld **VLAN-Zuweisung, Zusammenfassung** angezeigt.

VLANs für EAMs über die CMC-Webschnittstelle entfernen

So entfernen Sie VLANs von IOM(s) über die CMC-Webschnittstelle:

1. Wählen Sie in der Systemstruktur **E/A-Modulübersicht** aus und klicken Sie auf **Setup → VLAN-Manager**.
   Die Seite VLAN-Manager wird angezeigt.
2. Wählen Sie im Abschnitt **E/A-Modul auswählen** die erforderlichen IOMs aus.
3. Im Abschnitt **VLANs bearbeiten** wählen Sie **VLANs entfernen** aus der Dropdown-Liste aus und klicken Sie auf **Anwenden**.
   Die den ausgewählten IOMs zugewiesenen VLANs werden entfernt.
   Die Meldung „Vorgang erfolgreich" wird angezeigt. Die aktuellen den IOMs zugewiesenen VLAN-Einstellungen werden im Feld **VLAN-Zuweisung, Zusammenfassung** angezeigt.

Nicht gekennzeichnete VLANs für EAMs über die CMC-Webschnittstelle aktualisieren

So aktualisieren Sie nicht gekennzeichnete VLANs für EAMs über die CMC-Webschnittstelle:

1. Wählen Sie in der Systemstruktur **E/A-Modul-Übersicht** aus und klicken Sie auf **Setup → VLAN-Manager** .
   Die Seite **VLAN-Manager** wird angezeigt.
2. Wählen Sie im Abschnitt **E/A-Modul wählen** die erforderlichen EAMs.
3. Wählen Sie im Abschnitt **Port-Bereich angeben** den Bereich von Strukturports aus, die dem/den ausgewählten IOM(s) zugewiesen werden sollen.
   Weitere Informationen zu den Feldern finden Sie in der *CMC Online-Hilfe*.
4. Wählen Sie die Option **Alle auswählen/abwählen** aus, um die Änderungen an allen oder keinem EAM(s) vorzunehmen.

oder

Markieren Sie das Kontrollkästchen neben den entsprechenden Steckplätzen, um die erforderlichen EAMs auszuwählen.

5. Im Abschnitt **VLANs bearbeiten** wählen Sie **Nicht gekennzeichnete VLANs aktualisieren** aus der Dropdown-Liste aus und klicken Sie auf **Anwenden**.

   Es wird eine Warnungsmeldung angezeigt, dass die Konfigurationen des vorhandenen, nicht gekennzeichneten VLANs mit den Konfigurationen des neu zugewiesenen VLANs ohne Kennung überschrieben werden.

6. Klicken Sie zum Bestätigen auf **OK**.

   Die nicht gekennzeichneten VLANs werden mit den Konfigurationen des neu zugewiesenen VLANs ohne Kennung aktualisiert.

   Die Meldung „Vorgang erfolgreich“ wird angezeigt. Die aktuellen den EAMs zugewiesenen VLAN-Einstellungen werden im Feld VLAN-Zuweisung, Zusammenfassung angezeigt.

VLANs für EAMs über die CMC-Webschnittstelle zurücksetzen

So setzen Sie VLANs für IOM(s) auf die Standardkonfigurationen über die CMC-Webschnittstelle zurück:

1. Wählen Sie in der Systemstruktur **E/A-Modul-Übersicht** aus und klicken Sie auf **Setup → VLAN-Manager**.

   Die Seite **VLAN-Manager** wird angezeigt.

2. Wählen Sie im Abschnitt **E/A Modül wählen** die erforderlichen EAMs.
3. Im Abschnitt **VLANs bearbeiten** wählen Sie **VLANs zurücksetzen** aus der Dropdown-Liste aus und klicken Sie auf **Anwenden**.

   Es wird eine Warnungsmeldung angezeigt, dass die Konfigurationen der vorhandenen VLANs mit den Standardkonfigurationen überschrieben werden.

4. Klicken Sie zum Bestätigen auf **OK**.

   Die VLANs werden den ausgewählten IOMs gemäß den Standardkonfigurationen zugewiesen.

   Die Meldung „Vorgang erfolgreich“ wird angezeigt. Die aktuellen den EAMs zugewiesenen VLAN-Einstellungen werden im Feld VLAN-Zuweisung, Zusammenfassung angezeigt.

Energiesteuerungsvorgang für EAMs verwalten

Weitere Informationen zum Einstellen des Energiesteuerungsvorgangs für EAMs finden Sie unter Stromsteuerungsvorgänge für ein E/A-Modul ausführen.

Aktivieren oder Deaktivieren von LED-Blinken für EAMs

Weitere Informationen zur Aktivierung des Blinkens für IOM(s) finden Sie unter LEDs zum Identifizieren von Komponenten im Gehäuse konfigurieren.

14

iKVM konfigurieren und verwenden

Das 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.

Verwandte Links

iKVM-Benutzeroberfläche
Wichtige iKVM Funktionen
Physische Verbindungsschnittstellen

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.

Verwandte Links

OSCAR verwenden

Wichtige iKVM Funktionen

- Sicherheit – Schützt das System mit einem Bildschirmschonerkennwort. Nach einer benutzerdefinierten Zeit wird der Bildschirmschonermodus aktiviert und der Zugriff verhindert, bis das richtige Kennwort zum Reaktivieren von OSCAR eingegeben wird.
- Suchen – Sie können eine Liste mit Servern auswählen, die in der ausgewählten Reihenfolge angezeigt werden, während sich OSCAR im Scan-Modus befindet.
- Server-Identifikation – 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.

  Weitere Informationen zum Ändern von Einschubnamen über die CMC-Webschnittstelle finden Sie unter Steckplatznamen konfigurieren. 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.

Verwandte Links

OSCAR verwenden
Server mit iKVM verwalten
iKVM vom CMC aus verwalten

Aktualisieren der iKVM-Firmware

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 Modul nicht haben, können Sie die Anschlüsse am vorderen Bedienfeld nicht verwenden.

jiKVM-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:

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 vorliegen, 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

ANMERKUNG: 2161DS 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 finden Sie Informationen zum Starten, Konfigurieren und Verwenden der OSCAR-Benutzeroberfläche.

Verwandte Links

Starten des OSCAR
Navigationsgrundlagen
OSCAR konfigurieren

Starten des OSCAR

So starten Sie Oscar:

1. Drücken Sie die Taste <Druck>.

   Das Hauptdialogfeld wird angezeigt.

   Wenn ein Kennwort zugewiesen ist, wird das Dialogfeld **Kennwort** angezeigt nachdem die Taste <Druck> gedrückt wird.

2. Konfigurieren Sie das Kennwort und klicken Sie auf **OK**.

   Das Hauptdialogfeld wird angezeigt.

   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.

Verwandte Links

[Konsolensicherheit einstellen]
[Navigationsgrundlagen]

Navigationsgrundlagen

Tabelle 32. : 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 den Einstellungen unter **OSCAR aufrufen**. Sie können zwei, drei oder alle dieser Tastenfolgen aktivieren, indem Sie das jeweilige Kontrollkästchen im Abschnitt **OSCAR aufrufen** des **Haupt**dialogfeldes 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 **OK** aus und returns kehrt zum vorhergehenden Dialogfeld zurück.
<Eingabetaste>	Führt einen Umschaltvorgang im **Hauptdialogfeld** durch und beendet OSCAR.
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.

Taste oder Tastenfolge	Ergebnis
<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.
<Löschen>	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

Sie können die OSCAR-Einstellungen mithilfe des Dialogfeldes **Setup** konfigurieren.

Aufrufen des Setup-Dialogfelds

So rufen Sie das **Setup-Dialogfeld** auf:

1. Drücken Sie die Taste <Druck>, um die OSCAR-Benutzerschnittstelle aufzurufen.
   Das Dialogfeld **Hauptdialog** wird angezeigt.
2. Klicken Sie auf **Setup**.
   Das Dialogfeld **Setup** wird angezeigt.

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.
Markieren	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.

Verwandte Links

Anzeigeverhalten ändern
Zuweisung von Tastenfolgen für OSCAR
So legen Sie eine Anzeigeverzögerungszeit für OSCAR fest
Einstellen von Status-Flag Anzeige

Anzeigeverhalten ändern

Ändern Sie im **Menü**-Dialogfeld die Anzeigereihenfolge von Servern und legen Sie eine Bildschirmverzögerungszeit für OSCAR fest.

So ändern Sie die Anzeigeeinstellungen:

1. Drücken Sie <Druck>, um OSCAR zu starten.
   Das **Haupt**dialogfeld wird angezeigt.
2. Klicken Sie auf **Setup** und anschließend auf **Menü**.
   Das Dialogfeld **Menü** wird angezeigt.
3. Um die standardmäßige Anzeigereihenfolge von Servern auszuwählen, führen Sie einen der folgenden Vorgänge aus:
   - Wählen Sie **Name** aus, um die Server alphabetisch nach Namen sortiert anzuzeigen.
   - Wählen Sie die Option **Steckplatz** aus, um die Server nach Steckplatznummer anzuzeigen.
4. Klicken Sie auf **OK**.

Zuweisung von Tastenfolgen für OSCAR

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

Um eine Anzeigeverzögerungszeit für OSCAR festzulegen, drücken Sie auf <Druck>, geben Sie die Anzahl der Sekunden ein (0 bis 9), mit der die Anzeige von OSCAR verzögert werden soll, und klicken Sie auf **OK**.

Bei der Eingabe von <0> wird OSCAR ohne Verzögerung gestartet.

Das Festlegen einer Verzögerungszeit für die Anzeige von OSCAR ermöglicht Ihnen, einen Soft-Switch durchzuführen.

Verwandte Links

Soft-Switch ausführen

Einstellen von Status-Flag Anzeige

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.

Markieren	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 stellen Sie die Anzeige des Status-Flags ein:

1. Drücken Sie die Taste <Druck>, um OSCAR zu starten.

   Das **Hauptdialogfeld** wird angezeigt.
2. Klicken Sie auf **Setup** und anschließend auf **Flag**.

   Das Dialogfeld **Flag** wird aufgerufen.
3. 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 nur **Zeitlich bestimmt** auswählen, wird das Flag nicht angezeigt.
4. Wählen Sie im Abschnitt **Anzeigefarbe** eine Flag-Farbe aus. Es stehen Schwarz, Rot, Blau und Lila zur Auswahl.
5. Wählen Sie im **Anzeigemodus** die Option **Opak** für ein Flag in Volltobfarbe aus oder **Transparent**, damit der Desktop durch das Flag zu sehen ist.
6. Klicken Sie zum Platzieren des Status-Flags auf dem Desktop auf **Position festlegen**.

   Das Flag **Position festlegen** wird angezeigt.
7. Klicken Sie mit der linken Maustaste auf die Titelleiste und ziehen Sie sie an den gewünschten Speicherort auf dem Desktop und klicken Sie dann mit der rechten Maustaste, um zum Dialogfeld **Flag** zurückzukehren.
8. Klicken Sie auf **OK** und klicken Sie dann nochmals 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.

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.

Verwandte Links

Peripheriegerätekompatibilität und -Unterstützung

Anzeigen und Auswählen von Servern

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

Wenn Sie OSCAR starten, wird das **Haupt**dialogfeld angezeigt. Verwenden Sie das **Haupt**dialogfeld, um Server über das iKVM anzuzeigen, zu konfigurieren und zu verwalten. Sie können die Server nach Name oder nach Steckplatz anzeigen. Die Steckplatznummer ist die Nummer des Gehäusesteckplatzes, in dem der Server installiert ist. Die Steckplatznummer eines installierten Servers wird in der Spalte **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.

Verwandte Links

Soft-Switch ausführen
Anzeigen des Serverstatus
Server auswählen

Anzeigen des Serverstatus

Die rechten Spalten des **Haupt**dialogfeldes zeigen den Status der Server im Gehäuse an. In der folgenden Tabelle werden die Statussymbole beschrieben.

Tabelle 33. Statussymbole der OSCAR-Benutzeroberfläche

Symbole	Beschreibung
	Server ist online.
	Server ist offline oder nicht im Gehäuse.
	Server ist nicht verfügbar.
	Server wird über den Benutzerkanal genutzt, der mit den folgenden Buchstaben gekennzeichnet ist: • A=rückseitige Abdeckung • B=Frontblende

Server auswählen

Wählen Sie über das **Haupt**dialogfeld Server aus. Wenn Sie einen Server auswählen, konfiguriert das iKVM die Tastatur und Maus mit den ordnungsgemäßen Einstellungen für diesen Server neu.

- Führen Sie einen der folgenden Vorgänge aus, um einen Server auszuwählen:
  - Doppelklicken Sie auf den Servernamen oder die Steckplatznummer.
  - Wenn die Anzeigereihenfolge der Serverliste nach Steckplatz ist (d. h. die Schaltfläche Steckplatz ist aktiviert), geben Sie die Steckplatznummer ein und drücken Sie <Eingabe>.
  - 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>.

- Um zum vorhergehenden Server zurückzuschalten, drücken Sie <Druck> und dann 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.
  - 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 Bildschirm**

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 **Haupt**dialogfeld nach Drücken von <Druck> aufgerufen wird) festgelegt haben und die Tastenfolgen verwenden, bevor diese Zeit abgelaufen ist, wird die OSCAR-Benutzeroberfläche nicht angezeigt.

Verwandte Links

Soft Switching Konfigurieren
Soft-Switch zu einem Server ausführen

Soft Switching Konfigurieren

So konfigurieren Sie OSCAR für einen Soft-Switch:

1. Drücken Sie die Taste <Druck>, um die OSCAR-Benutzerschnittstelle aufzurufen.
   Das **Hauptdialogfeld** wird angezeigt.
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**.

Soft-Switch zu einem Server ausführen

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 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 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 <Eingabe>.
- Um zum vorhergehenden Server zurückzuschalten, drücken Sie <Druck> und dann <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.

Verwandte Links

jiKVM-Verbindungsrangfolge
Den Zugriff auf das iKVM über die Frontblende aktivieren oder deaktivieren

Verdrängungswarnung

Normalerweise hat sowohl ein Benutzer, der über das iKVM, als auch ein anderer Benutzer, der über die Konsolenumleitungsfunktion der iDRAC-Webschnittstelle 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 Konsolenumleitung der iDRAC-Webschnittstelle 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. Weitere Informationen finden Sie unter Serverstatus Anzeigen.

Verwandte Links

Anzeigen des Serverstatus

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** die Konsole mit einem Kennwort, 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.

Verwandte Links

Sicherheitsdialogfeld aufrufen
Setzen des Kennworts
Konsole mit Kennwort schützen
Automatische Abmeldung einstellen
Kennwortschutz von Konsole entfernen
Bildschirmschonermodus ohne Kennwortschutz aktivieren
Bildschirmschonermodus beenden
Verlorenes oder vergessenes Kennwort löschen

Sicherheitsdialogfeld aufrufen

So zeigen Sie das Dialogfeld „Sicherheit“ an:

1. Drücken Sie die Taste <Druck>.
   Das **Hauptdialogfeld** wird angezeigt.
2. Klicken Sie auf **Setup** und anschließend auf **Sicherheit**.
   Das Dialogfeld **Sicherheit** wird angezeigt.

Setzen des Kennworts

So setzen Sie das Kennwort:

1. Klicken Sie einmal und drücken Sie die Taste <Eingabe> oder doppelklicken Sie auf das Feld **Neu**.
2. Geben Sie das Neue Kennwort ein und drücken Sie <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 <Eingabe>.
4. Klicken Sie auf **OK** und schließen Sie das Dialogfeld.

Konsole mit Kennwort schützen

So sichern Sie die Konsole mit einem Kennwort:

1. Legen Sie das Kennwort fest, wie in Einrichten des Kennworts beschrieben.
2. Wählen Sie das Feld **Bildschirmschoner aktivieren** aus.
3. Geben Sie die Anzahl der Minuten für die **Inaktivitätszeit** (von 1 bis 99) ein, mit der der Kennwortschutz und die Bildschirmschoneraktivierung verzögert werden sollen.
4. Bei **Modus**: Wenn der Monitor ENERGY STAR-kompatibel ist, wählen Sie **Energie** aus, andernfalls, wählen Sie **Bildschirm** aus.
   - 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."

   VORSICHT: 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.

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 **Neues Feld**.
3. Lassen Sie **Neues Feld** leer und drücken Sie <Eingabe>.

4. Klicken Sie einmal und drücken Sie <Eingabe> oder doppelklicken Sie auf das Feld **Wiederholen**.
5. Lassen Sie **Neues Feld** leer und drücken Sie <Eingabe>.
6. Klicken Sie auf **OK**.

Bildschirmschonermodus ohne Kennwortschutz aktivieren

ANMERKUNG: Falls die Konsole kennwortgeschützt ist, müssen Sie zuerst den Kennwortschutz entfernen. Entfernen Sie das Passwort bevor sie den Bildschirmschonermodus ohne Kennwortschutz aktivieren.

So aktivieren Sie den Bildschirmschoner-Modus ohne Kennwortschutz:

1. Wählen Sie **Bildschirmschoner aktivieren** aus.
2. Geben Sie die Anzahl der 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.

   VORSICHT: 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 des Tests wird das Dialogfeld **Sicherheit** angezeigt.

   ANMERKUNG: Durch das Aktivieren des **Bildschirmschonermodus** wird die Verbindung des Benutzers zu einem Server getrennt. Folglich ist kein Server mehr ausgewählt. Das Status-Flag zeigt **Frei** an.

Bildschirmschonermodus beenden

Um den Bildschirmschonermodus zu beenden und zum **Hauptdialogfeld** zurückzukehren, drücken Sie eine beliebige Taste oder bewegen Sie die Maus.

Um den Bildschirmschoner auszuschalten, 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.

Um ein verlorenes oder vergessenes iKVM-Kennwort über die CMC-Webschnittstelle zurückzusetzen, gehen Sie zu **Geräuse-Übersicht → iKVM**, klicken Sie auf die Registerkarte **Setup**, und klicken Sie dann auf **Standardwerte wiederherstellen**.

Sie können das Kennwort von der Standardeinstellung des Kennworts über OSCAR ändern. Weitere Informationen zum Definieren eines Kennwortes finden Sie unter Kennwort festlegen.

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 weitere Informationen über den Unterbefehl `getconfig` im *Befehlszeilen-Referenzhandbuch für iDRAC7 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 angezeigt.
2. Klicken Sie auf **Setup** und anschließend auf **Sprache**.
   Das Dialogfeld **Sprache** erscheint.
3. Wählen Sie die erforderliche Sprache aus und klicken Sie 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 angezeigt.
2. Klicken Sie auf **Befehle** und dann auf **Versionen anzeigen**.
   Das Dialogfeld **Version** wird angezeigt. In der oberen Hälfte des Dialogfelds **Version** werden die Subsystemversionen 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.

Verwandte Links

Hinzufügen von Servern zu einer Scan-Liste
Entfernen eines Servers aus einer Scan-Liste
Camcorder-Modus starten
Abbrechen des Scan-Modus

Hinzufügen von Servern zu einer Scan-Liste

So fügen Sie der Scan-Liste Server hinzu:

1. Drücken Sie die Taste <Druck>.
   Das **Hauptdialogfeld** wird angezeigt.
2. Klicken Sie auf **Setup** und dann auf **Suchen**.
   Das Dialogfeld **Suchen** wird aufgerufen, in dem alle Server im Gehäuse aufgelistet werden.
3. Führen Sie eine der folgenden Funktionen aus:

- Wählen Sie die Server aus, die Sie scannen wollen
- Doppelklicken Sie auf den Servernamen oder den Steckplatz.
- Drücken Sie die Taste <Alt > und die Nummer der Server, die gescannt werden sollen. Es können bis zu 16 Server ausgewählt werden.

4. Geben Sie im Feld **Zeit** die Anzahl der Sekunden ein (zwischen 3 und 99), die iKVM abwarten soll, bevor der Scan zum nächsten Server der Folge übergeht.
5. Klicken Sie auf **Hinzufügen** und dann auf **OK**.

Entfernen eines Servers aus einer Scan-Liste

So entfernen Sie einen Server aus der Scan-Liste:

1. Führen Sie eine der folgenden Möglichkeiten im Dialogfeld **Scan** aus:
   - Wählen Sie den Server aus, den Sie entfernen wollen.
   - Doppelklicken Sie auf den Servernamen oder den Steckplatz.
   - Klicken Sie auf die Schaltfläche **Löschen**, um alle Server aus der **Scan**-Liste zu entfernen.
2. Klicken Sie auf **Hinzufügen/Entfernen** und anschließend auf **OK**.

Camcorder-Modus starten

So starten Sie den Camcorder-Modus:

1. Drücken Sie die Taste <Druck>.
   Das **Haupt**dialogfeld wird angezeigt.
2. Klicken Sie auf **Befehle**.
   Das **Befehls**dialogfeld wird angezeigt.
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.

Abbrechen des Scan-Modus

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
   Das **Hauptdialogfeld** wird angezeigt. Wählen Sie einen Server aus der Liste aus.
2. Klicken Sie auf **Befehle**.
   Das Dialogfeld **Befehle** wird angezeigt.
3. Löschen Sie die Option **Scan aktivieren** und klicken Sie dann auf **OK**.

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.

- 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.
- 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.

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 **Haupt**dialogfeld wird angezeigt.
2. Klicken Sie auf **Setup** und anschließend auf **Broadcast**.
   Das Dialogfeld **Broadcast** wird angezeigt.
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.
5. Klicken Sie auf  oder drücken Sie <Esc>, um zum **Hauptdialogfeld** zurückzukehren.
6. Klicken Sie auf **Befehle**.
   Das Dialogfeld **Befehle** wird angezeigt.
7. Klicken Sie auf das Feld **Broadcast aktivieren**, um Broadcasts zu aktivieren.
   Das Dialogfeld **Broadcast-Warnung** wird angezeigt.
8. Klicken Sie auf **OK**, um den Broadcast zu aktivieren. Um den Vorgang abzubrechen und zum Dialogfeld **Befehle** zurückzukehren, klicken Sie  oder drücken Sie zum Abbrechen auf <Esc>
9. 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.

iKVM vom CMC aus verwalten

Sie können auf Folgendes zugreifen:

- iKVM-Status und -Eigenschaften anzeigen
- Aktualisieren der iKVM-Firmware
- Aktivieren oder deaktivieren des Zugriffs auf das iKVM über die Frontblende
- Aktivieren oder deaktivieren des Zugriffs auf das iKVM über die Dell-CMC-Konsole

Verwandte Links

Aktualisieren der iKVM-Firmware
Den Zugriff auf das iKVM über die Frontblende aktivieren oder deaktivieren
iKVM-Informationen und Funktionszustand anzeigen

Aktivieren des iKVM-Zugangs über die Dell CMC-Konsole

Den Zugriff auf das iKVM über die Frontblende aktivieren oder deaktivieren

Sie können den Zugang zu dem iKVM mit der CMC-Webschnittstelle oder RACADM aktivieren oder deaktivieren.

Aktivieren oder Deaktivieren von Zugriff auf das iKVM von der Frontblende über die Webschnittstelle

So aktivieren oder deaktivieren Sie den Zugriff auf das iKVM über die CMC-Webschnittstelle von der Frontblende aus:

1. Gehen Sie in der Systemstruktur zu **Gehäuse-Übersicht** → **iKVM** und klicken Sie auf die Registerkarte **Setup**.
   Die Seite **iKVM-Konfiguration** wird angezeigt.
2. Wählen Sie zur Aktivierung die Option **Frontblenden-USB/Video aktiviert** aus. Löschen Sie zur Deaktivierung die Option **Frontblenden-USB/Video aktiviert**.
3. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

Zugriff auf das iKVM über RACADM von der Frontblende aus 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 Sie sich an und geben Sie Folgendes ein:

```
racadm config -g cfgKVMInfo -o cfgKVMFrontPanelEnable <Wert>
```

wobei <Wert> 1 (aktivieren) oder 0 (deaktivieren) bedeutet. Weitere Informationen über den

`config`

Unterbefehl finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC.*

Aktivieren des iKVM-Zugangs über die Dell CMC-Konsole

Um den Zugriff auf die CMC CLI von iKVM über die CMC-Webschnittstelle zu aktivieren, navigieren Sie in der Systemstruktur zu **Geräuse-Übersicht** → **iKVM** und klicken Sie auf die Registerkarte **Setup**. Wählen Sie die Option **Zugriff auf CMC-CLI über iKVM zulassen** aus und klicken Sie auf **Anwenden**, um die Einstellung zu speichern.

Um den Zugriff auf die CMC CLI über iKVM 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
```

Verwandte Links

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

15

Energieverwaltung und -überwachung

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.

Die Stromverwaltungsfunktionen des M1000e helfen Administratoren, das Gehäuse zu konfigurieren, um den Stromverbrauch zu reduzieren und die Stromverwaltung ggf. auf die bestimmte Umgebung zuzuschneiden.

Das modulare PowerEdge M1000e-Gehäuse verbraucht Wechselstrom und verteilt die Last auf alle aktiven internen Netzteileinheiten. Das System kann bis zu 16685 Watt Wechselstrom übertragen, der Servermodulen und der damit verbundenen Gehäuseinfrastruktur zugeteilt wird.

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.

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-Stromprotokollierung
- Serverleistung vor Stromredundanz
- Dynamische Netzteil-Einsatzfähigkeit
- 110 V Wechselstrombetrieb

PM3 verwaltet dann:

- Server-Stromversorgung
- Serverpriorität
- Eingangsstromkapazität des Systems
- Maximaler Stromsparmodus

ANMERKUNG: Die tatsächliche Stromzuteilung hängt von der Konfiguration und der Auslastung ab.

Sie können die CMC-Webschnittstelle oder RACADM verwenden, um Stromsteuerungen auf CMC zu verwalten und zu konfigurieren:

- Stromzuteilungen, Verbrauch und Status des Gehäuses, der Server und der Netzteile anzeigen
- Strombudget und Redundanzregel für das Gehäuse konfigurieren
- Stromsteuerungsvorgänge (Einschalten, Ausschalten, System-Reset, Aus- und Einschalten) für das Gehäuse ausführen

Verwandte Links

Redundanzregeln
Dynamische Netzteil-Einsatzfähigkeit
Standard-Redundanzkonfiguration

Sie können den folgenden Stromsteuerungsvorgang für das Gehäuse, Server und die E/A-Module ausführen.

Redundanzregeln

Eine Redundanzregel ist ein konfigurierbarer Satz von Eigenschaften, die festlegen, wie der CMC den Strom im Gehäuse verwaltet. Die folgenden Redundanzregeln sind mit oder ohne dynamische Zuschaltung von Netzteileinheiten konfigurierbar:

- Wechselstromredundanz
- Netzteil-Redundanz
- Keine Redundanz

Wechselstrom-Redundanzregel

Die Wechselstrom-Redundanzregel macht es möglich, dass ein modulares Gehäusesystem in einem Modus betrieben wird, in dem es Netzstromausfälle überbrücken kann. Diese Ausfälle können ihren Ursprung im Wechselstromnetz, in der Verkabelung oder in einer Netzteileinheit selbst haben.

Wenn ein System für Wechselstromredundanz konfiguriert wird, dann werden die Netzteileinheiten in Netze aufgeteilt: die Netzteileinheiten in den Steckplätzen 1, 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. Die folgende Abbildung zeigt 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.

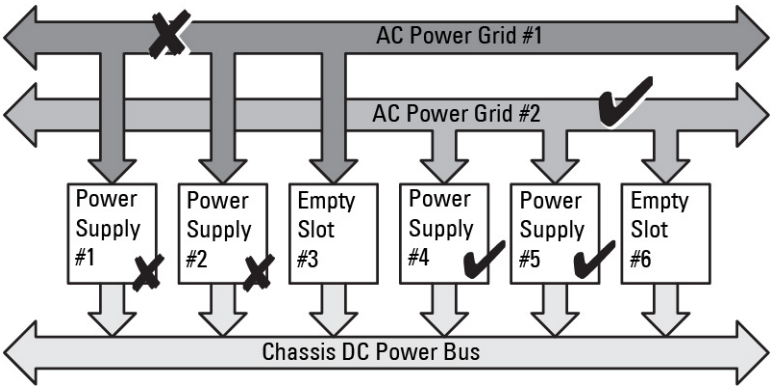


Abbildung 5. Netzteileinheiten pro Netz und ein Stromausfall in Netz 1

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.

Die Netzteilredundanz-Richtlinie

Der Netzteilredundanz-Richtlinie ist nützlich, wenn keine redundanten Stromnetze zur Verfügung stehen und Schutz gegen den Ausfall einer einzelnen Netzteileinheit erwünscht ist, um den Ausfall der Server in einem modularen Gehäuse zu vermeiden. Für diesen Zweck wird die Netzteileinheit mit der größten Kapazität als Onlinereserve gehalten. Das bildet einen Netzteilredundanzpool. Die Abbildung unten zeigt den Netzteilredundanz-Modus.

Etwaige über die für die Stromversorgung und Redundanz erforderlichen Netzteileinheiten sind weiterhin verfügbar und werden dem Pool im Falle eines Ausfalls hinzugefügt.

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

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

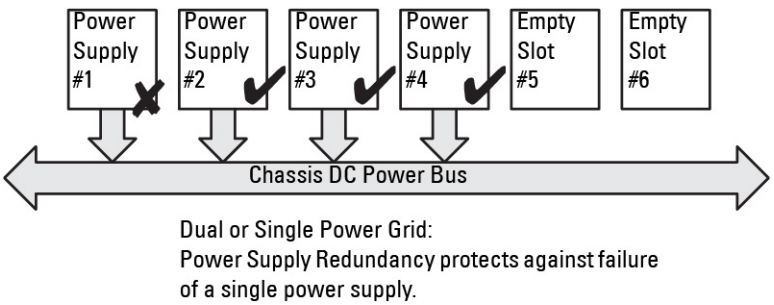


Abbildung 6. Netzteilredundanz: Insgesamt 4 Netzteileinheiten bei Ausfall einer Netzteileinheit.

Die Regel Keine Redundanz

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. Die Abbildung unten veranschaulicht, dass der Modus Keine Redundanz die Standardwerkseinstellung für eine Konfiguration mit drei 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** aufgeführt, 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.

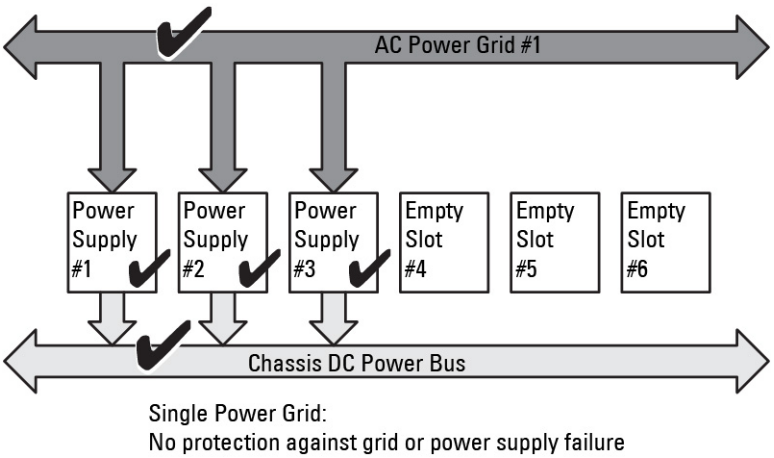


Abbildung 7. Keine Redundanz bei drei Netzteileinheiten im Gehäuse

Der Ausfall einer Netzteileinheit bewirkt, dass die anderen Netzteileinheiten nach Bedarf aus dem Standby-Modus geschaltet werden, um die Gehäusestromzuteilungen zu unterstützen. Wenn Sie vier Netzteileinheiten haben und nur drei benötigen, dann wird die vierte Netzteileinheit im Falle eines Ausfalls online gesetzt. Ein Gehäuse kann alle sechs 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 Standard-Redundanzkonfiguration.

Dynamische Netzteil-Einsatzfähigkeit

Der Modus „Dynamische Zuschaltung von Netzteileinheiten" (DPSE) ist standardmäßig deaktiviert. DPSE spart Strom, indem die Stromeffizienz der Netzteileinheiten optimiert wird, die das Gehäuse mit Strom versorgen. Dies führt zudem zu einer längeren Lebensdauer der Netzteileinheiten und geringerer Hitzeentwicklung.

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.

Betreiben der verbleibenden Netzteileinheiten mit maximaler Effizienz:

- 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 **Netzteilredundanz**modus mit dynamischer Zuschaltung von Netzteileinheiten (DPSE) bietet Energieeffizienz. Mindestens zwei Netzteileinheiten sind aktiv, wobei eine Netzteileinheit die Konfiguration versorgt und eine andere für Redundanz sorgt, falls eine Netzteileinheit ausfällt. Der Netzteileinheitredundanzmodus schützt vor dem Ausfall beliebiger Netzteileinheiten, bietet aber keinen Schutz bei einem Ausfall des Wechselstromnetzes.
- Beim **Wechselstromredundanzmodus** mit dynamischer Zuschaltung von Netzteileinheiten (DPSE) sind mindestens zwei Netzteileinheiten aktiv, eine in jedem Stromnetz. 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 O**nline**; es kann allerdings zwei 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 284 Managing and Monitoring Power Netzteileinheiten in den Zustand Standby gesetzt werden. In einer Konfiguration mit sechs Netzteileinheiten sind immer mindestens zwei Netzteileinheiten eingeschaltet.

  Da bei einem Gehäuse in der **Power Supply Redundancy**-Konfiguration immer eine weitere Netzteileinheit eingeschaltet ist, kann das Gehäuse mit dem Verlust einer Online-Netzteileinheit auskommen und dennoch genügend Strom für die installierten Servermodule zur Verfügung haben. Der Verlust der Online-Netzteileinheit führt dazu, dass eine Stanby-Netzteileinheit einspringt. Gleichzeitiges Versagen mehrerer Netzteileinheiten kann zu Stromverlust für einige Servermodule führen, während die Standby-Netzteileinheiten in Gang kommen.
- 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.

Standard-Redundanzkonfiguration

Die Standard-Redundanzkonfiguration eines Gehäuses hängt von der Zahl der enthaltenen Netzteileinheiten ab, wie in der folgenden Tabelle dargestellt.

Tabelle 34. 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.

VORSICHT: Um einen Systemfehler zu vermeiden und effizient funktionierende Wechselstromredundanz zu gewährleisten, muss sichergestellt werden, dass es einen ausgeglichenen Satz von Netzteileinheiten gibt, der mit separaten Wechselstromkreisen verkabelt ist.

Falls ein Wechselstromnetz ausfällt, übernehmen die Netzteileinheiten des funktionierenden Wechselstromnetzes die Funktion, ohne dass Unterbrechungen für Server oder Infrastruktur auftreten.

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

Netzteil-Redundanz

Wenn Netzteilredundanz aktiviert ist, befindet sich eine Ersatz-Netzteileinheit im Gehäuse. Diese stellt sicher, dass der Ausfall einer anderen Netzteileinheit nicht dazu führt, dass die Stromversorgung der Server oder des Gehäuses unterbrochen wird. Der Netzteilredundanzmodus erfordert 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.

VORSICHT: 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.

Strombudget für Hardwaremodule

Der CMC bietet einen Strombudgetdienst, mit dem Sie Strombudget, Redundanz sowie eine dynamische Stromversorgung für das Gehäuse konfigurieren können.

Mit dem Stromverwaltungsdienst kann der Stromverbrauch optimiert werden; den verschiedenen Modulen kann je nach Bedarf Strom neu zugewiesen werden.

Die folgende Abbildung zeigt ein Gehäuse mit einer Konfiguration von sechs Netzteileinheiten. Die Netzteileinheiten im Gehäuse sind von links nach rechts von 1 bis 6 nummeriert.

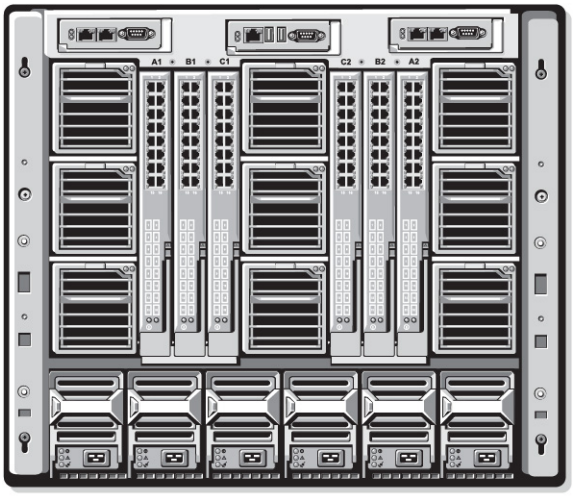


Abbildung 8. Gehäuse mit einer Konfiguration für sechs Netzteileinheiten

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 Spitzenleistung 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 *Systemeingangsstromobergrenze* 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 Systemeingangskapazität* und der benutzerdefinierten Einstellung *Systemeingangsstromobergrenze* 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 11637 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.

Servers teckplatz-Stromprioritätseinstellungen

Der CMC ermöglicht es Ihnen, eine Strompriorität für jeden der 16 Servers teckplätze 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 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.

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.

Anweisung der Prioritätsstufen an Server unter Verwendung der CMC-Webschnittstelle

So weisen Sie Prioritätsstufen unter Verwendung der CMC-Webschnittstelle zu:

1. Wählen Sie in der Systemstruktur **Server-Übersicht** aus und dann klicken Sie auf **Strom → Priorität**.
   Die Seite **Serverpriorität** führt alle Server in dem Gehäuse auf.
2. 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.
3. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

Vergabe von Prioritätsstufen an Server, die RACADM benutzen

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

```
racadm config -g cfgServerInfo -o cfgServer Priority -i <Steckplatznummer>
<Prioritätsstufe>
```

wobei sich <*Steckplatznummer*> (1-16) auf die Position des Servers bezieht und der Wert für die <*Prioritätsstufe*> zwischen 1 und 9 liegt

Beispiel: Um die Prioritätsstufe 1 für den Server in Steckplatz 5 einzustellen, geben Sie den folgenden Befehl ein:

```
racadm config -g cfgServerInfo -o cfgServerPriority -i 5 1
```

Anzeige des Stromverbrauchsstatus

Der CMC zeigt den tatsächlichen Eingangsstromverbrauch für das gesamte System auf der Seite Stromverbrauchsstatus an.

Anzeigen von Stromverbrauchsstatus über die CMC-Webschnittstelle

Um Stromverbrauchsstatus über die CMC-Webschnittstelle anzuzeigen, gehen Sie in der Systemstruktur zu **Gehäuse-Übersicht** und klicken Sie auf **Strom → Stromüberwachung** . Die Seite „Stromüberwachung“ zeigt Stromfunktionszustand, Systemstromstatus, Stromstatistik in Echtzeit und Energiestatistik in Echtzeit an. Weitere Informationen finden Sie in der *CMC-Online-Hilfe*.

ANMERKUNG: Der Stromredundanzstatus wird auch unter Netzteile **in der Systemstruktur → auf dem Register Status** angezeigt.

Anzeigen des Stromverbrauchsstatus mithilfe von RACADM

So zeigen Sie den Stromverbrauchsstatus mithilfe von RACADM an:

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

```
racadm getpminfo
```

Strombudgetstatus anzeigen

Sie können den Strombudgetstatus mit der CMC-Webschnittstelle oder RACADM anzeigen.

Strombudgetstatus über die CMC-Webschnittstelle anzeigen

Um Strombudgetstatus über die CMC-Webschnittstelle anzuzeigen, wählenSie in der Systemstruktur **Gehäuse-Übersicht** aus und klicken Sie auf **Strom** → **Budgetstatus**. Auf der Seite **Strombudgetstatus** werden die Regelkonfiguration des Systemstroms, Strombudgetdetails, Budgetzuweisung für die Servermodule und Informationen über das Netzteil des Gehäuses angezeigt. Weitere Informationen finden Sie unter *CMC-Online-Hilfe*.

Stromverbrauchsstatus mithilfe von RACADM anzeigen

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

```
racadm getpbinfo
```

Lesen Sie für weitere Informationen über **getpbinfo,** einschließlich der Ausgabedetails, den Abschnitt zum **getpbinfo**-Befehl im RACADM *Befehlszeilen-Referenzhandbuch für iDRAC6 und CMC.*

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.

Verwandte Links

Ausfall einer Netzteileinheit unter der Regeloption „Herabgesetzt“ oder „Keine Redundanz“
Entfernung von Netzteileinheiten unter der Regeloption „Herabgesetzt“ oder „Keine Redundanz“
Regel zur Zuschaltung neuer Server
Netzteil- und Redundanzregeländerungen im Systemereignisprotokoll

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. Informationen, um die Redundanzregel festzulegen, finden Sie unter Konfiguration von Stromversorgungsbudget und Redundanz.

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 aufgeführten Redundanzkonfigurationseinstellungen von Netzteileinheiten unter Standard-Redundanzkonfiguration auswählen.

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.

Die folgende Tabelle beschreibt die vom CMC ergriffenen Maßnahmen, wenn ein neuer Server im oben beschriebenen Szenario eingeschaltet wird.

Tabelle 35. 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.

Die folgende Tabelle beschreibt die Firmware-Reaktion, wenn eine Netzteileinheit heruntergefahren oder entfernt wird, hinsichtlich verschiedener Redundanzkonfigurationen von Netzteileinheiten.

Tabelle 36. Auswirkung auf das Gehäuse bei Ausfall oder Entfernung einer Netzteileinheit

Konfiguration der Netzteileinheiten	Dynamische Zuschaltung von Netzteileinheiten	Firmware-Reaktion
Wechselstromredundanz	Deaktiviert	Der CMC alarmiert bei Verlust der Wechselstromredundanz.
Netzteil-Redundanz	Deaktiviert	Der CMC alarmiert bei Verlust der Netzteilredundanz.
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.
Netzteil-Redundanz	Aktiviert	Der CMC alarmiert bei Verlust der Netzteilredundanz. Netzteile im Standby-Modus (wenn vorhanden) werden eingeschaltet, um den Stromverlust in Folge eines Netzteileinheitfehlers oder -ausfalls zu kompensieren.
Keine Redundanz	Aktiviert	Verringerung der Stromversorgung für Server mit niedriger Priorität, falls nötig.

Netzteil- und Redundanzregeländerungen im Systemereignisprotokoll

Änderungen des Netzteilzustands und der Stromredundanzregeln werden als Ereignisse protokolliert. Ereignisse, die mit den Netzteilen zusammenhängen und Einträge im Systemereignisprotokoll (SEL) verursachen, sind Hinzufügen und Entfernen von Netzteilen, Hinzufügen und Entfernen der Netzteileingangsleistung sowie Aussagen zur Netzteilausgangsleistung sowie deren Rücknahme.

Die folgende Tabelle listet die SEL-Einträge auf, die mit Netzteiländerungen zusammenhängen:

Tabelle 37. SEL-Ereignisse für Netzteiländerungen

Netzteilereignis	Systemereignisprotokoll (SEL)-Eintrag
Einfügen	Vorhandenes Netzteil festgestellt
Entfernung	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 **Wechselstromredundanz**regel oder eine **Netzteilredundanz**regel konfiguriert ist. Die folgende Tabelle listet die SEL-Einträge auf, die mit Änderungen der Stromredundanzregeln zusammenhängen.

Stromregelereignis	Systemereignisprotokoll (SEL)-Eintrag
Redundanzverlust	Redundanzverlust wurde festgestellt
Redundanz wiederhergestellt	Redundanzverlust nicht mehr feststellbar

Strombudget und Redundanz konfigurieren

Sie können das Strombudget, die Redundanz und den dynamischen Strom des gesamten Gehäuses (Gehäuse, Server, E/A- Module, iKVM, CMC und Netzteile) konfigurieren, für welches sechs Netzteileinheiten zur Verfügung stehen. Der Stromverwaltungsdienst optimiert den Stromverbrauch und weist den verschiedenen Modulen, basierend auf dem gegenwärtigen Bedarf, Strom zu.

Sie können Folgendes konfigurieren:

- Systemeingangsstrom-Obergrenze
- Redundanzregel
- Serverleistung vor Stromredundanz
- Dynamische Netzteil-Einsatzfähigkeit aktivieren
- Netzschalter des Gehäuses deaktivieren
- 110-V-Wechselstrombetrieb erlauben
- Max. Stromkonservierungsmodus
- Remote-Stromprotokollierung
- Remote-Stromverbrauchsprotokollierungszeitraum
- Serverbasierte Stromverwaltung

Verwandte Links

Stromeinsparung und Strombudget
Maximaler Stromsparmodus
Herabsetzen des Serverstroms zur Einhaltung des Strombudgets
110V Netzteileinheiten Wechselstrom-Betrieb
Serverleistung vor Stromredundanz
Remote-Protokollierung
Externe Energieverwaltung
Konfigurieren von Stromversorgungsbudget und Redundanz über die CMC-Webschnittstelle
Strombudget und Redundanz unter Verwendung von RACADM konfigurieren

Stromeinsparung und Strombudget

Der CMC kann Strom einsparen, wenn die vom Benutzer konfigurierte maximale Stromgrenze erreicht ist. Wenn der Strombedarf die benutzerdefinierte Systemeingangsstromobergrenze überschreitet, verringert der CMC die Stromzufuhr

zu den Servern mit niedriger Priorität, um Strom für Server und andere Module mit höherer Priorität im Gehäuse freizugeben.

Wenn alle oder mehrere Steckplätze im Gehäuse mit derselben Prioritätsstufe konfiguriert sind, verringert der CMC die Stromzufuhr zu den Servern in aufsteigender Steckplatznummernfolge. Beispiel: Wenn die Server in Steckplatz 1 und 2 dieselbe Prioritätsstufe haben, wird die Stromzufuhr für den Server in Steckplatz 1 verringert, bevor die Stromzufuhr für den Server in Steckplatz 2 verringert wird.

ANMERKUNG: Sie können jedem der Server im Gehäuse eine Prioritätsstufe zuweisen, indem Sie ihm eine Nummer von 1 bis einschließlich 9 geben. Die Standardprioritätsstufe für alle Server ist 1. Je niedriger die Zahl, desto höher die Prioritätsstufe.

Das Strombudget ist auf einen Maximalwert begrenzt, der anhand des jeweils schwächsten Satzes von drei Netzteileinheiten bestimmt wird. Wenn versucht wird, einen Wechselstrombudgetwert festzulegen, der die *Systemeingangsstromobergrenze* überschreitet, zeigt das CMC-Modul eine Fehlermeldung an. Das Strombudget ist auf 16685 Watt begrenzt.

Maximaler Stromsparmodus

Der CMC sorgt für maximale Stromeinsparung, wenn:

- Der maximale Stromsparmodus aktiviert ist
- Ein von einem UPS-Gerät automatisch ausgegebenes Befehlszeilenskript den maximalen Sparmodus aktiviert.

Im maximalen Stromsparmodus starten alle Server mit Minimalstrom und alle nachfolgenden Stromzuteilungsanforderungen von Servern werden abgelehnt. In diesem Modus kann es sein, dass die Leistung der eingeschalteten Server herabgesetzt ist. Zusätzliche Server können nicht eingeschaltet werden, unabhängig von deren Priorität.

Die volle Systemleistung wird wieder hergestellt, wenn der maximale Stromsparmodus aufgehoben wird.

Herabsetzen des Serverstroms zur Einhaltung des Strombudgets

Der CMC reduziert Stromzuteilungen von Servern mit niedriger Priorität, wenn zusätzlicher Strom benötigt wird, um den Systemstromverbrauch unterhalb der benutzerdefinierten *Systemeingangsstromobergrenze* zu halten. Wenn beispielsweise ein neuer Server zur Energieüberwachung und -verwaltung 297 zugeschaltet wird, kann der CMC die Stromzufuhr zu Servern mit niedriger Priorität verringern, um den neuen Server mit mehr Strom zu versorgen. Wenn die Strommenge nach der Verringerung der Stromzuteilung zu Servern mit niedriger Priorität nach wie vor nicht ausreicht, drosselt der CMC die Server mit höherer Priorität bis ausreichend Strom freigegeben ist, um den neuen Server mit Strom zu versorgen.

Der CMC reduziert Server-Stromzuteilung in zwei Fällen:

- Der Gesamtstromverbrauch übersteigt die konfigurierbare *Systemeingangsstromobergrenze*.
- Ein Stromausfall tritt in einer nicht-redundanten Konfiguration auf.

110V Netzteileinheiten Wechselstrom-Betrieb

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.

Stromversorgungseinträge werden im SEL-Protokoll protokolliert:

- Wenn 110 V Netzteile ermittelt oder entfernt werden.
- Wenn der 110V Wechselstrom-Eingabebetrieb aktiviert oder deaktiviert ist.

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 aktiviert hat. Das Symbol „Warnung" wird auf der Hauptseite der Webschnittstelle 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.

Serverleistung vor 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 298 Managing and Monitoring Power 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

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.

Externe Energieverwaltung

Die CMC-Energieverwaltung wird optional über die Konsole zum Messen, Verteilen und Steuern (PM3) gesteuert. 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
- Maximaler Stromsparmodus

CMC setzt die Aufrechterhaltung oder Verwaltung der folgenden Aktivitäten fort:

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

Nachdem der serverbasierte Energieverwaltungsmodus aktiviert wurde, ist das Gehäuse auf die PM3-Verwaltung vorbereitet. Die Prioritäten für alle Server der zwölften Generation sind auf „1" (Hoch) gesetzt. PM3 verwaltet die Server-Stromversorgung und die Prioritäten direkt. Da PM3 kompatible Serverstromversorgungszuweisungen steuert, steuert CMC nicht mehr den maximalen Stromsparmodus. Damit ist diese Option nicht mehr auswählbar.

Wenn der maximale Stromsparmodus aktiviert ist, setzt CMC die Eingangsstromkapazität des Systems auf den Maximalwert, den das Gehäuse verarbeiten kann. Bei CMC darf die Stromversorgung die höchst mögliche Kapazität nicht überschreiten. PM3 verarbeitet jedoch alle anderen Beschränkungen bei der Stromkapazität.

Wenn die Stromversorgung über die PM3-Verwaltung deaktiviert ist, geht CMC zu den Serverprioritätseinstellungen zurück, die vor der Aktivierung der externen Verwaltung gültig waren.

ANMERKUNG: Wenn die Verwaltung über PM3 deaktiviert ist, geht CMC nicht zur einer älteren Einstellung für die maximale Stromversorgung des Gehäuses zurück. Weitere Informationen zur früheren Einstellung für die manuelle Wiederherstellung des Wertes finden Sie im **CMC-Protokoll**.

Konfigurieren von Stromversorgungsbudget und Redundanz über die CMC-Webschnittstelle

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, müssen Sie die Berechtigung als **Gehäusekonfigurations-Administrator** besitzen.

So konfigurieren Sie den Strombudgetstatus mithilfe der Webschnittstelle:

1. Gehen Sie in der Systemstruktur zu **Gehäuse-Übersicht** und klicken Sie dann auf **Strom → konfiguration**
   Die Seite **Budget-/Redundanzkonfiguration** wird angezeigt.
2. Wählen Sie bei Bedarf jede oder alle der folgenden Eigenschaften. Weitere Informationen über die Felder finden Sie in der *CMC-Online-Hilfe*.
   - Serverbasierte Stromverwaltung aktivieren
   - Systemeingangsstrom-Obergrenze
   - Redundanzregel
   - Serverleistung vor Stromredundanz
   - Dynamische Netzteil-Einsatzfähigkeit aktivieren
   - Netzschalter des Gehäuses deaktivieren
   - 110-V-Wechselstrombetrieb erlauben
   - Max. Stromkonservierungsmodus
   - Remote-Stromverbrauchsprotokollierung 300 Stromverwaltung und -überwachung aktivieren
   - Remote-Stromverbrauchsprotokollierungszeitraum
3. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

Strombudget und Redundanz unter Verwendung von RACADM konfigurieren

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, müssen Sie die Berechtigung als **Gehäusekonfigurations-Administrator** besitzen.

So aktivieren Sie die Redundanz und legen die Redundanzregel fest:

1. Öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC und melden Sie sich an.
2. Legen Sie die Eigenschaften nach Bedarf fest:

   – Um eine Redundanzregel auszuwählen, geben Sie Folgendes ein:

   ```
   racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy <Wert>
   ```

   wobei der <Wert> 0 für „Keine Redundanz", 1 für „Wechselstromredundanz" und 2 für „Netzteilredundanz" steht. Die Standardeinstellung ist 0.

   Zum Beispiel legt der folgende Befehl die Redundanzregel auf 1 fest:

   ```
   racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy 1
   ```

   – Um einen Wechselstrombudgetwert festzulegen, geben Sie Folgendes ein:

   ```
   racadm config -g cfgChassisPower -o cfgChassisPowerCap <Wert>
   ```

   wobei <Wert> eine Zahl zwischen 2715 und 16685 ist und die maximale Stromgrenze in Watt angibt. Die Standardeinstellung ist 16685.

   Der folgende Befehl setzt zum Beispiel das maximale Strombudget mit 5400 Watt fest:

   ```
   racadm config -g cfgChassisPower -o cfgChassisPowerCap 5400
   ```

   .

   – Um die dynamische Zuschaltung von Netzteileinheiten zu aktivieren oder deaktivieren, geben Sie Folgendes ein:

   ```
   racadm config -g cfgChassisPower -o
   cfgChassisDynamicPSUEngagementEnable <Wert>
   ```

   wobei <Wert> 0 (deaktivieren) oder 1 (aktivieren) bedeutet.

   Der folgende Befehl deaktiviert zum Beispiel die dynamische Zuschaltung von Netzteileinheiten:

   ```
   racadm config -g cfgChassisPower -o
   cfgChassisDynamicPSUEngagementEnable 0
   ```

   .

   – Um den Modus für maximalen Stromverbrauch zu aktivieren, geben Sie Folgendes ein:

   ```
   racadm config -g cfgChassisPower -o cfgChassisMaxPowerConservationMode
   1
   ```

   – Um den Normalbetrieb wiederherzustellen, geben Sie Folgendes ein:

   ```
   racadm config -g cfgChassisPower -o cfgChassisMaxPowerConservationMode
   0
   ```

   – 110 V Wechselstrom-Netzteileinheiten aktivieren:

   ```
   racadm config -g cfgChassisPower -o cfgChassisAllow110VACOperation 1
   ```

   – Aktivieren von „Serverleistung über Stromredundanz":

   ```
   racadm config -g cfgChassisPower -o
   cfgChassisPerformanceOverRedundancy 1
   ```

   – Deaktivieren von Serverleistung über Stromredundanz:

   ```
   racadm config -g cfgChassisPower -o
   cfgChassisPerformanceOverRedundancy 0
   ```

   – Geben Sie zur Aktivierung der Remote-Stromverbrauchsprotokollierungsfunktion den folgenden Befehl ein:

   ```
   racadm config -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingEnabled 1
   ```

   – Geben Sie zur Angabe des gewünschten Protokollierungszeitraums den folgenden Befehl ein:

   ```
   racadm config -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingInterval
   n
   ```

   wobei n 1-1440 Minuten sein kann.

– Geben Sie zur Bestimmung dessen, ob die Remote-Stromverbrauchsprotokollierungsfunktion aktiviert ist den folgenden Befehl ein:

```
racadm getconfig -g cfgRemoteHosts -o
cfgRhostsSyslogPowerLoggingEnabled
```

– Geben Sie zur Bestimmung des Remote-Stromverbrauchsprotokollierungszeitraums den folgenden Befehl ein:

```
racadm getconfig -g cfgRemoteHosts -o
cfgRhostsSyslogPowerLoggingInterval
```

Die Remote-Stromverbrauchsprotokollierungsfunktion hängt von den bereits konfigurierten Remote-Syslog-Hosts ab. Die Protokollierung auf einem oder mehreren Remote-Syslog-Hosts muss aktiviert sein, anderenfalls wird der Stromverbrauch nicht protokolliert. Dies kann entweder mittels der Web-GUI oder RACADM-CLI erfolgen. Weitere Informationen finden Sie in der Anleitung zur Remote-Syslog-Konfiguration.

– Um die Remote-Energieverwaltung durch 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
```

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.

Stromsteuerungsvorgänge ausführen

Sie können den folgenden Stromsteuerungsvorgang für das Gehäuse, Server und die E/A-Module ausführen.

ANMERKUNG: Stromsteuerungsvorgänge wirken sich auf das gesamte Gehäuse aus.

Verwandte Links

Durchführen von Energieverwaltungsmaßnahmen am Gehäuse
Durchführen von Energieverwaltungsmaßnahmen an einem Server
Stromsteuerungsvorgänge für ein E/A-Modul ausführen

Durchführen von Energieverwaltungsmaßnahmen am Gehäuse

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.

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, müssen Sie die Berechtigung als **Gehäusekonfigurations-Administrator** besitzen.

Energieverwaltungsmaßnahmen am Gehäuse über die Webschnittstelle durchführen

So führen Sie auf dem Gehäuse Stromsteuerungsvorgänge unter Verwendung der CMC-Webschnittstelle durch:

1. Wählen Sie in der Systemstruktur **Gehäuse-Übersicht** aus und klicken Sie auf **Strom** → **Steuerung**.
   Die Seite **Gehäuse-Stromsteuerung** wird angezeigt.
2. Wählen Sie eine der folgenden Stromsteuerungsoptionen aus.
   Weitere Informationen zu jeder Option finden Sie in der *CMC-Online-Hilfe*.
   – System einschalten
   – System ausschalten

- System aus- und wieder einschalten (Hardwareneustart)
- Reset CMC (Warmstart)
- Nicht-ordentliches Herunterfahren

3. Klicken Sie auf **Anwenden**.
   Daraufhin werden Sie über ein Dialogfeld zur Bestätigung des Vorgangs aufgefordert.
4. Klicken Sie auf **OK**, um die Energieverwaltungsmaßnahme auszuführen (z. B. das System zurückzusetzen).

Energieverwaltungsmaßnahmen am Gehäuse über RACADM durchführen

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

```
racadm chassisaction -m chassis <Maßnahme>
```

wobei <*Maßnahme*> powerup, powerdown, powercycle, nongraceshutdown oder reset ist.

Durchführen von Energieverwaltungsmaßnahmen an einem Server

Sie können im Remote-Zugriff Stromverwaltungsmaßnahmen für mehrere Server gleichzeitig oder einen individuellen Server im Gehäuse durchführen.

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, müssen Sie die Berechtigung als **Gehäusekonfigurations-Administrator** besitzen.

Stromsteuerungsvorgänge für mehrere Server unter Verwendung der CMC-Webschnittstelle ausführen

So führen Sie Stromsteuerungsvorgänge unter Verwendung der Webschnittstelle für mehrere Server durch:

1. Gehen Sie in der Systemstruktur zu **Server-Übersicht** und dann klicken Sie auf **Strom → -Priorität**.
   Die Seite **Energiesteuerung** wird angezeigt.
2. In der Spalte **Operations** des Drop-Down-Menüs, Wählen Sie einen der nachfolgenden Stromsteuerungsvorgänge für die notwendingen Server aus.
   - Kein Vorgang
   - Server einschalten
   - Server ausschalten
   - Ordentliches Herunterfahren
   - Server zurücksetzen (Softwareneustart)
   - Server aus- und einschalten (Hardwareneustart)

   Weitere Informationen zu den verfügbaren Optionen finden Sie in der *CMC-Online-Hilfe*.
3. Klicken Sie auf **Anwenden**.
   Daraufhin werden Sie über ein Dialogfeld zur Bestätigung des Vorgangs aufgefordert.
4. Klicken Sie auf **OK**, um die Stromverwaltungsmaßnahme durchzuführen (z. B. den Server zurückzusetzen).

Durchführen von Energieverwaltungsmaßnahmen an einem Server unter Verwendung der CMC-Webschnittstelle

So führen Sie auf einem einzelnen Server Stromsteuerungsvorgänge unter Verwendung der CMC-Webschnittstelle durch:

1. Klicken Sie in der Systemstruktur auf . **Gehäuse Übersicht** und dann **Server-Übersicht.**
2. Wählen Sie den Server aus, an dem Sie eine Energieverwaltungsmaßnahme durchführen möchten, und klicken Sie anschließend auf die Registerkarte **Strom**.

Die Seite **Server-Stromverwaltung** wird angezeigt.

3. Wählen Sie eine der folgenden Optionen aus:
   - Server einschalten
   - Server ausschalten
   - Server zurücksetzen (Softwareneustart)
   - Server aus- und einschalten (Hardwareneustart)

   Weitere Informationen zu den verfügbaren Optionen finden Sie in der *CMC-Online-Hilfe*.
4. Klicken Sie auf **Anwenden**.
   Daraufhin werden Sie über ein Dialogfeld zur Bestätigung des Vorgangs aufgefordert.
5. Klicken Sie auf **OK**, um die Stromverwaltungsmaßnahme durchzuführen (z. B. den Server zurückzusetzen).

Durchführen von Energieverwaltungsmaßnahmen unter Verwendung von RACADM an einem Server

Um auf einem Server Stromsteuerungsvorgänge unter Verwendung von RACADM durchzuführen, öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC, melden Sie sich an und geben Sie Folgendes ein:

```
racadm serveraction -m <Modul> <Maßnahme>
```

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.
```

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.

Stromsteuerungsvorgänge auf EAMs unter Verwendung der CMC-Webschnittstelle durchführen

So führen Sie auf einem EAM Stromsteuerungsvorgänge unter Verwendung der CMC-Webschnittstelle durch:

1. Wählen Sie in der Systemstruktur **Gehäuse-Übersicht** → **E/A-Modul-Übersicht** aus und klicken Sie auf **Strom**.
   Die Seite **Stromsteuerung** wird angezeigt.
2. Für das EAM in der Liste wählen Sie aus dem Drop-Down-Menü den Vorgang, den Sie ausführen möchten (Zurücksetzen oder Aus- und einschalten).
3. Klicken Sie auf **Anwenden**.
   Daraufhin werden Sie über ein Dialogfeld zur Bestätigung des Vorgangs aufgefordert.
4. Klicken Sie auf **OK**, um die Stromverwaltungsmaßnahme auszuführen (z. B. um zu veranlassen, dass das E/A-Modul aus- und eingeschaltet wird).

Energieverwaltungsmaßnahmen an EAMs über RACADM durchführen

Um auf einem EAM Stromsteuerungsvorgänge unter Verwendung von RACADM auszuführen, öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole zum CMC, melden Sie sich an und geben Sie Folgendes ein:

```
racadm chassisaction –m switch-<n><Maßnahme>
```

wobei <*n*> als Ziffern 1-6 das EAM (A1, A2, B1, B2, C1, C2) angeben und <Maßnahme> den Vorgang anzeigt, den Sie ausführen möchten: Aus- und Einschalten oder Zurücksetzen.

16

Fehlerbehebung und Wiederherstellung

Dieser Abschnitt erklärt, wie Tasks unter Verwendung der CMC-Webschnittstelle ausgeführt werden, die sich auf die Wiederherstellung und Behebung eines Problems auf dem Remote-System beziehen.

- Gehäuseinformationen anzeigen.
- Ereignisprotokolle anzeigen.
- Konfigurationsinformationen sammeln, Fehlerstatus und Fehlerprotokolle.
- Diagnosekonsole verwenden.
- Strom auf einem Remote-System verwalten.
- Lifecycle Controller-Aufträge auf einem Remote-System verwalten.
- Komponenten zurücksetzen.
- Fehlerbehebung bei Network Time Protocol (NTP)-Problemen.
- Fehlerbehebung bei Netzwerkproblemen.
- Fehlerbehebung bei Warnmeldungsproblemen.
- Vergessenes Administratorkennwort zurücksetzen.
- Gehäusekonfigurationseinstellungen und Zertifikate speichern und wiederherstellen.
- Fehlercodes und -protokolle.

Konfigurationsinformationen und Gehäusestatus und Protokolle mit Verwendung von RACDUMP sammeln

Der Unterbefehl `racdump` bietet die Möglichkeit, mit einem einzigen Befehl umfassende Informationen zu Gehäusestatus, Konfigurationsstatus und den historischen Ereignisprotokollen abzufragen.

Der `racdump`-Unterbefehl zeigt die folgenden Informationen an:

- Allgemeine System-/RAC-Informationen
- CMC-Informationen
- Gehäuseinformationen
- Sitzungsinformationen
- Sensorinformationen
- Firmware-Build-Informationen

Unterstützte Schnittstellen

- CLI-RACADM
- Remote-RACADM
- Telnet-RACADM

Racdump beinhaltet die folgenden Untersysteme und verbindet die folgenden RACADM-Befehle: Weitere Informationen zu racdump finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC und CMC*.

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`
System-Ereignisprotokoll	`getsel`

Herunterladen der SNMP-MIB-Datei Verwaltungsinformationsbasis

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

So laden Sie die CMC-SNMP-MIB-Datei Verwaltungsinformationsbasis über die Web-Schnittstelle herunter:

1. Wählen Sie in der Systemstruktur die Option **Gehäuseübersicht** aus and klicken Sie auf **Netzwerk** → **Dienste** → **SNMP**.
   Daraufhin wird der Abschnitt **SNMP-Konfiguration** angezeigt.
2. 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 **dell.com/support/manuals**.

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:

- Ist das System ein- oder ausgeschaltet?
- Wenn eingeschaltet, funktioniert das Betriebssystem, ist es abgestürzt oder blockiert?
- Wenn ausgeschaltet, wurde der Strom unerwartet ausgeschaltet?

Strombezogene Fehlerbehebung

Die folgenden Informationen sind Ihnen bei der Fehlerbehebung bei Netzteilen und bei der Stromversorgung hilfreich:

- **Problem:** Die **Stromredundanzregel** ist auf **Wechselstromredundanz** eingestellt und es wurde ein Ereignis „Stromversorgungsredundanz verloren“ gemeldet.

- **Lösung A**: Diese Konfiguration erfordert mindestens ein Netzteil in Seite 1 (die linken 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 und 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:** 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 Gehäusestromrichtlinie 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 die Umgebungstemperatur im Rechenzentrum ansteigt.
  - **Lösung:** Dies kann auftreten, wenn die **Eingangsleistungsgrenze** des Systems auf einen Wert konfiguriert wurde, der zu einem erhöhten Strombedarf durch die Lüfter führt und durch Verringerung in der Stromzuweisung zu den Servern wettgemacht werden muss. Der Benutzer kann die **Eingangsleistungsgrenze des Systems** auf einen höheren Wert setzen, der zusätzliche Stromzuweisung zu den Lüftern ermöglicht, ohne die Serverleistung zu beeinträchtigen.

Fehlerbehebungs-Alarme

Verwenden Sie das CMC- und das Ablaufverfolgungsprotokoll, um CMC-Fehlermeldungen zu behandeln. Der Erfolg oder das Fehlschlagen jedes einzelnen E-Mail- und/oder SNMP-Trap-Sendeversuches wird im CMC-Protokoll gespeichert. Zusätzliche Informationen, die die speziellen Fehler beschreiben, werden im Ablaufverfolgungsprotokoll gespeichert. Da SNMP jedoch die Übergabe von Traps nicht bestätigt, ist es am besten, die Pakete auf dem verwalteten System mit Hilfe eines Netzwerkanalysators oder eines Hilfsprogramms wie snmputil von Microsoft zu verfolgen.

Verwandte Links

CMC für das Versenden von Warnungen konfigurieren

Ereignisprotokolle anzeigen

Sie können Hardware- und CMC-protokolle für Informationen über systemkritische Ereignisse, die auf dem verwalteten System auftreten, anzeigen.

Verwandte Links

Hardwareprotokoll anzeigen
CMC-Protokoll anzeigen

Hardwareprotokoll anzeigen

Der CMC erstellt ein Hardwareprotokoll von Ereignissen, die im Gehäuse auftreten. Sie können das Hardwareprotokoll über die Webschnittstelle und Remote-RACADM anzeigen.

ANMERKUNG: Um das Hardwareprotokoll zu löschen, müssen Sie die Berechtigung als **Administrator zum Löschen von Protokollen** besitzen.

ANMERKUNG: Sie können den CMC so konfigurieren, dass E-Mail- oder SNMP-Traps gesendet werden, wenn bestimmte Ereignisse auftreten. Informationen zur Konfiguration des CMC zum Aussenden von Warnungen finden Sie unter Configuring CMC to Send Alerts.

Beispiele von Hardwareprotokolleinträgen

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

Verwandte Links

Ereignisprotokolle anzeigen

Anzeigen von Hardwareprotokollen unter Verwendung der CMC-Webschnittstelle

Sie können das Hardwareprotokoll anzeigen, löschen oder als Textdatei speichern. Sie können die Protokolleinträge nach Schweregrad, Datum/Uhrzeit oder Beschreibung sortieren, indem Sie auf die Spaltenüberschrift klicken. Wenn Sie wiederholt auf eine Spaltenüberschrift klicken, wird die Sortierung rückgängig gemacht.

Um die Hardware-Protokolle unter Verwendung der CMC-Webschnittstelle in der Systemstruktur anzuzeigen, wählen Sie zu **Gehäuseübersicht** aus und klicken Sie auf **Protokolle → Hardwareprotokoll.**Die **Hardwareprotokoll** Seite wird angezeigt. Um eine Kope des Hardwareprotokolls zu speichern, klicken Sie auf **Protokoll speichern** und dann wählen Sie einen Speicherort für eine Textdatei des Protokolls aus.

ANMERKUNG: Weil das Protokoll als Textdatei gespeichert wurde, werden die Grafiken, die zur Kennzeichnung des Schweregrads in der Benutzeroberfläche verwendet werden, nicht angezeigt. In der Textdatei wird der Schweregrad mit den Worten OK, Zur Information, Unbekannt, Warnung und Schwerwiegend angezeigt. Die Einträge von Datum und Uhrzeit erscheinen in aufsteigender Reihenfolge. Wenn <SYSTEMSTART> in der Spalte **Datum/Uhrzeit** erscheint, bedeutet dies, dass das Ereignis während des 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.

Hardware-Protokoll unter Verwendung von RACADM anzeigen

Um das Hardware-Protokoll mit RACADM anzuzeigen, öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole zum CMC, melden Sie sich an und geben Sie Folgendes ein:

```
racadm getsel
```

Um das Hardwareprotokoll zu löschen, geben Sie Folgendes ein:

```
racadm clrsel
```

CMC-Protokoll anzeigen

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

ANMERKUNG: Um das CMC-Protokoll zu löschen, müssen Sie die Berechtigung als **Administrator zum Löschen von Protokollen** besitzen.

Verwandte Links

Ereignisprotokolle anzeigen

CMC Protokolle über die Webschnittstelle anzeigen

Sie können das CMC-Protokoll anzeigen, speichern und 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.

Um das CMC-Protokoll über die CMC-Webschnittstelle in der Systemstruktur anzuzeigen, wählen Sie **Gehäuseübersicht** aus und klicken Sie auf **Protokolle → CMC-Protokoll**. Die Seite **CMC-Protokoll** wird angezeigt.

Um eine Kopie des CMC-Protokolls auf der verwalteten Station oder im Netzwerk zu speichern, klicken Sie auf **Protokoll speichern** und dann geben Sie einen Speicherort an, um die Protokolldatei zu speichern.

Anzeigen von CMC Protokollen über RACADM

Um die Dell CMC-Protokollinformationen mit RACADM anzuzeigen, öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole zum CMC, melden Sie sich an und geben Sie Folgendes ein:

```
racadm getraclog
```

Um das Hardwareprotokoll zu löschen, geben Sie Folgendes ein:

```
racadm clrraclog
```

Diagnosekonsole verwenden

Wenn Sie ein fortgeschrittener Benutzer oder ein Benutzer unter der Leitung des technischen Supports sind, können Sie Probleme im Zusammenhang mit der Gehäuse-Hardware unter Verwendung von CLI-Befehlen diagnostizieren.

ANMERKUNG: Zum Modifizieren dieser Einstellungen müssen Sie die Berechtigung als **Administrator zum Ausführen von Debug-Befehlen** besitzen.

So greifen Sie auf die Diagnose-Konsole unter Verwendung der CMC-Webschnittstelle:

1. Gehen Sie in der Systemstruktur zu **Gehäuse-ÜbersichtFehlerbehebung → Diagnose**.
   Die Seite **Diagnosekonsole** wird angezeigt.
2. Geben Sie im Textfeld **Befehl** einen Befehl ein und klicken Sie auf **Senden. .**
   Weitere Informationen zu den Befehlen finden Sie in der *CMC-Online-Hilfe*.
   Es wird eine Seite mit Diagnoseergebnissen eingeblendet.

Komponenten zurücksetzen

Sie können den aktiven CMC und das iDRAC zurücksetzen, ohne das Betriebssystem neuzustarten, oder Server virtuell neu einsetzen und somit bewirken, dass sie sich so verhalten, als seien sie herausgenommen und wieder eingesetzt worden. Falls das Gehäuse einen Standby-CMC aufweist, bewirkt das Zurücksetzen des aktiven CMC einen Failover und der Standby-CMC wird aktiviert.

ANMERKUNG: Zum Zurücksetzen von Komponenten müssen Sie die Berechtigung als **Debug-Befehl-Administrator** besitzen.

So setzen Sie die Komponenten bei Verwendung der CMC-Webschnittstelle zurück:

1. Wählen Sie in der Systemstruktur **Gehäuseübersicht**und klicken Sie auf **Fehlerbehebung → Komponenten zurücksetzen**.

   Die Seite **Aktualisierbare Komponenten** wird angezeigt.
2. Um den aktiven CMC zurückzusetzen, klicken Sie im Abschnitt **CMC-Status** auf **CMC zurücksetzen/Failover**. Wenn ein Standby-CMC vorhanden ist und ein Gehäuse vollständig redundant ist, tritt ein Failover auf und bewirkt, dass der Standby-CMC aktiv wird.
3. Um nur den iDRAC zurückzusetzen, ohne den Neustart des Betriebssystems durchzuführen, klicken Sie im Abschnitt **Server zurücksetzen** auf **iDRAC-Reset** im Drop-Down-Menü **Reset** für die Server, deren iDRAC Sie zurücksetzen möchten und klicken Sie auf **Auswahl anwenden**. Dies setzt die iDRACs der Server ohne den Neustart des Betriebssystems zurück.

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

   Weitere Informationen zum ausschließlichen Zurücksetzen des iDRACs, ohne den Neustart des Betriebssystems unter Verwendung von RACADM finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC.*

   ANMERKUNG: Nachdem iDRAC zurückgesetzt wurde, werden die Lüfter des Servers auf 100% gesetzt.

   ANMERKUNG: Es wird empfohlen, zuerst iDRAC zurückzusetzen, bevor Sie versuchen, die Server virtuell neueinzusetzen.
4. Um die Server virtuell neueinzusetzen, klicken Sie im Abschnitt **Server zurücksetzen** für die Server, die Sie Neueinsetzen möchten, auf **Virtuelles Neueinsetzen** im Drop-Down-Menü **Reset** und dann auf **Auswahl anwenden**.

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

   Dieser Vorgang simuliert das Entfernen und Wiedereinsetzen eines Servers.

Gehäusekonfiguration speichern oder wiederherstellen.

So führen Sie eine Speicherung oder Wiederherstellung einer Gehäusekonfiguration mithilfe der CMC Webschnittstelle durch:

1. Wählen Sie in der Systemstruktur **Gehäuse-Übersicht** aus und klicken Sie anschließend auf **Setup → Gehäusesicherung**. Die Seite **Gehäusesicherung** wird angezeigt.
2. Klicken Sie zum Speichern der Gehäusekonfiguration auf **Speichern**. 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.
3. Klicken Sie zum Wiederherstellen der Gehäusekonfiguration auf **Datei auswählen**, geben Sie die Sicherungsdatei an, und klicken Sie auf **Wiederherstellen**.

   ANMERKUNG: CMC wird beim Wiederherstellen der Konfiguration nicht zurückgesetzt, jedoch kann es einige Zeit dauern, bis jedwede geänderte oder neue Konfiguration effektiv durch die CMC-Dienste durchgesetzt wird. Nach der erfolgreichen Fertigstellung werden alle aktuellen Sitzungen beendet.

Fehlerbehebung bei Network Time Protocol (NTP)-Fehlern

Nach der Konfiguration des CMC zur Synchronisierung der Uhr mit einem Remote-Zeitserver über das Netzwerk, kann es 2-3 Minuten dauern, bevor eine Änderung des Datums und der Uhrzeit in Kraft tritt. Falls nach dieser Zeit nach wie vor keine Änderung auftritt, handelt es sich möglicherweise um ein Problem, das untersucht werden muss. Der CMC kann seine Uhr möglicherweise aus diesen Gründen nicht synchronisieren:

- Es könnte ein Problem mit den NTP-Server 1-, NTP-Server 2- und NTP-Server 3-Einstellungen vorliegen.
- Es wurden versehentlich ein ungültiger Hostname oder eine ungültige IP-Adresse eingegeben.

- Es könnte ein Netzwerkverbindungsproblem geben, das verhindert, dass der CMC mit den konfigurierten NTP-Servern kommunizieren kann.
- Es könnte ein DNS-Problem geben, das verhindert, dass NTP-Server-Hostnamen aufgelöst werden können.

Überprüfen Sie zur Behebung dieser Fehler die Informationen im CMC-Ablaufverfolgungsprotokoll. Dieses Protokoll enthält eine Fehlermeldung für NTP-bezogene Ausfälle. Falls der CMC sich nicht mit einem konfigurierten NTP-Server synchronisieren kann, dann ist CMC-Zeit mit der lokalen Systemuhr synchronisiert und das Ablaufverfolgungsprotokoll enthält einen Eintrag der folgenden Art:

```
Jan 8 20:02:40 cmc ntpd[1423]: synchronized to LOCAL(0), stratum 10
```

Sie können den ntpd-Status auch prüfen, indem Sie den folgenden racadm-Befehl eingeben:

```
racadm getractime –n
```

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

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

Um den Parameter zu ändern, geben Sie folgenden Befehl ein:

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpMaxDist 32
```

Nach Durchführung der Änderung deaktivieren Sie NTP,warten Sie 5-10 Sekunden und dann aktivieren Sie den NTP neu.

ANMERKUNG: NTP könnte drei zusätzliche Minuten benötigen, um neu zu synchronisieren.

Um NPT zu deaktivieren, geben Sie Folgendes ein:

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpEnable 0
```

Um NPT zu aktivieren, geben Sie Folgendes ein:

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpEnable 1
```

Wenn die NTP-Server richtig konfiguriert sind und dieser Eintrag im Ablaufverfolgungsprotokoll steht, dann bestätigt dies, dass sich der CMC nicht mit einem der konfigurierten NTP-Server synchronisieren kann.

Wenn die NTP-Server-IP-Adresse nicht konfiguriert ist, könnte ein Eintrag der folgenden Art vorhanden sein:

```
Jan 8 19:59:24 cmc ntpd[1423]: Cannot find existing interface for address
1.2.3.4 Jan 8 19:59:24 cmc ntpd[1423]: configuration of 1.2.3.4 failed
```

Falls eine NTP-Server-Einstellung mit einem ungültigen Hostnamen konfiguriert wurde, enthält das Ablaufverfolgungsprotokoll u. U. einen Eintrag der folgenden Art:

```
Aug 21 14:34:27 cmc ntpd_initres[1298]: host name not found: blabla Aug 21
14:34:27 cmc ntpd_initres[1298]: couldn't resolve `blabla', giving up on it
```

Weitere Informationen zur Eingabe des Befehls `gettracelog` zur Prüfung des Ablaufverfolgungsprotokolls unter Verwendung der CMC-Schnittstelle finden Sie unter Diagnosekonsole verwenden.

LED-Farben und Blinkmuster interpretieren

Die LEDs am Gehäuse geben Aufschluss über den Status der Komponenten wie folgt:

- 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 Herunterladen der SNMP-MIB-Datei (Verwaltungsinformationsbasis)).

Tabelle 38. 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	Bereitschaftsmodus
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
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

Komponente	LED-Farbe, Blinkmuster	Bedeutung
	Blau, dunkel	Kein Fehler/untergeordneter Stapel
E/A (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
Netzteil	(Oval) Grün, beständig leuchtend	Wechselstrom OK
	(Oval) Grün, blinkend	Nicht verwendet
	(Oval) Grün, dunkel	Wechselstrom nicht OK
	Gelb, beständig leuchtend	Nicht verwendet
	Gelb blinkend	Fehler
	Gelb, dunkel	Kein Fehler
	(Kreis) Grün, beständig leuchtend	Gleichstrom OK
	(Kreis) Grün, dunkel	Gleichstrom nicht OK

Fehlerbehebung an einem CMC, der nicht mehr reagiert

Wenn Sie sich nicht über eine der Schnittstellen beim CMC anmelden können (Webschnittstelle, Telnet, SSH, Remote-RACADM oder seriell), können Sie die Funktionsfähigkeit des CMC durch Beobachtung der LEDs auf dem CMC überprüfen, Wiederherstellungsinformationen über die serielle DB-9-Schnittstelle abrufen oder das CMC-Firmware-Abbild wiederherstellen.

ANMERKUNG: Es ist nicht möglich, sich über eine serielle Konsole beim Standby-CMC anzumelden.

Problem durch Beobachtung der LEDs erkennen

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:
  - Überprüfen Sie, dass mindestens ein Netzteil mit Netzstrom versorgt wird.
  - Überprüfen Sie, dass die CMC-Karte korrekt eingesetzt ist. Sie können die Entriegelung betätigen, den CMC entfernen, den CMC neu installieren und sicherstellen, dass die Platine vollständig eingeschoben ist und der Riegel richtig einrastet.
- 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, stehen über die serielle DB-9-Schnittstelle, die sich an der Vorderseite des CMC befindet, Wiederherstellungsinformationen zur Verfügung.

So rufen Sie Wiederherstellungsinformationen ab:

1. Installieren Sie ein NULL-Modemkabel zwischen 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 `recover` ein und dann drücken Sie die Taste <Eingabe>.

   Beispiele von Eingabeaufforderungen:

   ```
   recover1[self test] CMC 1 Selbsttestfehler

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

   - Wenn die Eingabeaufforderung auf einen Selbsttestfehler hinweist, befinden sich keine betriebsfähigen Komponenten auf dem CMC. Der CMC ist unbrauchbar und muss zu Dell zurückgesendet werden.
   - Wenn die Eingabeaufforderung **Beschädigte Firmware-Images** anzeigt, folgen Sie den Schritten unter Firmware-Image wiederherstellen, 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 Wiederherstellungsvorgang zeigt die laufende Aktivität an und startet am Ende das CMC-Betriebssystem.

Wenn Sie recover eingeben und dann bei der Eingabeaufforderung zur Wiederherstellung die Taste <Eingabe> drücken, werden der Wiederherstellungsgrund und die verfügbaren Unterbefehle angezeigt. Ein Beispiel einer Wiederherstellungsabfolge könnte folgendermaßen lauten:

```
recover getniccfg recover setniccfg 192.168.0.120 255.255.255.0 192.168.0.1
recover ping 192.168.0.100 recover fwupdate -g -a 192.168.0.100
```

ANMERKUNG: Schließen Sie das Netzwerkkabel an den RJ45 ganz links an.

ANMERKUNG: Im Wiederherstellungsmodus können Sie den CMC normalerweise nicht pingen, da kein aktiver Netzwerkstapel vorhanden ist. Mit dem Befehl `recover ping <TFTP-Server-IP>` können Sie den TFTP-Server pingen, um die LAN-Verbindung zu überprüfen. Möglicherweise müssen Sie auf einigen Systemen den Befehl `recover reset` nach `setniccfg` verwenden.

Fehlerbehebung bei Netzwerkproblemen

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

Das Ablaufverfolgungsprotokoll verfolgt die folgenden Informationen:

- DHCP - Verfolgt Pakete, die an einen DHCP-Server gesendet und von ihm empfangen werden.
- DDNS - Verfolgt dynamische Aktualisierungsanfragen und Antworten des DNS-Servers.
- Konfigurationsänderungen an den Netzwerkschnittstellen.

Das Ablaufverfolgungsprotokoll kann auch spezifische Fehlercodes der CMC-Firmware enthalten, die sich auf die interne CMC-Firmware beziehen und nicht auf das Betriebssystem des verwalteten Systems.

Zurücksetzen des Administratorkennworts

VORSICHT: Viele Reparaturen am Computer dürfen nur von einem zertifizierten Servicetechniker ausgeführt werden. Sie sollten nur die Behebung von Störungen sowie einfache Reparaturen unter Berücksichtigung der jeweiligen Angaben in den Produktdokumentationen von Dell durchführen, bzw. die elektronischen oder telefonischen Anweisungen des Service- und Supportteams von Dell befolgen. Schäden durch nicht von Dell genehmigte Wartungsversuche werden nicht durch die Garantie abgedeckt. Lesen und beachten Sie die Sicherheitshinweise, die Sie zusammen mit Ihrem Produkt erhalten haben.

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 wiederhergestellt werden.

Die CMC-Platine hat einen zweipoligen Reset-Jumper, wie in der folgenden Abbildung zu sehen ist. 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, wie in der folgenden Abbildung zu sehen ist.

Während der PASSWORD_RST-Jumper installiert wird, wird das standardmäßige Administratorkonto und Kennwort aktiviert und auf die folgenden Standardwerte eingestellt:

```
Benutzername: root
Kennwort: 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. Die folgende Abbildung zeigt die Position des Kennwort-Jumpers auf der CMC-Systemplatine.

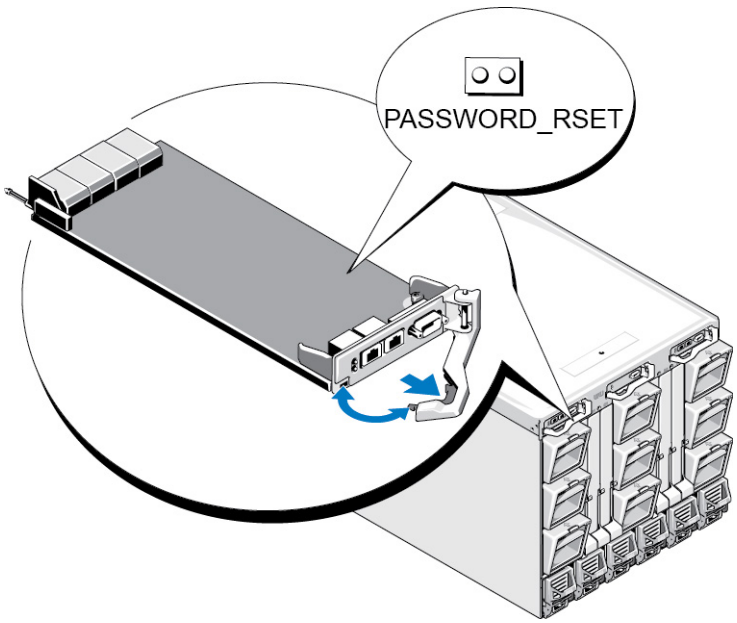


Abbildung 9. Kennwort-Reset-Jumperposition

Tabelle 39. CMC Kennwort-Jumpereinstellungen

PASSWORD_RSET		(Standardeinstellung)	Die Kennwort-Resetfunktion ist deaktiviert.
			Die Kennwort-Resetfunktion ist aktiviert.

3. Schieben Sie das CMC-Modul in das Gehäuse. Schließen Sie alle Kabel wieder an, die eventuell getrennt 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, bis der Neustart abgeschlossen ist. Wenn es ein redundantes CMC im Gehäuse gibt, dann leiten Sie eine Umschaltung ein, um das überbrückte CMC-Modul zu aktivieren. In der Strukturansicht der Web-Schnittstelle, gehen Sie zu **Gehäuseübersicht** und klicken Sie **Energie → Steuerung**. Wählen Sie die Option **Reset CMC (Warmstart)** aus, 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 die erforderlichen Verwaltungsmaßnahmen durch, einschließlich der Erstellung eines neuen Administrator-Kennwortes.

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.

17

LCD-Schnittstelle verwenden

Über das LCD-Bedienfeld des Gehäuses können Sie Konfigurationen und Diagnosen durchführen und Statusinformationen zum Gehäuse und dessen Inhalt abrufen.

In der folgenden Abbildung wird das LCD Bedienfelt veranschaulicht. Auf dem LCD-Bildschirm werden Menüs, Symbole, Bilder und Meldungen angezeigt.

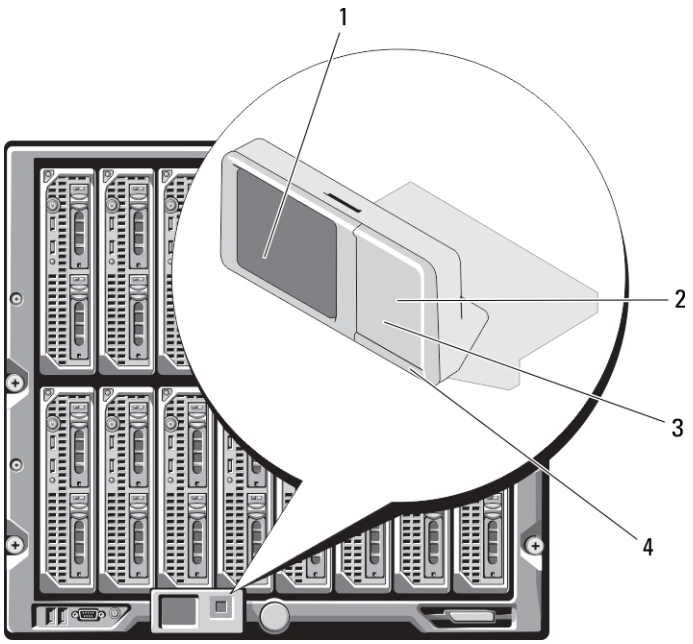


Abbildung 10. LCD-Anzeige

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

Verwandte Links

- LCD-Navigation
- Diagnose
- LCD Hardware-Fehlerbehebung
- Frontblenden-LCD-Meldungen
- LCD-Fehlermeldungen
- LCD-Modul- und Serverstatusinformationen

LCD-Navigation

Die rechte Seite des LCD-Bedienfelds umfasst fünf Schaltflächen: vier Pfeilschaltflächen (nach oben, unten, links und rechts) und eine Schaltfläche in der Mitte.

- *Um zwischen Bildschirmen zu wechseln, verwenden Sie die Pfeilschaltflächen nach rechts (nächster) und nach links (vorhergehender). Während Sie das Bedienfeld verwenden, können Sie jederzeit zum vorhergehenden Bildschirm zurückkehren.*
- *Um auf einem Bildschirm zwischen Optionen zu wechseln, verwenden Sie die Pfeilschaltfläche nach unten und nach oben.*
- *Um auf einem Bildschirm ein Element auszuwählen und zu speichern und zum nächsten Bildschirm zu wechseln, verwenden Sie die Pfeilschaltfläche in der Mitte.*

Anhand der Schaltflächen Nach oben, Nach unten, Nach links und Nach rechts können Sie die ausgewählten Menüelemente oder Symbole auf dem Bildschirm ändern. Das ausgewählte Element wird mit einem hellblauen Hintergrund oder Rahmen dargestellt.

Wenn die auf dem LCD-Bildschirm angezeigten Meldungen nicht auf den Bildschirm passen, führen Sie anhand der Schaltflächen Nach links bzw. Nach rechts einen Bildlauf nach links und rechts durch.

Die in der folgenden Tabelle beschriebenen Symbole werden zum Wechseln zwischen LCD-Bildschirmen verwendet.

Tabelle 40. LCD-Bedienfeld-Navigationssymbole

Symbol Normal	Symbol markiert	Symbolname und -beschreibung
		**Zurück** – Markieren und drücken Sie die mittlere Schaltfläche, um zum vorhergehenden Bildschirm zurückzukehren.
		**Annehmen/Ja** – Markieren und drücken Sie die mittlere Schaltfläche, um eine Änderung anzunehmen und zum vorhergehenden Bildschirm zurückzukehren.
		**Überspringen/Weiter** – Markieren und drücken Sie die mittlere Schaltfläche, um Änderungen zu überspringen und zum nächsten Bildschirm fortzufahren.
		**Nein** – Markieren und drücken Sie die mittlere Schaltfläche, um auf eine Frage mit „Nein“ zu antworten und zum nächsten Bildschirm fortzufahren.
		**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.

Komponente identifizieren – Bringt blaue LED an einem Bauteil zum Blinken.

ANMERKUNG: Um dieses Symbol herum ist ein blinkendes, blaues Rechteck vorhanden, wenn Komponenten identifizieren aktiviert ist.

Eine LED-Statusanzeige auf dem LCD-Bedienfeld zeigt den Gesamtfunktionszustand des Gehäuses und seiner Komponenten an.

- Beständig leuchtendes Blau zeigt einen guten Funktionszustand an.
- Blinkendes Gelb zeigt an, dass sich mindestens eine Komponente in einem fehlerhaften Betriebszustand befindet.
- Blinkendes Blau ist ein ID-Signal, das zur Identifikation eines einzelnen Gehäuses in einer Gruppe von Gehäusen verwendet wird.

Verwandte Links

Hauptmenü
LCD Setup Menu (Menü LCD-Setup)
Spracheinstellungsbildschirm
Standardbildschirm
Graphischer Serverstatusbildschirm
Graphischer Modulstatus-Bildschirm
Gehäuse-Menübildschirm
Modulstatusbildschirm
Gehäusestatus-Bildschirm
IP-Zusammenfassungs-Bildschirm

Hauptmenü

Vom **Haupt**menü 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.

Verwenden Sie die Schaltflächen Nach oben bzw. Nach unten, um ein Element zu markieren.

Drücken Sie die mittlere Schaltfläche, um die Auswahl zu aktivieren.

LCD Setup Menu (Menü LCD-Setup)

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.

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.

Drücken Sie die mittlere Schaltfläche, um die Auswahl zu aktivieren.

Spracheinstellungsbildschirm

Auf dem **Spracheinstellungs**bildschirm 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.

Markieren Sie zur Ansicht des Bildschirms **Graphischer Modulstatus** das Drehen-Symbol und drücken Sie die mittlere Schaltfläche.

Verwenden Sie zur Ansicht des Statusbildschirms für den Server die Pfeilschaltflächen, um den gewünschten Server zu markieren, und drücken Sie die mittlere Schaltfläche. Der Bildschirm **Server-Status** wird angezeigt.

Um zum Hauptmenü zurückzukehren, markieren Sie das **Zurück**-Symbol mit den Pfeilschaltflächen und 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.

Um den Graphischen **Serverstatusbildschirm** anzuzeigen, markieren Sie das Drehen-Symbol und drücken Sie die mittlere Schaltfläche.

Um den Statusbirdschirm für ein Modul anzuzeigen, verwenden Sie die vier Pfeil-Schaltflächen, um das gewünschte Modul zu markieren und klicken Sie auf die mittlere Schaltfläche. Der **Modulstatus**bildschirm wird angezeigt.

Um zum **Hauptmenü** zurückzukehren, markieren Sie das Zurück-Symbol mit den Pfeilschaltflächen und klicken Sie auf 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**

Markieren Sie das gewünschte Element mit den Navigationsschaltflächen (markieren Sie das **Zurück**-Symbol, um zum **Hauptmenü** zurückzukehren) und drücken Sie die mittlere Taste. Der ausgewählte Bildschirm wird angezeigt.

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 und LCD-Fehlermeldungen.

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. Informationen zu den Meldungen, die auf diesem Bildschirm angezeigt werden können, finden Sie unter LCD-Fehlermeldungen. 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-Zusammenfassungs-Bildschirm

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, die nicht auf den Bildschirm passen, einen Bildlauf ausführen.

Wählen Sie mit den Schaltflächen Nach oben und Nach unten das **Zurück**-Symbol aus, und drücken Sie die mittlere Schaltfläche, um zum **Gehäuse**-Menü zurückzuwechseln.

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 bzw. der Server entfernt wird, das/der die Ursache des Problems darstellt, oder indem Sie das Hardwareprotokoll für das Modul oder den Server löschen. Für Serverfehler benutzen Sie die iDRAC Web-Schnittstelle oder Befehlszeilenschnittstelle zum Löschen des Systemereignisprotokolls (SEL/System Event Log). Verwenden Sie für Gehäusefehler die CMC-Webschnittstelle oder die Befehlszeilenschnittstelle, um das Hardwareprotokoll zu löschen.

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.

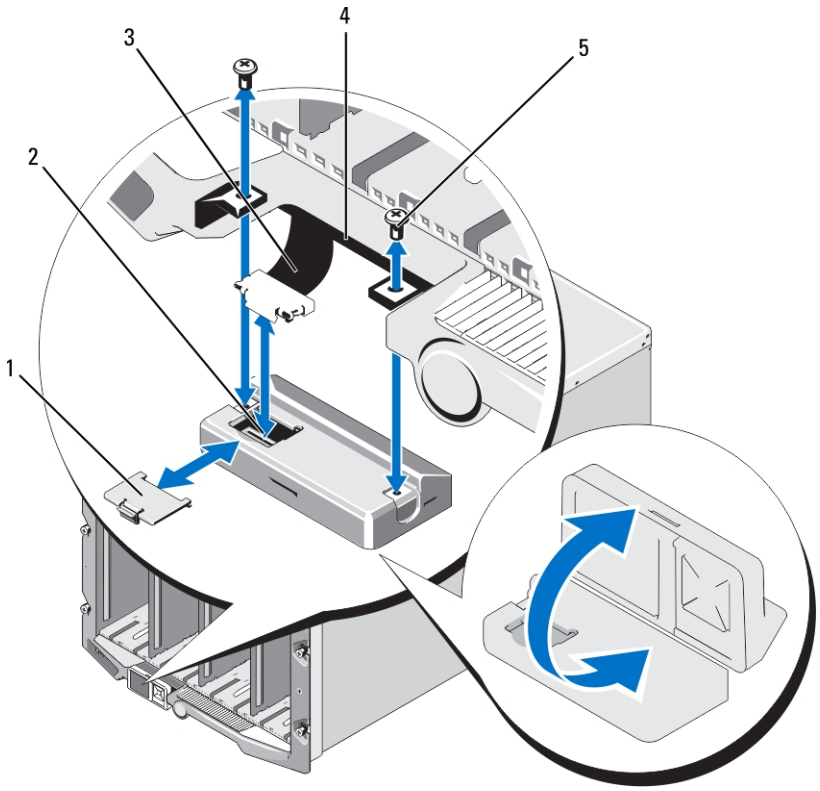


Abbildung 11. LCD-Modul entfernen und installieren

1	Kabelabdeckung	2	LCD-Modul
3	Flachbandkabel	4	Scharniere (2)
5	Schrauben (2)		

Tabelle 41. 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 is durcheinander.	Defekter LCD-Bildschirm.	Tauschen Sie das LCD-Modul aus.
LED und LCD sind aus.	Das LCD-Kabel ist nicht ordnungsgemäß verbunden oder	Zeigen Sie das Hardwareprotokoll mittels GUI oder RACADM-Befehlen an. Suchen Sie nach folgenden Meldungen:

	fehlerhaft; oder das LCD-Modul ist fehlerhaft.	• `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 42. 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. Softwareinkompatibilität zwischen iDRAC in Steckplatz <Nummer> und dem CMC festgestellt.	Die Firmware der beiden Geräte stimmt nicht überein, sodass eine oder mehrere Funktionen nicht unterstützt werden.
Warnung	Es wurde eine Firmware- bzw. Softwareinkompatibilität zwischen dem System-BIOS in Steckplatz <Nummer> und dem CMC festgestellt.	Die Firmware der beiden Geräte stimmt nicht überein, sodass eine oder mehrere Funktionen nicht unterstützt werden.
Warnung	Es wurde eine Firmware- bzw. Softwareinkompatibilität zwischen CMC 1 und CMC 2 festgestellt.	Die Firmware der beiden Geräte stimmt nicht überein, sodass eine oder mehrere Funktionen nicht unterstützt werden.

Tabelle 43. 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. Keine ausreichenden Ressourcen zur Beibehaltung 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.
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	Die gesamte Ereignisprotokollierung wird 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 44. 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 45. 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 46. 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 behebbar	Lokales KVM funktioniert nicht und wurde ausgeschaltet.	Serieller RIP-Fehler oder USB-Host-Chip-Fehler.

Tabelle 47. 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.
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 48. 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

Schweregrad	Meldung	Ursache
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	Der Speicherakku ist fast erschöpft.	Niedriger Batteriestand des ROMB.
Kritisch	Ausfall der Batterie des Speichers.	CMOS-Batterie ist nicht vorhanden oder weist keine Spannung auf.
Kritisch	CPU-Spannung <Nummer> <Spannungssensorname> befindet sich außerhalb des zulässigen Bereichs.	
Kritisch	Systemplatinenspannung <Spannungssensorname> befindet sich außerhalb des zulässigen Bereichs.	
Kritisch	Mezzanine-Kartenspannung <Nummer> <Spannungssensorname> befindet sich außerhalb des zulässigen Bereichs.	
Kritisch	Speicherspannung <Spannungssensorname> befindet sich außerhalb des zulässigen Bereichs.	
Kritisch	Prozessor <Nummer> weist einen internen Fehler auf [IERR].	CPU-Fehler.
Kritisch	Prozessor <Nummer> weist ein Übertemperaturereignis (thermischer Auslöser) auf.	CPU überhitzt.
Kritisch	Die Konfiguration von Prozessor <Nummer> wird nicht unterstützt.	Falscher Prozessortyp oder an falscher Position.
Kritisch	Prozessor <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.
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> festgestellt.	Speicherlaufwerk fehlerhaft.

Schweregrad	Meldung	Ursache
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	Der Watchdog-Zeitmesser hat das System 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.
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	Bei einer Komponente auf Steckplatz <Nummer> wurde ein PCI-Paritätsfehler festgestellt.	Auf dem PCI-Bus wurde ein Paritätsfehler festgestellt.

Schweregrad	Meldung	Ursache
Kritisch	Es wurde ein PCI-Systemfehler an einer Komponente auf Bus <Nummer> Gerät <Nummer> erkannt.	PCI-Fehler wurde von Komponente erkannt.
Kritisch	Bei einer Komponente auf Steckplatz <Nummer> wurde ein PCI-Systemfehler festgestellt.	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	Die gesamte Ereignisprotokollierung wird deaktiviert.	
Nicht behebbar	Prozessorprotokollfehler erkannt.	Das Prozessorprotokoll ist in einen nicht wiederherstellbaren Zustand übergegangen.
Nicht behebbar	Paritätsfehler am Prozessorbus festgestellt.	Der Prozessor-Bus-PERR ist in einen nicht wiederherstellbaren Zustand übergegangen.
Nicht behebbar	Prozessorinitialisierungsfehler erkannt.	Die Prozessorinitialisierung ist in einen nicht wiederherstellbaren Zustand übergegangen.
Nicht behebbar	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.
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 FlexAddress oder Link-Tuning durch Geräte-Options-ROM auf Zusatzkarte <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 49. CMC-Status

Element	Beschreibung
Beispiel: CMC1, CMC2	Name/Standort.
Keine Fehler	Wenn kein Fehler auftritt, wird „Keine Fehler“ angezeigt, ansonsten werden Fehlermeldungen aufgeführt.
Firmware-Version	Wird nur auf einem aktiven CMC angezeigt. Zeigt für den Standby-CMC Standby an.
IP4 <aktiviert, deaktiviert>	Zeigt den aktuellen IPv4-Aktivierungsstatus nur auf einem aktiven CMC an.
IP4 Adresse: <Adresse, wird bezogen>	Wird nur dann angezeigt, wenn IPv4 nur auf einem aktiven CMC aktiviert wurde.
IP6 <aktiviert, deaktiviert>	Zeigt den aktuellen IPv6-Aktivierungsstatus nur auf einem aktiven CMC an.
Lokale IP6-Adresse: <Adresse>	Wird nur dann angezeigt, wenn IPv6 nur auf einem aktiven CMC aktiviert wurde.
Globale IP6-Adresse: <Adresse>	Wird nur dann angezeigt, wenn IPv6 nur auf einem aktiven CMC aktiviert wurde.

Tabelle 50. Gehäusestatus

Element	Beschreibung
Benutzerdefinierter Name	Beispiel: „Dell-Rack-System“. Dies ist über die CMC-CLI oder die Web-GUI einstellbar.
Fehlermeldungen	Bei keinem Fehler wird Keine Fehler angezeigt; ansonsten werden Fehlermeldungen aufgelistet - zuerst schwerwiegende Fehler und danach Warnungen.
Modellnummer	Beispiel „PowerEdgeM1000“.
Stromverbrauch	Aktueller Stromverbrauch in Watt.
Spitzenleistung	Spitzenstromverbrauch in Watt.
Minimaler Strom	Mindeststromverbrauch in Watt.
Umgebungstemperatur	Umgebungstemperatur in Grad Celsius.
Service-Tag-Nummer	Die vom Werk zugewiesene Service-Tag-Nummer.
CMC-Redundanzmodus	Nicht-redundant oder Redundant.

Netzteileinheit-Redundanzmodus	Nicht-redundant, wechselstromredundant oder gleichstromredundant.

Tabelle 51. 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 52. 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 53. 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	Die vom Werk zugewiesene Service-Tag-Nummer.

Tabelle 54. 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	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 55. 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.
Name	Name des Servers, dies kann durch den Benutzer über Dell OpenManage eingestellt werden. Der Name wird nur dann angezeigt, wenn iDRAC den Startvorgang abgeschlossen hat und der Server diese Funktion unterstützt, anderenfalls werden iDRAC-Startmeldungen angezeigt.
Modellnummer	Wird angezeigt, wenn der iDRAC den Bootvorgang abgeschlossen hat.
Service-Tag	Wird angezeigt, wenn der iDRAC den Bootvorgang abgeschlossen hat.
BIOS Version	Firmwareversion des Server BIOS.
Letzter POST-Code	Zeigt die letzte Meldungszeichenkette mit Server-BIOS POST-Codes an.
iDRAC-Firmware-Version	Wird angezeigt, wenn der iDRAC den Bootvorgang abgeschlossen hat. **ANMERKUNG:** iDRAC Version 1.01 wird als 1.1 angezeigt. Es gibt keine iDRAC-Version 1.10.

IP4 <aktiviert, deaktiviert>	Zeigt den aktuellen IPv4-Aktivierungsstatus an.
IP4 Adresse: <Adresse, wird bezogen>	Wird nur bei aktiviertem IPv4 angezeigt.
IP6 <aktiviert, deaktiviert>	Wird nur dann angezeigt, wenn iDRAC IPv6 unterstützt. Zeigt den aktuellen IPv6-Aktivierungsstatus an.
Lokale IP6-Adresse: <Adresse>	Wird nur angezeigt, wenn iDRAC IPv6 unterstützt und IPv6 aktiviert ist.
Globale IP6-Adresse: <Adresse>	Wird nur angezeigt, wenn iDRAC IPv6 unterstützt und IPv6 aktiviert ist.
FlexAddress aktiviert auf Strukturen	Wird nur angezeigt, wenn die Funktion installiert ist. Listet die für diesen Server aktivierten Strukturen auf (d.h., A, B, C).

Die Informationen in Tabelle 17-16 werden dynamisch aktualisiert. Wenn der Server diese Funktion nicht unterstützt, dann werden die folgenden Informationen nicht angezeigt, anderenfalls lauten die Server-Administratoroptionen wie folgt:

- Option „Keine“ = Es müssen keine Zeichenketten auf dem LCD angezeigt werden.
- Option „Standard“ = Keine Auswirkung.
- Option „Benutzerdefiniert“ = Ermöglicht Ihnen die Eingabe eines Zeichenkettennamens für den Server.

Die Informationen werden nur angezeigt, wenn der iDRAC den Startvorgang abgeschlossen hat. Weitere Informationen zu dieser Funktion finden Sie im *RACADM-Befehlszeilen-Referenzhandbuch für iDRAC7 und CMC*.

18

Häufig gestellte Fragen (FAQs)

In diesem Abschnitt werden häufig gestellte Fragen zu den folgenden Themen aufgelistet:

RACADM

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

```
racadm <Unterbefehl> Transport: ERROR: (RC=-1)
```

Was bedeutet diese Meldung?

Ein anderer Befehl muss nur dann ausgegeben werden, nachdem CMC-Reset abgeschlossen ist.

Durch die Verwendung der RACADM-Unterbefehle wird manchmal ein oder mehrere der folgenden Fehler angezeigt:

- Lokale RACADM-Fehlermeldungen - Probleme wie Syntax, typografische Fehler und falsche Namen. Beispiel: `FEHLER: <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 comman failed" (racadm-Befehl fehlerhaft) sein.

Geben Sie für Informationen zum Debuggen `racadm gettracelog` ein.

Während ich Remote-RACADM verwendet habe, wechselt die Eingabeaufforderung zu „>" und die Eingabeaufforderung „$" wird nicht wieder angezeigt.

Wenn ein nicht übereinstimmendes doppeltes Anführungszeichen (") oder ein nicht übereinstimmendes einfaches Anführungszeichen (') als Teil des Befehls eingegeben wird, dann wechselt die Befehlszeile zur Aufforderung „>" und stellt alle Befehle in die Warteschlange.

Um zur Eingabeaufforderung „$" zurückzukehren, geben Sie <Strg>–d ein.

Eine Fehlermeldung „Nicht gefunden" wird beim Verwenden der Befehle `$ logout`- und `$ quit` angezeigt.

Die Abmelden- und Beenden-Befehle sind in der CMC-RACADM-Befehlszeilenschnittstelle nicht unterstützt.

Remote-System verwalten und wiederherstellen

Wenn ich auf die CMC-Schnittstelle zugreife, erhalte ich eine Sicherheitswarnung, die besagt, dass der Host-Name des SSL-Zertifikats nicht mit dem Host-Namen des CMC übereinstimmt.

Der CMC enthält ein Standard-CMC-Serverzertifikat zur Sicherung der Netzwerksicherheit für die Webschnittstelle und die Remote-RACADM-Funktionen. Wenn dieses Zertifikat verwendet wird, zeigt der Webbrowser eine

Sicherheitswarnung an, weil das Standardzertifikat als CMC-Standardzertifikat ausgegeben wird, was nicht mit dem Host-Namen des CMC (z. B. IP-Adresse) übereinstimmt.

Um dieses Sicherheitsproblem zu beseitigen, laden Sie ein CMC-Serverzertifikat herunter, das auf die IP-Adresse des CMC ausgestellt ist. Wenn Sie die Zertifikatsignierungsanforderung (CSR) zur Ausgabe des Zertifikats erstellen, müssen Sie sicherstellen, dass der allgemeine Name (CN) des CSR der IP-Adresse des CMC (z. B. 192.168.0.120) oder dem eingetragenen DNS-CMC-Namen entspricht.

So stellen Sie sicher, dass die CSR dem eingetragenen DNS-CMC-Namen entspricht:

1. 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. Wählen Sie das **Kontrollkästchen CMC** auf DNS Option.
4. Geben Sie den CMC-Namen in das Feld **DNS-CMC-Name** ein.
5. Klicken Sie auf **Änderungen anwenden**.

   Weitere Informationen über die Erstellung von Zertifikatsignierungsanforderungen und die Ausgabe von Zertifikaten finden Sie unter Zertifikate Erhalten.

   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:

   - Änderung der Netzwerkkonfiguration oder Netzwerksicherheitseigenschaften über die CMC-Webschnittstelle.
   - Die Eigenschaft cfgRacTuneHttpsPort wird geändert (einschließlich der Änderung durch eine config -f-<Konfigurationsdatei>).
   - Bei Verwendung von `racresetcfg` oder Wiederherstellen einer Gehäusekonfigurationssicherung.
   - CMC wird zurückgesetzt.
   - Ein neues SSL-Serverzertifikat wird hochgeladen.

   Warum registriert mein DNS-Server meinen CMC nicht?

   Einige DNS-Server registrieren nur Namen mit höchstens 31 Zeichen.

   Wenn ich auf die CMC-Webschnittstelle zugreife, erhalte ich eine Sicherheitswarnung, die aussagt, dass das SSL-Zertifikat durch eine nicht vertrauenswürdige Zertifizierungsstelle ausgegeben wurde.

   Der CMC enthält ein Standard-CMC-Serverzertifikat zur Sicherung der Netzwerksicherheit für die Webschnittstelle und die Remote-RACADM-Funktionen. Dieses Zertifikat wurde nicht von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt. Um dieses Sicherheitsproblem zu beseitigen, laden Sie ein CMC-Serverzertifikat von einer vertrauenswürdigen Zertifizierungsstelle (z. B. Thawte oder Verisign) hoch. Weitere Informationen über Zertifikate finden Sie unter Zertifikate Erhalten.

   Warum wird die folgende Meldung aus unbekannten Gründen angezeigt?

   `Remote-Zugriff: SNMP-Authentifizierungsfehler`

   Als Teil der Ermittlung versucht IT Assistant, die **Get**- und **Set**-Community-Namen des Geräts zu überprüfen. Im IT Assistant ist der **Get-Community-Name = public** und der **Set-Community-Name = private**. Standardmäßig ist der Community-Name für den CMC-Agenten „public“. Wenn IT Assistant eine Set-Aufforderung sendet, erstellt der CMC-Agent den SNMP-Authentifizierungsfehler, da er nur Aufforderungen von **Community = public** akzeptiert.

   Ändern des CMC-Community-Namens mit RACADM. Um den CMC Community-Namen zu sehen, verwenden Sie den folgenden Befehl:

   ```
   racadm getconfig -g cfgOobSnmp
   ```

   Um den CMC Community-Namen anzugeben, verwenden Sie den folgenden Befehl:

```
racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <Community-Name>
```

Um die Erzeugung von SNMP-Authentifizierungs-Traps zu verhindern, geben Sie Community-Namen ein, die vom Agenten akzeptiert werden. Da der CMC nur einen Community-Namen zulässt, geben Sie den gleichen Get- und Set-Community-Namen für das IT Assistant-Ermittlungs-Setup ein.

Geben Sie ein Beispiel ein, dass die aktuelle Aufgabe illustriert (optional).

Geben Sie ein Beispiel ein, dass der Benutzer nach der Beendigung der Aufgabe durchführen sollte (optional).

Active Directory

Unterstützt Active Directory CMC-Anmeldung über mehrfache Strukturen?

Ja. Der Abfragealgorithmus des CMC-Active Directory unterstützt mehrere Strukturen in einer Gesamtstruktur.

Funktioniert die Anmeldung am CMC unter Verwendung des Active Directory im gemischten Modus (d. h. die Domänen-Controller der Gesamtstruktur führen verschiedene Betriebssysteme aus, wie z. B. Microsoft Windows 2000 oder Windows Server 2003)?

Ja. Im gemischten Modus müssen sich alle Objekte, die vom CMC-Abfrageverfahren verwendet werden, (unter Benutzer, RAC-Geräteobjekt und Zuordnungsobjekt) in derselben Domäne befinden.

Das Dell-erweiterte Active Directory-Benutzer- und Computer-Snap-In überprüft den Modus und beschränkt Benutzer, um Objekte über Domänen hinweg zu erstellen (nur im gemischten Mischmodus).

Unterstützt die Verwendung des CMC mit Active Directory mehrfache Domänenumgebungen?

Ja. Die Domänen-Gesamtstrukturfunktionsebene muss sich im Native-Modus oder Windows-2003-Modus befinden. Außerdem müssen die Gruppen unter Zuordnungsobjekt, RAC-Benutzerobjekten und RAC-Geräteobjekten (einschließlich Zuordnungsobjekt) Universal-Gruppen sein.

Können diese Dell-erweiterten Objekte (Dell-Zuordnungsobjekt, Dell RAC-Gerät und Dell-Berechtigungsobjekt) in verschiedenen Domänen sein?

Das Zuordnungsobjekt und das Berechtigungsobjekt müssen sich in derselben Domäne befinden. Beim Dell-erweiterten Active Directory-Benutzer- und -Computer-Snap-In können Sie diese zwei Objekte nur in derselben Domäne erstellen. Andere Objekte können sich in verschiedenen Domänen befinden.

Gibt es Beschränkungen der Domänen-Controller SSL-Konfiguration?

Ja. Alle SSL-Zertifikate für Active Directory-Server in der Gesamtstruktur müssen von dem gleichen, von der root-Zertifizierungsstelle signierten, Zertifikat signiert werden, da der CMC nur erlaubt, ein einziges von einer vertrauenswürdigen Zertifizierungsstelle signiertes SSL-Zertifikat, hochzuladen.

Die Webschnittstelle startet nicht nach dem Erstellen und Hochladen eines neuen RAC-Zertifikats.

Wenn Sie Zertifikatsdienste von Microsoft verwenden, um das RAC-Zertifikat zu erstellen, haben Sie beim Erstellen des Zertifikats möglicherweise versehentlich Benutzerzertifikat ausgewählt anstatt Webzertifikat.

Generieren Sie zur Wiederherstellung eine CSR, erstellen Sie ein neues Webzertifikat von Microsoft Certificate Services und laden Sie es mit Hilfe der folgenden RACADM-Befehle hoch:

```
racadm sslcsrgen [-g] [-f {filename}]
racadm sslcertupload -t 1 -f {web_sslcert}
```

FlexAddress und FlexAddressPlus

Was geschieht bei Entfernen einer Funktionskarte?

Wenn eine Funktionskarte entfernt wird, gibt es keine sichtbare Veränderung. Funktionskarten können entfernt und aufbewahrt oder im System belassen werden.

Was passiert, wenn eine Funktionskarte, die in einem Gehäuse verwendet wurde, entfernt und in ein anderes Gehäuse gesteckt wird?

Die Webschnitstelle zeigt die folgende Fehlmeldung an:

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

Was passiert, wenn die Funktionskarte entfernt und eine Karte, die FlexAddress nicht unterstützt, eingesetzt wird?

Es findet keine Aktivierung oder Änderung der Karte statt. Die Karte wird vom CMC ignoriert. In dieser Situation gibt der Befehl **$racadm featurecard -s** folgende Meldung zurück:

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

Was passiert mit einer ans Gehäuse gebundenen Funktionskarte, wenn die Gehäuse-Service-Tag-Nummer neu programmiert wird?

- Wenn die Original-Funktionskarte im aktiven CMC auf diesem oder einem beliebigen anderen Gehäuse vorhanden ist, zeigt die Webschnittstelle die folgende Fehlermeldung an:

  ```
  Diese Funktionskarte wurde auf einem anderen Gehäuse aktiviert. Sie muss
  vor einem Zugriff auf die Funktion FlexAddress entfernt werden.
  Aktuelle Gehäuse-Service-Tag-Nummer = XXXXXXXX
  Gehäuse-Service-Tag-Nummer der Funktionskarte = YYYYYYYY
  ```

  Die Original-Funktionskarte ist ni:cht mehr für Deaktivierung auf diesem oder einem beliebigen anderen Gehäuse berechtigt, es sei denn Dell-Service programmiert das Original-Gehäuse-Service-Tag wieder in ein Gehäuse zurück, und der CMC, der die Original-Funktionskarte besitzt, wird auf diesem Gehäuse aktiviert.
- Die FlexAddress-Funktion bleibt auf dem ursprünglich gebundenen Gehäuse aktiviert. Die Funktion *Bindung* dieses Gehäuses wird aktualisiert, um das neue Service-Tag widerzuspiegeln.

Erhalte ich eine Fehlermeldung, wenn in meinem redundanten CMC-System zwei Funktionskarten installiert sind?

Die Funktionskarte im aktiven CMC wird aktiv und im Gehäuse installiert sein. Die zweite Karte wird vom CMC ignoriert.

Hat die SD-Karte einen Schreibschutz?

Ja. Bevor Sie die SD-Karte in das CMC-Modul installieren, bestätigen Sie, dass sich die Schreibschutzsperre in der „Entsperr"-Position befindet. Die FlexAddress-Funktion kann nicht aktiviert werden, wenn die SD-Karte schreibgeschützt ist. In dieser Situation gibt der Befehl **$racadm feature -s** folgende Meldung zurück:

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

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

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

```
Keine Funktionskarte eingesetzt.
```

Was passiert mit der FlexAddress-Funktion, wenn das Server-BIOS von Version 1.xx auf Version 2.xx aktualisiert wird?

Das Servermodul muss 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.

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.

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 in einem Gehäuse mit redundanten CMCs ein CMC durch einen CMC mit einer Firmware vor Version 1.10 ersetzt wird, muss das folgende Verfahren verwendet werden, um sicherzustellen, dass die derzeitige FlexAddress-Funktion und die Konfiguration NICHT entfernt werden.

- Versichern Sie sich, dass der aktive CMC stets die Firmwareversion 1.10 oder höher aufweist.
- Entfernen Sie den Standby-CMC und setzen Sie den neuen CMC ein.
- Erweitern Sie die Firmware des neuen Standby-CMC über den aktiven CMC auf Version 1.10 oder höher.

ANMERKUNG: Wenn die Standby-CMC-Firmware nicht auf Version 1.10 oder höher aktualisiert wird und es findet ein Failover statt, wird die Funktion FlexAddress nicht konfiguriert. Die Funktion muss reaktiviert und neu konfiguriert werden.

Wie kann eine SD-Karte wiederhergestellt werden, wenn die SD-Karte nicht im Gehäuse war, als der Deaktivierungsbefehl auf der FlexAddress ausgeführt wurde?

Das Problem ist, dass die SD-Karte nicht zur Installation von FlexAddress auf einem anderen Gehäuse verwendet werden kann, wenn sie sich nicht im CMC befand, als FlexAddress deaktiviert wurde. Um die Nutzung der Karte wiederherzustellen, führen Sie die Karte wieder in einen CMC in dem Gehäuse ein, das damit gebunden ist, installieren Sie FlexAddress neu und deaktivieren Sie FlexAddress erneut.

Die SD-Karte sowie sämtliche Firmware/Software-Aktualisierungen sind korrekt installiert. Die FlexAddress ist aktiv, auf dem Serverbereitstellungsbildschirm werden die Optionen zum Bereitstellen nicht angezeigt? Was ist falsch?

Das ist ein Problem des Browser-Cache; schließen Sie den Browser und starten Sie ihn neu.

Was geschieht mit FlexAddress, wenn ich meine Gehäusekonfiguration mit dem RACADM-Befehl `racresetcfg` zurücksetzen muss?

Die FlexAddress-Funktion bleibt aktiviert und verfügbar. Alle Strukturen und Steckplätze werden als Standard ausgewählt.

ANMERKUNG: Es wird dringend empfohlen, dass Sie das Gehäuse herunterfahren, bevor Sie den RACADM-Befehl `racresetcfg` verwenden.

Warum schlägt der Befehl `racadm setflexaddr` auf dem weiterhin aktiven CMC fehl, nachdem nur die FlexAddressPlus-Funktion (die FlexAddress ist weiterhin aktiv) deaktiviert wurde?

Wenn der CMC anschließend wieder aktiv ist und sich die FlexAddressPlus-Funktionskarte noch im Kartensteckplatz befindet, wird die FlexAddressPlus-Funktion reaktiviert, und die Flexaddress-Konfigurationsänderungen für den Steckplatz bzw. den Fabric können wieder aufgenommen werden.

iKVM

Die Meldung „Benutzer wurde durch die CMC-Steuerung deaktiviert" wird auf dem Monitor angezeigt, der an der Frontblende angeschlossen ist. Warum?

Die Frontblendenverbindung wurde vom CMC deaktiviert. Sie können die Frontblende entweder mit der CMC-Webschnittstelle oder RACADM aktivieren.

Um die Frontblende mit der CMC Webschnittstelle zu aktivieren, gehen Sie zu der Registerkarte **iKVM** → **Setup** , wählen Sie die Option **Frontblenden-USB/Video aktiviert** aus, und klicken Sie auf **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. Warum?

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.

Die Meldung „Benutzer wurde deaktiviert, da ein weiteres Gerät derzeit Vorrang hat" wird auf dem Monitor angezeigt, der an der rückseitigen Abdeckung angeschlossen ist. Warum?

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.

Die gelbe iKVM-LED blinkt. Warum?

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.
- **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.

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.

Um die Frontblende unter Verwendung der Webschnittstelle zu deaktivieren, wählen Sie die Registerkarte **iKVM** → **Setup** aus, löschen Sie die **Frontblenden-USB/Video aktiviert** Option und klicken Sie auf Anwenden.

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

Im OSCAR-Menü zeigt die Dell-CMC-Verbindung ein rotes X an, und ein Verbindungsaufbau zum CMC ist nicht möglich. Warum?

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.
- **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.

Der Steckplatzname für einen Server wird in OSCAR als „Initialisiert" angezeigt und er kann nicht ausgewählt werden. Warum?

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. Der Server kann dannausgewählt werden.

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.

EAM

Nach einer Konfigurationsänderung zeigt CMC manchmal die IP-Adresse als 0.0.0.0. an.

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 *White Paper zum Dell PowerConnect 6220 Series Port Aggregator*.