Dell Chassis Management Controller Version 1.1 für PowerEdge FX2/FX2s

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.

2014 - 12

Rev. A00

Inhaltsverzeichnis

1

Übersicht

Der Dell Chassis Management Controller (CMC) für PowerEdge FX2/FX2s ist eine Systemverwaltungs-Hardware- und -Software-Lösung zur Verwaltung von **PowerEdge FX2/FX2s**-Gehäusen. 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
- Remote-Ein- und Ausschalten von Gehäusen und Servern
- Aktivieren von Warnungen für Ereignisse auf Servern und Komponenten im Servermodul
- Anzeigen der PCIe-Zuordnungsinfo.
- Bereitstellen einer Eins-zu-Vielen-Verwaltungsschnittstelle zu den iDRACs und E/A-Modulen im Gehäuse

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

- Automatische Energie- und Temperaturverwaltung in Echtzeit für das gesamte Gehäuse.
  - Der CMC meldet den Leistungsbedarf in Echtzeit und zeichnet Hoch- und Tiefpunkte mit Zeitstempel auf.
  - Der CMC ermöglicht das Einrichten einer optionalen maximalen Gehäusestromobergrenze (Systemeingangsstromobergrenze), die warnt und Maßnahmen wie die Beschränkung des Stromverbrauchs der Server ausführt und/oder das Einschalten von neuen Servern verhindert, um das Gehäuse unter der festgelegten Stromgrenze zu halten.
  - Der CMC überwacht und steuert automatisch die Lüfterfunktionen auf der Grundlage tatsächlicher Messwerte der Umgebungs- und internen Temperatur.
  - Der CMC stellt umfassende Informationen zu den Komponenten im Gehäuseinneren sowie Status- und Fehlerberichte bereit.
- Der CMC bietet einen Mechanismus zur zentralisierten Konfiguration der folgenden Elemente:
  - Netzwerk- und Sicherheitseinstellungen auf den PowerEdge FX2/FX2s-Gehäusen.
  - Einstellungen der Stromredundanz und der Obergrenze für den Stromverbrauch.
  - E/A-Switches und iDRAC-Netzwerkeinstellungen.
  - Das erste Startgerät auf den Serverblades.
  - Übereinstimmungsprüfungen der E/A-Struktur zwischen den E/A-Modulen und Servern. CMC deaktiviert auch wenn notwendig Komponente, um die Systemhardware zu schützen.
  - Sicherheitsmerkmale für den Benutzerzugriff.
  - PCIe-Steckplätze.

Sie können den CMC so konfigurieren, dass E-Mail-Warnungen oder SNMP-Trap-Warnungen versendet werden, wenn Warnungen oder Fehler in Verbindung mit der Temperatur, der Hardwarekonfiguration, der Stromversorgung und der Lüftergeschwindigkeit auftreten.

Wichtige Funktionen

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

Was ist neu in dieser Version?

Diese Version von CMC für Dell PowerEdge FX2/FX2s unterstützt Folgendes:

- Blade-Server der 13. Generation
- Verbesserte WWN/MAC-Adressbestandsaufnahme mit WWN/MAC-Adressen, die einem LOM/Select Network Adapter (SNA) über die E/A-Identitätsfunktion von iDRAC zugewiesen wurden
- Anzeigen des Status von NIC-Partitionen im Rahmen des WWN/MAC-Adressbestands, unabhängig vom Betriebssystem
- Verwenden von Verzeichnissen im Remote-NFS-/CIFS-Verzeichnis für Serverprofile und von benutzerdefinierten Repositories von DUPs
- Option zur Verwendung einer externen Bibliothek (CIFS/NFS-Verzeichnis) zum Aktualisieren von Repositories und Profilen
- Option zum Anzeigen und Verwenden erfasster Profile, die in einer externen Bibliothek gespeichert sind
- Verbesserte WWN/MAC-Adressbestandserfassung über die E/A-Identitätsfunktion von iDRAC
- Durchsetzung der Signaturüberprüfung für CMC-Firmware-Images
- Aktualisierung der CMC-Firmware über DUPs

Verwaltungsfunktionen

Der CMC enthält die folgenden Verwaltungsfunktionen:

- Registrierung des dynamischen Domänennamensystems (DDNS) für IPv4 und IPv6.
- Anmeldungsverwaltung und Konfiguration für lokale Benutzer, Active Directory und LDAP
- Remote-Systemverwaltung und -überwachung über SNMP, Webschnittstelle, integriertes KVM, Telnet- oder SSH-Verbindung.
- Überwachung - Zugriff auf Systeminformationen und Komponentenstatus.
- Zugriff auf Systemereignisprotokolle – Bietet Zugriff auf das Hardwareprotokoll und das Gehäuse-Protokoll.
- Firmware-Aktualisierungen für verschiedene Gehäusekomponenten – Damit können Sie die Firmware für CMC, iDRAC auf Servern und die Gehäuseinfrastruktur aktualisieren.
- Firmware-Aktualisierung von Serverkomponenten, wie z. B. BIOS, Netzwerk-Controller usw. auf mehreren Servern im Gehäuse mithilfe von Lifecycle Controller.
- Dell OpenManage Software Integration – Ermöglicht es Ihnen, die CMC-Web-Schnittstelle vom Dell OpenManage Server Administrator oder OpenManage Essentials (OME) 1.2 zu starten.
- CMC-Warnung – Warnt Sie anhand einer Remote syslog-E-Mail-Benachrichtigung oder eines SNMP-Traps über potenzielle Probleme mit verwalteten Knoten.

- Remote-Stromverwaltung – Bietet Remote-Stromverwaltungsfunktionen wie z. B. Ausschalten und Reset einer beliebigen Gehäusekomponente von einer Verwaltungskonsole aus.
- Stromverbrauchsberichte.
- SSL-Verschlüsselung (Secure Sockets Layer) – Bietet sichere Remote-Systemverwaltung über die Webschnittstelle.
- Startpunkt für die Web-Schnittstelle des Integrated Dell Remote Access Controller (iDRAC).
- Unterstützung für WS-Management.
- Multi-Node-Schlitten-Anpassung. PowerEdge FM120x4 ist ein Multi-Node-Schlitten.
- Überwachung der Gehäusestromgrenze.
- Unterstützung für iDRAC-E/A-Identitätsfunktion für erweiterte WWN/MAC-Adressbestandsaufnahme
- 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.
- Einfache iDRAC-Anmeldung.
- Network Time Protocol (NTP)-Unterstützung.
- Verbesserte Server-Übersichts-, Stromberichts- und Stromsteuerungsseiten
- Verwaltung mehrerer Gehäuse (Multi-Chassis-Management), wodurch bis zu 19 weitere Gehäuse vom Hauptgehäuse aus sichtbar sind

  ANMERKUNG: Multi-Chassis-Management wird nicht unterstützt für IPv6-Netzwerke.

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.
- Signiertes CMC-Image – Wird verwendet, um mithilfe von digitalen Signaturen das Firmware-Image vor nicht erkannten Änderungen zu schützen.

Gehäuseübersicht

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

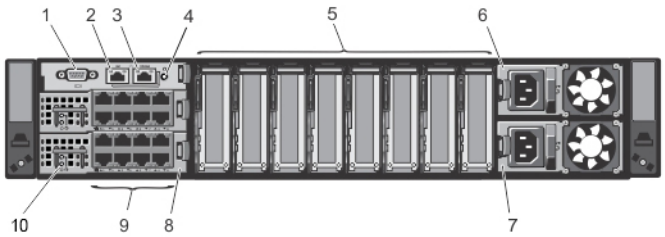
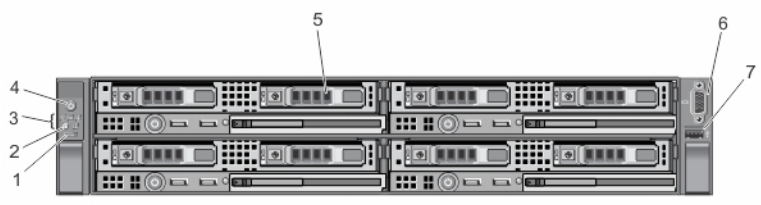


Abbildung 1.

Element	Anzeige, Taste oder Anschluss
1	Serieller Anschluss
2	Ethernet-Anschluss Gb1
3	STK/Gb2 Ethernet-Anschluss (Stack)
4	Systemidentifikationstaste
5	Erweiterungssteckplätze für PCI-Erweiterungskarten mit flachem Profil
6	Netzteil (PSU1)
7	Netzteil (PSU2)
8	E/A-Module (2)
9	E/A-Modulschnittstellen
10	E/A-Modulanzeigen

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



Element	Anzeige, Taste oder Anschluss
1	KVM-Auswahltaste
2	Systemidentifikationstaste
3	Diagnoseanzeigen
4	Betriebsanzeige, Netzschalter des Gehäuses
5	Schlitten
6	Bildschirmanschluss
7	USB-Anschluss

Unterstützte Remote-Zugriffsverbindungen

Die folgende Tabelle führt die unterstützten Remote-Access-Verbindungen auf.

Tabelle 1. Unterstützte Remote-Zugriffsverbindungen

Verbindung	Funktionen
CMC-Netzwerkschnittstellen	• -Gb-Schnittstelle: Dedizierte Netzwerkschnittstelle für die CMC-Web-Schnittstelle. Der CMC hat zwei RJ-45-Ethernet-Schnittstellen: – Gb1 (Uplink-Schnittstelle) – Gb2 (Stacking- oder Kabelkonsolidierungs-Schnittstelle). Die STK/Gb2-Schnittstelle kann auch für CMC-NIC-Failover-Vorgänge verwendet werden. **ANMERKUNG:** Stellen Sie sicher, dass die CMC-Einstellung von der Standardeinstellung **Stacking** auf **Redundant** geändert wurde, um NIC-Failover zu implementieren. **VORSICHT: Das Verbinden der STK/Gb2-Schnittstelle mit dem Verwaltungsnetzwerk kann zu unvorhersehbaren Ergebnissen führen, wenn die CMC-Einstellung von der standardmäßigen Einstellung Stacking auf Redundant geändert wurde, um NIC-Failover zu implementieren. Im Standardmodus Stacking kann die Verkabelung der Gb1- und STK/Gb2-Ports mit demselben Netzwerk (Broadcast-Domäne) zu einer Broadcast-Überlastung führen. Ein Broadcast Storm kann auch auftreten, wenn die CMC-Einstellung auf den Modus Redundant geändert wird, aber die Verkabelung zwischen den Gehäusen im Stacking-Modus verkettet ist. Stellen Sie sicher, dass das Verkabelungsmodell der CMC-Einstellung für die vorgesehene Verwendung entspricht.** • DHCP-Unterstützung. • SNMP-Traps und E-Mail-Ereignisbenachrichtigung. • Netzwerkschnittstelle für den iDRAC und E/A-Module (EAMs)

Verbindung	Funktionen
	• Unterstützung für die Telnet/SSH-Befehlskonsole und RACADM CLI-Befehle einschließlich Systemstart-,Reset-, Hochfahren-, und Herunterfahren-Befehle.
Serieller Port	• Unterstützung für serielle Konsolen- und RACADM-CLI-Befehle einschließlich Systemstart-, Reset-, Hochfahren- und Herunterfahren-Befehle. • Unterstützung für binären Austausch für Anwendungen, die speziell dafür vorgesehen sind, über ein Binärprotokoll mit einem bestimmten Typ von 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.

Unterstützte Plattformen

Der CMC unterstützt die Gehäusemodelle **PowerEdge FX2** und **FX2s**. Folgende Plattformen werden unterstützt: PowerEdge FC630 und PowerEdge FM120x4. Informationen zur CMC-Kompatibilität finden Sie in der Dokumentation zu Ihrem Gerät.

Informationen über die derzeit unterstützten Betriebssysteme finden Sie in den Versionshinweisen *Dell Chassis Management Controller (CMC) Version 1.1 for Dell PowerEdge FX2/FX2s Release Notes* (Dell Chassis Management Controller (CMC) Version 1.1 für Dell PowerEdge FX2/FX2s Versionshinweise), verfügbar unter **dell.com/support/manuals**.

Unterstützte Web-Browser

Die neusten Informationen zu unterstützten Web-Browsern finden Sie in den Versionshinweisen *Dell Chassis Management Controller (CMC) Version 1.1 for Dell PowerEdge FX2/FX2s Release Notes* (Dell Chassis Management Controller (CMC) Version 1.1 für Dell PowerEdge FX2/FX2s Versionshinweise), die unter **dell.com/support/manuals** verfügbar sind.

Lizenzenverwaltung

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

Lizenztypen

Die folgenden Lizenztypen sind verfügbar:

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

Lizenzen anfordern

Verwenden Sie zum Anfordern von Lizenzen eines der folgenden Verfahren:

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

Lizenzvorgänge

Bevor Sie die Lizenzverwaltungsschritte ausführen, müssen Sie sicherstellen, dass Sie die erforderlichen Lizenzen besitzen. Weitere Informationen finden Sie im Abschnitt Anfordern von Lizenzen sowie im Übersichts- und Funktionshandbuch unter support.dell.com.

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

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

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

  ANMERKUNG: Bei einigen neuen Funktionen ist für die Aktivierung dieser Funktionen ein CMC-Neustart erforderlich.
- Exportieren – Exportieren Sie die installierte Lizenz zu Sicherungszwecken oder für eine spätere Neuinstallation nach einem Austausch eines Service-Teils auf ein externes Speichergerät. Der Dateiname und das Format der exportieren Lizenz lauten wie folgt: <EntitlementID>.xml.
- Löschen – Löschen Sie die Lizenz, die mit einer Komponente verknüpft ist, wenn diese Komponente nicht vorhanden ist. Nach dem Löschen der Lizenz wird diese nicht mehr auf CMC gespeichert, und die Basisproduktfunktionen werden aktiviert.
- Ersetzen – Ersetzen Sie die Lizenz, um eine Evaluierungslizenz zu verlängern, um einen Lizenztyp zu ändern, z. B. eine Evaluierungslizenz in eine erworbene Lizenz, oder um eine abgelaufene Lizenz zu verlängern.
- Eine Evaluierungslizenz kann durch eine umfangreichere Evaluierungslizenz oder eine erworbene Lizenz ersetzt werden.
- Eine erworbene Lizenz kann durch eine aktualisierte Lizenz oder durch eine aufgerüstete Lizenz ersetzt werden. Weitere Informationen finden Sie im Dell Software License Management Portal unter HTTPS://WWW.DELL.COM/SUPPORT/LICENSING/US/EN/19.
- Weitere Informationen – Hier finden Sie weitere Informationen zur installierten Lizenz oder zu den Lizenzen, die für eine auf dem Server installierte Komponente verfügbar sind.

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

ANMERKUNG: Wenn Sie versuchen, die Lizenz für PowerEdge FM120x4 auf PowerEdge FC630 zu installieren, schlägt die Lizenz-Installation fehl. Weitere Informationen zur Lizenzierung finden Sie im iDRAC-Benutzerhandbuch *Integrated Dell Remote Access Controller (iDRAC) User's Guide*.

Lizenzierbare Funktionen in CMC

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

Funktion	Express	Enterprise
CMC-Netzwerk	Ja	Ja
Serielle CMC-Schnittstelle	Ja	Ja
RACADM (SSH, Lokal und Remote)	Ja	Ja
WS-MAN	Ja	Ja
SNMP	Ja	Ja
Telnet	Ja	Ja
SSH	Ja	Ja
Internet-basierte Schnittstelle	Ja	Ja
E-Mail-Warnungen	Ja	Ja
CMC-Einstellungen, Backup	Nein	Ja
CMC-Einstellungen, Wiederherstellung	Ja	Ja
Remote-Syslog	Nein	Ja
Verzeichnisdienste	Nein	Ja
Support für Single Sign-On	Nein	Ja
Zweifaktor-Authentifizierung	Nein	Ja
PK-Authentifizierung	Nein	Ja
Remote-Dateifreigabe	Nein	Ja
Gehäuseebenen-Stromobergrenzen	Nein	Ja
Verwaltung von mehreren Gehäusen	Nein	Ja

FlexAddress-Aktivierung	Nein	Ja
Eins-zu-viele-Server-Firmware-Aktualisierungen	Nein	Ja
Eins-zu-viele-Konfiguration für iDRAC	Nein	Ja

Status und Zustand von Lizenzkomponenten und verfügbare Optionen

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

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

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

Lokalisierte Versionen der CMC-Webschnittstelle anzeigen

Um lokalisierte Versionen der CMC Web-Schnittstelle anzuzeigen, lesen Sie die Dokumentation zu Ihrem Web-Browser. Zur Anzeige der lokalisierten Versionen stellen Sie den Browser auf die gewünschte Sprache ein.

Unterstützte Verwaltungskonsolenanwendungen

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

Verwendung dieses Benutzerhandbuchs

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

- Die Webschnittstelle: Hier erhalten Sie nur Informationen in Beziehung zu Tasks. Informationen über die Felder und Optionen finden Sie unter der *CMC for Dell PowerEdge FX2/FX2s Online Help* (CMC für Dell PowerEdge FX2/FX2s Online-Hilfe), die Sie von der Webschnittstelle aus öffnen können.
- Die RACADM-Befehle: Der RACADM-Befehl oder das Objekt, das Sie verwenden müssen, wird hier angezeigt. Weitere Informationen zu RACADM-Befehlen finden Sie im *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (Dell RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge FX2/FX2s) unter dell.com/support/manuals.

Weitere nützliche Dokumente

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

- Die *FX2/FX2s CMC-Online-Hilfe* enthält Informationen zur Verwendung der Webschnittstelle. Um auf diese Online-Hilfe zuzugreifen, klicken Sie auf **Hilfe** auf der CMC-Webschnittstelle.
- Im Dokument *Chassis Management Controller Version 1.1 for Dell PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller Version 1.1 für Dell PowerEdge FX2/FX2s) finden Sie Informationen zur Verwendung der Funktionen in Verbindung mit FX2/FX2s.
- Die Versionshinweise *Dell Chassis Management Controller (CMC) for Dell PowerEdge FX2/FX2s Version 1.1 Release Notes* (Dell Chassis Management Controller (CMC) für Dell PowerEdge FX2/FX2s Version 1.1 Versionshinweise) enthalten den letzten Stand der Änderungen am System oder an der Dokumentation bzw. erweitertes technisches Referenzmaterial für erfahrene Benutzer oder Techniker.
- Das iDRAC-Benutzerhandbuch *Integrated Dell Remote Access Controller 7 (iDRAC) User's Guide* bietet Informationen zur Installation, Konfiguration und Wartung des iDRAC7 auf verwalteten Systemen.
- Das *Dell OpenManage Server Administrator-Benutzerhandbuch* enthält Informationen über die Installation und Anwendung von Server Administrator.
- Das *Benutzerhandbuch zu den Dell Update Packages* enthält Informationen über das Abrufen und Verwenden von Dell Update Packages als Teil Ihrer Systemaktualisierungsstrategie.
- Die Dokumentation zur Dell-Systemverwaltungsanwendung enthält Informationen über das Installieren und Verwenden der Systemverwaltungssoftware.

Die folgenden Systemdokumente enthalten weitere Informationen über das System, auf dem CMC PowerEdege FX2/FX2s 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 Setup-Platzset, das mit Ihrem System geliefert wurde, enthält Informationen über die Systemersteinrichtung und Konfiguration.
- Das *Owner's Manual* (Benutzerhandbuch) des Servermoduls gibt Informationen über die Funktionen des Servermoduls an, beschreibt den Fehlerbehebungsvorgang für das Servermodul und das Installieren oder Austauschen der Komponenten des Servermoduls. Dieses Dokument steht online unter dell.com/poweredgemanuals zur Verfügung.
- In der zusammen mit der Rack-Lösung gelieferten Rack-Dokumentation ist beschrieben, wie das System in einem Rack installiert wird.
- Die vollständigen Namen der in diesem Dokument verwendeten Abkürzungen und Akronyme finden Sie im Glossar unter dell.com/support/manuals.
- In der Dokumentation zur Systemverwaltungssoftware sind die Merkmale, die Anforderungen, die Installation und die grundlegende Funktion der Software beschrieben.

- Die Dokumentation für alle separat erworbenen Komponenten enthält Informationen zur Konfiguration und zur Installation dieser Optionen.
- Alle im Lieferumfang des Systems enthaltenen Medien mit Dokumentationen und Hilfsmitteln zur Konfiguration und Verwaltung des Systems, insbesondere in Bezug auf Betriebssystem, Systemverwaltungssoftware, System-Aktualisierungen und mit dem System erworbene Komponenten. Für weitere Informationen über das System durchsuchen Sie den Quick Resource Locator (QRL) (Schnellen Ressourcenfinder), der auf Ihrem System und auf dem System-Setup-Platzset, das mit Ihrem System geliefert wurde, verfügbar ist. Laden Sie die QRL-Anwendung von Ihrer mobilen Plattform herunter, um die Anwendung auf Ihren Mobilgeräten zu aktualisieren.

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

Zugriff auf Dokumente der Dell Support-Website

Sie können auf eine der folgenden Arten auf die folgenden Dokumente zugreifen:

- Verwendung der folgenden Links:
  - Für alle Enerprise Systems Management-Dokumente – **dell.com/softwaresecuritymanuals**
  - Für Enterprise Systems Management-Dokumente – **dell.com/openmanagemanuals**
  - Für Remote Enterprise Systems Management-Dokumente – **dell.com/esmmanuals**
  - Für OpenManage Connections Enterprise Systems Management-Dokumente – **dell.com/OMConnectionsEnterpriseSystemsManagement**
  - Für Tools für die Betriebsfähigkeitsdokumente – **dell.com/serviceabilitytools**
  - Für Client Systems Management-Dokumente – **dell.com/clientsystemsmanagement**
  - Für OpenManage Connections Client Systems Management-Dokumente – **dell.com/connectionsclientsystemsmanagement**
- Gehen Sie auf der Dell Support-Website folgendermaßen vor:
  a. Rufen Sie die Website **dell.com/support/home** auf.
  b. Klicken Sie unter **Allgemeiner Support** auf **Software & Sicherheit**.
  c. Klicken Sie im Gruppenfeld **Software & Sicherheit** auf einen der folgenden Links:
     - **Enterprise Systems Management**
     - **Remote Enterprise Systems Management**
     - **Tools für die Betriebsfähigkeit**
     - **Client Systems Management**
     - **Connections Client Systems Management**
  d. Um ein Dokument anzuzeigen, klicken Sie auf die jeweilige Produktversion.
- Verwendung von Suchmaschinen:
  - Geben Sie den Namen und die Version des Dokuments in das Kästchen „Suchen" ein.

2

Installation und Setup des CMC

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

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

Installieren der CMC-Hardware

Der CMC ist in Ihrem Gehäuse vorinstalliert und es ist demzufolge keine Installation erforderlich.

Prüfliste zur Gehäusegruppen-Einrichtung

Mit den folgenden Tasks können Sie das Gehäuse korrekt einrichten:

1. Der für den CMC und die Management Station verwendete Browser muss sich in demselben Netzwerk befinden, das als das Verwaltungsnetzwerk bezeichnet wird. Verbinden Sie ein Ethernet-Netzwerkkabel vom Port mit der Bezeichnung **GB1** mit dem Verwaltungsnetzwerk.

   Management-Netzwerk: CMC und der iDRAC (auf jedem Server) und die Netzwerkverwaltungsschnittstellen für alle Switch-E/A-Module sind mit einem gemeinsamen internen Netzwerk im PowerEdge FX2-/FX2s-Gehäuse verbunden. Damit kann das Verwaltungsnetzwerk vom Serverdatennetzwerk getrennt werden.

   Anwendungsnetzwerk: Der Zugriff auf die verwalteten Server erfolgt über Netzwerkverbindungen zum E/A-Modul (EAM). Dies ermöglicht, dass das Anwendungsnetzwerk und das Verwaltungsnetzwerk voneinander getrennt sind. Es ist wichtig, diesen Datenverkehr zu trennen, um ununterbrochenen Zugriff auf die Gehäuseverwaltung zu haben.

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

2. Die STK/Gb2-Schnittstelle kann auch für CMC-NIC-Failover-Vorgänge verwendet werden. Stellen Sie sicher, dass die CMC-Einstellung von der Standardeinstellung **Stacking** auf **Redundant** geändert wurde, um NIC-Failover zu implementieren. Weitere Informationen finden Sie unter Verwaltungsschnittstelle 2 konfigurieren.

   VORSICHT: Das Verbinden der STK/Gb2-Schnittstelle mit dem Verwaltungsnetzwerk kann zu unvorhersehbaren Ergebnissen führen, wenn die CMC-Einstellung von der standardmäßigen Einstellung Stacking auf Redundant geändert wurde, um NIC-Failover zu implementieren. Im Standardmodus Stacking kann die Verkabelung der Gb1- und STK/Gb2-Ports mit demselben Netzwerk (Broadcast-Domäne) zu einer Broadcast-Überlastung führen. Ein Broadcast Storm kann auch auftreten, wenn die CMC-Einstellung auf den Modus Redundant geändert wird, aber die Verkabelung zwischen den Gehäusen im Stacking-Modus verkettet ist. Stellen Sie sicher, dass das Verkabelungsmodell der CMC-Einstellung für die vorgesehene Verwendung entspricht.

3. Installieren Sie das E/A-Modul im Gehäuse und verbinden Sie das Netzwerkkabel mit dem E/A-Modul.
4. Schieben Sie die Server in das Gehäuse ein.
5. Schließen Sie das Gehäuse an der Stromquelle an.
6. Drücken Sie zum Hochfahren des Gehäuses den Netzschalter, oder verwenden Sie die folgenden Schnittstellen nach Abschluss der Aufgabe 6. Gehen Sie auf der Webschnittstelle zu **Gehäuseübersicht → Strom → Steuerung → Stromsteuerungsoptionen → System einschalten**. Klicken Sie auf **Anwenden**.

   Sie können das Gehäuse auch über die Befehlszeilenschnittstelle hochfahren. Verwenden Sie hierzu den Befehl `racadm chassisaction powerup`.

   ANMERKUNG: Schalten Sie die Server nicht ein.

7. Die Standard-CMC-Netzwerkkonfiguration lautet „Statisch" mit CMC-IP-Adresse 192.168.0.120. Wenn Sie die Standard-Netzwerkkonfiguration in DHCP ändern möchten, schließen Sie ein serielles Kabel an die serielle CMC-Schnittstelle an. Weitere Informationen zur seriellen Verbindung finden Sie unter „Einrichten der seriellen Schnittstelle/Protokoll" im Abschnitt Verwenden von Remote-Zugriffssoftware von einer Management Station.

   Nachdem die serielle Verbindung hergestellt ist, melden Sie sich an, und verwenden Sie den Befehl `racadm setniccfg –d`, um die Netzwerkkonfiguration auf DHCP zu ändern. CMC benötigt ungefähr 30 bis 60 Sekunden, um die IP-Adresse vom DHCP-Server abzurufen.

   Um die von DHCP zugewiesene CMC-IP-Adresse anzuzeigen, wählen Sie eine der folgenden Vorgehensweisen:

   - Um die CMC-IP-Adresse über die serielle Verbindung mit CMC anzuzeigen, führen Sie die folgenden Schritte aus:

     1. Schließen Sie ein Ende des seriellen Nullmodemkabels an den seriellen Anschluss an der Rückseite des Gehäuses an.
     2. Verbinden Sie das andere Ende des Kabels mit der seriellen Schnittstelle des Managementsystems.
     3. Nachdem die Verbindung hergestellt wurde, melden Sie sich am CMC unter Verwendung der Standard-Anmeldeinformationen für das root-Konto an.
     4. Führen Sie den Befehl `racadm getniccfg` aus.

        Suchen Sie in der Ausgabe nach **Aktuelle IP-Adresse**.

   - Um die CMC-IP-Adresse über eine Verbindung zum Server unter Verwendung von KVM anzuzeigen, führen Sie die folgenden Schritte aus:

     1. Stellen Sie unter Verwendung von KVM eine Verbindung zu einem Server im Gehäuse her.

ANMERKUNG: Weitere Informationen dazu finden Sie im Abschnitt Unter Verwendung von KVM auf den Server zugreifen.

2. Schalten Sie den Server ein.
3. Stellen Sie sicher, dass der Server so konfiguriert ist, dass er im UEFI-Modus startet (Unified Extensible Firmware Interface).
4. Drücken Sie die Taste F2, um die Seite „System-Setup" aufzurufen.
5. Klicken Sie auf der Seite **System-Setup** auf **iDRAC-Einstellungen** → **Systemzusammenfassung**.

   Die CMC-IP-Adresse wird im Abschnitt **Chassis Management Controller** angezeigt.

   Weitere Informationen zur Seite **iDRAC-Einstellungen** der iDRAC-GUI-Seite finden Sie im iDRAC-Benutzerhandbuch *Dell Integrated Dell Remote Access Controller (iDRAC) User's Guide*.

8. Stellen Sie unter Verwendung des Webbrowsers eine Verbindung mit der CMC-IP-Adresse her, indem Sie die Standard-Anmeldeinformation für das root-Konto eingeben.
9. Konfigurieren Sie die iDRAC-Netzwerkeinstellungen nach Bedarf. Standardmäßig ist die iDRAC-LAN mit statischer IP-Adresse konfiguriert. Zum Ermitteln der statischen Standard-IP-Adresse mit einer **Enterprise-Lizenz**, gehen Sie zu **Serverübersicht** → **Setup** → **iDRAC**. Sie können auch die statische IP-Adresse mit einer **Express-Lizenz** ermitteln. Gehen Sie zu **Serverübersicht** → **Server-Steckplatz-** → **Setup** → **iDRAC**.
10. Geben Sie dem E/A-Modul in der eine IP-Adresse für die externe Verwaltung in der CMC-Webschnittstelle (sofern zutreffend). Sie können die IP-Adresse durch Klicken auf **E/A-Modulübersicht** und dann auf **Setup** erhalten.
11. Stellen Sie über die Web-Schnittstelle eine Verbindung zu jedem iDRAC unter Verwendung der Standard-Anmeldeinformation für das root-Konto her, und vervollständigen Sie die erforderliche Konfiguration.
12. Schalten Sie die Server ein und installieren Sie das Betriebssystem.

ANMERKUNG: Die Anmeldeinformationen für das lokale Standard-Konto lauten „root" (Benutzername) und „calvin" (Benutzerkennwort).

Verwenden von Remote-Zugriffssoftware auf einer Management Station

Sie können mithilfe verschiedener Remote-Zugriffssoftware von einer Management Station aus auf CMC zugreifen. Hier finden Sie eine Liste von RAS-Software von Dell, die von Ihrem Betriebssystem aus verfügbar ist.

Schnittstelle/Protokoll	Beschreibung
Seriell	CMC unterstützt eine serielle Textkonsole, die mit einer beliebigen Terminal-Emulationssoftware gestartet werden kann. Im Folgenden einige Beispiele für Terminal-Emulationssoftware, die verwendet werden kann, um eine Verbindung zu CMC herzustellen. • Linux Minicom • Hilgraeve-HyperTerminal für Windows Schließen Sie ein Ende des seriellen Null-Modem-Kabels (an beiden Enden vorhanden) an den seriellen Anschluss auf der Rückseite des Gehäuses an. Schließen Sie das andere Ende des Kabels an den seriellen Anschluss der Management Station

	an. Weitere Informationen über das Anschließen der Kabel finden Sie im Abschnitt über die Rückseite des Gehäuses unter Gehäuse-Übersicht. Konfigurieren Sie Ihre Terminal-Emulationssoftware mit den folgenden Parametern: • Baudrate: 115200 • Port: COM1 • Daten: 8 Bit • Parität: keine • Stopp: 1 Bit • Hardware-Ablaufsteuerung: Ja • Software-Ablaufsteuerung: Nein
Remote-RACADM-CLI	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. CMC IP-Benutzername und -Kennwort sind erforderlich. 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. Weitere Informationen zu Remote-RACADM siehe
Webschnittstelle	Ermöglicht Remote-Zugriff auf CMC über eine grafische Benutzeroberfläche. Die Webschnittstelle ist in die CMC-Firmware integriert, und der Zugriff darauf erfolgt über die NIC-Schnittstelle von einem unterstützten Webbrowser auf der Management Station. Eine Liste der unterstützten Webbrowser finden Sie im Abschnitt **Unterstützte Webbrowser** in der Dell Systems Software Support Matrix unter **dell.com/support/manuals**.
Telnet	Ermöglicht Befehlszeilenzugriff auf den CMC über das Netzwerk. Die RACADM-Befehlszeilenschnittstelle und der connect-Befehl, der zum Herstellen einer Verbindung zur seriellen Konsole eines Servers oder E/A-Moduls verwendet wird, sind über die CMC-Befehlszeile verfügbar. **ANMERKUNG:** Telnet ist kein sicheres Protokoll und ist standardmäßig deaktiviert. In Telnet werden alle Daten, einschließlich der Kennwörter, im Klartext übertragen.

SNMP

Simple Network Management Protocol (SNMP) ist ein Satz von Protokoll-Definitionen für die Verwaltung von Geräten im Netzwerk. Der CMC ermöglicht den Zugriff auf SNMP, so dass Sie SNMP-Tools verwenden können, um den CMC auf Systems Management-Informationen abzufragen. Die CMC-MIB-Datei kann von der CMC-Webschnittstelle heruntergeladen werden; wählen Sie hierzu **Gehäuseübersicht → Netzwerk → Dienste → SNMP**. Weitere Informationen über die CMC-MIB finden Sie im *Dell OpenManage SNMP Reference Guide* (Dell OpenManage SNMP-Referenzhandbuch).

Das folgende Beispiel zeigt, wie der Befehl `net-snmp snmpget` verwendet werden kann, um die Gehäuse-Service-Tag-Nummer vom CMC abzurufen.

```
snmpget -v 1 -c <CMC-Community-Name>
<CMC IP address>.
1.3.6.1.4.1.674.10892.2.1.1.6.0
```

WS-MAN

Die WSMAN-Services basieren auf dem Web Services for Management (WSMAN)-Protokoll für 1-zu-n-Verwaltungsaufgaben. Sie können einen WS-MAN-Client verwenden, z. B. den WinRM-Client (Windows) oder den OpenWSMAN-Client (Linux), um die LC-Remote Services-Funktion zu verwenden. Sie können außerdem Power Shell- und Python-Skript verwenden, um auf die WS-MAN-Schnittstelle zu schreiben.

WSMAN ist ein SOAP-basiertes (Simple Object Access Protocol) Protokoll, das für Systemverwaltung verwendet wird. CMC verwendet WS–Management zum Übermitteln von DMTF-CIM-basierten Verwaltungsinformationen (Distributed Management Task Force; Common Information Model). Die CIM-Informationen definieren die Semantik- und Informationstypen, die in einem verwalteten System geändert werden können.

Die CMC WS-MAN-Implementierung verwendet SSL auf Schnittstelle 443 für Transportsicherheit und unterstützt Standardauthentifizierung. Die durch WS-Management zur Verfügung gestellten Daten werden durch die CMC-Instrumentierungsschnittstelle bereitgestellt, die den DMTF-Profilen und den Erweiterungsprofilen zugeordnet ist.

ANMERKUNG: Die SSL-Schnittstelle für Transportsicherheit ist die gleiche wie die CMC-HTTPS-Schnittstelle.

Für weitere Informationen, siehe:

- MOFs und Profile – **delltechcenter.com/page/DCIM.Library**
- DTMF-Website – **www.dmtf.org/standards/profiles/**
- WS-MAN Versionshinweisdatei.
- **www.wbemsolutions.com/ws_management.html**
- DMTF WS-Management-Spezifikationen: **www.dmtf.org/standards/wbem/wsman**

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**>.

Starten von CMC mit anderen Systems Management Tools

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

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

Remote-RACADM-Installation

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 *Dell OpenManage Installation and Security User's Guide* (Dell OpenManage-Installation und Sicherheit-Benutzerhandbuch) unter **dell.com/support/manuals**. Sie können auch die neueste Version der Dell DRAC Tools unter **dell.com/support** herunterladen.

Installieren von Remote-RACADM auf einer Windows-Management-Station

Wenn Sie die DVD verwenden, führen Sie die folgende Datei aus: ***<Pfad>*\SYSMGMT\ManagementStation\windows\DRAC*<.MSI-Dateiname>***

Wenn Sie die Software von **dell.com/support**heruntergeladen haben:

1. Entpacken Sie die heruntergeladene Datei, und führen Sie die bereitgestellte **.msi**-Datei aus.

Je nach heruntergeladener Version lautet der Dateiname DRAC.msi, RACTools.msi oder RACTools64Bit.msi.

2. Akzeptieren Sie die Lizenzvereinbarung, und klicken Sie auf **Weiter**.
3. Wählen Sie den Installationsort, und klicken Sie auf **Weiter**.
4. Klicken Sie auf **Installieren**.

   Das Installationsfenster wird angezeigt.
5. Klicken Sie auf **Fertigstellen**.

Öffnen Sie eine Administrator-Eingabeaufforderung, geben Sie `racadm` ein, und drücken Sie die **Eingabetaste**. Wenn die RACADM-Hilfe angezeigt wird, bedeutet dies, dass die Software fehlerfrei installiert wurde.

Installieren von RACADM auf einer Linux-Management-Station

1. Melden Sie sich als „root" bei einem System unter dem Red Hat Enterprise Linux- oder SUSE Linux Enterprise Server-Betriebssystem an, auf dem Sie die Komponenten des verwalteten Systems installieren möchten.
2. Legen Sie die DVD *Dell Systems Management Tools and Documentation* in das DVD-Laufwerk ein.
3. Um die DVD am erforderlichen Standort bereitzustellen, verwenden Sie den Befehl mount oder einen ähnlichen Befehl.

   ANMERKUNG: Auf dem Red Hat Enterprise Linux 5-Betriebssystem werden DVDs automatisch mit der Ladeoption `–noexec mount` geladen. Diese Option erlaubt Ihnen nicht, beliebige ausführbare Datei von der DVD auszuführen. Sie müssen die DVD-ROM manuell laden und dann die Befehle ausführen.
4. Navigieren Sie zum Verzeichnis **SYSMGMT/ManagementStation/linux/rac**. Geben Sie den folgenden Befehl ein, um die RAC-Software zu installieren:

   ```
   rpm –ivh *.rpm
   ```
5. Um Hilfe zum RACADM-Befehl zu erhalten, geben Sie nach der Eingabe der vorherigen Befehle `racadm help` ein. Weitere Informationen über RACADM finden Sie im *Chassis Management Controller for Dell PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge FX2/FX2s).

   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>`

Deinstallieren von RACADM von einer Linux-Management-Station

1. Melden Sie sich als `root` beim System an, auf dem die Funktionen der Management Station deinstalliert werden sollen.
2. Führen Sie den rpm-Abfragebefehl aus, um zu bestimmen, welche Version der DRAC-Hilfsprogramme installiert ist:

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

Einen Webbrowser konfigurieren

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

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

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

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

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

Proxy-Server

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

Microsoft Phishing-Filter

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

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

Dateien mit dem Internet Explorer vom CMC herunterladen

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

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

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

CMCNoble_Animationen im Internet Explorer erlauben

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

So konfigurieren Sie Internet Explorer zum Abspielen von Animationen:

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

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 **cmc-„Service-Tag-Nummer“**). Beispiel: Eine SNMP-Anfrage für den Gehäusenamen gibt den von Ihnen konfigurierten Namen aus.

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

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

1. Wählen Sie im rechten Fensterbereich **Gehäuseübersicht** aus, und klicken Sie auf **Setup**.
2. Geben Sie auf der Seite **Allgemeine Gehäuseeinstellungen** den physischen Standort und den Gehäusenamen ein. Weitere Informationen zum Festlegen der Gehäuseeigenschaften finden Sie in der *Online Hilfe*.

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

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

Informationen zum Einrichten von Gehäusenamen, Standort, Datum und Uhrzeit für die Befehlszeilenschnittstelle finden Sie in den Abschnitten zu den Befehlen **setsysinfo** und **setchassisname**.

Beispiel: `racadm setsysinfo -c chassisname` oder `racadm setsysinfo -c chassislocation`

Weitere Informationen finden Sie im *Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge FX2/FX2s).

Datum und Uhrzeit auf dem CMC einstellen

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

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

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

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht → Setup → Datum/Uhrzeit**.
2. Datum und Uhrzeit können mit einem NTP-Server (Network Time Protocol) auf der Seite **Datum/Uhrzeit** synchronisiert werden, indem Sie **NTP aktivieren** auswählen und bis zu drei NTP-Server festlegen. Für die manuelle Einstellung von Datum und Uhrzeit deaktivieren Sie die Option **NTP aktivieren** und bearbeiten Sie dann die Felder **Datum** und **Zeit**.
3. Wählen Sie im Drop-Down-Menü **Zeitzone** aus und klicken dann auf **Anwenden**.

Datum und Uhrzeit auf dem CMC mittels RACADM einstellen

Anleitungen zum Einstellen von Datum und Uhrzeit mit der Befehlszeilenschnittstelle finden Sie in den Abschnitten zum Befehl **config** und zu den Datenbankeigenschaftengruppen `cfgRemoteHosts` im *Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge FX2/FX2s), der unter **dell.com/support/manuals** verfügbar ist.

Zum Beispiel `racadm setractime -l 20140207111030`.

Verwenden Sie zum Ablesen von Datum und Uhrzeit den Befehl `racadm getractime`.

LEDs zum Identifizieren von Komponenten im Gehäuse konfigurieren

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

ANMERKUNG: Um diese Einstellungen ändern zu können, müssen Sie die Berechtigung als **Administrator für Debug-Befehle** auf einem CMC haben.

Konfigurieren von LED-Blinken über die CMC-Webschnittstelle

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

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

    ANMERKUNG: Auf dieser Seite können nur Server ausgewählt werden.

Um den Blinkvorgang für eine Komponenten-LED zu aktivieren, wählen Sie die betreffende Komponente aus, und klicken Sie dann auf **Blinken**. Zur Deaktivierung des Blinkens einer Komponenten-LED, heben Sie die Auswahl des Servers auf, und klicken Sie dann auf **Blinken beenden**.

LED-Blinken mittels RACADM konfigurieren

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

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

- `server-n` , wobei *n* = 1-4 (PowerEdge FM120x4) und `server-nx`, wobei *n* = 1–4 und *x* = a nach b (PowerEdge FC630).
- `switch-1`
- `cmc-active`

und *<ledState>* 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 RACACM-Befehle konfigurieren.

Frontblende konfigurieren

Mithilfe der Seite „Frontblende" können Sie Folgendes konfigurieren:

- Netzschalter
- KVM

Netzschalter konfigurieren

So gehen Sie for, um den Netzschalter zu konfigurieren

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht → Frontblende → Setup**.
2. Wählen Sie auf der Seite **Frontblendenkonfiguration** im Abschnitt **Netzschalterkonfiguration** die Option **Netzschalter des Gehäuses deaktivieren** und klicken Sie dann auf **Anwenden**.

   Der Gehäusenetzschalter ist deaktiviert.

Zugriff auf einen Server unter Verwendung von KVM

So ordnen Sie einen Server über die Webschnittstelle zu KVM zu:

1. Schließen Sie einen Monitor an den Videoanschluss und eine Tastatur an einen USB-Anschluss auf der Vorderseite des Gehäuses an.
2. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht → Frontblende → Setup**.
3. Wählen Sie auf der Seite **Frontblendenkonfiguration** im Abschnitt **KVM-Konfiguration** die Option **KVM-Zuordnung aktivieren** aus.
4. Wählen Sie auf der Seite **Frontblendenkonfiguration** im Abschnitt **KVM-Konfiguration** für die Option **KVM zugeordnet** den gewünschten Server aus der Drop-Down-Liste aus.
5. Klicken Sie auf **Anwenden**.

Verwenden Sie für die Zuordnung eines Servers zu KVM mit RACADM den Befehl `racadm config -g cfgKVMInfo -o cfgKvmMapping [server slot #]`.

Verwenden Sie zum Anzeigen der aktuellen KVM-Zuordnung mit RACADM den Befehl `racadm getconfig -g cfgKVMInfo`.

Konfigurieren der Gehäuseverwaltung im Servermodus

Diese Funktion bietet die Möglichkeit zur Verwaltung und Überwachung der gemeinsam genutzten Komponenten im Gehäuse und der Gehäuseknoten als Rack-Server. Wenn diese Funktion aktiviert ist, können Sie die Gehäuselüfter, Netzteile und Temperatursensoren verwalten und überwachen und die CMC-Firmware über die folgenden Komponenten aktualisieren und konfigurieren:

- iDRAC
- Blade-Server-Betriebssystem
- Lifecycle-Controller

Konfigurieren der Gehäuseverwaltung auf dem Server unter Verwendung der CMC Web-Schnittstelle

So aktivieren Sie die Gehäuseverwaltung im Server-Modus:

1. Klicken Sie im linken Fensterbereich auf **Gehäuse-Übersicht → Setup → Allgemein**.
2. Wählen Sie auf der Seite **Allgemeine Gehäuse-Einstellungen** im Drop-Down-Menü **Gehäuseverwaltung im Server-Modus** einen der folgenden Modi aus:
   - **Keiner** – In diesem Modus können Sie keine Gehäusekomponenten über iDRAC, das Betriebssystem oder Lifecycle Controller überwachen oder verwalten.
   - **Überwachen** – Dieser Modus ermöglicht Ihnen die Überwachung der Gehäusekomponenten, aber Sie können keine Firmware-Aktualisierung über iDRAC, das Betriebssystem oder Lifecycle Controller durchführen.
   - **Verwalten und Überwachen** – Dieser Modus ermöglicht Ihnen die Überwachung der Gehäusekomponenten und die Aktualisierung der CMC-Firmware unter Verwendung von DUPs über iDRAC, das Betriebssystem oder Lifecycle Controller.

Konfigurieren der Gehäuseverwaltung im Servermodus unter Verwendung von RACADM

Verwenden Sie zum Aktivieren der Gehäuseverwaltung im Servermodus unter Verwendung von RACADM die folgenden Befehle:

- Deaktivieren der Gehäuseverwaltung im Servermodus:
  ```
  racadm config –g cfgRacTuning – cfgRacTuneChassisMgmtAtServer 0
  ```
- Ändern der Gehäuseverwaltung im Servermodus in „Überwachen“:
  ```
  racadm config –g cfgRacTuning – cfgRacTuneChassisMgmtAtServer 1
  ```
- Ändern der Gehäuseverwaltung im Servermodus in „Verwalten und überwachen“:
  ```
  racadm config –g cfgRacTuning – cfgRacTuneChassisMgmtAtServer 2
  ```

3

Anmeldung beim CMC

Sie können sich beim CMC als lokaler CMC-Benutzer, als Microsoft Active Directory-Benutzer oder als LDAP-Benutzer anmelden. Sie können sich auch unter Verwendung von Single Sign-On oder einer Smart Card anmelden.

Authentifizierung mit öffentlichem Schlüssel über SSH

Sie können bis zu 6 öffentliche Schlüssel konfigurieren, die mit dem Dienst-Benutzernamen über eine SSH-Schnittstelle verwendet werden können. Verwenden Sie vor dem Hinzufügen oder Löschen öffentlicher Schlüssel unbedingt den `view`befehl, um zu sehen, welche Schlüssel bereits eingerichtet sind, sodass kein Schlüssel versehentlich überschrieben oder gelöscht wird. Der Dienst-Benutzername ist ein spezielles Benutzerkonto, das für den Zugriff auf den CMC über SSH verwendet werden kann. Wenn der PKA über SSH eingerichtet ist und korrekt verwendet wird, dann müssen Sie den Benutzernamen und das Kennwort nicht mehr eingeben, wenn Sie sich beim CMC anmelden. Es kann sehr hilfreich sein, automatisierte Skripts einzurichten, um verschiedene Funktionen auszuführen.

ANMERKUNG: Es gibt keine GUI-Unterstützung zur Verwaltung dieser Funktionen; Sie können nur RACADM verwenden.

Beim Hinzufügen neuer öffentlicher Schlüssel müssen Sie sicherstellen, dass bestehende Schlüssel nicht bereits den Index belegen, zu dem der neue Schlüssel hinzugefügt werden soll. Der CMC führt vor dem Hinzufügen eines Schlüssels keine Prüfungen durch, um sicherzustellen, dass keine vorherigen Schlüssel gelöscht werden. Sobald ein neuer Schlüssel hinzugefügt wurde, tritt er automatisch in Kraft, solange die SSH-Schnittstelle aktiviert ist.

Beachten Sie bei Verwendung des Anmerkungsabschnitts des öffentlichen Schlüssels, dass nur die ersten 16 Zeichen vom CMC verwendet werden. Die Anmerkung des öffentlichen Schlüssels wird vom CMC verwendet, um SSH-Benutzer bei Verwendung des RACADM-Befehls `getssninfo` zu unterscheiden, weil alle PKA-Benutzer den Dienst-Benutzernamen zur Anmeldung verwenden.

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

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

Weitere Informationen zu `sshpkauth` finden Sie im *Chassis Management Controller for PowerEdge FX2/FX2s Command Line Reference Guide* (Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge FX2/FX2s).

Generieren öffentlicher Schlüssel für Systeme, die Windows ausführen

Vor dem Hinzufügen eines Kontos ist ein öffentlicher Schlüssel von dem System erforderlich, das über SSH auf den CMC zugreift. Es gibt zwei Möglichkeiten, das öffentliche/private Schlüsselpaar zu generieren: mit der Schlüsselgeneratoranwendung PuTTY für Clients unter Windows bzw. mit ssh-keygen CLI für Clients unter Linux.

Dieser Abschnitt enthält einfache Anweisungen zum Generieren eines öffentlichen/privaten Schlüsselpaars für beide Anwendungen. Weitere Informationen über erweiterte Funktionen dieser Hilfsprogramme finden Sie in der Anwendungshilfe.

So verwenden Sie den PuTTY-Schlüsselgenerator für Clients, die Windows ausführen, zum Erstellen eines Grundschlüssels:

1. Starten Sie die Anwendung und wählen Sie entweder SSH-2 RSA oder SSH-2 DSA als Typ des zu generierenden Schlüssels aus (SSH-1 wird nicht unterstützt).
2. Geben Sie die Anzahl Bits für den Schlüssel ein. Die RSA-Schlüsselgröße sollte zwischen 768 und 4096 liegen, die empfohlene DSA-Schlüsselgröße ist 1024.

   ANMERKUNG:
   - CMC blendet möglicherweise keine Meldung ein, wenn Sie Schlüssel mit einem Wert kleiner als 768 oder größer als 4096 hinzufügen, doch wenn Sie versuchen, sich mit diesen Schlüsseln anzumelden, schlägt der Vorgang fehl.
   - Für DSA-Schlüssel größer als 2048 verwenden Sie den folgenden racadm-Befehl. CMC akzeptiert zwar RSA-Schlüssel bis zu einer Schlüsselstärke von 4096, die empfohlene Schlüsselstärke ist jedoch 1024.

     ```
     racadm -r 192.168.8.14 -u <default root account username> -p <default root account password> sshpkauth -i svcacct -k 1 -p 0xfff -f dsa_2048,pub
     ```
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 Systeme, die Linux ausführen

Die Anwendung ssh-keygen für Linux-Clients ist ein Befehlszeilendienstprogramm ohne grafische Benutzeroberfläche. Öffnen Sie ein Terminalfenster und geben Sie bei der Shell-Eingabeaufforderung Folgendes ein:

```
ssh-keygen –t rsa –b 1024 –C testing
```

wobei

`–t` „dsa" oder „rsa" sein muss.

`–b` die Bit-Verschlüsselungsgröße zwischen 768 und 4096 angibt.

`–c` das Ändern der Anmerkung des öffentlichen Schlüssels ermöglicht und optional ist.

Der < *passphrase* > ist optional. Wenn der Befehl beendet ist, verwenden Sie die öffentliche Datei zur Übergabe an den RACADM zum Hochladen der Datei.

Auf die CMC-Webschnittstelle zugreifen

Stellen Sie vor der Anmeldung bei CMC über die Webschnittstelle sicher, dass Sie einen unterstützten Webbrowser konfiguriert haben, und dass das Benutzerkonto mit den erforderlichen Berechtigungen erstellt wurde.

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

So greifen Sie auf die CMC-Webschnittstelle zu:

1. Öffnen Sie einen auf Ihrem System unterstützten Webbrowser.
   Die neuesten Informationen über unterstützte Webbrowser finden Sie in der *Dell Systems Software Support Matrix* unter **dell.com/support/manuals**.
2. Geben Sie in das Feld **Adresse** die folgende URL ein und drücken Sie die Eingabetaste:
   - Um mit einer IPv4-Adresse auf CMC zuzugreifen, geben Sie `https://<CMC IP address>` ein.
     Wenn die Standard-HTTPS-Anschlussnummer, Anschluss 443, geändert wurde, geben Sie Folgendes ein: `https://<CMC IP address>:<port number>`
   - Um mit einer IPv6-Adresse auf CMC zuzugreifen, geben Sie `https://[<CMC IP address>]` ein.
     Wenn die standardmäßige HTTPS-Schnittstellennummer (Schnittstelle 443) geändert wird, geben Sie Folgendes ein: `https://[<CMC IP address>]:<port number>`, wobei <*CMC-IP-Adresse*> für die CMC-IP-Adresse und <*Schnittstellennummer*> für die HTTPS-Schnittstellennummer steht.

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

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

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

Um sich am CMC anzumelden, müssen Sie ein CMC-Konto mit der Berechtigung zum **Anmelden am CMC** besitzen. Das Standard-root-Konto 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.

ANMERKUNG: Wenn die Zertifikatüberprüfung aktiviert ist, müssen Sie die FQDN des Systems angeben. Wenn die Zertifikatüberprüfung aktiviert und die IP-Adresse für den Domänen-Controller angegeben wird, schlägt die Anmeldung fehl.

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

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

1. Geben Sie im Feld **Benutzername** Ihren Benutzernamen ein:
   - CMC-Benutzername: <Benutzername>

ANMERKUNG: Die CMC-Benutzername darf nur alphanumerische Zeichen und bestimmte Sonderzeichen enthalten. Das @-Symbol und die folgenden Sonderzeichen werden nicht unterstützt:

- Schrägstrich nach rechts (/)
- Schrägstrich nach links (\)
- Strichpunkt (;)
- Anführungszeichen nach links (`)
- Doppelte Anführungszeichen (")

- Active Directory-Benutzername: <Domäne>\<Benutzername>, <Domäne>/<Benutzername> oder <Benutzer>@<Domäne>.
- LDAP-Benutzername: <Benutzername>

ANMERKUNG: Dieses Feld unterscheidet Groß- und Kleinschreibung.

2. Geben Sie im Feld **Kennwort** das Benutzerkennwort ein.

   ANMERKUNG: Für Active Directory-Benutzer ist das Feld **Benutzername** abhängig von Groß-/Kleinschreibung.

3. Wählen Sie im Feld **Domäne** aus dem Drop-Down-Menü die erforderliche Domäne aus.
4. Optional können Sie eine Sitzungszeitüberschreitung wählen. Dies ist die Dauer, die Sie ohne Aktivität angemeldet bleiben können, bevor Sie automatisch abgemeldet werden. Der Standardwert ist die **Web Service-Leerlaufzeitüberschreitung**.
5. Klicken Sie auf **OK**.

   Sie sind bei CMC mit den erforderlichen Berechtigungen angemeldet.

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

Anmeldung beim CMC mit Smart Card

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

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

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

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

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

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

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

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

   ANMERKUNG: Falls Sie die Standard-HTTPS-Schnittstellennummer (80) geändert haben, greifen Sie mit `<cmcname.domain-name>:<port number>` auf den CMC zu, wobei „cmcname" der CMC-Hostname für den CMC ist; *domain-name* ist der Domänenname und *port number* die HTTPS-Schnittstellennummer.
2. Legen Sie die Smart Card ein und klicken Sie auf **Anmeldung**.
   Das Dialogfeld PIN wird angezeigt.
3. Geben Sie die PIN ein und klicken Sie auf **Senden**.

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

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

Anmelden beim CMC unter Verwendung einfacher Anmeldung

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

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

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

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

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

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

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

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

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

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

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

Nachdem Sie die Terminal-Emulationssoftware Ihrer Management Station und haben, führen Sie die folgenden Tasks aus, um sich beim CMC anzumelden:

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

   Sie sind am CMC angemeldet.

Anmeldung beim CMC mit Authentifizierung mit öffentlichem Schlüssel

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

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

Beispiel:

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

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

CMC-Mehrfachsitzungen

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

Tabelle 2. CMC-Mehrfachsitzungen

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

4

Aktualisieren der Firmware

Sie können die Firmware für Folgendes aktualisieren:

- Der CMC
- Gehäuseinfrastruktur
- E/A-Modul
- PERC
- Expander und HDD

Sie können die Firmware für folgende Serverkomponenten aktualisieren:

- BIOS
- iDRAC7 auf FM120x4 (Server der 12. Generation)
- iDRAC8 auf FC630 (Server der 13. Generation)
- Lifecycle-Controller
- 32–Bit-Diagnose
- Treiberpaket des Betriebssystems
- Netzwerkschnittstellen-Controller
- RAID-Controller

Signiertes CMC-Firmware-Image

Die CMC-Firmware enthält eine Signatur. Die CMC-Firmware führt eine Signaturüberprüfung durch, um die Authentizität der hochgeladenen Firmware sicherzustellen. Die Firmware-Aktualisierung ist nur erfolgreich, wenn das Firmware-Image vom CMC als gültiges und nicht verändertes Image des Dienstanbieters authentifiziert wird. Die Firmware-Aktualisierung wird gestoppt, wenn der CMC die Signatur des hochgeladenen Firmware-Images nicht überprüfen kann. In dem Fall wird ein Warnungsereignis protokolliert und eine entsprechende Fehlermeldung angezeigt.

Wenn Sie versuchen, die CMC-Firmware-Version zu aktualisieren, überprüft der CMC-Firmware-Aktualisierungsprozess, ob das Firmware-Image der ausgewählten Version die Signatur des Dienstanbieters enthält. Die Firmware-Aktualisierung wird gestoppt, wenn die Signatur nicht gefunden wird oder wenn die Verifizierung des Images nicht erfolgreich ist. In dem Fall wird ein Warnungsereignis protokolliert und eine entsprechende Fehlermeldung angezeigt.

Wird eine Firmware-Zurückstufung auf eine frühere Version versucht, überprüft der CMC-Firmware-Aktualisierungsprozess, ob diese früheren Versionen die Signatur des Dienstanbieters enthalten. Die Zurückstufung der Firmware wird gestoppt, wenn die Signatur der früheren Version nicht von der aktuellen CMC-Version erkannt wird. Die CMC-Firmware protokolliert dann ein Warnungsereignis und es wird eine entsprechende Fehlermeldung angezeigt.

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.

Es wird empfohlen, bei der Aktualisierung der Firmware für das Gehäuse die folgende Reihenfolge einzuhalten:

- Blade-Komponenten-Firmware
- CMC-Firmware
- Gehäuseinfrastruktur-Firmware

Aktuelle Firmware-Versionen anzeigen

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

Anzeige der aktuell installierten Firmwareversionen über die CMC-Webschnittstelle

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

- **Gehäuseübersicht → Aktualisieren**
- **Gehäuseübersicht → Gehäuse-Controller → Aktualisieren**
- **Gehäuseübersicht → Server-Übersicht → Serverkomponentenaktualisierung**

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

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

Anzeige der aktuell installierten Firmwareversionen über RACADM

Sie können die aktuell installierte Firmware-Versionen mit dem Befehl `racadm getversion` anzeigen. Weitere Informationen über andere RACADM-Befehle finden Sie im *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Dell Chassis Management Controller für PowerEdge FX2/FX2s).

CMC-Firmware aktualisieren

Sie können die CMC-Firmware unter Verwendung der CMC-Webschnittstelle oder RACADM aktualisieren. Die Firmware-Aktualisierung behält standardmäßig die aktuellen CMC-Einstellungen bei.

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

ANMERKUNG: Die CMC-Firmware wird nicht aktualisiert, wenn die Firmware-Image-Datei keine Überprüfungssignatur enthält oder diese vorhanden, aber ungültig oder beschädigt ist.

ANMERKUNG: Es ist nicht möglich, die CMC-Firmware auf eine ältere Version zurückzustufen, wenn die berechnete Signatur von der aktuellen CMC-Firmware nicht erkannt wird.

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

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

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

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

CMC-Firmware über die Webschnittstelle aktualisieren

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

1. Gehen Sie im linken Fensterbereich zu einer der folgenden Seiten:
   - **Gehäuseübersicht → Aktualisieren**
   - **Gehäuseübersicht → Gehäuse-Controller → Aktualisieren**
2. Wählen Sie auf der Seite **Firmware-Aktualisierung** im Abschnitt **CMC-Firmware** die erforderlichen Komponenten in der Spalte **Aktualisierungsziele** für den CMC aus, den Sie aktualisieren möchten und klicken Sie dann auf **CMC-Aktualisierung anwenden**.
3. Geben Sie im Feld **Firmware-Image** den Pfad zur Firmware-Image-Datei auf der Management Station oder dem gemeinsam genutzten Netzwerk ein, oder klicken Sie auf **Durchsuchen**, um zum Dateispeicherort zu navigieren. Der Standardname der CMC-Firmware-Image-Datei ist `fx2_cmc.bin`.
4. Klicken Sie auf **Firmware-Aktualisierung beginnen** und klicken Sie dann auf **Ja**. Der Abschnitt **Fortschritt der Firmware-Aktualisierung** enthält Statusinformationen zur Firmware-Aktualisierung. Ein Statusindikator wird auf der Seite während des Aktualisierungsvorgangs angezeigt. Die Übertragungszeit kann je nach Verbindungsgeschwindigkeit variieren. Wenn der interne Aktualisierungsprozess beginnt, wird die Seite laufend aktualisiert und der Zeitgeber für die Firmware-Aktualisierung wird angezeigt. Weitere Informationen zu den verschiedenen Firmware-Status finden Sie in der Online-Hilfe.
5. Während der abschließenden Phase der Firmware-Aktualisierung ist für den CMC die Browsersitzung und die Verbindung zum CMC vorübergehend unterbrochen, da der CMC nicht mit dem Netzwerk verbunden ist. Sie müssen sich nach einigen Minuten anmelden, nachdem der CMC neu gestartet ist. Nach dem Zurücksetzen des CMC wird die neue Firmwareversion auf der Seite **Firmware-Aktualisierung** angezeigt.

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

Zusätzliche Anweisungen:

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

  ANMERKUNG: Der Aktualisierungsvorgang kann einige Minuten dauern.

Aktualisieren der CMC-Firmware über RACADM

Verwenden Sie zum Aktualisieren der CMC-Firmware mit RACADM den Unterbefehl `fwupdate`.

Beispiel: `racadm fwupdate <options> <firmware image>`.

Weitere Informationen über RACADM-Befehle finden Sie im *Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge FX2/FX2s).

Aktualisieren der CMC-Firmware unter Verwendung von DUPs

Sie können die Firmware-Version des CMC unter Verwendung eines Dell Update Package (DUP) über die folgenden Komponenten aktualisieren:

- iDRAC
- Blade-Server-Betriebssystem
- Lifecycle-Controller

Weitere Informationen zum Aktualisieren des CMC über iDRAC finden Sie im iDRAC-Benutzerhandbuch *Integrated Dell Remote Access Controller User's Guide*.

Bevor Sie den CMC unter Verwendung eines DUP aktualisieren, stellen Sie Folgendes sicher:

- Das CMC-Firmware-Paket ist als DUP auf einem lokalen System oder einer Netzwerkfreigabe verfügbar.
- **Gehäuseverwaltung im Servermodus** ist auf **Verwalten und Überwachen** gesetzt.

  Weitere Informationen finden Sie unter Konfigurieren der Gehäuseverwaltung im Servermodus.
- Bei Aktualisierungen über das Betriebssystem oder Lifecycle Controller muss die iDRAC-Option **Aktualisierung freigegebener Komponenten über BS/USC aktivieren** aktiviert sein. Weitere Informationen zum Aktivieren dieser Option finden Sie im iDRAC-Benutzerhandbuch *Integrated Dell Remote Access Controller User's Guide*.

ANMERKUNG: Wenn Sie den CMC unter Verwendung eines DUP aktualisieren, werden die im CMC-Image verfügbaren Aktualisierungen am EAM-Coprozessor beim nächsten Einschaltzyklus des Gehäuses wirksam.

Gehäuseinfrastruktur-Firmware aktualisieren

Der Aktualisierungsvorgang für die Gehäuseinfrastruktur-Firmware aktualisiert die Hauptplatinenkomponente.

ANMERKUNG: Bevor Sie die Firmware der Gehäuseinfrastruktur aktualisieren, fahren Sie ggf. alle Server im Gehäuse herunter.

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

1. Gehen Sie zu einer der folgenden Seiten:
   - **Gehäuseübersicht → Aktualisieren**
   - **Gehäuseübersicht → Gehäuse-Controller → Aktualisieren**
2. Wählen Sie auf der Seite **Firmware-Aktualisierung** im Abschnitt **Gehäuseinfrastruktur-Firmware** in der Spalte **Ziele aktualisieren** die Option und klicken Sie dann auf **Gehäuseinfrastruktur-Firmware anwenden** .
3. Klicken Sie auf der Seite **Firmware-Aktualisierung** auf **Durchsuchen** und wählen Sie dann die entsprechende Gehäuseinfrastruktur-Firmware.
4. Klicken Sie auf **Firmware-Aktualisierung beginnen** und dann klicken Sie auf **Ja**.

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

Zusätzliche Anweisungen:

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

Wenn die Aktualisierung abgeschlossen ist, geht die CMC-Verbindung verloren, da der gesamte CMC zurückgesetzt wird. Aktualisieren Sie die Webschnittstelle, um sich erneut anzumelden. Gehen Sie zu **Gehäuse-Übersicht → Gehäuse-Controller**.

Nachdem die Aktualisierung abgeschlossen ist, wird die aktualisierte Firmwareversion der Hauptplatine angezeigt.

.

Aktualisierung der Gehäuseinfrastruktur-Firmware mit RACADM

Verwenden Sie zum Aktualisieren der Gehäuseinfrastruktur-Firmware mit RACADM den Unterbefehl `fwupdate`.

Beispiel: `racadm fwupdate <options> <Firmware-Image>`.

Weitere Informationen über RACADM-Befehle finden Sie im *Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge FX2/FX2s).

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

Server-iDRAC-Firmware aktualisieren

Sie können die Firmware für iDRAC7 oder iDRAC8 aktualisieren. Voraussetzungen für die Verwendung dieser Funktion:

- Sie verfügen über eine Enterprise-Lizenz.
- Die iDRAC7-Firmware-Version muss mindestens 1.57.57 lauten.
- Die iDRAC8-Firmware-Version muss mindestens 2.05.05 lauten.

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

Server-iDRAC Firmware über die Webschnittstelle aktualisieren

So aktualisieren Sie die iDRAC-Firmware im Server:

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

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

   ANMERKUNG:
   Sie können auch Server-iDRAC-Firmware unter **Gehäuseübersicht → Server-Übersicht → Aktualisierung** aktualisieren. Weitere Informationen finden Sie unter Aktualisieren der Serverkomponenten-Firmware.
2. Um die iDRAC7- oder iDRAC8-Firmware zu aktualisieren, klicken Sie im Abschnitt **iDRAC<Revisionsnummer> Enterprise Firmware** auf den Link **Aktualisierung** des Servers, für den Sie die Firmware aktualisieren möchten.

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

Aktualisieren der Serverkomponenten-Firmware

Die Eins-zu-viele-Aktualisierungsfunktion in CMC ermöglicht Ihnen die Aktualisierung der Firmware von Serverkomponenten für mehrere Server. Sie können die Aktualisierung unter Verwendung der Dell Update Packages durchführen, die auf dem lokalen System oder einer Netzwerkfreigabe verfügbar sind. Dieser Vorgang basiert auf der Lifecycle Controller-Funktionalität auf dem Server.

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

Der Lifecycle Controller bietet eine Modulaktualisierungsunterstützung für iDRAC7 und Server mit neueren Versionen. Die iDRAC-Firmware muss Version 2.3 oder höher sein, um die Firmware mithilfe von Lifecycle Controller aktualisieren zu können.

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

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

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

- Bei Servern ab der 12. Generation – Wählen Sie nach dem Neustart des Servers aus dem F2-Setup **iDRAC-Einstellungen → Lifecycle Controller** aus, aktivieren Sie **CSIOR**, und speichern Sie die Änderungen.
- Bei Servern ab der 13. Generation – Drücken Sie nach dem Serverneustart bei entsprechender Aufforderung die Taste F10, um Lifecycle Controller aufzurufen. Wechseln Sie zur Seite **Hardware-Bestandsaufnahme**, indem Sie **Hardware-Konfiguration → Hardware-Bestandsaufnahme** auswählen. Klicken Sie auf der Seite **Hardware-Bestandsaufnahme** auf **Systembestandsaufnahme bei Neustart durchführen**.

Die Methode **Aktualisierung über Datei** ermöglicht Ihnen die Aktualisierung der Serverkomponenten-Firmware unter Verwendung von auf dem lokalen System gespeicherten DUP-Dateien. Sie können die einzelnen Serverkomponenten, deren Firmware aktualisiert werden soll, über die jeweils erforderliche DUP-Datei auswählen. Sie können eine große Anzahl von Komponenten gleichzeitig aktualisieren, indem Sie zum Speichern der DUP-Datei eine SD-Karte mit mehr als 48 MB Speicherkapazität verwenden.

ANMERKUNG: Beachten Sie Folgendes:

- Stellen Sie bei der Auswahl der einzelnen Serverkomponenten sicher, dass keine Abhängigkeiten zwischen den ausgewählten Komponenten bestehen. Anderenfalls kann es sein, dass der Server während der Aktualisierung unerwartet ausfällt.
- Halten Sie die empfohlene Reihenfolge für die Aktualisierung der Serverkomponenten ein. Andernfalls kann die Aktualisierung der Komponenten-Firmware möglicherweise nicht erfolgreich abgeschlossen werden.

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

  – iDRAC
  – Lifecycle-Controller
  – BIOS

Mit der Aktualisierung aller Blades mit nur einem Klick oder der Methode **Aktualisierung über Netzwerkfreigabe** können Sie die Firmware der Serverkomponenten anhand von DUP-Dateien durchführen, die auf einer Netzwerkfreigabe gespeichert sind. Mit der auf Dell Repository Manager (DRM) basierenden Aktualisierungsfunktion können Sie auf die auf der Netzwerkfreigabe gespeicherten DUP-Dateien zugreifen und die Serverkomponenten in einem einzigen Vorgang aktualisieren. Sie haben die Möglichkeit, ein benutzerdefiniertes Remote-Repository mit Firmware-DUPs und binären Images zu

erstellen und dieses unter Verwendung von Dell Repository Manager auf der Netzwerkfreigabe freizugeben. Alternativ können Sie mit Dell Repository Manager (DRM) nach den neuesten Firmware-Aktualisierungen suchen. Dell Repository Manager (DRM) sorgt dafür, dass Ihre Dell Systeme stets über das neueste BIOS sowie aktuelle Treiber, Firmware und Software verfügen. Auf der Support-Website (**support.dell.com**) können Sie eine Suche nach neuesten Aktualisierungen für die unterstützten Plattformen nach Marke und Modell oder nach Service-Tag-Nummer durchführen. Sie können die Aktualisierungen herunterladen oder anhand der Suchergebnisse ein Repository anlegen. Weitere Informationen zur Verwendung von DRM zum Suchen nach den neuesten Firmware-Aktualisierungen finden Sie unter http://en.community.dell.com/TECHCENTER/EXTRAS/M/WHITE_PAPERS/20438118/DOWNLOAD im Dell Tech Center. Informationen zum Speichern der Bestandsdatei, die DRM als Eingabe für die Repository-Erstellung heranzieht, finden Sie unter Speichern des Bestandsaufnahmenreports des Gehäuses unter Verwendung der CMC Web-Schnittstelle

ANMERKUNG: Das Aktualisieren aller Blades mit einem einzigen Klick bietet folgende Vorteile:

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

Es wird empfohlen, die CMC-Firmware zu aktualisieren, bevor die Firmwaremodule der Serverkomponenten aktualisiert werden. Sie können nach der Aktualisierung der CMC-Firmware, über die CMC Web-Schnittstelle, auf der Seite **Gehäuse-Übersicht → Server-Übersicht → Aktualisierung → Serverkomponentenaktualisierung**, die Firmware der Serverkomponenten aktualisieren. Es wird außerdem empfohlen, alle Komponentenmodule eines Servers auszuwählen und zusammen zu aktualisieren. Dadurch können die optimierten Algorithmen von Lifecycle Controllers zur Aktualisierung der Firmware verwendet und die Anzahl der Neustarts verringert werden.

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

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 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. Diese Datei ermöglicht Ihnen, die Lifecycle Controller-Firmware über die Firmware-Aktualisierungseinrichtung zu installieren, die auf der systemeigenen iDRAC-Web-Browser-Schnittstelle verfügbar ist.

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

Wenn der Lifecycle Controller-Dienst auf dem Server deaktiviert ist, wird im Abschnitt **Komponente/ Gerät-Firmware-Bestandsaufnahme** Folgendes angezeigt:

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

Sequenz der Serverkomponentenaktualisierung

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

- iDRAC
- Lifecycle-Controller
- BIOS
- Diagnose (optional)
- BS-Treiberpaket (optional)
- RAID
- NIC
- CPLD
- Sonstige Komponenten

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

Aktivierung des Lifecycle Controllers

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

- Klicken Sie für iDRAC-Server auf der Startkonsole auf die Taste F2, um das **System-Setup** aufzurufen.
- Gehen Sie auf der Seite **System-Setup-Hauptmenü** zu **iDRAC-Einstellungen** → **Lifecycle-Controller** und klicken Sie auf **Aktiviert**. Gehen Sie auf die Seite **System-Setup Hauptmenü** und klicken Sie auf **Fertigstellen**, um die Einstellungen zu speichern.
- Das Abbrechen der Systemdienste ermöglicht Ihnen, alle zeitlich eingeplanten, anstehenden Aufträge abzubrechen und aus der Warteschlange zu entfernen. Weitere Informationen über den Lifecycle Controller, unterstützte Server-Komponenten und die Gerätefirmware-Verwaltung finden Sie im *Lifecycle Controller-Remote Services Quick Start Guide* (Erste Schritte mit Lifecycle Controller-Remote-Diensten) oder auf **delltechcenter.com/page/Lifecycle+Controller**.
- Auf der Seite **Serverkomponenten-Aktualisierung** können Sie verschiedene Firmware-Komponenten auf dem Server aktualisieren. Zur Verwendung der Merkmale und Funktionen dieser Seite müssen Sie über folgendes verfügen:
  - Für CMC: Server Administrator-Berechtigung.

– Für iDRAC: iDRAC-Konfigurationsberechtigung und iDRAC-Anmeldeberechtigung.

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

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

So wählen Sie den Typ der Serverkomponentenaktualisierung aus:

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

Filtern von Komponenten für Firmware-Aktualisierungen

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

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

Der Abschnitt **Komponente/Geräteaktualisierungsfilter** der Seite **Serverkomponentenaktualisierung**, mit dem Sie Informationen basierend auf der Komponente filtern können, steht nur im Modus **Aktualisierung über Datei** 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.
- Um die Kategorie einer bestimmten Komponente bzw. eines Gerätes basierend auf Typen oder Modellen einzuengen, filtern Sie automatisch die ausgewählten Komponenten und Geräte.

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

Es folgen einige Beispiele für die Anwendung der Filtermechanismen:

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

  In manchen Fällen kann ein BIOS-Firmware-Aktualisierungs-Image über mehrere Servermodelle hinweg kompatibel sein. Derartige Optimierungen werden für den Fall ignoriert, dass diese Kompatibilität zukünftig nicht länger gegeben ist.

- Automatisches Filtern ist für Firmware-Aktualisierungen von NICs (Network Interface Controllers) und RAID-Controllern von Bedeutung. Diese Gerätekategorien haben verschiedene Typen und Modelle. Analog dazu können die Firmware-Aktualisierungs-Images (DUPs) in optimierter Form zur Verfügung stehen, wobei ein einziges DUP zur Aktualisierung mehrerer Typen oder Modelle von Geräten einer gegebenen Kategorie programmiert werden kann.

Anzeigen der Firmware-Bestandsliste

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

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

Firmwarebestandsaufnahme über die CMC-Webschnittstelle anzeigen

So zeigen Sie die Firmware-Bestandsaufnahme an:

1. Klicken Sie im linken Fensterbereich auf **Server-Übersicht** und klicken Sie dann auf **Aktualisierung**.
2. Zeigen Sie auf der Seite **Serverkomponenten-Aktualisierung** die Firmware-Bestandsaufnahmedetails im Abschnitt **Komponente/Gerät-Firmware-Bestandsaufnahme** an. Sie können auf dieser Seite folgende Informationen anzeigen:
   - 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.
   - Ein Hyperlink zu einer alternativen Seite wird bereitgestellt, auf der Sie lediglich die iDRAC-Firmware aktualisieren können. Diese Seite unterstützt nur iDRAC-Firmware-Aktualisierungen und keine anderen Komponenten oder Geräte auf dem Server. Die iDRAC-Firmware-Aktualisierung ist unabhängig vom Lifecycle-Controller-Dienst.
   - Wenn die Bestandsaufnahme der Komponenten und Geräte nicht dem entspricht, was physisch auf dem Server installiert ist, dann müssen Sie während des Server-Startvorgangs Lifecycle-Controller aufrufen. Dies ist beim Aktualisieren der internen Komponenten- und Geräteinformationen hilfreich und stellt eine Möglichkeit zur Prüfung der derzeit installierten Komponenten und Geräte dar. Dieses Verhalten tritt auf, wenn:

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

     Um diese Maßnahme für das iDRAC-Einstellungsdienstprogramm zu automatisieren, steht Ihnen eine Option zur Verfügung, auf die über die Startkonsole zugegriffen werden kann:

     1. Um auf das **System-Setup** zuzugreifen, drücken Sie auf der Startkonsole auf <F2>.
     2. Klicken Sie auf der Seite **System-Setup-Hauptmenü** auf**iDRAC-Einstellungen** → **Systeminventar beim Neustart erfassen**, wählen Sie **Aktiviert** und gehen Sie zurück zur Seite **System-Setup-Hauptmenü**. Klicken Sie dann auf **Fertigstellen**, um die Einstellungen zu speichern.

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

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

Tabelle 3. Komponenten- und Geräteinformationen

Feld	Beschreibung
Steckplatz	Zeigt den vom Server im Gehäuse besetzten Steckplatz an. Steckplatznummern sind sequentielle IDs für die vier im Gehäuse verfügbaren Steckplätze: • 1, 1a, 1b, 1c: 1d • 2, 2a, 2b, 2c 2d • 3; 3a, 3b, 3c, 3d • 4, 4a, 4b, 4c, 4d Das Nummerierungsschema hilft Ihnen bei der Identifizierung der Position des Servers im Gehäuse. Wenn weniger als vier Steckplätze mit Servern belegt sind, werden nur die mit Servern bestückten Steckplätze angezeigt.
Name	Zeigt den Namen des Servers in den einzelnen Steckplätzen an.
Modell	Zeigt das Modell des Servers an.
Komponente/ Gerät	Zeigt eine Beschreibung der Komponente oder des Geräts auf dem Server an. Wenn die Spaltenbreite zu schmal ist, stellt das Mouse-Over-Hilfswerkzeug eine Ansicht mit der Beschreibung bereit.
Aktuelle Version	Zeigt die aktuelle Version der Komponente oder des Geräts auf dem Server an.
Rollback-Version	Zeigt die Rollback-Version der Komponente oder des Geräts auf dem Server an.
Jobstatus	Zeigt den Jobstatus von jeglichen Vorgängen an, die auf dem Server geplant sind. Der Jobstatus wird kontinuierlich dynamisch aktualisiert. Wenn ein Jobabschluss über den Status als abgeschlossen erkannt wird, werden für den Fall, dass sich bei einer der Komponenten oder Geräte die Firmwareversion geändert hat, die Firmwareversionen der Komponenten und Geräte auf dem Server automatisch aktualisiert. Neben dem aktuellen Status ist auch ein Info-Symbol vorhanden, das zusätzliche Informationen über den aktuellen Jobstatus bereitstellt. Diese Informationen können angezeigt werden, indem auf das Symbol geklickt wird oder der Mauszeiger über dem Symbol angehalten wird.
Aktualisierung	Klicken Sie, um die Komponenten oder das Gerät für die Firmware-Aktualisierung auf dem Server auszuwählen.

Anzeigen der Firmware-Bestandsliste über RACADM

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

```
racadm getversion -l [-m <module>] [-f <filter>]
```

Weitere Informationen finden Sie im *Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge FX2/FX2s) unter **dell.com/support/manuals**.

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

So speichern Sie den Bestandsaufnahmenreport des Gehäuses:

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

   Die Seite **Serverkomponentenaktualisierung** wird angezeigt.
2. Klicken Sie auf **Bestandsaufnahmenreport speichern**.

   Die Datei *Inventory.xml* ist in einem externen System gespeichert.

   ANMERKUNG: Die Dell Repository Manager-Anwendung verwendet die Datei *Inventory.xml* als Eingabe, um ein Repository der Aktualisierungen für alle Blades im Gehäuse zu erstellen. Dieses Repository kann später in eine Netzwerkfreigabe exportiert werden. Im Modus **Aktualisierung über Netzwerkfreigabe** der Firmware-Aktualisierung wird diese Netzwerkfreigabe zur Aktualisierung der Komponenten sämtlicher Server verwendet. Die CSIOR-Funktion muss auf jedem Server aktiviert sein und der Bestandsaufnahmenreport des Gehäuses muss nach jeder Änderung an der Hardware- und Softwarekonfiguration des Gehäuses gespeichert werden.

Konfigurieren der Netzwerkfreigabe mit der CMC Web-Schnittstelle

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

1. Wechseln Sie in der CMC Web-Schnittstelle in der Systemstruktur zu **Server-Übersicht** und klicken Sie anschließend auf **Netzwerkfreigabe**.

   Die Seite **Netzwerkfreigabe bearbeiten** wird angezeigt.
2. Konfigurieren Sie im Abschnitt **Einstellungen für Netzwerkfreigabe** die folgenden Einstellungen nach Bedarf:
   - Protokoll
   - IP-Adresse oder Host-Name
   - Freigabenname
   - Aktualisierungsordner
   - Dateiname (optional)

     ANMERKUNG: **Dateiname** ist nur dann optional, wenn der standardmäßige Katalogdateiname *catalog.xml* lautet. Wenn der Katalogdateiname geändert wird, dann muss der neue Name in dieses Feld eingegeben werden.
   - Profil-Ordner
   - Domänenname
   - Benutzername
   - Kennwort

   Weitere Informationen finden Sie in der Online-Hilfe zu *CMC für Dell PowerEdge FX2/FX2s*.
3. Klicken Sie auf **Verzeichnis testen**, um zu überprüfen, ob die Verzeichnisse lesbar und beschreibbar sind.
4. Klicken Sie auf **Netzwerkverbindung testen**, um zu überprüfen, ob der Speicherort der Netzwerkfreigabe zugreifbar ist.
5. Klicken Sie auf **Anwenden**, um die Änderungen an den Eigenschaften der Netzwerkfreigabe zu übernehmen.

ANMERKUNG:

Klicken Sie auf **Zurück**, um zurück zur Seite **Serverkomponentenaktualisierung** zu gelangen.

Lifecycle-Controller-Jobvorgänge

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

Sie können Lifecycle-Controller-Vorgänge wie diese durchführen:

- Neuinstallation
- Rollback
- 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-Anmeldeberechtigung.

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

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

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

Serverkomponenten-Firmware neu installieren

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

Neuinstallation der Serverkomponenten-Firmware über die Webschnittstelle

So führen Sie eine Neuinstallation der Serverkomponenten-Firmware aus:

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht → Aktualisierung**.
2. Klicken Sie auf der Seite **Serverkomponentenaktualisierung** auf den entsprechenden Typ im Abschnitt **Aktualisierungstyp auswählen**.
3. Wählen Sie in der Spalte **Aktuelle Version** die Option für die Komponente oder das Gerät aus, für die oder das Sie die Firmware neu installieren möchten.
4. Wählen Sie eine der folgenden Optionen:
   - **Jetzt neu starten** - Server sofort neu starten.
   - **Bei nächstem Neustart** – Manuell zu einem späteren Zeitpunkt neu starten.
5. Klicken Sie auf **Neu installieren**. Die Firmware-Version für die ausgewählte Komponente oder das Gerät wird neu installiert.

Zurücksetzen der Serverkomponenten-Firmware

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

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

Zurücksetzen der Serverkomponenten-Firmware über die CMC-Webschnittstelle

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

1. Klicken Sie im linken Fensterbereich auf **Server-Übersicht→ Aktualisieren**.
2. Klicken Sie auf der Seite **Serverkomponentenaktualisierung** auf den entsprechenden Typ im Abschnitt **Aktualisierungstyp auswählen**.
3. Wählen Sie in der Spalte **Version zurücksetzen** die Option für die Komponente oder das Gerät, für die oder das Sie die Firmware zurücksetzen möchten.
4. Wählen Sie eine der folgenden Optionen:
   - **Jetzt neu starten** - Server sofort neu starten.
   - **Bei nächstem Neustart** – Manuell zu einem späteren Zeitpunkt neu starten.
5. Klicken Sie auf **Zurücksetzen**. Die vorher installierte Firmware-Version für die ausgewählten Komponenten oder Geräte wird neuinstalliert.

Aktualisieren der Serverkomponenten-Firmware

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

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

Es wird empfohlen, die Jobswarteschlange zu löschen, bevor Sie die Aktualisierung einer Serverkomponentenfirmware initialisieren. Auf der Seite **Lifecycle Controller-Jobs** ist eine Liste mit allen

Jobs auf den Servern vorhanden. Diese Seite ermöglicht die Löschung einzelner/mehrerer Jobs oder die Bereinigung aller Jobs auf dem Server.

BIOS-Aktualisierungen sind Servermodell-spezifisch. Manchmal wird die Aktualisierung möglicherweise auf alle NIC-Geräte auf dem Server angewendet, obwohl ein einzelnes NIC-Gerät (Network Interface Controller) für eine Firmwareaktualisierung ausgewählt wurde. Dieses Verhalten gehört zur Lifecycle Controller-Funktionalität und insbesondere zur im DUP (Dell Update Package) enthaltenen Programmierung. Derzeit werden DUPs (Dell Update Packages) mit einer Größe von weniger als 85 MB unterstützt.

Wenn die Größe des Aktualisierungsdatei-Images größer ist, zeigt der Jobsstatus an, dass das Herunterladen fehlgeschlagen ist. Werden auf einem Server mehrere Serverkomponenten-Aktualisierungen versucht, überschreitet die kombinierte Größe aller Firmware-Aktualisierungen möglicherweise 85 MB. In einem solchen Fall schlägt eine der Komponenten-Aktualisierungen fehl, da deren Aktualisierungsdatei abgeschnitten wird. Zum Aktualisieren mehrerer Komponenten auf einem Server wird empfohlen, zuerst die Lifecycle-Controller- und 32-Bit-Diagnose-Komponenten zusammen zu aktualisieren. Diese benötigen keinen Neustart des Servers und können relativ schnell abgeschlossen werden. Die anderen Komponenten können anschließend zusammen aktualisiert werden.

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

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

So aktualisieren Sie die Version der Serverkomponenten-Firmware auf die nächste Version unter Verwendung der Methode „Aktualisierung über Datei“:

1. Wechseln Sie in der CMC Web-Schnittstelle in der Systemstruktur zu **Server-Übersicht**, und klicken Sie anschließend auf **Aktualisieren → Serverkomponentenaktualisierung**.

   Die Seite **Serverkomponentenaktualisierung** wird angezeigt.
2. Wählen Sie im Abschnitt **Aktualisierungstyp auswählen** die Option **Aktualisierung über Datei**. Weitere Informationen finden Sie unter Auswählen des Aktualisierungstyps der Serverkomponenten-Firmware
3. Filtern Sie im Abschnitt **Komponenten-/Geräte-Aktualisierungsfilter** die Komponente oder das Gerät (optional). Weitere Informationen finden Sie unter Filtern von Komponenten für Firmware-Aktualisierungen.
4. Markieren 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** markieren.

   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 Konfigurieren der erweiterten CMC-Speicherkarte.

5. Geben Sie die Firmware-Image-Datei für die ausgewählte(n) Komponente(n) bzw. das/die ausgewählte(n) Gerät(e) an. Das ist eine Microsoft Windows Dell Update Package (DUP)-Datei.
6. Wählen Sie eine der folgenden Optionen:
   - **Jetzt neustarten** – Sofort neustarten. Die Firmware-Aktualisierung wird sofort angewandt.
   - **Beim nächsten Neustart** – Der Server kann zu einem späteren Zeitpunkt manuell neu gestartet werden. Die Firmware-Aktualisierung wird nach dem nächsten Neustart angewandt.

     ANMERKUNG: Dieser Schritt gilt nicht für Lifecycle Controller- und 32-Bit-Diagnose-Firmware-Aktualisierungen. Für diese Geräte ist kein Serverneustart erforderlich.
7. Klicken Sie auf **Aktualisieren**. Die Firmware-Version für die ausgewählten Komponenten oder Geräte wird aktualisiert.

Aktualisieren von Serverkomponenten mit einem Klick unter Verwendung der Netzwerkfreigabe

Die Server- oder Serverkomponentenaktualisierung über eine Netzwerkfreigabe unter Verwendung von Dell Repository Manager und der modularen Gehäuse-Integration von Dell PowerEdge FX2/FX2s vereinfacht die Aktualisierung enorm, da Sie mit der benutzerdefinierten Bündel-Firmware Ihre Systeme schneller und einfacher bereitstellen können. Mit der flexiblen Aktualisierung über eine Netzwerkfreigabe können Sie gleichzeitig alle 12G-Serverkomponenten mit einem einzigen Katalog (CIFS oder NFS) aktualisieren.

Diese Methode ermöglicht eine schnelle und einfache Erstellung eines eigenen, benutzerdefinierten Repositorys für verbundene Systeme unter Verwendung von Dell Repository Manager (DRM) und der Gehäuse-Bestandsdatei, die mithilfe der CMC Web-Schnittstelle exportiert wurde. Mit DRM können Sie ein vollständig benutzerdefiniertes Repository erstellen, das nur die Aktualisierungspakete für die jeweilige Systemkonfiguration enthält. Ferner können Sie Repositories für Aktualisierungen erstellen, die nur Aktualisierungen für veraltete Geräte enthalten, oder Sie erstellen ein Baseline Repository mit Aktualisierungen für alle Geräte. Je nach erforderlichem Aktualisierungsmodus können Sie außerdem Aktualisierungsbündel für Linux oder Windows erstellen. Mit DRM können Sie das Repository auf einer CIFS- oder NFS-Freigabe speichern. Unter Verwendung der CMC Web-Schnittstelle können Sie die Anmeldeinformationen und Angaben zum Speicherort für die Freigabe konfigurieren. Ebenfalls unter Verwendung der CMC Web-Schnittstelle können Sie anschließend die Serverkomponentenaktualisierung für einen einzelnen oder mehrere Server durchführen.

Voraussetzungen für die Verwendung des Netzwerkfreigabe-Modus

Folgende Voraussetzungen müssen erfüllt sein, um die Aktualisierung der Serverkomponenten-Firmware im Netzwerkfreigabe-Modus durchzuführen:

- Die Server müssen über eine iDRAC Enterprise-Lizenz verfügen.
- Lifecycle Controller muss auf den Servern aktiviert sein.
- Dell Repository Manager 1.8 oder höher muss auf dem System installiert sein.

- Sie müssen über CMC-Administratorrechte verfügen.

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

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

1. Wechseln Sie in der CMC Web-Schnittstelle in der Systemstruktur zu **Server-Übersicht**, und klicken Sie anschließend auf **Aktualisieren → Serverkomponentenaktualisierung**.

   Die Seite **Serverkomponentenaktualisierung** wird angezeigt.
2. Wählen Sie im Abschnitt **Aktualisierungstyp auswählen** die Option **Aktualisierung über Netzwerkfreigabe** aus. Weitere Informationen finden Sie unter „Auswählen des Aktualisierungstyps der Serverkomponenten-Firmware".
3. Wenn die Netzwerkfreigabe nicht angeschlossen ist, konfigurieren Sie die Netzwerkfreigabe für das Gehäuse. Zum Konfigurieren oder bearbeiten der Details der Netzwerkfreigabe, klicken Sie in der Tabelle mit den Eigenschaften der Netzwerkfreigabe auf **Bearbeiten**. Weitere Informationen finden Sie unter „Konfigurieren der Netzwerkfreigabe unter Verwendung der CMC Web-Schnittstelle".
4. Klicken Sie auf **Bestandsaufnahmenreport speichern**, um die Datei mit der Gehäusebestandsaufnahme zu exportieren, die die Komponenten- und Firmwaredetails enthält.

   Die Datei *inventory.xml* wird auf einem externen System gespeichert. Der Dell Repository Manager verwendet die Datei *inventory.xml* zur Erstellung von benutzerdefinierten Aktualisierungsbündeln. Dieses Repository befindet sich auf der CIFS- oder NFS-Freigabe, die vom CMC konfiguriert wurde. Weitere Informationen zum Erstellen eines Repositorys unter Verwendung von Dell Repository Manager finden Sie in den Benutzerhandbüchern *Dell Repository Manager Data Center Version 1.8 User's Guide* und *Dell Repository Manager Business Client Version 1.8 User's Guide* **unter dell.com/support/manuals**.
5. Klicken Sie auf **Auf Aktualisierung prüfen**, um die in der Netzwerkfreigabe verfügbaren Aktualisierungen anzuzeigen.

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

   ANMERKUNG: Klicken Sie für einen Steckplatz auf **Minimieren**, um die Datails zur Komponente und Gerätefirmware für den jeweiligen Steckplatz zu minimieren. Um wieder alle Details anzuzeigen, klicken Sie auf **Erweitern**.
6. Wählen Sie im Abschnitt **Firmware-Bestandsaufnahme der Komponenten/Geräte** das gegenüberliegende Kontrollkästchen **Alle auswählen/abwählen** aus, um alle unterstützten Server auszuwählen. Wählen Sie alternativ das Kontrollkästchen gegenüber dem Server aus, für den Sie die Serverkomponenten-Firmware aktualisieren möchten. Sie können für den Server keine individuellen Komponenten auswählen.
7. Wählen Sie eine der folgenden Optionen aus, um anzugeben, ob ein Systemneustart erforderlich ist, nachdem die Aktualisierungen geplant sind:
   - Jetzt neu starten – Aktualisierungen werden geplant, und der Server wird neu gestartet, wobei die Aktualisierungen sofort an den Serverkomponenten angewandt werden.
   - Beim nächsten Neustart – Aktualisierungen werden geplant, aber erst nach dem nächsten Neustart des Servers angewandt.
8. Klicken Sie auf **Aktualisieren**, um die Firmwareaktualisierungen für die verfügbaren Komponenten der ausgewählten Server zu planen.

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

9. Klicken Sie auf **OK**, um fortzufahren und die Planung der Firmware-Aktualisierung für die ausgewählten Server abzuschließen.

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

Geplante Serverkomponenten-Firmware-Jobs löschen

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

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

Geplante Serverkomponenten-Firmware-Jobs über die Webschnittstelle löschen

So löschen Sie geplante Serverkomponenten-Firmware-Jobs:

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

iDRAC-Firmware mittels CMC wiederherstellen

Die iDRAC-Firmware wird normalerweise unter Verwendung der iDRAC-Schnittstellen aktualisiert, z. B. über die iDRAC-Web-Schnittstelle oder die SM-CLP-Befehlszeilenschnittstelle, oder unter Verwendung von betriebssystemspezifischen Aktualisierungspaketen, die von der Website **support.dell.com** heruntergeladen werden können. Weitere Informationen finden Sie im iDRAC-Benutzerhandbuch *Dell Integrated Dell Remote Access Controller (iDRAC) User's Guide*.

5

Gehäuseinformationen anzeigen und Funktionszustandsüberwachung von Gehäuse und individuellen Komponenten

Sie können Informationen anzeigen und den Funktionszustand für Folgendes überwachen:

- CMC
- Alle Server und einzelne Server
- E/A-Module
- Lüfter
- Netzteile
- Temperatursensoren
- PCIe-Geräte

Gehäuse- und Komponenten-Zusammenfassungen anzeigen

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

Um den Gehäuse-Funktionszustand anzuzeigen, klicken Sie auf **Gehäuse-Übersicht**. Das System zeigt den Gesamtfunktionszustand von Gehäuse, CMC, Servermodulen, E/A-Modulen (EAMs), Lüftern, Netzteileinheiten (PSUs) und PCIe-Geräten an. Detaillierte Informationen über die einzelnen Komponenten erhalten Sie, wenn Sie auf die jeweilige Komponente klicken. Außerdem werden die neuesten Ereignisse im CMC-Hardwareprotokoll angezeigt. Weitere Informationen finden Sie im iDRAC-Benutzerhandbuch *Dell Integrated Dell Remote Access Controller (iDRAC) User's Guide*.

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 sowie in der Draufsicht dargestellt (jeweils die oberen und unteren Bilder). Server und KVMs werden in der Vorderansicht gezeigt und die restlichen Komponenten werden in der Rückansicht gezeigt. Die Komponentenauswahl wird durch eine blaue Einfärbung angezeigt und wird durch Anklicken des Bildes der erforderlichen Komponente gesteuert.

Wenn eine Komponente im Gehäuse vorhanden ist, dann wird ein Symbol dieses Komponententyps in der Grafik auf der Position (Steckplatz) angezeigt, in der die Komponente installiert ist. Leere Positionen werden mit einem anthrazitfarbenen Hintergrund angezeigt. Das Komponentensymbol zeigt visuell den Zustand der Komponenten an. Andere Komponenten zeigen Symbole an, die die physische Komponente visuell darstellen. Wenn der Cursor auf einer Komponente positioniert wird, wird eine Quickinfo mit zusätzlichen Informationen über diese Komponente angezeigt.

Ausgewählte Komponenteninformationen

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

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

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

Komponente	Funktionszustand und Leistungseigenschaften	Eigenschaften	Quicklinks
CMC	• MAC-Adresse • IPv4 • IPv6	• Firmware • Standby-Firmware • Letzte Aktualisierung • Hardware	• CMC-Status • Netzwerkbetrieb • Firmware-Aktualisierung
Alle Server und einzelne Server	• Stromzustand • Stromverbrauch • Funktionszustand • Zugeteilter Strom • Temperatur	• Name • Modell • Service-Tag-Nummer • Host-Name • iDRAC • CPLD • BIOS • Betriebssystem • CPU-Informationen • Gesamtsystemspeicher	• Serverstatus • Remote-Konsole starten • iDRAC-GUI starten • Server ausschalten • Ordentliches Herunterfahren • Remote-Dateifreigabe • iDRAC-Netzwerk bereitstellen • Serverkomponentenaktualisierung

Komponente	Funktionszustand und Leistungseigenschaften	Eigenschaften	Quicklinks
			ANMERKUNG: Die Quicklinks für „Server ausschalten" und „Ordentliches Herunterfahren" werden nur dann angezeigt, wenn der Server-Stromzustand „Ein" lautet. Wenn der Server-Stromzustand „Aus" lautet, wird der Quicklink für „Server einschalten" angezeigt.
Netzteileinheiten	Stromstatus	Kapazität	• Netzteilstatus • Stromverbrauch • Systembudget
PCIe-Geräte	• Installiert • Zugewiesen	• Modell • Zuweisung • Hersteller-ID • Geräte-ID • Steckplatztyp • Modultyp • Struktur • Stromstatus	• PCIe-Status • PCIe-Setup
Lüfter	• Geschwindigkeit • PWM (% von Max.) • Lüfter-Offset	• Warnungsschwelle • Kritischer Schwellenwert	• Lüfterstatus • Lüfterkonfiguration
EAM-Steckplatz	• Stromzustand • Rolle	• Modell • Service-Tag-Nummer	EAM-Status

Servermodellnamen und Service-Tag-Nummer anzeigen

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

1. Im linken Fensterbereich werden unter dem Strukturknoten **Server-Übersicht** alle Server in der Serverliste angezeigt (STECKPLATZ-01 bis STECKPLATZ-04). Wenn ein Server nicht im Steckplatz vorhanden ist, wird das entsprechende Bild in der Grafik grau unterlegt.
2. Positionieren Sie den Cursor auf dem Steckplatznamen oder der Steckplatznummer eines Servers. Falls verfügbar, wird eine Quickinfo mit dem Modellnamen und der Service-Tag-Nummer des Servers angezeigt.

Gehäusezusammenfassung anzeigen

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

Die Seite **Gehäusezusammenfassung** wird angezeigt. Weitere Informationen zu dieser Seite finden Sie in der *Online-Hilfe zu CMC für Dell PowerEdge FX2/FX2s*.

Gehäuse-Controllerinformationen und Status anzeigen

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

Die Seite **Gehäuse-Controller-Status** wird angezeigt. Weitere Informationen finden Sie in der *Online-Hilfe zu CMC für Dell PowerEdge FX2/FX2s.*

Informationen und Funktionszustand von allen Servern anzeigen

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

- Klicken Sie auf **Gehäuse-Übersicht.** Die Seite **Gehäuse-Funktionszustand** bietet einen grafischen Überblick über alle Server, die im Gehäuse installiert sind. Der Serverfunktionszustand wird durch die Farbe der Server-Untergrafik angegeben. Weitere Informationen über den Gehäuse-Funktionszustand finden Sie in der *Online-Hilfe zu CMC für Dell PowerEdge FX2/FX2s*.
- Klicken Sie auf **Gehäuseübersicht → Serverübersicht**. Die Seite **Serverstatus** enthält eine Übersicht zu den Servern im Gehäuse. Weitere Informationen finden Sie in der *Online-Hilfe*.

Anzeigen der Informationen und des Funktionszustands von EAMs

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

1. Klicken Sie auf **Gehäuseübersicht**.

   Die Seite **Gehäusefunktionszustand** wird angezeigt. Die Grafik im linken Fensterbereich zeigt die Rück- und Vorderansicht sowie die Draufsicht des Gehäuses an und enthält den Funktionszustand für das EAM. Der EAM-Funktionszustand wird durch die Farbe der EAM-Untergrafik angegeben. Positionieren Sie den Cursor auf der einzelnen EAM-Untergrafik. Der Texthinweis liefert zusätzliche Informationen zu diesem EAM. Klicken Sie auf die EAM-Untergrafik, um die EAM-Informationen im rechten Fensterbereich anzuzeigen.
2. Wählen Sie **Gehäuseübersicht → E/A-Modul-Übersicht** .

   Die Seite **E/A-Modul-Status** enthält eine Übersicht zu einem mit dem Gehäuse verbundenen EAM. Weitere Informationen finden Sie in der *Online-Hilfe zu CMC für Dell PowerEdge FX2/FX2s*.

Informationen und Funktionszustand der Lüfter anzeigen

Das CMC steuert die Geschwindigkeit des Gehäuselüfters, indem es die Lüftergeschwindigkeit, basierend auf Systemereignissen erhöht oder vermindert. Sie können den Lüfter in den drei Modi Niedrig, Mittel und

Hoch (Lüfter-Offset) betreiben. Weitere Informationen über die Konfiguration eines Lüfters finden Sie in der *Online-Hilfe zu CMC für Dell PowerEdge FX2/FX2s*.

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

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

ANMERKUNG: Der CMC überwacht die Temperatursensoren im Gehäuse und reguliert die Lüftergeschwindigkeit automatisch nach Bedarf. Wenn dieser Befehl außer Kraft gesetzt wird, betreibt CMC den Lüfter immer in der ausgewählten Geschwindigkeit, selbst wenn das Gehäuse es nicht erfordert, dass die Lüfter bei dieser Geschwindigkeit laufen. Sie können dies jedoch außer Kraft setzen, um eine minimale Lüftergeschwindigkeit durch den RACADM-Befehl `fanoffset` aufrechtzuerhalten.

Weitere Informationen über die RACADM-Befehle finden Sie im *Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge FX2/FX2s), verfügbar unter dell.com/support/manuals.

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

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

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

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

1. Gehen Sie zu **Chassis Overview**.

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

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

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

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

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

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

Konfigurieren von Lüftern

Lüfter-Offset – Diese Funktion ermöglicht es Ihnen, den Luftstrom zu den PCIe-Steckplätzen zu erhöhen. Ein Beispiel der Nutzung von Lüfter-Offset ist, wenn Sie Hochleistungs- oder benutzerdefinierte PCIe-Karten verwenden, die eine höhere Kühlung als normal erfordern. Die Lüfter-Offset-Funktion verfügt über die Optionen Aus, Niedrig, Mittel und Hoch. Diese Einstellungen entsprechen einem Lüfterdrehzahl-Offset (Erhöhung) von 20 %, 50% und 100 % der maximalen Geschwindigkeit. Gleichfalls gibt es Mindesteinstellungen für jede Option: 35 % für Niedrig, 65 % für Mittel und 100 % für Hoch.

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

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

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

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

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

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

Anzeigen von Frontblenden-Eigenschaften

So zeigen Sie die Frontblenden-Eigenschaften an:

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht → Frontblende**.
2. Auf der Seite **Eigenschaften** können Sie Folgendes anzeigen:
   - **Netzschaltereigenschaften**
   - **KVM – Eigenschaften**
   - **Anzeigen auf der Vorderseite**

KVM-Informationen und Funktionszustand anzeigen

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

Klicken Sie auf **Gehäuseübersicht → Frontblende**.

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

Informationen und Funktionszustand der Temperatursensoren anzeigen

So zeigen Sie den Funktionszustand der Temperatursensoren an:

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

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

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

6

Den CMC konfigurieren

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

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

Sie können den CMC mithilfe der Webschnittstelle konfigurieren oder den Erstzugriff auf CMC RACADM einrichten.

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

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

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

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

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

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 deaktiviert.

Sie können den DHCP-Server dazu aktivieren, automatisch eine IP-Adresse vom DHCP abzurufen.

Aktivieren der CMC-Netzwerkschnittstelle

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

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

ANMERKUNG:
Bei Deaktivierung der CMC-Netzwerkschnittstelle werden durch den Deaktivierungsvorgang die folgenden Maßnahmen durchgeführt:

- Deaktivierung des Netzwerkschnittstellen-Zugriffs auf die Out-of-Band-Gehäuseverwaltung, einschließlich iDRAC- und EAM-Verwaltung
- Keine Erkennung des Status „Link deaktiviert"

  Wenn Sie nur den CMC-Netzwerkzugriff deaktivieren möchten, deaktivieren Sie CMC-IPv4 und CMC-IPv6.

ANMERKUNG: Der CMC NIC ist standardmäßig aktiviert.

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

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

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

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

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

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

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

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

DHCP ist standardmäßig deaktiviert. Geben Sie zum Aktivieren und Verwenden des DHCP-Servers auf dem Netzwerk für die Zuweisung von iDRAC-oder CMC-IPv4-Adresse, Subnetzmaske und Gateway Folgendes ein:

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

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

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

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

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

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

Um die Funktion DHCP für DNS-Server-Adressfunktionen zu aktivieren und bevorzugte statische und alternative DNS-Server-Adressen anzugeben, geben Sie Folgendes ein:

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

Um die Funktion DHCP für DNS-Server-Adressfunktionen für IPv6 zu aktivieren und bevorzugte statische und alternative DNS-Server-Adressen anzugeben, geben Sie Folgendes ein:

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6DNSServersFromDHCP6 1
```

Statische DNS-Server-IP-Adressen einrichten

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

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

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

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

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

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

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

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

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

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

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

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

Verwenden Sie zum Anzeigen von IPv4-Einstellungen das Objekt `cfgCurrentLanNetworking` mit den folgenden Unterbefehlen:

- `getniccfg`
- `getconfig`

Verwenden Sie zum Anzeigen von IPv6-Einstellungen das Objekt `cfgIpv6LanNetworking` mit dem Unterbefehl `getconfig`.

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

Weitere Informationen über die Unterbefehle und Objekte finden Sie im *Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge FX2/FX2s).

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.

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

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

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

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

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

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

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

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

wobei:

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

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

wobei:

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

Konfigurieren des Management-Anschlusses 2

Der zweite Netzwerkanschluss des CMC kann für die Verkettung von CMCs verwendet werden, um die Verkabelung zu reduzieren, oder als redundanter Anschluss für den Netzwerk-Failover-Betrieb. Der **Management-Anschluss 2** kann an den Top-of-Rack (TOR)-Switch oder an einen anderen Switch angeschlossen werden. Es ist nicht erforderlich, dass die beiden CMC-NIC-Ports mit dem gleichen Subnetz verbunden sind.

Der CMC kann nicht zwecks Verwaltungsnetzwerk-Portredundanz angeschlossen werden, bevor er für diesen Vorgang konfiguriert ist. Der CMC muss für die Bereitstellung die standardmäßige Einzel-Netzwerkverbindung verwenden; erst danach kann die zweite redundante Verbindung hergestellt werden.

ANMERKUNG: Wenn der Management-Anschluss 2 auf „Redundant" eingestellt, aber für „Stapeln" verkabelt ist, haben die Downstream-CMCs (weiter vom TOR-Switch entfernt) keine Netzwerkverbindung.

ANMERKUNG: Wenn die Verwaltungsschnittstelle 2 jedoch für „Stacking“ eingestellt, aber für „Redundant“ verkabelt ist (zwei Verbindungen zum TOR-Switch), könnten Routing-Schleifen einen Netzwerksturm verursachen.

Verwenden Sie zum Festlegen der Redundanz den Befehl `racadm config –g cfgNetTuning –o cfgNetTuningNicRedundant 1`.

Verwenden Sie zum Festlegen des Stapelbetriebs den Befehl `racadm config –g cfgNetTuning –o cfgNetTuningNicRedundant 0`.

Standardmäßig wird der Management-Anschluss 2 für „Stapeln“ eingestellt.

Konfigurieren von Verwaltungsschnittstelle 2 unter Verwendung der CMC Web-Schnittstelle

So konfigurieren Sie die Verwaltungsschnittstelle unter Verwendung der CMC-Web-Schnittstelle:

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** → **Netzwerk** und dann auf das Register **Netzwerk**.
2. Wählen Sie auf der Seite **Netzwerkkonfiguration** im Abschnitt **Allgemeine Einstellungen** neben **Verwaltungsschnittstelle 2** entweder **Redundant** oder **Stacking** aus.
3. Klicken Sie auf **Änderungen anwenden**.

    - Wenn die Verwaltungsschnittstelle 2 auf „Redundant“ eingestellt aber für „Stacking“ verkabelt ist, haben die Downstream-CMCs (weiter vom obersten Switch im Rack entfernt) keine Netzwerkverbindung.
    - Wenn die Verwaltungsschnittstelle 2 jedoch für „Stacking“ eingestellt, aber für „Redundant“ verkabelt ist (zwei Verbindungen zum TOR-Switch), könnten Routing-Schleifen einen Netzwerksturm verursachen.

Konfigurieren von Verwaltungsschnittstelle 2 unter Verwendung von RACADM

Verwenden Sie zum Festlegen der Redundanz den Befehl `racadm config –g cfgNetTuning –o cfgNetTuningNicRedundant 1`.

Verwenden Sie zum Festlegen des Stapelbetriebs den Befehl `racadm config –g cfgNetTuning –o cfgNetTuningNicRedundant 0`.

Standardmäßig wird der Management-Anschluss 2 für „Stapeln“ eingestellt.

Dienste konfigurieren

Sie können die folgenden Dienste auf CMC konfigurieren und aktivieren:

- CMC Serielle Konsole – Aktivieren Sie den Zugriff auf CMC unter Verwendung der seriellen Konsole.
- Web Server – Aktivieren Sie den Zugriff auf CMC Web-Schnittstelle. Die Deaktivierung des Web Servers deaktiviert auch den Remote-RACADM.
- SSH – Aktivieren Sie den Zugriff auf CMC über Firmware RACADM.
- Telnet – Aktivieren Sie den Zugriff auf CMC über Firmware RACADM

- Remote-RACADM – Aktivieren Sie den Zugriff auf CMC mittels RACADM.
- SNMP – Aktivieren Sie CMC zum Versenden von SNMP-Traps für Ereignisse.
- Remote-Syslog – Aktivieren Sie CMC, um Ereignisse auf einem Remote-Server zu protokollieren. Um diese Funktion zu nutzen, benötigen Sie eine Enterprise-Lizenz.

ANMERKUNG: Vermeiden Sie beim Ändern von CMC-Service-Schnittstellennummern für SSH, Telnet, HTTP oder HTTPS die Verwendung von Schnittstellen, die häufig von Betriebssystemdiensten verwendet werden, wie z. B. Schnittstelle 111. Lesen Sie die Informationen zu reservierten Schnittstellen der Internet Assigned Numbers Authority (IANA) unter http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml.

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

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

- Die Netzwerkkonfiguration oder Netzwerksicherheitseigenschaften wurden über die CMC-Webbenutzerschnittstelle oder RACADM geändert.
- Die Web Server-Schnittstellenkonfiguration wird über die Webbenutzerschnittstelle oder RACADM geändert.
- CMC wird zurückgesetzt.
- Ein neues SSL-Serverzertifikat wird hochgeladen.

ANMERKUNG: Zum Modifizieren von Diensteeinstellungen müssen Sie Berechtigungen als Gehäusekonfiguration-Administrator aufweisen.

Remote-Syslog ist ein zusätzliches Protokollziel für den CMC. Nach der Konfiguration von Remote-Syslog wird jeder neue vom CMC erzeugte Protokolleintrag an die Ziele weitergeleitet.

ANMERKUNG: Weil das Netzwerkübertragungsprotokoll für die weitergeleiteten Protokolleinträge UDP ist, gibt es weder eine Garantie, dass Protokolleinträge zugestellt werden, noch gibt es Feedback an CMC darüber, ob die Protokolleinträge erfolgreich empfangen wurden.

Dienste über RACADM konfigurieren

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

- `cfgRacTuning`
- `cfgRacTuneRemoteRacadmEnable`

Weitere Informationen über diese Objekte finden Sie im *Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge FX2/FX2s) unter dell.com/support/manuals.

Wenn die Firmware auf dem Server eine Funktion nicht unterstützt, bewirkt das Konfigurieren einer Eigenschaft zu dieser Funktion, dass ein Fehler angezeigt wird. Wenn zum Beispiel RACADM verwendet

wird, um Remote-Syslog auf einem nicht unterstützten iDRAC zu aktivieren, wird eine Fehlermeldung angezeigt.

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

Beispiel:

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

Erweiterte CMC-Speicherkarte konfigurieren

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

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

1. Gehen Sie im linken Fensterbereich auf **Gehäuseübersicht** und klicken Sie dann auf **Gehäuse-Controller → Flash-Datenträger**.
2. Wählen Sie aus der Seite **Wechselbarer Flash-Datenträger** aus dem Drop-Down-Menü je nach Bedarf eine der folgenden Optionen aus:
   - **Datenträger des aktiven Controllers reparieren**
   - **Verwendung des Flash-Datenträgers zum Speichern von Gehäusedaten abbrechen**

   Weitere Informationen zu diesen Optionen finden Sie in der *Online-Hilfe zu CMC für Dell PowerEdge FX2/FX2s*.
3. Klicken Sie auf **Anwenden**, um die ausgewählten Optionen anzuwenden.

Einrichten einer Gehäusegruppe

CMC ermöglicht Ihnen die Überwachung mehrerer Gehäuse von einem einzigen Führungsgehäuse aus. Bei aktivierter Gehäusegruppe erzeugt der CMC des Führungsgehäuses eine grafische Darstellung des Status des Führungsgehäuses und von allen in der Gehäusegruppe enthaltenen Gehäusen. Um diese Funktion zu nutzen, benötigen Sie eine Enterprise-Lizenz.

Im Folgenden werden die Gehäusegruppenfunktionen dargestellt:

- Zeigt Abbildungen der Vorder- und Rückseite jedes Gehäuses an, wobei ein Satz für die Führung und ein Satz für jedes Mitglied angezeigt wird.
- Mögliche Beeinträchtigungen des Funktionszustands der Gruppenführung und der Gruppenmitglieder sind jeweils an der Komponente, die entsprechende Symptome aufweist an roten bzw. gelben Overlays und einem X bzw. ! zu erkennen. Details sind unterhalb der Gehäuseabbildung abzulesen, wenn Sie auf die Gehäuseabbildung oder **Details** klicken.
- Es sind Schnellstart-Links zum Öffnen von Webseiten für Mitgliedsgehäuse oder Server verfügbar.
- Für eine Gruppe sind ein Server und eine Eingabe-/Ausgabebestandsliste verfügbar.

- Es ist eine Option verfügbar, um die Eigenschaften eines neuen Mitglieds mit den Eigenschaften des Führungsgehäuses zu synchronisieren, wenn das neue Mitglied zur Gruppe hinzugefügt wird.

Eine Gehäuseguppe kann maximal 19 Mitglieder enthalten. Des Weiteren kann ein Führungs- bzw. ein Mitgliedsgehäuse nur Teil einer Gruppe sein. Wenn diese bereits Teil einer Gruppe sind, können weder Führungs- noch Mitgliedsgehäuse einer weiteren Gruppe beitreten. Gehäuse können aus einer Gruppe gelöscht werden und später zu einer anderen Gruppe hinzugefügt werden.

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

1. Melden Sie sich mit Gehäuseadministratorrechten am Führungsgehäuse an.
2. Klicken Sie auf **Setup** → **Gruppenverwaltung**.
3. Wählen Sie auf der **Gehäusegruppen**seite unter **Rolle Führung**. Es wird ein Feld zum Hinzufügen des Gruppennamens angezeigt.
4. Geben Sie den Gruppennamen im Feld **Gruppenname** ein und klicken Sie anschließend auf **Anwenden.**

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

   Die Gehäusegruppe wechselt beim Erstellen der Gehäusegruppe automatisch zur **Gehäusegruppen**-Seite. Der linke Fensterbereich zeigt die Gruppe über den Gruppennamen an und das Führungsgehäuse sowie die nicht bestückten Mitgliedergehäuse werden im linken Fensterbereich angezeigt.

   ANMERKUNG: Wenn die Gehäusegruppe erstellt wurde, wird das Element **Gehäuse-Übersicht** in der Baumstruktur durch den Namen des Führungsgehäuses ersetzt.

Hinzufügen von Mitgliedern zu einer Gehäusegruppe

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

1. Melden Sie sich mit Gehäuseadministratorrechten am Führungsgehäuse an.
2. Wählen Sie in der Struktur das Führungsgehäuse aus.
3. Klicken Sie auf **Setup** → **Gruppenverwaltung**.
4. Geben Sie unter **Gruppenverwaltung** die IP-Adresse des Mitglieds, oder seinen DNS-Namen im Feld **Hostname/IP-Adresse** an.

   ANMERKUNG: Damit MCM ordnungsgemäß funktioniert, müssen Sie die Standard-HTTPS-Schnittstelle (443) auf allen Mitgliedern der Gruppe und auf dem Führungsgehäuse verwenden.
5. Geben Sie im Feld **Benutzername** einen Benutzernamen mit Gehäuseadministratorrechten für das Mitgliedsgehäuse an.
6. Geben Sie im Feld **Kennwort** das zugehörige Kennwort an.
7. Wählen Sie die Option **Neues Mitglieds mit den Eigenschaften des Führungsgehäuses synchronisieren** aus, um die Eigenschaften des Führungsgehäuses auf das Mitglied zu übertragen. Weitere Informationen über das Hinzufügen von Mitgliedern zu einer Gehäusegruppe finden Sie unter Synchronisieren eines neuen Mitglieds mit den Eigenschaften des Führungsgehäuses.
8. Klicken Sie auf **Apply** (Anwenden).
9. Um maximal acht Mitglieder hinzuzufügen, schließen Sie die Tasks in Schritt 4 bis Schritt 8 ab. Die Gehäusenamen der neuen Mitglieder werden im Dialogfeld **Mitglieder** angezeigt.

ANMERKUNG: Die für ein Mitglied eingegebenen Anmeldeinformationen werden sicher an das Mitgliedsgehäuse weitergegeben, um zwischen dem Mitglieds- und dem Führungsgehäuse eine Vertrauensstellung einzurichten. Die Anmeldeinformationen werden auf keinem der Gehäuse dauerhaft gespeichert und nach dem anfänglichen Einrichten der Vertrauensstellung nie wieder ausgetauscht.

Entfernen eines Mitglieds aus der Führung

Sie können ein Mitglied aus der Gruppe des Führungsgehäuses entfernen. Entfernen eines Mitglieds:

1. Melden Sie sich mit Gehäuseadministratorrechten am Führungsgehäuse an.
2. Wählen Sie im linken Fensterbereich das Führungsgehäuse aus.
3. Klicken Sie auf **Setup** → **Gruppenverwaltung**.
4. Wählen Sie aus der Liste **Mitglieder entfernen** den zu löschenden Mitgliedernamen aus, und klicken Sie anschließend auf **Anwenden**.

   Das Führungsgehäuse benachrichtigt anschließend das Mitglied, bzw. die Mitglieder, sollten mehr als eines ausgewählt worden sein, dass es bzw. sie aus der Gruppe entfernt wurde(n). Der Mitgliedsname wird aus dem Dialogfeld entfernt. Das Mitgliedsgehäuse erhält die Nachricht möglicherweise nicht, wenn der Kontakt zwischen dem Führung und dem Mitglied aufgrund eines Netzwerkproblems verhindert wird. Deaktivieren Sie in diesem Falle das Mitglied des Mitgliedsgehäuses, um das Entfernen abzuschließen.

Auflösen einer Gehäusgruppe

So lösen Sie eine Gehäusegruppe vom Führungsgehäuse aus auf:

1. Melden Sie sich mit Administratorrechten am Führungsgehäuse an.
2. Wählen Sie im linken Fensterbereich das Führungsgehäuse aus.
3. Klicken Sie auf **Setup** → **Gruppenverwaltung**.
4. Wählen Sie auf der Seite **Gehäusegruppen** unter **Rolle**, **Keine** aus und klicken Sie anschließend auf **Anwenden**.

   Das Führungsgehäuse benachrichtigt anschließend alle Mitglieder, dass sie aus der Gruppe entfernt wurden. Das Führungsgehäuse kann einer anderen Gruppe als Führung oder Mitglied zugewiesen werden.

   Wenn der Kontakt zwischen der Führung und dem Mitglied aufgrund eines Netzwerkproblems verhindert wird, erhält das Mitgliedsgehäuse die Nachricht möglicherweise nicht. Deaktivieren Sie in diesem Falle das Mitglied des Mitgliedsgehäuses, um das Entfernen abzuschließen.

Deaktivieren eines einzelnen Mitglieds am Mitgliedsgehäuse

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

1. Melden Sie sich mit Gehäuseadministratorrechten am Mitgliedsgehäuse an.
2. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** → **Setup** → **Gruppenverwaltung**.
3. Wählen Sie **Keine** und klicken Sie anschließend auf **Anwenden**.

Starten der Webseite eines Mitgliedsgehäuses oder Servers

Von der Gruppenseite des Führungsgehäuses aus können Sie auf die Webseite des Mitgliedsgehäuses, die Remote-Konsole des Servers oder die Webseite des iDRAC-Servers zugreifen. Wenn das Mitgliedsgerät die gleichen Anmeldeinformationen hat wie das Führungsgehäuse, können Sie für den Zugriff auf das Mitgliedsgehäuse die gleichen Anmeldeinformationen verwenden.

ANMERKUNG: Die Anmeldung über Single Sign-On oder eine Smart Card werden bei der Verwaltung mehrerer Gehäuse (Multiple Chassis Management) nicht unterstützt. Das Starten von Mitgliedern mit Single Sign-On über das Führungsgehäuse setzt voraus, dass Führungsgehäuse und Mitgliedsgehäuse den gleichen Benutzernamen und das gleiche Kennwort verwenden. Die Verwendung identischer Anmeldeinformationen funktioniert nur bei Active Directory-Benutzern, lokalen Benutzern und LDAP-Benutzern.

So navigieren Sie zu Mitgliedsgeräten:

1. Melden Sie sich am Führungsgehäuse an.
2. Wählen Sie in der Struktur **Gruppe: Name** aus.
3. Wenn ein Mitglieds-CMC das benötigte Ziel ist, dann wählen Sie für das gewünschte Gehäuse **CMC starten** aus.

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

   a. Wählen Sie das Bild des Zielgehäuses aus.
   b. Wählen Sie in der Gehäuseabbildung im Abschnitt **Funktionszustand** 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 **Save** (Speichern).

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

Synchronisieren eines neuen Mitglieds mit den Eigenschaften des Führungsgehäuses

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

1. Melden Sie sich mit Administratorrechten am Führungsgehäuse an.
2. Wählen Sie in der Struktur das Führungsgehäuse aus.
3. Klicken Sie auf **Setup** → **Gruppenverwaltung**.
4. Wählen Sie, während Sie ein neues Mitglied zur Gruppe hinzufügen, auf der Seite **Gehäusegruppe** die Option **Neues Mitglied mit Eigenschaften des Führungsgehäuses synchronisieren** aus.
5. Klicken Sie auf **Anwenden**. Das Mitglied übernimmt die Eigenschaften des Führungsgehäuses.

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

Tabelle 4. Konfigurationsdiensteigenschaften

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

Blade-Bestandsaufnahme für MCM-Gruppe

Eine Gruppe ist ein Führungsgehäuse, das zwischen 0 und 19 Gehäusegruppenmitglieder hat. Auf der Seite **Funktionszustand der Gehäusegruppe** werden alle Mitgliedsgehäuse angezeigt. Hier können Sie den Server-Bestandsaufnahmereport unter Verwendung der Download-Funktion eines Standard-Internet-Browsers als Datei speichern. Der Bericht enthält Daten zu:

- allen Servern, die sich derzeit in der Gehäusegruppe befinden (einschließlich Führungsgehäuse).
- leeren Steckplätzen und Erweiterungssteckplätzen.

Speichern des Berichts zur Serverbestandsaufnahme

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

1. Wählen Sie im linken Fensterbereich die **Gruppe** aus.
2. Klicken Sie auf der Seite **Funktionszustand der Gehäusegruppe** auf **Bericht zur Bestandsliste speichern**. Das Dialogfeld **Datei-Download** wird angezeigt und Sie werden dazu aufgefordert, die Datei zu öffnen oder zu speichern.
3. Klicken Sie auf **Speichern**, und geben Sie den Pfad- und Dateinamen für den Bericht zur Serverbestandsaufnahme ein.

   ANMERKUNG: Das Führungsgehäuse der Gehäusegruppe, sowie die Mitgliedsgehäuse der Gehäusegruppe und die Servermodule im zugeordneten Gehäuse müssen eingeschaltet sein, um einen präzisen Bericht zur Server-Bestandsaufnahme anzuzeigen.

Mehrere CMCs über RACADM konfigurieren

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

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

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

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

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

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

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

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

   ```
   racadm reset
   ```

   Der Unterbefehl `getconfig -f myfile.cfg` fordert die CMC-Konfiguration für den CMC an und erstellt die Datei **myfile.cfg**. Falls erforderlich, können Sie die Datei umbenennen oder an einem anderen Ort speichern.

Sie können den Befehl `getconfig` dazu ausführen, die folgenden Maßnahmen auszuführen:

- Alle Konfigurationseigenschaften in einer Gruppe anzeigen (nach Gruppenname und -index).
- Alle Konfigurationseigenschaften für einen Benutzer nach Benutzernamen anzeigen.

Der Unterbefehl `config` lädt die Informationen auf andere CMCs. Der Server Administrator verwendet den Befehl `config` zur Synchronisierung der Benutzer- und Kennwort-Datenbank.

Parsing-Regeln

- Zeilen, die mit dem Raute-Zeichen (#) beginnen, werden als Anmerkungen behandelt.
  Eine Kommentarzeile muss in Spalte 1 beginnen. Ein „#"-Zeichen in jeder anderen Spalte wird als das Zeichen # behandelt.

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

  Beispiel:

  ```
  # # This is a comment [cfgUserAdmin] cfgUserAdminPageModemInitString= <Modem init # not a comment>
  ```
- Alle Gruppeneinträge müssen in Klammern stehen ([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 zu den Datenbankeigenschaften im *RACADM Command Line Reference Guide for iDRAC and CMC* (RACADM-Befehlszeilen-Referenzhandbuchs für iDRAC und CMC) definiert. Das folgende Beispiel zeigt einen Gruppennamen, ein Objekt und den Eigenschaftswert des Objekts an:

  ```
  [cfgLanNetworking] -{group name} cfgNicIpAddress=143.154.133.121 {object name} {object value}
  ```
- Alle Parameter werden als „Objekt=Wert"-Paare ohne Leerzeichen zwischen „Objekt", „=" und „Wert" angegeben. Leerzeichen nach dem Wert werden ignoriert. Ein Leerzeichen innerhalb einer Wertezeichenkette bleibt unverändert. Jedes Zeichen rechts neben dem = (z. B. ein zweites =, ein #, [,] usw.) wird wie eingegeben übernommen. Bei diesen Zeichen handelt es sich um gültige Modemchat-Skriptzeichen.

  ```
  [cfgLanNetworking] -{group name} cfgNicIpAddress=143.154.133.121 {object value}
  ```
- Der **.cfg**-Parser ignoriert einen Index-Objekt-Eintrag.
  Benutzer können nicht angeben, welcher Index verwendet werden soll. Wenn der Index bereits vorhanden ist, wird dieser entweder verwendet oder ein neuer Eintrag wird im ersten verfügbaren Index für diese Gruppe erstellt.

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

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

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

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

  Benutzer müssen ein indiziertes Objekt manuell mit folgendem Befehl entfernen:

  ```
  racadm config -g <groupname> -o <objectname> -i <index 1-16> ""
  ```

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

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

  ```
  racadm getconfig -g <groupname> -i <index 1-16>
  ```

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

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

- Wenn bei Verwendung von Remote-RACADM zur Erfassung der Konfigurationsgruppen in eine Datei eine Schlüsseleigenschaft innerhalb einer Gruppe nicht festgelegt ist, wird die Konfigurationsgruppe nicht als Teil der Konfigurationsdatei gespeichert. Falls diese Konfigurationsgruppen auf andere CMCs geklont werden müssen, muss die Schlüsseleigenschaft vor Ausführung des Befehls `getconfig -f` festgelegt werden. Oder Sie können die fehlenden Eigenschaften nach Ausführung des Befehls `getconfig -f` manuell in die Konfigurationsdatei eingeben. Dies gilt für alle racadm-indizierten Gruppen.

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

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

CMC-IP-Adresse modifizieren

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

Beispiel:

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

Die Datei wird aktualisiert wie folgt:

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

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

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

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

7

Server konfigurieren

Sie können die folgenden Einstellungen eines Servers konfigurieren:

- Steckplatznamen
- iDRAC-Netzwerkeinstellungen
- DRAC VLAN-Tag-Einstellungen
- Erstes Startgerät
- Server-FlexAddress
- Remote-Dateifreigabe
- BIOS-Einstellungen unter Verwendung der Funktion zum Klonen von Servern

Steckplatznamen konfigurieren

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

- Namen dürfen maximal 15 nicht erweiterte ASCII-Zeichen enthalten (ASCII-Codes 32 bis 126). Außerdem sind Standard- und Sonderzeichen im Namen erlaubt.
- 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, and SERVER-1` gelten als gleiche Namen.
- Steckplatznamen dürfen nicht mit einer der folgenden Zeichenketten beginnen:
  - Switch-
  - Lüfter-
  - PS-
  - DRAC-
  - MC-
  - Gehäuse
  - Housing-Left
  - Housing-Right
  - Housing-Center
- Die Zeichenketten `Server-1` bis `Server-4` können verwendet werden, allerdings nur für den entsprechenden Steckplatz. Z. B. ist `Server-3` ein gültiger Name für Steckplatz 3, aber nicht für Steckplatz 4. `Server-03` ist jedoch ein gültiger Name für einen beliebigen Steckplatz.

  ANMERKUNG: Um einen Steckplatznamen zu ändern, müssen Sie Berechtigungen als **Gehäusekonfiguration-Administrator** besitzen.

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

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

So bearbeiten Sie einen Steckplatznamen über die CMC-Webschnittstelle:

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht → Serverübersicht → Setup → Steckplatznamen**.
2. Bearbeiten Sie auf der Seite **Steckplatznamen** im Feld **Steckplatznamen** den Steckplatzname.
3. Um einen Serverhostnamen als Steckplatznamen zu verwenden, wählen Sie **Hostname verwenden für den Steckplatzname** aus. Dadurch werden die statischen Steckplatznamen mit dem Host-Namen des Servers (oder dem Systemnamen) überschrieben, falls verfügbar. Dazu muss der OMSA-Agent auf dem Server installiert sein. Weitere Informationen zu dem OMSA-Agent finden Sie im *Dell OpenManage Server Administrator User's Guide* (Dell OpenManage Server Administrator-Benutzerhandbuch) unter dell.com/support/manuals.
4. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

Um den Standardsteckplatznamen (STECKPLATZ-01 bis STECKPLATZ-4) basierend auf der Position des Serversteckplatzes) zum Server wiederherzustellen, klicken sie auf **Standardwert wiederherstellen**.

iDRAC Netzwerkeinstellungen konfigurieren

Um diese Funktion zu verwenden, müssen Sie eine Enterprise-Lizenz aufweisen. Sie können die iDRAC-Netzwerkkonfigurationseinstellungen für einen Server konfigurieren. Sie können die QuickDeploy-Einstellungen verwenden, um die Standard- iDRAC-Netzwerkkonfigurationseinstellungen und das Stammkennwort für Server, die zu einem späteren Zeitpunkt installiert werden, zu konfigurieren. Diese Standardeinstellungen sind die Einstellungen der schnellen iDRAC Bereitstellung.

Weitere Informationen zu iDRAC finden Sie im iDRAC-Benutzerhandbuch *iDRAC User's Guide* unter dell.com/support/manuals.

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

Verwenden Sie die QuickDeploy-Einstellungen, um die Netzwerkeinstellungen für neu eingefügte Server zu konfigurieren.

So aktivieren Sie die iDRAC-Einstellungen für die schnelle Bereitschaft und stellen sie ein:

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht → Setup → iDRAC**.
2. Legen sie auf der Seite **iDRAC bereitstellen**, im Abschnitt **QuickDeploy-Einstellungen**, die Einstellungen fest, die in der folgenden Tabelle erwähnt wurden. Weitere Informationen über die Felder finden Sie in der *Online-Hilfe*.

Tabelle 5. QuickDeploy-Einstellungen

Einstellung	Beschreibung
Aktion, wenn der Server eingefügt wird	Wählen Sie eine der folgenden Optionen aus der Liste:

Einstellung	Beschreibung
	• **Keine Maßnahme** – Keine Maßnahme wird ausgeführt, wenn der Server eingefügt wird. • **Nur QuickDeploy** – Wählen Sie diese Option aus, um iDRAC-Netzwerkeinstellungen zu aktivieren, wenn ein neuer Server in das Gehäuse eingesetzt wird. Die angegebenen Einstellungen zur automatischen Bereitstellung werden zum Konfigurieren des neuen iDRAC verwendet. Hierzu zählt auch das root-Benutzerkennwort, wenn **root-Kennwort ändern** ausgewählt ist. • **Nur Serverprofil** – Wählen Sie diese Option aus, um das zugewiesene Serverprofil anzuwenden, wenn ein neuer Server in das Gehäuse eingesetzt wird. • **Quick Deploy und Serverprofil** – Wählen Sie diese Option aus, um zuerst die iDRAC-Netzwerkeinstellungen und dann das zugewiesene Serverprofil anzuwenden, wenn ein neuer Server in das Gehäuse eingesetzt wird.
iDRAC-root-Kennwort nach Einsetzen des Servers einstellen	Wählen Sie die Option zur Änderung des iDRAC-Stammkennworts, um den Wert, der im Feld **iDRAC-Stammkennwort** bereitgestellt ist, anzupassen.
iDRAC-root-Kennwort	Wenn **iDRAC-Stammkennwort bei Servereinfügung einstellen** und **QuickDeploy aktiviert** gewählt wird, wird der Kennwortwert einem Server-iDRAC-Stammbenutzerkennwort zugewiesen, wenn der Server in ein Gehäuse eingefügt wird. Das Kennwort kann 1 bis 20 druckbare Zeichen (einschließlich Leerzeichen) aufweisen.
iDRAC-root-Kennwort bestätigen	Mit dieser Option können Sie das Kennwort noch einmal in das Feld **Kennwort** eingeben.
iDRAC-LAN aktivieren	Aktiviert oder deaktiviert den iDRAC-LAN-Kanal. Diese Option ist standardmäßig gelöscht.
iDRAC IPv4 aktivieren	Aktiviert oder deaktiviert IPv4 auf dem iDRAC. Diese Option ist standardmäßig ausgewählt.
iDRAC-IPMI-über-LAN aktivieren	Aktiviert oder deaktiviert den IPMI-über-LAN-Kanal für jeden iDRAC, der sich in dem Gehäuse befindet. Standardmäßig ist diese Option ausgewählt.
iDRAC IPv4 DHCP aktivieren	Aktiviert oder deaktiviert DHCP für jeden iDRAC, der sich in dem Gehäuse befindet. Wenn diese Option aktiviert ist, sind die Felder **QuickDeploy-IP**, **QuickDeploy-Subnetzmaske** und **QuickDeploy-Gateway** deaktiviert und können

Einstellung	Beschreibung
	nicht geändert werden, da DHCP verwendet wird, um diese Einstellungen automatisch für jeden iDRAC zuzuweisen. Um diese Option auszuwählen, müssen Sie die Option **iDRAC IPv4 aktivieren** auswählen. Die Option „QuickDeploy-IP-Adresse“ ist für die Werte 4 und 2 verfügbar.
Reservierte QuickDeploy-IP-Adresse	Wählen Sie die Nummer der statischen IPv4-Adressen aus, die für iDRACs im Gehäuse reserviert sind. Die IPv4-Adressen ab **Start-iDRAC IPv4-Adresse (Steckplatz 1)** werden als reserviert betrachtet, und es wird angenommen, dass sie nicht anderswo im selben Netzwerk verwendet werden. Die Funktion „Quick Deploy“ funktioniert nicht für Server, die in Steckplätze eingefügt sind, für die es keine reservierte statische IPv4-Adresse gibt.
iDRAC-IPv4-Adresse starten (Steckplatz 1)	Gibt die statische IP-Adresse des iDRAC des Servers in Steckplatz 1 des Gehäuses an. Die IP-Adresse jedes nachfolgenden iDRAC wird für jeden Steckplatz jeweils um 1 erhöht, angefangen mit der statischen IP-Adresse von Steckplatz 1. Falls die IP-Adresse plus die Steckplatznummer größer als die Subnetzmaske ist, wird eine Fehlermeldung angezeigt. **ANMERKUNG:** Die Subnetzmaske und das Gateway werden nicht wie die IP-Adresse erhöht. Wenn zum Beispiel die ursprüngliche IP-Adresse `192.168.0.250` und die Subnetzmaske `255.255.0.0` lautet, dann lautet die IP-Adresse für QuickDeploy für Steckplatz 4c: `192.168.0.265`. Wenn die Subnetzmaske `255.255.255.0` wäre, würde die Fehlermeldung `QuickDeploy IP address range is not fully within QuickDeploy Subnet` angezeigt, wenn Sie entweder auf **QuickDeploy-Einstellungen speichern** oder auf **Automatische Bestückung mit QuickDeploy-Einstellungen** klicken.
iDRAC IPv4-Netzmaske	Gibt die QuickDeploy-Subnetzmaske an, die allen neu eingefügten Servern zugewiesen ist.
iDRAC IPv4-Gateway	Gibt den schnellen Bereitstellungs-Standard-Gateway an, der allen DRACs, die sich im Gehäuse befinden, zugewiesen ist.

Einstellung	Beschreibung
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 für die schnelle Bereitstellung wird nur ausgeführt, wenn sie aktiviert ist und ein Server im Gehäuse eingesetzt ist.

   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.

QuickDeploy-IP-Adresszuweisungen für Server

Die folgenden Tabellen zeigen, wie IP-Adressen mit QuickDeploy basierend auf den im FX2-/FX2s-Gehäuse vorhandenen Schlitten den Servern zugewiesen werden:

- Zwei Schlitten mit voller Breite im Gehäuse:

START IP + 0 (SLOT1)
START IP + 2 (SLOT3)

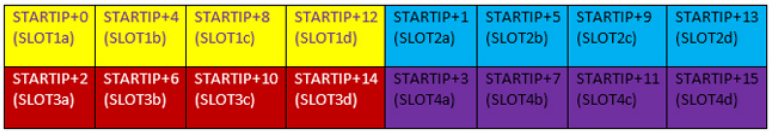
- Vier Schlitten mit halber Breite im Gehäuse:

  ANMERKUNG: Damit QuickDeploy die IP-Adressen dem unteren Schlitten zuweist, muss das Feld **Reservierte QuickDeploy-IP-Adressen** für den unteren Schlitten-iDRAC auf `4` gesetzt sein.

START IP + 0 (SLOT1)	START IP + 1(SLOT2)
START IP + 2 (SLOT3)	START IP + 3 (SLOT4)

- Acht Schlitten mit Viertelbreite im Gehäuse:

- Vier FM120x4-Schlitten im Gehäuse:



- Die obere Reihe enthält nur Schlitten mit Viertelbreite und die untere Reihe enthält nur Schlitten mit halber Breite:

- Die obere Reihe enthält nur Schlitten mit voller Breite und die untere Reihe enthält nur Schlitten mit halber Breite:

- Die obere Reihe enthält Schlitten mit voller Breite und die untere Reihe enthält nur Schlitten mit Viertelbreite:

iDRAC-Netzwerkeinstellungen für individuelle Server-iDRAC ändern

Mithilfe dieser Funktion können Sie die iDRAC-Netzwerkkonfigurationseinstellungen für jeden installierten Server konfigurieren. Die anfänglichen Werte, die für jedes Feld angezeigt werden, sind die aktuellen vom iDRAC gelesenen Werte. Um diese Funktion zu verwenden, müssen Sie eine Enterprise-Lizenz aufweisen.

So ändern Sie die iDRAC-Netzwerkeinstellungen:

1. Klicken Sie im linken Fensterbereich auf **Server-Übersicht**, und klicken Sie dann auf **Setup**. Auf der Seite **iDRAC bereitstellen** führt der Abschnitt **iDRAC-Netzwerkeinstellungen** die iDRAC IPv4- und IPv6-Netzwerkkonfigurationseinstellungen aller installierten Server auf.
2. Ändern Sie die iDRAC-Netzwerkeinstellungen entsprechend den Serveranforderungen.

   ANMERKUNG: Sie müssen die Option **LAN aktivieren** auswählen, um die IPv4- oder IPv6-Einstellungen festzulegen. Weitere Informationen über die Felder finden Sie in der *Online-Hilfe zu CMC für Dell PowerEdge FX2/FX2s*.
3. Um die Einstellung auf dem iDRAC bereitzustellen, klicken Sie auf **iDRAC-Netzwerkeinstellungen anwenden**. Alle Änderungen an den **Einstellungen zur schnellen Bereitstellung** werden ebenfalls gespeichert.

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

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

iDRAC-Netzwerkeinstellungen über RACADM ändern

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

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

Weitere Informationen über die Standardwerte und Bereiche der einzelnen Eigenschaften finden Sie im *Dell Integrated Dell Remote Access Controller (iDRAC) RACADM Command Line Reference Guide* (iDRAC-RACADM-Befehlszeilen-Referenzhandbuch) und im *Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge FX2/FX2s) unter dell.com/support/manuals.

Konfigurieren der iDRAC-VLAN-Einstellungen

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

iDRAC-VLAN-Tag-Einstellungen mittels der Webschnittstelle konfigurieren

So konfigurieren Sie VLAN für Server

1. Gehen Sie zu einer der folgenden Seiten:
   - Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** → **Netzwerk** → **VLAN**.
   - Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht** → **Server-Übersicht** und dann auf **Setup** → **VLAN**.
2. Aktivieren Sie auf der Seite **VLAN-Tag-Einstellungen** im Abschnitt **iDRAC** VLAN für die Server, legen Sie die Priorität fest und geben Sie die ID ein. Weitere Informationen über die Felder finden Sie in der Online-Hilfe zu *CMC für Dell PowerEdge FX2/FX2s*.
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 1–4.

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

Gültige Werte für <*VLAN priority*> sind 0 – 7. Die Standardeinstellung ist 0.

Beispiel:

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

Beispiel:

- Um ein Server-VLAN zu entfernen, deaktivieren Sie die VLAN-Funktionen des angegebenen Servernetzwerks:

  ```
  racadm setniccfg -m server-<n> -v
  ```

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

  Beispiel:

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

Erstes Startlaufwerk einstellen

Sie können das CMC-Startlaufwerk für jeden Server festlegen. Dieses muss nicht unbedingt das erste Startlaufwerk für den Server sein und könnte nicht unbedingt ein Gerät in diesem Server repräsentieren; stattdessen stellt es ein Gerät dar, das vom CMC als erstes Startlaufwerk für diesem Server verwendet wird. Dieses Gerät kann als erstes Startgerät oder als Gerät für einen einmaligen Start festgelegt werden. So können Sie ein spezielles Image starten, um beispielsweise Diagnoseaufgaben durchzuführen oder ein Betriebssystem neu zu installieren.

Sie können das erste Startgerät nur für den nächsten Start oder für alle nachfolgenden Neustarts einstellen. Sie können auch das erste Startgerät für den Server einstellen. Beim nächsten und allen nachfolgenden Neustarts startet das System von dem ausgewählten Gerät, das in der BIOS-Startreihenfolge an erster Stelle bleibt, bis eine erneute Änderung entweder von der CMC-Webschnittstelle oder von der BIOS-Startreihenfolge aus erfolgt.

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

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

Sie können die folgenden Geräte als Erststartgeräte einstellen. Wenn Sie jedoch ein Gerät als standardmäßiges erstes Startgerät festlegen möchten, wählen Sie **Standard** aus.

Um die Firmware-Version des Servers außer Kraft zu setzen, falls die Firmware-Version, die auf dem Server ausgeführt wird, mit der im Erststartgerät identisch ist, wählen Sie **Keine** aus.

Sie können die folgenden Geräte für ersten Start einstellen.

Tabelle 6. Startlaufwerke

Startlaufwerk	Beschreibung
PXE	Start von einem PXE (Preboot Execution Environment)-Protokoll über die Netzwerkschnittstellenkarte.
Festplattenlaufwerk	Der Start erfolgt unter Verwendung eines Festplattenlaufwerks.
Lokale CD/DVD	Start von einem CD- oder DVD-Laufwerk auf dem Server.
BIOS-Setup	Der Start erfolgt während des BIOS-Setup.
Virtuelle Diskette	Der Start erfolgt über ein virtuelles Diskettenlaufwerk.
Virtuelle CD/DVD	Der Start erfolgt über ein virtuelles CD- oder DVD-Laufwerk.
Lokale SD-Karte	Der Start erfolgt über die lokale SD-Karte (Secure Digital).
Remote-Dateifreigabe	Der Start erfolgt über die Remote-Dateifreigabe.
BIOS Boot Manager	Der Start erfolgt unter Verwendung des BIOS-Boot-Managers.
Lifecycle-Controller	Der Start erfolgt unter Verwendung des Lifecycle Controllers.
Lokale Diskette	Start von einer Diskette im lokalen Diskettenlaufwerk.

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

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

So stellen Sie das erste Startlaufwerk für mehrere Server ein:

1. Klicken Sie im linken Fensterbereich auf **Server-Übersicht** → **Setup** → **Erstes Startgerät**. Eine Serverliste wird angezeigt.
2. In der Spalte **Erstes Startgerät** im Drop-Down-Menü des entsprechenden Servers, wählen Sie das zu verwendende Startlaufwerk für einen Server aus.
3. Wenn der Server bei jedem Hochfahren von dem ausgewählten Gerät starten soll, deaktivieren Sie die Option **Einmalig starten** für den betreffenden Server. Wenn der Server beim nächsten Hochfahren einmalig von dem ausgewählten Laufwerk starten soll, aktivieren Sie die Option **Einmalig starten** für den betreffenden Server.
4. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

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

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

So stellen Sie das erste Startlaufwerk für einzelne Server ein:

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

Erstes Startgerät über RACADM festlegen

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

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

Weitere Informationen über diese Objekte finden Sie im *Chassis Management Controller for PowerEdge FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge FX2s) unter dell.com/support/manuals.

Konfigurieren des Netzwerk-Uplinks des Schlittens

Sie können den Netzwerk-Uplink des Schlittens nur auf PowerEdge FM120x4-Schlitten mit internem Netzwerkschalter konfigurieren.

Wechseln Sie zum Konfigurieren des Netzwerk-Uplinks des Schlittens zu **Gehäuse-Übersicht** → **Server-Übersicht** → **Setup** → **Schlitten-Netzwerk-Uplink.**

Wählen Sie einen der folgenden Werte für die Eigenschaft der Schlitten-Netzwerk-Uplink-Konfiguration aus:

- Standard (aggregiert): Uplink-Konfiguration, bei der sich alle vier EAM-Uplink-Schnittstellen in einer einzigen Trunk-Gruppe befinden und alle LOMs dieser Gruppe zugeordnet sind. Diese Option ist die Standardeinstellung.
- Netzwerk-Adapter-Isolierung (erweiterte Sicherheit): Uplink-Konfiguration ähnlich der Standardeinstellung, allerdings ist die Routing-Funktion zwischen lokalen Knoten nicht zulässig.
- Isolierte Netzwerke: Uplink-Konfiguration, bei der jeder LOM1 des Knotens EAM A1 und jeder LOM2 des Knotens EAM A2 zugeordnet ist.

Bereitstellen der Remote-Dateifreigabe

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

Zur Ausführung eines Remote-Dateifreigabevorgangs (verbinden, trennen oder bereitstellen) müssen Sie über die Berechtigung als **Gehäusekonfiguration-Administrator** oder **Server Administrator** verfügen. Um diese Funktion zu verwenden, müssen Sie eine Enterprise-Lizenz aufweisen.

So konfigurieren Sie die Remote-Dateifreigabe:

1. Klicken Sie im linken Fensterbereich auf **Server-Übersicht → Setup → Remote-Dateifreigabe**.
2. Geben Sie auf der Seite **Remote-Dateifreigabe bereitstellen** die entsprechenden Daten in die Felder ein. Weitere Informationen über die Feldbeschreibungen finden Sie in der Online-Hilfe zu *CMC für Dell PowerEdge FX2/FX2s*.
3. Klicken Sie auf **Verbinden**, um eine Verbindung zu einer Remote-Dateifreigabe herzustellen. Geben Sie für die Verbindung den Pfad, den Benutzernamen und das Kennwort an. War der Vorgang erfolgreich, erhalten Sie Zugriff auf den Datenträger.

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

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

   ANMERKUNG: Bevor Sie auf die Schalfläche Bereitstellen klicken, stellen Sie sicher, dass alle Arbeitsdateien gespeichert wurden, da diese Maßnahme den Server neu startet.

   Wenn Sie auf **Bereitstellen** klicken, werden die folgendenTasks ausgeführt:
   - Die Remote-Dateifreigabe ist verbunden.
   - Die Datei ist als erstes Startgerät für die Server ausgewählt.
   - Der Server wird neu gestartet.
   - Strom wird an den Server geliefert, falls der Server ausgeschaltet ist.

Server-FlexAddress konfigurieren

Weitere Informationen über die Konfiguration von FlexAddress für Server finden Sie unter Konfigurieren von FlexAddress für Chassis-Level Fabric und Steckplätze unter Verwendung der CMC Web Interface. Um diese Funktion zu verwenden, müssen Sie eine Enterprise-Lizenz aufweisen.

Konfiguration von Profileinstellungen durch das Replizieren von Serverkonfigurationen

Die Funktion zur Replikation von Serverkonfigurationen ermöglicht es Ihnen, alle Profileinstellungen von einem bestimmten Server auf einen oder mehrere andere Server anzuwenden. Profileinstellungen, die repliziert werden können, sind diejenigen Einstellungen, die geändert werden können und zur Replikation auf andere Server gedacht sind. Die folgenden drei Profilgruppen für Server werden angezeigt und können repliziert werden:

- BIOS – Diese Gruppe umfasst ausschließlich die BIOS-Einstellungen eines Servers.
- BIOS und Start – Diese Gruppe umfasst die BIOS- und Starteinstellungen eines Servers.
- Alle Einstellungen – Diese Version umfasst alle Einstellungen eines Servers und der Komponenten auf diesem Server. Diese Profile werden generiert von:
  - Servern der 12. Generation mit iDRAC7 1.57.57 oder später und Lifecycle Controller 2 ab Version 1.1
  - Servern der 13. Generation mit iDRAC8 2.05.05 mit Lifecycle Controller ab 2.00.00.00

Die Funktion zum Klonen von Servern unterstützt iDRAC7- und iDRAC8-Server. Es werden auch frühere Generationen von RAC-Servern aufgelistet, sie sind auf der Hauptseite jedoch ausgegraut und für diese Funktion nicht aktiviert.

So verwenden Sie die Funktion zum Replizieren von Serverkonfigurationen:

- iDRAC muss in der jeweils erforderlichen Mindestversion vorliegen. iDRAC7-Server benötigen mindestens Version 1.57.57 und iDRAC8-Server die Version 2.05.05.
- Der Server muss eingeschaltet sein.

Sie können Folgendes durchführen:

- Anzeigen der Profil-Einstellungen eines Servers oder eines gespeicherten Profils.
- Speichern eines Profils eines Servers.
- Anwenden eines Profils auf andere Server.
- Importieren von gespeicherten Profilen von einer Management Station oder Remote-Dateifreigabe.
- Bearbeiten des Profilnamens und der Beschreibung.
- Exportieren von gespeicherten Profilen in eine Management Station oder Remote-Dateifreigabe.
- Löschen von gespeicherten Profilen.
- Bereitstellen ausgewählter Profile für Zielgeräte unter Verwendung der Option **Quick Deploy**.
- Anzeigen der Protokollaktivität für letzte Server-Profil-Tasks.

Zugreifen auf die Profilseite

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

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

Verwalten von gespeicherten Profilen

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

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

- Um ein Profil zu bearbeiten, klicken Sie auf **Bearbeiten**.
- Um BIOS-Einstellungen anzuzeigen, klicken Sie auf **Anzeigen**.
- Um ein Profil zu entfernen, klicken Sie auf **Löschen**. Weitere Informationen zu den Feldbeschreibungen finden Sie in der Online-Hilfe zu *CMC für Dell PowerEdge FX2/FX2s*.

Hinzufügen oder Speichern eines Profils

Bevor Sie die Eigenschaften eines Servers kopieren, übernehmen Sie die Eigenschaften zunächst in ein gespeichertes Profil. Erstellen Sie ein gespeichertes Profil, und versehen Sie dieses mit einem Namen und (optional) mit einer Beschreibung. Sie können auf dem nicht flüchtigen, erweiterten CMC-Speichermedium bis zu 16 gespeicherte Profile vorhalten.

ANMERKUNG: Wenn eine Remote-Freigabe verfügbar ist, können Sie maximal 100 Profile unter Verwendung des erweiterten CMC-Speichers und der Remote-Freigabe speichern. Weitere Informationen finden Sie unter Konfigurieren der Netzwerkfreigabe unter Verwendung der CMC Web-Schnittstelle

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

So fügen Sie ein Profil hinzu:

1. Wechseln Sie zur Seite **Serverprofile**. Klicken Sie im Abschnitt **Serverprofile** auf **Profile anwenden und speichern**.
2. Wählen Sie den Server aus, dessen Einstellungen Sie zum Generieren des Profils verwenden möchten, und klicken Sie dann auf **Profil speichern**. Der Abschnitt **Profil speichern** wird angezeigt.
3. Wählen Sie **Erweiterter Speicher** oder **Netzwerkfreigabe** als Speicherort für das Profil aus.

   ANMERKUNG: Die Option „Netzwerkfreigabe" ist nur dann aktiviert und es werden nur dann Details im Abschnitt „Gespeicherte Profile" angezeigt, wenn die Netzwerkfreigabe bereitgestellt wurde und zugreifbar ist. Wenn die Netzwerkfreigabe nicht angeschlossen ist, konfigurieren Sie die Netzwerkfreigabe für das Gehäuse. Klicken Sie dazu im Abschnitt „Gespeicherte Profile" auf „Bearbeiten". Weitere Informationen finden Sie unter Konfigurieren der Netzwerkfreigabe unter Verwendung der CMC Web-Schnittstelle.
4. Geben Sie in die Felder **Profilname** und **Beschreibung** den Profilnamen und (optional) eine Beschreibung ein, und klicken Sie auf **Profil speichern**.

   ANMERKUNG:
   Beim Speichern eines Serverprofils schließt die Liste der Zeichen, die für den Profilnamen nicht unterstützt werden, die Zeichen Raute (#), Komma (,) und Fragezeichen (?) ein.

   Der erweiterte Standard-ASCII-Zeichensatz wird unterstützt. Die folgenden Sonderzeichen werden nicht unterstützt:

   ), ", ., *, >, <, \, /, :, und |

   Der CMC kommuniziert mit dem LC, um die verfügbaren Serverprofileinstellungen abzurufen und diese als ein Profil mit Namen zu speichern.

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

   ANMERKUNG: Der Prozess zur Übernahme der Einstellungen läuft im Hintergrund. Es kann eine gewisse Zeit dauern, bis das neue Profil angezeigt wird. Wird das neue Profil nicht angezeigt, überprüfen Sie das Profilprotokoll auf Fehler.

Profil anwenden

Das Klonen von Servern ist nur dann möglich, wenn auf dem nicht flüchtigen CMC-Speichermedium oder auf der Remote-Freigabe Serverprofile als gespeicherte Profile verfügbar sind. Um den Klonvorgang zu starten, können Sie ein gespeichertes Profil auf einen oder mehrere Server anwenden.

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

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

So wenden Sie ein Profil auf einem oder mehreren Servern an:

1. Wählen Sie auf der Seite **Serverprofile** im Abschnitt **Profile speichern und anwenden** die Server aus, auf die Sie das ausgewählte Profil anwenden möchten.

   Das Drop-Down-Menü **Profil auswählen** wird aktiviert.

   ANMERKUNG: Das Drop-Down-Menü **Profil auswählen** zeigt die verfügbaren Profile nach Typ sortiert an, einschließlich derjenigen, die sich im Repository und auf der SD-Karte befinden.
2. Wählen Sie aus dem Drop-Down-Menü **Profil auswählen** das Profil aus, das Sie anwenden möchten.

   Die Option **Profil anwenden** wird aktiviert.
3. Klicken Sie auf **Profil anwenden**.

   Eine Warnmeldung erscheint mit dem Hinweis, dass das Anwenden eines neuen Serverprofils die aktuellen Einstellungen überschreibt und die ausgewählten Server neu startet. Sie werden dazu aufgefordert, dies zu bestätigen, falls Sie mit dem Vorgang fortfahren möchten.

   ANMERKUNG: Um den Klonvorgang für Server durchführen zu können, muss die Option CSIOR (Collect System Inventory on Restart) für die Server aktiviert sein. Ist die Option CSIOR deaktiviert, erscheint eine Warnmeldung mit dem Hinweis, dass CSIOR für die Server nicht aktiviert ist. Um den Blade-Klonvorgang abschließen zu können, stellen Sie sicher, dass die Option CSIOR auf den Servern aktiviert ist.
4. Klicken Sie auf **OK**, um das Profil auf den ausgewählten Server anzuwenden.

   Das ausgewählte Profil wird auf den oder die Server angewendet, wobei bei Bedarf ein sofortiger Neustart des bzw. der Server erfolgen kann. Weitere Informationen finden Sie in der Online-Hilfe zu *CMC für Dell PowerEdge FX2/FX2s*.

Importieren eines Profils

Sie können ein Serverprofil, das auf einer Management Station gespeichert wurde, in den CMC importieren.

So importieren Sie ein gespeichertes Profil in den CMC:

1. Klicken Sie auf der Seite **Serverprofile**, im Abschnitt **Gespeicherte Profile** auf **Profil importieren**.

   Der Abschnitt **Serverprofil importieren** wird angezeigt.
2. Klicken Sie auf **Durchsuchen**, um auf das Profil an dem erforderlichen Standort zuzugreifen und klicken Sie dann auf **Profil importieren**.

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

Exportieren eines Profils

Sie können ein gespeichertes Profil in einen festgelegten Pfad auf einer Management Station exportieren.

Zum Exportieren eines gespeicherten Profils:

1. Rufen Sie die Seite **Serverprofile** auf. Wählen Sie im Abschnitt **Gespeicherte Profile** das erforderliche Profil aus, und klicken Sie dann auf **Kopie des Profils exportieren**.

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

   ANMERKUNG: Wenn sich das Quellprofil auf der SD-Karte befindet, wird eine Warnmeldung angezeigt, die darauf hinweist, dass die Beschreibung beim Exportieren des Profils verloren geht. Klicken Sie auf **OK**, um den Exportvorgang für das Profil fortzusetzen.

   Eine Meldung wird angezeigt, in der Sie aufgefordert werden, das Ziel für die Datei auszuwählen:

   - Wählen Sie „Lokal“ oder „Netzwerkfreigabe“, wenn sich die Quelldatei auf einer SD-Karte befindet.

     ANMERKUNG: Die Option **Netzwerkfreigabe** ist nur dann aktiviert und es werden nur dann Details im Abschnitt **Gespeicherte Profile** angezeigt, wenn die Netzwerkfreigabe bereitgestellt wurde und zugreifbar ist. Wenn die Netzwerkfreigabe nicht angeschlossen ist, konfigurieren Sie die Netzwerkfreigabe für das Gehäuse. Klicken Sie dazu im Abschnitt **Gespeicherte Profile** auf **Bearbeiten**. Weitere Informationen finden Sie unter Konfigurieren der Netzwerkfreigabe unter Verwendung der CMC Web-Schnittstelle.
   - Wählen Sie „Lokal“ oder „SD-Karte“, wenn sich die Quelldatei auf der Netzwerkfreigabe befindet.

   Weitere Informationen finden Sie in der *Online-Hilfe*.
3. Wählen Sie **Lokal**, **Erweiterter Speicher** oder **Netzwerkfreigabe** als Zielspeicherort aus, je nachdem, welche Optionen angezeigt werden.
   - Wenn Sie **Lokal** auswählen, wird ein Dialogfeld angezeigt, mit dem Sie das Profil in einem lokalen Verzeichnis speichern können.
   - Wenn Sie die Option **Erweiterter Speicher** oder **Netzwerkfreigabe** auswählen, wird das Dialogfeld **Profil speichern** angezeigt.
4. Klicken Sie auf **Profil speichern**, um das Profil am ausgewählten Speicherort zu speichern.

Bearbeiten des Profils

Sie können den Namen und die Beschreibung eines Serverprofils, das auf dem nicht flüchtigen CMC-Datenträger (SD-Karte) gespeichert ist, bearbeiten.

So bearbeiten Sie ein gespeichertes Profil:

1. Wechseln Sie zur Seite **Serverprofile**. Wählen Sie im Abschnitt **Gespeicherte Profile** das benötigte 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 Serverprofils wie erforderlich, und klicken Sie dann auf **Profil bearbeiten**.

   ANMERKUNG: Sie können die Beschreibung nur für Profile bearbeiten, die auf SD-Karten gespeichert sind.

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

Anzeigen der Profileinstellungen

Um die Profileinstellungen eines ausgewählten Servers anzuzeigen, rufen Sie die Seite **Serverprofile** auf. Klicken Sie im Abschnitt **Serverprofile** in der Spalte **Serverprofil** des erforderlichen Servers auf **Anzeigen**. Die Seite **Einstellungen anzeigen** wird angezeigt.

Weitere Informationen über die angezeigten Einstellungen finden Sie in der *Online-Hilfe*.

ANMERKUNG: Mit der CMC Serverkonfigurations-Replikation werden die korrekten Einstellungen für einen bestimmten Server nur dann abgerufen und angezeigt, wenn die CSIOR-Option (**Systembestandsaufnahme bei Neustart durchführen**) aktiviert ist.

Zum Aktivieren von CSIOR wählen Sie nach dem Neustart des Servers aus dem **F2**-Setup **iDRAC-Einstellungen → Lifecycle Controller** aus, aktivieren Sie **CSIOR**, und speichern Sie die Änderungen.

So aktivieren Sie CSIOR auf:

1. Servern der 12. Generation – Wählen Sie nach dem Neustart des Servers aus dem F2-Setup **iDRAC-Einstellungen → Lifecycle Controller** aus, aktivieren Sie **CSIOR**, und speichern Sie die Änderungen.
2. Servern der 13. Generation – Drücken Sie nach dem Serverneustart bei entsprechender Aufforderung die Taste F10, um Lifecycle Controller aufzurufen. Wechseln Sie zur Seite **Hardware-Bestandsaufnahme**, indem Sie **Hardware-Konfiguration → Hardware-Bestandsaufnahme** auswählen. Klicken Sie auf der Seite **Hardware-Bestandsaufnahme** auf **Systembestandsaufnahme bei Neustart durchführen**.

Gespeicherte Profileinstellungen anzeigen

Zum Anzeigen der Profileinstellungen der gespeicherten Serverprofile wechseln Sie zur Seite **Serverprofile**. Klicken Sie im Abschnitt **Serverprofile** in der Spalte **Profil anzeigen** für den erforderlichen Server auf **Anzeigen**. Die Seite **Einstellungen anzeigen** wird angezeigt. Weitere Informationen zu den angezeigten Einstellungen finden Sie in der *Online-Hilfe zu CMC für Dell PowerEdge FX2/FX2s*.

Profilprotokoll anzeigen

Um sich das Profilprotokoll anzeigen zu lassen, navigieren Sie auf der Seite **Serverprofile** zum Abschnitt **Neu erstelltes Profilprotokoll**. Dieser Abschnitt listet die 10 letzten Profilprotokolleinträge direkt von Serverklonvorgängen auf. In jedem Profileintrag sind der Schweregrad, Zeit und Datum der Übermittlung des Serverreplikationsvorgangs der Konfiguration und die Beschreibung der Replikationsprotokollmeldung aufgeführt. Die Protokolleinträge sind auch im RAC-Protokoll verfügbar. Um sich weitere verfügbare Einträge anzeigen zu lassen, klicken Sie auf **Gehe zu Profilprotokoll**. Die Seite **Profilprotokoll** wird angezeigt. Weitere Informationen finden Sie in der *Online-Hilfe*.

Fertigstellungsstatus und Fehlerbehebung

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

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht → Serverübersicht → Setup → Profile**.
2. Notieren Sie sich auf der Seite **Serverprofile** die Job-ID (JID) des übermittelten Jobs aus dem Abschnitt **Protokoll mit neuesten Profilen**.
3. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht → Fehlerbehebung → Lifecycle-Controller-Aufträge**. Suchen Sie die gleiche JID in der Tabelle **Aufträge.** Weitere Informationen über die Ausführung von Lifecycle-Controller-Aufträgen finden Sie in Lifecycle-Controller-Auftragsvorgänge.

Quick Deploy von Profilen

Mit der Quick Deploy-Funktion können Sie gespeicherte Profile einem Serversteckplatz zuweisen. Jeder Server, der die Replikation der Serverkonfiguration unterstützt und in einen Steckplatz eingesetzt wird, wird mit dem zugewiesenen Profil dieses Steckplatzes konfiguriert. Sie können die Quick Deploy-Aktion nur ausführen, wenn die Option **Aktion, wenn der Server eingefügt wird** auf der Seite „iDRAC bereitstellen" auf **Serverprofil** oder auf **Quick Deploy und Serverprofil** gesetzt ist. Wenn Sie diese Option auswählen, kann das zugewiesene Serverprofil angewandt werden, wenn ein neuer Server in das Gehäuse eingesetzt wird. Um zur Seite **iDRAC bereitstellen** zu gelangen, wählen Sie **Server-Übersicht → Setup → iDRAC** aus. Profile, die bereitgestellt werden können, befinden sich auf der SD-Karte.

ANMERKUNG: Zur Einstellung der Profile für Quick Deploy müssen Sie über die Rechte eines **Gehäuseadministrators** verfügen.

Zuweisen von Serverprofilen zu Steckplätzen

Über die Seite **Serverprofile** können Sie Serverprofile Steckplätzen zuweisen. So weisen Sie ein Profil einem Gehäusesteckplatz zu:

1. Klicken Sie auf der Seite **Serverprofile** auf den Abschnitt **Profile für QuickDeploy**.
   Die aktuellen Zuweisungen der Profile zu den Steckplätzen, die in der Auswahlliste in der Spalte **Profil zuweisen** aufgeführt sind, werden angezeigt.

   ANMERKUNG: Sie können die Quick Deploy-Aktion nur ausführen, wenn die Option **Aktion, wenn der Server eingefügt wird** auf der Seite **iDRAC bereitstellen** auf **Serverprofil** oder auf **Quick Deploy dann Serverprofil** gesetzt ist. Wenn Sie diese Option auswählen, kann das zugewiesene Serverprofil angewandt werden, wenn ein neuer Server in das Gehäuse eingesetzt wird.
2. Wählen Sie aus dem Drop-Down-Menü das Profil aus, das dem erforderlichen Steckplatz zugewiesen werden soll. Sie können ein ausgewähltes Profil auf mehrere Steckplätze anwenden.
3. Klicken Sie auf **Profil zuweisen**.
   Die Profile werden auf die ausgewählten Steckplätze angewendet.

ANMERKUNG: Wenn der FM120x4-Schlitten eingesetzt wird, wird das gespeicherte, dem Serversteckplatz zugewiesene Profil auf alle vier Server angewandt.

ANMERKUNG:

- Ein Steckplatz, dem kein Serverprofil zugewiesen wurde, wird durch den Zusatz „Kein Profil ausgewählt" gekennzeichnet, der in der Auswahlliste erscheint.
- Um die Zuweisung eines Profils zu einem oder mehreren Steckplätzen aufzuheben, wählen Sie den oder die Steckplätze aus, und klicken Sie dann auf **Zuweisung entfernen**. Es wird eine Warnung mit dem Hinweis angezeigt, dass durch das Entfernen des Profils aus einem oder mehreren Steckplätzen die Einstellungen in der XML-Konfiguration für das Profil aus jedem Server entfernt werden, der sich in einem der betroffenen Steckplätze befindet, wenn die Funktion **Profile über QuickDeploy bereitstellen** aktiviert ist. Klicken Sie auf **OK**, um die Profilzuweisungen zu entfernen.
- Um alle Profilzuweisungen eines Steckplatzes zu entfernen, wählen Sie im Drop-Down-Menü **Kein Profil ausgewählt.**

ANMERKUNG: Wenn ein Profil mit der Funktion **Quick Deploy-Profil** für einen Server bereitgestellt wird, werden die Fortschritte und Ergebnisse der Anwendung im Profilprotokoll festgehalten.

ANMERKUNG:

Die Option **Netzwerkfreigabe** ist nur dann aktiviert und es werden nur dann Details im Abschnitt **Gespeicherte Profile** angezeigt, wenn die Netzwerkfreigabe bereitgestellt wurde und zugreifbar ist. Wenn die Netzwerkfreigabe nicht angeschlossen ist, konfigurieren Sie die Netzwerkfreigabe für das Gehäuse. Klicken Sie dazu im Abschnitt „Gespeicherte Profile" auf **Bearbeiten**. Weitere Informationen finden Sie unter Konfigurieren der Netzwerkfreigabe unter Verwendung der CMC Web-Schnittstelle.

iDRAC mit einfacher Anmeldung starten

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

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

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

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

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

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

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

iDRAC von der Seite Serverstatus starten

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

1. Erweitern Sie im linken Fensterbereich **Server-Übersicht**. Es werden alle vier Server in der erweiterten Liste **Server-Übersicht** angezeigt.
2. Klicken Sie auf den Server, für den Sie die iDRAC-Webschnittstelle starten möchten.
3. Klicken Sie auf der Seite **Serverstatus** auf **iDRAC-GUI starten**.

   Die iDRAC-Web-Schnittstelle wird angezeigt. Informationen zu den Feldbeschreibungen finden Sie in der *Online-Hilfe zu CMC für Dell PowerEdge FX2/FX2s*.

iDRAC über die Seite Serverstatus starten

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

1. Klicken Sie im linken Fensterbereich auf **Server-Übersicht**.
2. Klicken Sie auf der Seite **Servers-Status** auf **iDRAC starten** für den Server, für den Sie die iDRAC-Webschnittstelle starten wollen.

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

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

1. Erweitern Sie im linken Fensterbereich **Serverübersicht**. Alle vier Server werden in der erweiterten Liste der Server angezeigt.
2. Klicken Sie auf den Server, für den Sie die Remote-Konsole starten möchten.
3. Klicken sie auf der Seite **Serverstatus** auf **Remote-Konsole starten**.

ANMERKUNG: Die Schaltfläche oder Verknüpfung **Remote-Konsole starten** ist nur aktiviert, wenn auf dem Server eine Enterprise-Lizenz installiert ist.

8

CMC für das Versenden von Warnungen konfigurieren

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

So konfigurieren Sie CMC zum Versenden von Warnungen:

1. Aktivieren Sie die Option **Gehäuseereigniswarnungen**.
2. Optional können Sie die Warnungen auf der Basis der Kategorie oder des Schweregrads filtern.
3. Konfigurieren Sie die Einstellungen für die E-Mail-Warnung oder die SNMP-Trap-Einstellungen.
4. Aktivieren Sie die Gehäuseereigniswarnungen, um eine E-Mail-Warnung oder SNMP-Traps an konfigurierte Ziele zu senden.

Warnungen aktivieren und deaktivieren

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

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

Warnungen über die CMC-Web-Schnittstelle aktivieren oder deaktivieren

So aktivieren oder deaktivieren Sie die Generierung von Warnungen:

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht → Warnungen**.
2. Wählen Sie auf der Seite **Gehäuseereignisse**, im Abschnitt **Aktivierung der Gehäusewarnung,** die Option **Gehäuseereigniswarnungen aktivieren** aus, um die Aktivierung der Warnung zu aktivieren oder das Löschen der Warnung zu aktivieren.
3. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

Warnungen über RACADM aktivieren oder deaktivieren

Um die Generierung von Warnungen zu aktivieren oder zu deaktivieren, verwenden Sie das RACADM-Objekt **cfgIpmiLanAlertEnable**. Weitere Informationen finden Sie im *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Dell Chassis Management Controller für PowerEdge FX2/FX2s).

Warnungen filtern

Sie können Warnungen auf der Basis der Kategorie und des Schweregrads filtern.

Konfiguration von Warnungszielen

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

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

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

SNMP-Trap-Warnungsziele konfigurieren

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

SNMP-Trap-Warnungsziele über die CMC-Webschnittstelle konfigurieren

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

1. Wählen Sie in der Systemstruktur die **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-teilige Punkt-IPv4-Format, die 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.

     ANMERKUNG: Der CMC verwendet die standardmäßige SNMP-Community-Zeichenkette öffentlich. Um eine bessere Sicherheit zu gewährleisten, wird empfohlen, dass die standardmäßige Community-Zeichenkette geändert und ein Wert eingestellt 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 die Filtermaske bereits ausgewählt haben.
2. Aktivieren Sie die Erstellung von Warnungen:

   ```
   racadm config -g cfgAlerting -o cfgAlertingEnable 1
   ```
3. 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.
4. Bestimmen Sie eine Ziel-IP-Adresse, um Trap-Warnungen zu erhalten:

   ```
   racadm config -g cfgTraps -o cfgTrapsAlertDestIPAddr <IP address> -i <index>
   ```

   wobei `<IP address>` ein gültiges Ziel ist und `<index>` der Indexwert, der in Schritt 4 angegeben wurde.
5. 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.

   ANMERKUNG: Der CMC verwendet die standardmäßige SNMP-Community-Zeichenkette öffentlich. Um eine bessere Sicherheit zu gewährleisten, wird empfohlen, dass die standardmäßige Community-Zeichenkette geändert und ein Wert eingestellt wird.

   Sie können bis zu vier Ziele für den Empfang von Trap-Warnungen konfigurieren. Um weitere Ziele hinzuzufügen, wiederholen Sie die Schritte 2 bis 5.

   ANMERKUNG: Die Befehle in Schritten 2 bis 5 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 getconfig -g cfgTraps -i <index>`. Wenn der Index konfiguriert ist, werden für die Objekte **cfgTrapsAlertDestIPAddr** und **cfgTrapsCommunityName** Werte angezeigt.
6. 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 Sie als Mail-Server Microsoft Exchange Server 2007 verwenden, stellen Sie sicher, dass der CMC-Domänenname so konfiguriert ist, dass der Mail-Server die E-Mail-Warnungen vom CMC empfangen kann.

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 CMC-Webschnittstelle 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, die die Warnungen empfangen sollen. 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 unter **Test-E-Mail** auf **Senden**, um eine Test-E-Mail an ein angegebenes E-Mail-Warnungsziel zu senden.

E-Mail-Warnungseinstellungen mit RACADM konfigurieren

Um eine Test-E-Mail an ein E-Mail-Warnungsziel unter Verwendung von RACADM zu senden, gehen Sie wie folgt vor:

1. Öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC und melden Sie sich an.
2. Aktivieren Sie die Erstellung von Warnungen:
   ```
   racadm config -g cfgAlerting -o cfgAlertingEnable 1
   ```
3. So aktivieren Sie die Erstellung von E-Mail-Warnungen:
   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable 1 -i <index>
   ```
   wobei `<index>` ein Wert von 1-4 ist. Die Indexnummer wird vom CMC verwendet, um bis zu vier konfigurierbare Ziel-E-Mail-Adressen zu unterscheiden.
4. So geben Sie die Ziel-E-Mail-Adresse zum Erhalt von E-Mail-Warnungen an:
   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertAddress <email address> -i
   <index>
   ```

wobei `<email address>` eine gültige E-Mail-Adresse ist und `<index>` der Indexwert, den Sie in Schritt 4 angegeben haben.

5. Geben Sie den Namen des Teilnehmers an, der E-Mail-Warnungen empfangen soll:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEmailName <email name> -i
   <index>
   ```

   wobei `<email name>` (<E-Mail-Name>) der Name der Person oder Gruppe ist, die E-Mail-Warnungen empfängt, und `<index>` der Indexwert ist, den Sie in Schritt 4 und 5 angegeben haben. Der E-Mail-Name darf bis zu 32 alphanumerische Zeichen, Bindestriche, Unterstriche und Punkte enthalten. Leerstellen sind nicht gültig.

6. 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 2-5.

   ANMERKUNG: Die Befehle in den Schritten 2 bis 5 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: `xracadm getconfig -g cfgEmailAlert — I <Index>`. Wenn der Index konfiguriert ist, werden für die Objekte **cfgEmailAlertAddress** und **cfgEmailAlertEmailName** Werte angezeigt.

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

9

Benutzerkonten und Berechtigungen konfigurieren

Sie können Benutzerkonten mit spezifischen Berechtigungen (rollenbasierte Autorität) einrichten, um Ihr System mit CMC zu verwalten und die Systemsicherheit zu gewährleisten. Standardmäßig ist CMC mit einem Standard-root-Konto konfiguriert. Als Administrator können Sie Benutzerkonten einrichten, damit andere Benutzer auf CMC zugreifen können.

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

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

Typen von Benutzern

Es gibt zwei Typen von Benutzern:

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

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

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

Tabelle 7. Benutzertypen

Berechtigung	Beschreibung
CMC-Anmeldung, Benutzer	Der Benutzer kann sich am CMC anmelden und alle CMC-Daten anzeigen. Er kann aber keine Daten hinzufügen oder ändern oder Befehle ausführen.

Berechtigung	Beschreibung
	Es ist möglich, dass ein Benutzer andere Berechtigungen ohne CMC-Anmeldebenutzerberechtigung besitzt. Diese Funktion ist sinnvoll, wenn sich ein Benutzer vorübergehend nicht anmelden darf. Wenn die CMC-Anmeldeberechtigung dieses Benutzers wiederhergestellt ist, erhält der Benutzer alle zuvor gewährten Berechtigungen zurück.
Gehäusekonfiguration-Administrator	Benutzer können Daten hinzufügen oder ändern, die: • das Gehäuse identifizieren, z. B. den Gehäusenamen und die Gehäuseposition. • 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 Hochfahren und Herunterfahren sowie Strom ein- und ausschalten.
Benutzerkonfigurations-Administrator	Ein Benutzer kann: • Einen neuen Benutzer hinzufügen. • Das Kennwort eines Benutzers ändern. • Die Berechtigungen eines Benutzers ändern. • Die Anmeldungsberechtigung eines Benutzers unter Beibehaltung des Namens des Benutzers und anderer Berechtigungen in der Datenbank aktivieren oder deaktivieren.
Administrator zum Löschen von Protokollen	Ein Benutzer kann das Hardwareprotokoll und das CMC-Protokoll löschen.
Gehäusesteuerungs-Administrator (Strombefehle)	CMC-Benutzer mit einer Berechtigung als Administrator für die **Gehäusestromversorgung** können alle Vorgänge im Zusammenhang mit der Stromversorgung ausführen. Sie können

Berechtigung	Beschreibung
	Gehäusestromvorgänge steuern, einschließlich Strom einschalten, Strom ausschalten und Strom aus- und einschalten. ANMERKUNG: Für die Konfiguration von Stromversorgungseinstellungen ist eine Berechtigung als **Administrator für die Gehäusekonfiguration** erforderlich.
Server Administrator	Die Server-Administrator-Berechtigung ist eine Pauschalberechtigung, die einem CMC-Benutzer alle Rechte zum Ausführen beliebiger Vorgänge auf beliebigen, im Gehäuse vorhandenen Servern gewährt. Wenn eine **Server Administrator**-Berechtigung eine Maßnahme zum Ausführen auf einem Server ausgibt, sendet die CMC-Firmware den Befehl zum Zielserver, ohne die Berechtigungen des Benutzers auf dem Server zu überprüfen. Mit anderen Worten: die **Server Administrator**-Berechtigung setzt alle fehlenden Administratorrechte auf dem Server außer Kraft. 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

Berechtigung	Beschreibung
	Benutzer konfigurieren: • iDRAC-Stammkennwort einstellen • iDRAC-Reset Serversteuerung-Administrator: • Einschalten • Ausschalten • Aus- und einschalten • Ordentliches Herunterfahren • Serverneustart
Warnungstests für Benutzer	Benutzer kann Testwarnungsmeldungen senden.
Administrator für Debug-Befehle	Benutzer kann Systemdiagnosebefehle ausführen.
Struktur A-Administrator	Benutzer kann die Struktur A-EAM festlegen und konfigurieren.

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 8. CMC-Gruppenberechtigungen

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

Benutzergruppe	Gewährte Berechtigungen
	• Benutzerkonfigurations-Administrator • Administrator zum Löschen von Protokollen • Gehäusesteuerungs-Administrator (Strombefehle) • Server Administrator • Warnungstests für Benutzer • Administrator für Debug-Befehle • Struktur A-Administrator
Keine	Keine zugewiesenen Berechtigungen

Tabelle 9. Vergleich der Berechtigungen zwischen CMC-Administrator, Hauptbenutzer und Gastbenutzer

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

Ändern der Einstellungen für Stammbenutzer-Administratorkonto

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

So ändern Sie das Standardkennwort für das Stammkonto:

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht**, und dann auf **Benutzerauthentifizierung**.
2. Klicken Sie auf der Seite **Benutzer,** in der Spalte **Benutzer-ID** auf **1**.

ANMERKUNG: Die Benutzer-ID **1** ist das Stammbenutzerkonto, das standardmäßig mit CMC geliefert wird. Dies kann nicht geändert werden.

3. Wählen Sie auf der Seite **Benutzerkonfiguration** die Option **Kennwort ändern** aus.
4. Geben Sie das neue Kennwort in das Feld **Kennwort** ein und geben Sie dann dasselbe Kennwort in **Kennwort bestätigen** ein.
5. Klicken Sie auf **Anwenden**. Das Kennwort für Benutzer-ID**1** wurde geändert.

Lokale Benutzer konfigurieren

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

Lokale Benutzer über die CMC-Webschnittstelle konfigurieren

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

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

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht**, und dann auf **Benutzerauthentifizierung**.
2. Klicken Sie auf der Seite **Lokale Benutzer** in der Spalte **Benutzer-ID** auf eine Benutzer-ID-Nummer. Die Seite **Benutzerkonfiguration** wird angezeigt.

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

Lokale Benutzer über RACADM konfigurieren

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

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

Wenn Sie einen neuen CMC konfigurieren möchten oder den Befehl racadm `racresetcfg` verwendet haben, ist das einzige aktuelle Benutzerkonto das Standard-root-Konto. Der Unterbefehl `racresetcfg` setzt alle Konfigurationsparameter auf die Standardeinstellungen zurück. Alle vorherigen Änderungen gehen verloren.

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

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

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

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

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

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

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

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

Das Zeichen „#“ in den Befehlsobjekten gibt an, dass es ein Nur-Lesen-Objekt ist. Ebenso: Wenn der Befehl `racadm config -f racadm.cfg` zur Angabe einer beliebigen Anzahl von zu schreibenden Gruppen/Objekten verwendet wird, kann der Index nicht angegeben werden. Ein neuer Benutzer wird zum ersten verfügbaren Index hinzugefügt. Dieses Verhalten bietet größere Flexibilität bei der Konfiguration eines zweiten CMC mit denselben Einstellungen wie der Haupt-CMC.

Konfigurieren von Active Directory-Benutzern

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

ANMERKUNG: Auf den folgenden Betriebssystemen können Sie die Benutzer der CMC-Benutzer unter Verwendung des Active Directory erkennen.

- Microsoft Windows 2000
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008

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

Unterstützte Active Directory-Authentifizierungsmechanismen

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

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

Übersicht des Standardschema-Active Directory

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

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

Tabelle 10. Standardeinstellungsberechtigungen der Rollengruppe

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

Rollengruppe	Standard-Berechtigungsebene	Gewährte Berechtigungen	Bitmaske
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.

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 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.

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.

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.

Konfiguration des allgemeinen LDAP-Verzeichnisdienstes mit der CMC-Webschnittstelle

So konfigurieren Sie den allgemeinen LDAP-Verzeichnisdienst:

ANMERKUNG: Sie müssen die Berechtigung als **Gehäusekonfiguration-Administrator** besitzen.

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht → Benutzerauthentifizierung → Verzeichnisdienst**.
2. Wahlen Sie **Allgemeines LDAP** aus.
   Die Einstellungen, die für das Standardschema konfiguriert werden sollen, werden auf derselben Seite angezeigt.
3. Geben Sie Folgendes an:

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

   - Allgemeine Einstellungen
   - Für LDAP zu verwendenden Server:
     - Statischer Server – Geben Sie den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse und die LDAP-Schnittstellennummer ein.
     - DNS-Server – Geben Sie den DNS-Server an, um eine Liste von LDAP-Servern durch Suchen nach deren SRV-Einträgen im DNS abzurufen.
       Die folgende DNS-Abfrage wird für SRV-Einträge durchgeführt:
       `_[Service Name]._tcp.[Search Domain]`
       wobei < *Search Domain* > die root-Ebenendomäne ist, die für die Abfrage verwendet wird, und < *Service Name* > der Dienstname, der für die Abfrage verwendet wird.
       Beispiel:
       `_ldap._tcp.dell.com`
       wobei `ldap` der Dienstname ist und `dell.com` die Suchdomäne.
4. Klicken Sie auf **Anwenden**, um die Einstellungen zu speichern.

ANMERKUNG: Sie müssen die Einstellungen anwenden, bevor Sie fortfahren. Wenn Sie die Einstellungen nicht anwenden, verlieren Sie die eingegebenen Einstellungen, wenn Sie zur nächsten Seite wechseln.

5. Klicken Sie im Abschnitt **Gruppeneinstellungen** auf eine **Rollengruppe**.
6. Geben Sie auf der Seite **LDAP-Rollengruppe konfigurieren** den Gruppendomänenname und die Rollengruppen-Berechtigungen ein.
7. Klicken Sie auf **Anwenden**, um die Einstellungen der Rollengruppe zu speichern, Klicken Sie auf **Zurück zur Seite Konfiguration**, und dann wählen Sie **Generisches LDAP**.
8. Wenn Sie **Überprüfung des Zertifikats aktiviert** gewählt haben, geben Sie das CA-Zertifikat im Abschnitt **Zertifikate verwalten** an, um das LDAP-Serverzertifikat während des Secure Socket Layer (SSL)-Handshake zu validieren. Klicken Sie auf **Hochladen**. Das Zertifikat wird auf den CMC heraufgeladen und weitere Details werden angezeigt.
9. Klicken Sie auf **Anwenden**.

   Der allgemeine LDAP-Verzeichnisdienst ist damit konfiguriert.

Konfiguration des allgemeinen LDAP-Verzeichnisdienstes mittels RACADM

Um den LDAP-Verzeichnisdienst zu konfigurieren, verwenden Sie die Objekte in `cfgLdap` und `cfgLdapRoleGroup` RACADM-Gruppen.

Es gibt viele Möglichkeiten zur Konfiguration von LDAP-Anmeldungen. Meistens können einige Optionen in der Standardeinstellung verwendet werden.

ANMERKUNG: Wir empfehlen dringend die Verwendung des Befehls racadm `testfeature -f LDAP`, um die LDAP-Einstellungen bei Ersteinrichtungen zu testen. Diese Funktion unterstützt sowohl IPv4 wie auch IPv6.

Die erforderlichen Eigenschaftenänderungen sind zum Beispiel die Aktivierung von LDAP-Anmeldungen, die Einstellung des Server-FQDN oder der -IP und die Konfiguration der Base-DN des LDAP-Servers.

- `$ racadm config -g cfgLDAP -o cfgLDAPEnable 1`
- `$ racadm config -g cfgLDAP -o cfgLDAPServer 192.168.0.1`
- `$ racadm config -g cfgLDAP -o cfgLDAPBaseDN dc= company,dc=com`

Der CMC kann so konfiguriert werden, dass er optional einen DNS-Server auf SRV-Einträge abfragt. Falls die Eigenschaft `cfgLDAPSRVLookupEnable` aktiviert ist, wird die Eigenschaft `cfgLDAPServer` ignoriert. Die folgende Abfrage wird für die Suche nach SRV-Einträgen im DNS verwendet:

`_ldap._tcp.domainname.com`

`ldap` in der obigen Abfrage ist die Eigenschaft `cfgLDAPSRVLookupServiceName`.

`cfgLDAPSRVLookupDomainName` ist als **domainname.com** konfiguriert.

Weitere Informationen über die RACADM-Befehle finden Sie im Referenzhandbuch *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Dell Chassis Management Controller für PowerEdge FX2/FX2s) unter **dell.com/support/manuals**.

10

CMC für die einfache Anmeldung oder Smart Card-Anmeldung konfigurieren

Dieser Abschnitt enthält Informationen zum Konfigurieren von CMC für die Smart Card-Anmeldung sowie für die einfache Anmeldung (Single Sign-On, SSO) von Active Directory-Benutzern.

SSO verwendet Kerberos als Authentifizierungsmethode, die Benutzern, die sich mit automatischer oder einfacher Anmeldung angemeldet haben, nachfolgende Anwendungen wie Exchange ermöglicht. Bei der einfachen Anmeldung verwendet der CMC die Anmeldeinformationen des Clientsystems, die im Betriebssystem zwischengespeichert werden, nachdem Sie sich mit einem gültigen Active Directory-Konto angemeldet haben.

Die Zweifaktor-Authentifizierung bietet eine höhere Sicherheitsstufe, indem Benutzer aufgefordert werden, ein Kennwort oder eine PIN sowie eine physische Karte mit einem privaten Schlüssel oder einem digitalen Zertifikat bereitzustellen. Kerberos verwendet diesen Zweifaktor-Authentifizierungsmechanismus und ermöglicht es Systemen, ihre Authentizität zu beweisen.

ANMERKUNG: Die Auswahl einer Anmeldemethode legt keine Richtlinienattribute hinsichtlich anderer Anmeldeschnittstellen, z. B. SSH, fest. Sie müssen auch sonstige Richtlinienattribute für andere Anmeldeschnittstellen festlegen. Falls Sie alle anderen Anmeldeschnittstellen deaktivieren möchten, navigieren Sie zur Seite **Dienste** und deaktivieren Sie alle (oder bestimmte) Anmeldeschnittstellen.

Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7 und Windows Server 2008 können Kerberos als Authentifizierungsmethode für SSO- und Smart Card-Anmeldung verwenden.

Weitere Informationen über Kerberos finden Sie auf der Microsoft-Website.

Systemanforderungen

Zur Verwendung der Kerberos-Authentifizierung muss Ihr Netzwerk Folgendes enthalten:

- DNS-Server
- Microsoft Active Directory-Server

ANMERKUNG: Falls Sie Active Directory unter Microsoft Windows 2003 verwenden, müssen Sie sicherstellen, dass die neuesten Service-Packs auf dem Clientsystem installiert sind. Falls Sie Active Directory unter Microsoft Windows 2008 verwenden, müssen Sie sicherstellen, dass SP1 sowie die folgenden Hotfixes installiert sind:

Windows6.0-KB951191-x86.msu für das Dienstprogramm KTPASS. Ohne dieses Patch erzeugt das Dienstprogramm fehlerhafte Keytab-Dateien.

Windows6.0-KB957072-x86.msu für Verwendung von GSS_API- und SSL-Transaktionen während einer LDAP-Bindung.

- Kerberos-Schlüsselverteilungscenter – KDC (mit der Active Directory-Serversoftware)
- DHCP-Server (empfohlen).
- Die DNS-Server-Reverse-Zone muss einen Eintrag für den Active Directory-Server und den CMC enthalten.

Client-Systeme

- Für reine Smart Card-Anmeldung muss das Clientsystem die verteilbare Komponente von Microsoft Visual C++ 2005 enthalten. Weitere Informationen finden Sie unter **www.microsoft.com/downloads/details.aspx?FamilyID= 32BC1BEEA3F9-4C13-9C99-220B62A191EE&displaylang=en**
- Für einfache Anmeldung oder Smart Card-Anmeldung muss das Clientsystem ein Teil der Active Directory-Domäne und des Kerberos-Bereichs sein.

CMC

- Jeder CMC muss ein Active Directory-Konto haben.
- Der CMC muss ein Teil der Active Directory-Domäne und des Kerberos-Bereichs sein.

Vorbedingungen für die einfache Anmeldung oder Smart Card-Anmeldung

Die Voraussetzungen für die Konfiguration der SSO- oder Smart Card-Anmeldungen lauten wie folgt:

- Einrichtung des Kerberos-Bereichs und Key Distribution Centers (KDC) für Active Directory (ksetup).
- Gewährleisten Sie eine robuste NTP- und DNS-Infrastruktur zur Vermeidung von Problemen mit Clock-Drift und Reverse-Lookup.
- Konfiguration des CMC mit der Standardschema-Rollengruppe mit autorisierten Mitgliedern.
- Erstellen Sie für Smart Card „Active Directory-Benutzer" für jeden CMC und konfigurieren Sie Kerberos-DES-Verschlüsselung, jedoch nicht Vorauthentifizierung.
- Browser für SSO oder Smart Card-Anmeldung konfigurieren
- Registrieren Sie die CMC-Benutzer mit Ktpass beim Schlüsselverteilungscenter (dies erzeugt auch einen Schlüssel zum Hochladen auf den CMC).

Kerberos Keytab-Datei generieren

Zur Unterstützung der SSO- und Smart Card-Anmeldungs-Authentifizierung unterstützt CMC das Windows-Kerberos-Netzwerk. Mit dem ktpass-Hilfsprogramm werden die Bindungen des Dienstprinzipalnamens (SPN =Service Principal Name) zu einem Benutzerkonto erstellt und die Vertrauensinformationen in eine MIT-artige Kerberos-Keytab-Datei exportiert. Weitere Informationen zum Dienstprogramm ktpass finden Sie auf der Microsoft-Website.

Sie müssen vor dem Erstellen einer Keytab-Datei ein Active Directory-Benutzerkonto zur Benutzung mit der Option **-mapuser** des Befehls ktpass einrichten. Außerdem müssen Sie denselben Namen verwenden wie den CMC-DNS-Namen, zu dem Sie die erstellte Keytab-Datei hochladen.

So generieren Sie eine Keytab-Datei mithilfe des ktpass-Tools:

1. Führen Sie das Dienstprogramm *ktpass* auf dem Domänen-Controller (Active Directory-Server) aus, auf dem Sie den CMC einem Benutzerkonto in Active Directory zuordnen möchten.
2. Verwenden Sie den folgenden `ktpass`-Befehl, um die Kerberos-Keytab-Datei zu erstellen:

   ```
   C:\>ktpass -princ HTTP/cmcname.domain_name.com@REALM_NAME.COM - mapuser
   dracname -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -pass * -out c:
   \krbkeytab
   ```

   ANMERKUNG: Der `cmcname.domainname.com` muss gemäß RFC in Kleinbuchstaben und der `@REALM_NAME` muss in Großbuchstaben angegeben werden. Darüber hinaus unterstützt der CMC den DES-CBC-MD5-Typ von Kryptographie für Kerberos-Authentifizierung.

   Dieses Verfahren erstellt eine Keytab-Datei, die Sie zum CMC hochladen müssen.

   ANMERKUNG: Das Keytab enthält einen Verschlüsselungsschlüssel und muss an einem sicheren Ort aufbewahrt werden. Weitere Informationen zum Dienstprogramm *ktpass* finden Sie auf der **Microsoft**-Website.

Konfigurieren des CMC für das Active Directory-Schema

Weitere Informationen über die Konfiguration des CMC für das Active Directory-Standardschema finden Sie unter Active Directory-Standardschema konfigurieren.

Weitere Informationen über die Konfiguration des CMC für Erweitertes Schema für Active Directory finden Sie unter Übersicht des Active Directory mit erweitertem Schema.

Browser für SSO-Anmeldung konfigurieren

Einfache Anmeldung (SSO) wird von Internet Explorer Version 6.0 und höher und Firefox Version 3.0 und höher unterstützt.

ANMERKUNG: Die folgenden Anweisungen gelten nur, wenn der CMC die einfache Anmeldung mit Kerberos-Authentifizierung verwendet.

Internet Explorer

So bearbeiten Sie die Ausnahmeliste in Internet Explorer:

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

Mozilla Firefox

So bearbeiten Sie die Ausnahmeliste in Mozilla Firefox Version 19.0:

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

Browser für Smart Card-Anmeldung konfigurieren

Internet Explorer – Stellen Sie sicher, dass der Webbrowser zum Herunterladen von Active-X-Plug-Ins konfiguriert ist.

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`

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 Optionen finden Sie in der *Online-Hilfe zu CMC für Dell PowerEdge FX2/FX2s*.

1. Führen Sie beim Konfigurieren von Active Directory zum Einstellen des Benutzerkontos die folgenden zusätzlichen Schritte aus:
   - Laden Sie die Keytab-Datei hoch.
   - Um SSO (Single Sign-On) zu aktivieren, wählen Sie die Option **Einfache Anmeldung aktivieren** aus.
   - Um Smart Card-Anmeldung zu aktivieren, wählen Sie die Option **Smart-Card-Anmeldung aktivieren** aus.

ANMERKUNG: Wenn diese zwei Schritte ausgewählt werden, bleiben alle bandexternen Schnittstellen, einschließlich Secure Shell (SSH), Telnet, Seriell und Remote-RACADM für diese Option unverändert.

2. Klicken Sie auf **Apply** (Anwenden).

   Die Einstellungen werden gespeichert.

   Sie können das Active Directory mit Kerberos-Authentifizierung testen, indem Sie den RACADM-Befehl verwenden:

   ```
   testfeature -f adkrb -u <user>@<domain>
   ```

   wobei *<user>* für ein gültiges Active Directory-Benutzerkonto steht.

   Wenn der Befehl erfolgreich durchgeführt wird, bedeutet das, dass der CMC Kerberos-Anmeldeinformationen beschaffen und auf das Active Directory-Konto des Benutzers zugreifen kann. Wenn der Befehl nicht erfolgreich ist, müssen Sie den Fehler beseitigen und den Befehl erneut ausführen. Weitere Informationen finden Sie im Referenzhandbuch *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Dell Chassis Management Controller für PowerEdge FX2/FX2s) unter dell.com/support/manuals.

Keytab-Datei hochladen

Die Kerberos-Keytab-Datei liefert die CMC-Benutzername-Kennwort-Anmeldeinformationen für das KDC (Kerberos Data Center), das wiederum Zugriff auf das Active Directory ermöglicht. Jeder CMC im Kerberos-Bereich muss beim Active Directory registriert sein und eine eindeutige Keytab-Datei aufweisen.

Sie können einen Kerberos-Keytab hochladen, der auf dem zugeordneten Active Directory-Server erstellt wurde. Sie können die Kerberos-Keytab-Datei vom Active Directory-Server aus erzeugen, indem Sie das Dienstprogramm **ktpass.exe** ausführen. Diese Keytab-Datei stellt eine Vertrauensstellung zwischen dem Active Directory-Server und dem CMC her.

So laden Sie die Keytab-Datei hoch:

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht → Benutzerauthentifizierung → Verzeichnisdienst**.
2. Wählen Sie **Microsoft Active Directory (Standardschema)** aus.
3. Klicken Sie im Abschnitt **Kerberos-Keytab** auf **Durchsuchen**, wählen Sie eine Keytab-Datei aus und klicken Sie auf **Hochladen**.

   Wenn der Vorgang beendet ist, wird eine Meldung angezeigt, die anzeigt ob die Keytab-Datei erfolgreich hochgeladen wurde.

Konfiguration der CMC SSO- oder Smart Card-Anmeldung für Active Directory-Benutzer über RACADM

Neben den im Rahmen der Konfiguration von Active Directory ausgeführten Schritten führen Sie zum Aktivieren von SSO den folgenden Befehl aus:

```
racadm -g cfgActiveDirectory -o cfgADSSOEnable 1
```

Neben den im Rahmen der Konfiguration von Active Directory ausgeführten Schritten verwenden Sie zum Aktivieren der Smart Card-Anmeldung die folgenden Objekte:

- `cfgSmartCardLogonEnable`

- cfgSmartCardCRLEnable

11

CMC zur Verwendung von Befehlszeilenkonsolen konfigurieren

Dieser Abschnitt enthält Informationen über die Funktionen der CMC-Befehlszeilenkonsole (bzw. die serielle/Telnet-/Secure Shell-Konsole) und erklärt, wie das System eingerichtet wird, sodass Systemverwaltungsmaßnahmen über die Konsole ausgeführt werden können. Weitere Informationen zur Verwendung der RACADM-Befehle im CMC über die Befehlszeilenkonsole finden Sie unter *Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge FX2/FX2s).

Funktionen der CMC-Befehlszeilenkonsolenverbindung

Der CMC unterstützt die folgenden Funktionen von seriellen, Telnet- und SSH-Konsolen:

- Eine serielle Client-Verbindung und bis zu vier gleichzeitige Telnet-Client-Verbindungen.
- Bis zu vier gleichzeitige Secure Shell- (SSH-) Client-Verbindungen.
- RACADM-Befehlsunterstützung.
- Integrierter connect-Befehl zum Anschließen an die serielle Konsole von Servern und E/A-Modulen; auch als `racadm connect`-Befehl verfügbar.
- Befehlszeilenbearbeitung und Verlauf
- Steuerung der Sitzungszeitüberschreitung auf allen Konsolen-Schnittstellen.

CMC-Befehlszeilenoberflächenbefehle

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

Tabelle 11. CMC-Befehlszeilenbefehle

Befehl	Beschreibung
`racadm`	RACADM-Befehle beginnen mit dem Stichwort `racadm`, gefolgt von einem Unterbefehl. Weitere Informationen finden Sie im Referenzhandbuch *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Dell Chassis Management Controller für PowerEdge FX2/FX2s).
`connect`	Stellt eine Verbindung zur seriellen Konsole eines Servers oder eines E/A-Moduls her. Weitere Informationen finden Sie unter Herstellen einer

Befehl	Beschreibung
	Verbindung mit Servern oder E/A-Modulen mit dem connect-Befehl. ANMERKUNG: Sie können auch den RACADM Befehl `connect` verwenden.
`exit`, `logout` und `quit`	Alle diese Befehle führen die gleiche Maßnahme aus. Sie beenden die aktuelle Sitzung und kehren zu einer Anmeldungsbefehlszeilenschnittstelle zurück.

Telnet-Konsole mit dem CMC verwenden

Mit CMC können Sie bis zu vier Telnet-Sitzungen gleichzeitig durchführen.

Wenn Ihre Management Station Microsoft Windows XP oder Microsoft Windows Server 2003 ausführt, kann ein Problem mit den Zeichen in einer CMC-Telnet-Sitzung auftreten. Dieses Problem kann sich als eingefrorene Anmeldung äußern, bei der die Eingabetaste nicht reagiert und keine Kennwort-Eingabeaufforderung eingeblendet wird.

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

SSH mit dem CMC verwenden

SSH ist eine Befehlszeilensitzung, die über die gleichen Merkmale wie eine Telnet-Sitzung verfügt, allerdings mit Sitzungsverhandlung und Verschlüsselung für verbesserte Sicherheit. CMC unterstützt SSH Version 2 mit Kennwortauthentifizierung. SSH ist beim CMC standardmäßig aktiviert.

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

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

ANMERKUNG: `OpenSSH` muss unter Windows von einem VT100 oder ANSI-Terminalemulator ausgeführt werden. Sie können `OpenSSH` auch mithilfe von **Putty.exe** ausführen. Das Ausführen von `OpenSSH` an der Windows-Eingabeaufforderung ergibt keine vollständige Funktionalität (d. h. einige Tasten reagieren nicht und es werden keine Grafiken angezeigt). Führen Sie auf Servern, die Linux ausführen SSH-Client-Dienste aus, um über beliebige Shells eine Verbindung zum CMC herzustellen.

Vier gleichzeitige SSH-Sitzungen werden jeweils zu einem gegebenen Zeitpunkt unterstützt. Die Sitzungszeitüberschreitung wird durch die Eigenschaft `cfgSsnMgtSshIdleTimeout` gesteuert. Weitere Informationen über die RACADM-Befehle finden Sie im Referenzhandbuch *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Dell Chassis Management Controller für PowerEdge FX2/FX2s), das unter dell.com/support/Manuals verfügbar ist.

Der CMC unterstützt auch die Authentifizierung mit öffentlichem Schlüssel (PKA) über SSH. Diese Authentifizierungsmethode verbessert die SSH-Scripting-Automatisierung, da es überflüssig ist, die Benutzer-ID/das Kennwort einzubetten bzw. anzufordern.

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

Unterstützte SSH-Verschlüsselungssysteme

Um mit CMC über das SSH-Protokoll zu kommunizieren, unterstützt es verschiedene Verschlüsselungsschemas, die in der folgenden Tabelle aufgelistet sind.

Tabelle 12. Verschlüsselungsschemata

Schematyp	Schema
Asymmetrische Verschlüsselung	Diffie-Hellman DSA/DSS 512-1024 (zufallsbestimmt) Bits gemäß NIST-Spezifikation
Symmetrische Verschlüsselung	• AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
Meldungsintegrität	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
Authentifizierung	Kennwort

Authentifizierung mit öffentlichem Schlüssel über SSH

Sie können bis zu 6 öffentliche Schlüssel konfigurieren, die mit dem Dienst-Benutzernamen über eine SSH-Schnittstelle verwendet werden können. Verwenden Sie vor dem Hinzufügen oder Löschen öffentlicher Schlüssel unbedingt den `view`befehl, um zu sehen, welche Schlüssel bereits eingerichtet sind, sodass kein Schlüssel versehentlich überschrieben oder gelöscht wird. Der Dienst-Benutzername ist ein spezielles Benutzerkonto, das für den Zugriff auf den CMC über SSH verwendet werden kann. Wenn der PKA über SSH eingerichtet ist und korrekt verwendet wird, dann müssen Sie den Benutzernamen und das Kennwort nicht mehr eingeben, wenn Sie sich beim CMC anmelden. Es kann sehr hilfreich sein, automatisierte Skripts einzurichten, um verschiedene Funktionen auszuführen.

ANMERKUNG: Es gibt keine GUI-Unterstützung zur Verwaltung dieser Funktionen; Sie können nur RACADM verwenden.

Beim Hinzufügen neuer öffentlicher Schlüssel müssen Sie sicherstellen, dass bestehende Schlüssel nicht bereits den Index belegen, zu dem der neue Schlüssel hinzugefügt werden soll. Der CMC führt vor dem Hinzufügen eines Schlüssels keine Prüfungen durch, um sicherzustellen, dass keine vorherigen Schlüssel

gelöscht werden. Sobald ein neuer Schlüssel hinzugefügt wurde, tritt er automatisch in Kraft, solange die SSH-Schnittstelle aktiviert ist.

Beachten Sie bei Verwendung des Anmerkungsabschnitts des öffentlichen Schlüssels, dass nur die ersten 16 Zeichen vom CMC verwendet werden. Die Anmerkung des öffentlichen Schlüssels wird vom CMC verwendet, um SSH-Benutzer bei Verwendung des RACADM-Befehls `getssninfo` zu unterscheiden, weil alle PKA-Benutzer den Dienst-Benutzernamen zur Anmeldung verwenden.

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

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

Weitere Informationen zu `sshpkauth` finden Sie im *Chassis Management Controller for PowerEdge FX2/FX2s Command Line Reference Guide* (Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge FX2/FX2s).

Terminalemulationssoftware konfigurieren

CMC unterstützt eine serielle Textkonsole, die mit einer beliebigen Terminal-Emulationssoftware gestartet werden kann. Im Folgenden finden Sie einige Beispiele von Terminal-Emulationssoftware, mit der eine Verbindung zum CMC hergestellt werden kann.

1. Linux Minicom
2. HyperTerminal für Windows von Hilgraveve

Schließen Sie ein Ende des seriellen Null-Modem-Kabels (an beiden Enden vorhanden) an den seriellen Anschluss auf der Rückseite des Gehäuses an. Schließen Sie das andere Ende des Kabels an den seriellen Anschluss der Management Station an. Weitere Informationen über das Anschließen der Kabel finden Sie im Abschnitt über die Rückseite des Gehäuses unter Gehäuse-Übersicht.

Konfigurieren Sie Ihre Terminal-Emulationssoftware mit den folgenden Parametern:

- **Baudrate**: 115200
- **Port**: COM1
- **Daten**: 8 Bit
- **Parität**: keine
- **Stopp**: 1 Bit
- **Hardware-Ablaufsteuerung**: Ja
- **Software-Ablaufsteuerung**: Nein

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

Der CMC kann eine Verbindung herstellen, um die serielle Konsole von Servern oder E/A-Modulen umzuleiten.

Für Server kann die serielle Konsolenumleitung so erreicht werden:

- CMC Befehlszeilenschnittstelle (CLI) oder der Befehl RACADM `connect`. Weitere Informationen über die Ausführung von RACADM-Befehlen finden Sie im *Chassis Management Controller for PowerEdge*

FX2/FX2s RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge FX2/FX2s).

- Serielle Konsolenumleitungsfunktion der iDRAC-Webschnittstelle.
- iDRAC-Seriell-über-LAN (SOL)-Funktionalität.

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

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

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

ANMERKUNG: Wird die EAM-Konsolenumleitung nicht unterstützt, wird beim Befehl `connect` eine leere Konsole angezeigt. Wenn Sie in diesem Fall zur CMC-Konsole zurückkehren möchten, geben Sie die Escape-Sequenz ein. Die standardmäßige Konsolen-Escape-Sequenz ist <Strg><\>.

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

`connect switch-`*`n`*

wobei `n` eine EAM-Kennungszeichnung A1 ist.

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

Tabelle 13. E/A-Module zu Switches zuordnen

E/A-Modulkennzeichnung	Switch
A1	switch-a1 oder switch-1
A2	switch-a2 oder switch-2

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

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

Um eine Verbindung zu einer verwalteten seriellen Serverkonsole herzustellen, verwenden Sie den Befehl `connect server-`*`n`*, wobei *n* = 1-4 (PowerEdge FM120x4) und *n* = 1-8 (PowerEdge FC630) 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, wird die Fehlermeldung `No route to host` angezeigt.

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

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

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

BIOS des verwalteten Servers für die serielle Konsolenumleitung konfigurieren

Sie können über eine Remote-Konsolensitzung eine Verbindung zum verwalteten System unter Verwendung der iDRAC7-Web-Schnittstelle herzustellen (siehe iDRAC-Benutzerhandbuch *Dell Integrated Dell Remote Access Controller (iDRAC) User's Guide* unter **dell.com/support/manuals**.

Die serielle Kommunikation ist im BIOS standardmäßig ausgeschaltet. Um die Daten der Hosttextkonsole zu „Seriell über LAN" umzuleiten, müssen Sie die Konsolenumleitung über COM1 aktivieren. So ändern Sie die BIOS-Einstellung:

1. Schalten Sie den Verwaltungsserver ein.
2. Drücken Sie auf die Schaltfläche <F2>, um das BIOS-Setup-Dienstprogramm während POST einzugeben.
3. Wechseln Sie zu **Serielle Kommunikation** und drücken Sie die <Eingabetaste>. Im Dialogfeld wird die Liste zur seriellen Kommunikation mit den folgenden Optionen angezeigt:
   - **off**
   - **Ein ohne Konsolenumleitung**
   - **Ein mit Konsolenumleitung über COM1**

   Um zwischen Optionen hin und her zu navigieren, verwenden Sie die entsprechenden Pfeiltasten.

   ANMERKUNG: Achten Sie darauf, dass die Option **Ein mit Konsolenumleitung über COM1** ausgewählt ist.
4. Aktivieren Sie **Umleitung nach Start** (Standardwert ist **deaktiviert**). Durch diese Option wird die BIOS-Konsolenumleitung für nachfolgende Neustarts aktiviert.
5. Speichern Sie die Änderungen und beenden Sie.

   Das verwaltete System wird neu gestartet.

Windows für serielle Konsolenumleitung konfigurieren

Es ist keine Konfiguration erforderlich für Server, die unter den Microsoft Windows Server-Versionen laufen, beginnend mit Windows Server 2003. Windows erhält Informationen vom BIOS und aktiviert die spezielle Verwaltungskonsole (SAC) auf COM1.

Linux während des Starts für die Umleitung der seriellen Konsole konfigurieren

Die folgenden Schritte beziehen sich speziell auf den Linux Grand Unified Bootloader (GRUB). Ähnliche Änderungen sind erforderlich, um einen anderen Bootloader zu verwenden.

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

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

1. Suchen Sie die allgemeinen Einstellungsabschnitte in der Datei und geben Sie die folgenden zwei Zeilen ein:

   ```
   serial --unit=1 --speed=57600 terminal --timeout=10 serial
   ```

2. Hängen Sie zwei Optionen an die Kernel-Zeile an:

   ```
   kernel console=ttyS1,57600
   ```

3. Wenn **/etc/grub.conf** eine `splashimage`-Direktive enthält, kommentieren Sie sie aus.

   Im folgenden Beispiel sind die Änderungen zu sehen, die in diesem Verfahren beschrieben werden.

   ```
   # grub.conf generated by anaconda # # Note that you do not have to rerun
   grub after making changes # to this file # NOTICE: You do not have a /boot
   partition. This means that # all kernel and initrd paths are relative to /,
   e.g. # root (hd0,0) # kernel /boot/vmlinuz-version ro root= /dev/sda1 #
   initrd /boot/initrd-version.img # #boot=/dev/sda default=0 timeout=10
   #splashimage=(hd0,2)/grub/splash.xpm.gz serial --unit=1 --speed=57600
   terminal --timeout=10 serial title Red Hat Linux Advanced Server (2.4.9-e.
   3smp) root (hd0,0) kernel /boot/vmlinuz-2.4.9-e.3smp ro root= /dev/sda1
   hda=ide-scsi console=ttyS0 console= ttyS1,57600 initrd /boot/initrd-2.4.9-e.
   3smp.img title Red Hat Linux Advanced Server-up (2.4.9-e.3) root (hd0,00)
   kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 initrd /boot/initrd-2.4.9-
   e.3.img
   ```

   Folgen Sie beim Bearbeiten der Datei **/etc/grub.conf** diesen Richtlinien:

   - Deaktivieren Sie die GRUB-Grafikschnittstelle und verwenden Sie die textbasierte Schnittstelle. Ansonsten wird der GRUB-Bildschirm nicht in der Konsolenumleitung angezeigt. Zum Deaktivieren der grafischen Schnittstelle kommentieren Sie die Zeile aus, die mit `splashimage` beginnt.
   - Zum Starten mehrerer GRUB-Optionen, um Konsolensitzungen über die serielle Verbindung zu beginnen, fügen Sie allen Optionen die folgende Zeile hinzu:

     ```
     console=ttyS1,57600
     ```

     Das Beispiel zeigt, dass `console=ttyS1,57600` nur zur ersten Option hinzugefügt wurde.

Linux für die Umleitung der seriellen Konsole nach Start konfigurieren

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

Fügen Sie eine neue Zeile hinzu, um `agetty` auf der seriellen COM2-Schnittstelle zu konfigurieren:

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

Das folgende Beispiel zeigt die Datei mit der neuen Zeile.

```
# # inittab This file describes how the INIT process # should set up the system
in a certain # run-level. # # Author: Miquel van Smoorenburg # Modified for RHS
Linux by Marc Ewing and # Donnie Barnes # # Default runlevel. The runlevels
used by RHS are: # 0 - halt (Do NOT set initdefault to this) # 1 - Single user
mode # 2 - Multiuser, without NFS (The same as 3, if you # do not have
networking) # 3 - Full multiuser mode # 4 - unused # 5 - X11 # 6 - reboot (Do
NOT set initdefault to this) # id:3:initdefault: # System initialization.
si::sysinit:/etc/rc.d/rc.sysinit l0:0:wait:/etc/rc.d/rc 0 l1:1:wait:/etc/
rc.d/rc 1 l2:2:wait:/etc/rc.d/rc 2 l3:3:wait:/etc/rc.d/rc 3 l4:4:wait:/etc/
rc.d/rc 4 l5:5:wait:/etc/rc.d/rc 5 l6:6:wait:/etc/rc.d/rc 6 # Things to run in
every runlevel. ud::once:/sbin/update # Trap CTRL-ALT-DELETE ca::ctrlaltdel:/
sbin/shutdown -t3 -r now # When our UPS tells us power has failed, assume we
have a few # minutes of power left. Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have power installed and your # UPS is
connected and working correctly. pf::powerfail:/sbin/shutdown -f -h +2 "Power
```

```
Failure; System Shutting Down" # If power was restored before the shutdown
kicked in, cancel it. pr:12345:powerokwait:/sbin/shutdown -c "Power Restored;
Shutdown Cancelled" # Run gettys in standard runlevels co:2345:respawn:/sbin/agetty -
h -L 57600 ttyS1 ansi 1:2345:respawn:/sbin/mingetty tty1 2:2345:respawn:/sbin/
mingetty tty2 3:2345:respawn:/sbin/mingetty tty3 4:2345:respawn:/sbin/mingetty
tty4 5:2345:respawn:/sbin/mingetty tty5 6:2345:respawn:/sbin/mingetty tty6 #
Run xdm in runlevel 5 # xdm is now a separate service x:5:respawn:/etc/X11/
prefdm -nodaemon
```

Edit the **/etc/securetty**file as follows:

Fügen Sie eine neue Zeile mit dem Namen des seriellen tty für COM2 hinzu:

```
ttyS1
```

Das folgende Beispiel zeigt eine Beispieldatei mit der neuen Zeile.

```
vc/1 vc/2 vc/3 vc/4 vc/5 vc/6 vc/7 vc/8 vc/9 vc/10 vc/11 tty1 tty2 tty3 tty4
tty5 tty6 tty7 tty8 tty9 tty10 tty11 ttyS1
```

12

Verwenden von FlexAddress- und FlexAdress Plus-Karten

Dieser Abschnitt enthält Informationen über FlexAddress und die Verwendung der FlexAddress Plus-Karte zur Konfiguration von FlexAddress.

ANMERKUNG: Die FlexAddress-Funktion ist lizenziert. Diese Lizenz ist in der Enterprise-Lizenz enthalten.

Über FlexAddress

FlexAddress ermöglicht es dem CMC, WWN/MAC-IDs einem bestimmten Steckplatz zuzuweisen und die werksseitigen 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, die SAN-Ressourcen, DHCP-Server und Router für verschiedene Fabrics für ein neues Servermodul neu zu konfigurieren.

Jedem Servermodul wird als Teil des Herstellungsprozesses eine eindeutige WWN- und/oder MAC-Kennung (WWN/MAC-ID) zugewiesen. Wenn Sie früher (ohne FlexAddress) ein Servermodul durch ein anderes ersetzen wollten, mussten die WWN/MAC-ID-Änderungen, die Ethernet-Netzwerkverwaltungsinstrumente und die SAN-Ressourcen neu konfiguriert werden, damit das neue Servermodul erkannt wird.

Wenn der Server in einen neuen Steckplatz oder ein neues Gehäuse eingesetzt wird, wird die serverzugewiesene WWN/MAC-Adresse verwendet, es sei denn, im Gehäuse ist die FlexAddress-Funktion für den neuen Steckplatz aktiviert. Wenn Sie den Server wieder entfernen, wechselt die Adresse zurück zur serverzugewiesenen Adresse.

Außerdem erfolgt das *außer Kraft setzen* 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 werksseitig zugewiesenen WWN/MAC-IDs verwendet.

Das CMC FX2/FX2S-Gehäuse wird mit einer FlexAddress Plus-SD-Karte ausgeliefert, welche die Funktionen FlexAddress, FlexAddress Plus und Erweiterter Speicher unterstützt.

ANMERKUNG: Die auf der FlexAddress Plus-SD-Karte befindlichen Daten sind verschlüsselt und dürfen nicht vervielfältigt oder verändert werden, da dies die Systemfunktion beeinträchtigen und zu Fehlfunktionen führen könnte.

ANMERKUNG: Die Verwendung der FlexAddress Plus-SD-Karte ist auf ein einziges Gehäuse beschränkt. Sie können die gleiche FlexAddress Plus-SD-Karte nicht auf einem anderen Gehäuse verwenden.

Über FlexAddress Plus

Jede FlexAddress Plus-Funktionskarte enthält einen eindeutigen Pool aus MAC/WWNs, mit dessen Hilfe das Gehäuse World Wide Name/Media Access Control (WWN/MAC)-Adressen für Fibre Channel- und Ethernet-Geräte zuweisen kann. Die vom Gehäuse zugewiesenen WWN/MAC-Adressen sind global eindeutig und gelten für einen bestimmten Serversteckplatz.

Vor der Installation von FlexAddress können Sie den Bereich der MAC-Adressen auf einer FlexAddress-Funktionskarte festlegen, indem Sie die SD-Karte in einen USB-Speicherkartenleser einlegen und die Datei **pwwn_mac.xml** anzeigen. Diese XML-Datei mit Klartext auf der SD-Karte enthält den XML-Tag `mac_start`, die erste hex-MAC-Anfangsadresse, die für diesen eindeutigen MAC-Adressbereich verwendet wird. Der Tag `mac_count` ist die Gesamtzahl der MAC-Adressen, die von der SD-Karte vergeben wird. Der gesamte zugewiesene MAC-Bereich kann anhand der folgenden Formel ermittelt werden:

<mac_start> + *<mac_count>* - 1 = *<mac_end>*

Beispiel:

```
(starting_mac)00:18:8B:FF:DC:FA + (mac_count)0xCF – 1 =
(ending_mac)00:18:8B:FF:DD:C8
```

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

Bestätigung FlexAddress-Aktivierung

Um den Aktivierungsstatus der FlexAddress-Funktion anzuzeigen, führen Sie den folgenden RACADM-Befehl aus:

```
racadm featurecard -s

       Feature Name = FlexAddress Date/time Activated = 05 Oct 2013 - 11:50:49
Feature installed from SD-card serial number = CN0H871T1374036T00MXA00

       Feature Name = FlexAddressPlus Date/time Activated = 05 Oct 2013 -
11:50:49 Feature installed from SD-card serial number = CN0H871T1374036T00MXA00

       Feature Name = ExtendedStorage Current Status = redundant, active Date/
time Activated = 05 Oct 2013 - 11:50:58 Feature installed from SD-card serial
number = CN0H871T1374036T00MXA00
```

Wenn keine aktiven Funktionen auf dem Gehäuse vorhanden sind, gibt der Befehl folgende Meldung zurück: „racadm feature -s Keine Funktionen auf dem Gehäuse aktiviert“

```
racadm feature -s No features active on the chassis
```

So zeigen Sie die SD-Karteninformationen an:

```
$ racadm featurecard -s Active CMC: The feature card inserted is valid, serial
number CN0H871T1374036T00MXA00 The feature card contains the following
feature(s) FlexAddress: bound FlexAddressPlus: bound ExtendedStorage: bound
```

Tabelle 14. Statusmeldungen, zurückgegeben vom Befehl featurecard -s

Statusmeldung	Maßnahmen
`No feature card inserted.`	Prüfen Sie den CMC um sicherzustellen, dass die SD-Karte korrekt eingesetzt wurde.
`Die eingesetzte Funktionskarte ist gültig und enthält die folgenden Funktion(en) FlexAddress: gebunden.`	Keine Maßnahme erforderlich.
`The feature card inserted is valid and contains the following feature(s) FlexAddress: bound to another chassis, svctag=ABC1234, SD card SN = 1122334455.`	Entfernen Sie die SD-Karte; bestimmen und installieren Sie die SD-Karte für das aktuelle Gehäuse.
`The feature card inserted is valid and contains the following feature(s) FlexAddress: not bound.`	The feature card can be moved to another chassis or can be reactivated on the current chassis. To reactivate on the current chassis, enter `racadm racreset` until the CMC module with the feature card installed becomes active.

Dell-Funktionskarten können mehr als eine Funktion enthalten. Sobald eine auf einer Dell-Funktionskarte enthaltene Funktion auf einem Gehäuse aktiviert ist, können keine anderen Funktionen, die möglicherweise auf der Dell-Funktionskarte enthalten sind, auf einem anderen Gehäuse aktiviert werden. In diesem Fall zeigt der Befehl „racadm feature -s" die folgende Meldung für die betroffenen Funktionen an:

```
ERROR: One or more features on the SD card are active on another chassis
```

Weitere Informationen über die Befehle `feature` und `featurecard` finden Sie im Referenzhandbuch *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Dell Chassis Management Controller für PowerEdge FX2/FX2s).

Deaktivierung von FlexAddress

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

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

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

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

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

Der Befehl gibt die folgende Statusmeldung bei erfolgreicher Ausführung zurück:

```
feature FlexAddress is deactivated on the chassis successfully.
```

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

```
ERROR: Unable to deactivate the feature because the chassis is powered ON
```

ANMERKUNG: Um die FlexAddress-Funktion erneut zu aktivieren, starten Sie den CMC neu.

Weitere Informationen zu diesem Befehl finden Sie im Abschnitt zum **feature**-Befehl im Referenzhandbuch *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Dell Chassis Management Controller für PowerEdge FX2/FX2s).

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: Mithilfe des `racresetcfg`-Unterbefehls können Sie die Flex-Adresse eines CMC zur Standardwerkseinstellung „Deaktiviert" zurücksetzen. Die RACADM-Syntax ist:

```
racadm racresetcfg –c flex
```

Weitere Informationen über RACADM-Befehle, die sich auf die FlexAddress beziehen, sowie Daten über andere werksseitig eingestellte Eigenschaften finden Sie im Referenzhandbuch *Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Chassis Management Controller für PowerEdge FX2/FX2s) unter **dell.com/support/manuals**.

Der Server muss ausgeschaltet sein, bevor Sie mit der Konfiguration beginnen. Sie können FlexAddress auf Basis der jeweiligen Struktur aktivieren oder deaktivieren. Zusätzlich können Sie die Funktion steckplatzbasiert aktivieren 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.

ANMERKUNG: Wenn die FlexAddress-Funktion zum ersten Mal auf einem Servermodul bereitgestellt wird, erfordert dies ein Herunterfahren und erneutes Hochfahren, damit FlexAddress wirksam wird. Auf Ethernet-Geräten wird FlexAddress vom BIOS des Systemmoduls programmiert. Damit das BIOS des Servermoduls die Adresse programmieren kann, muss es in Betrieb sein, was erfordert, dass das Servermodul eingeschaltet ist. Ist das Herunter-/Hochfahren abgeschlossen, sind die gehäusezugewiesenen MAC-IDs für die Wake-On-LAN (WOL)-Funktion verfügbar.

Konfiguration der FlexAddress Struktur und Steckplatz auf Gehäuseebene

Auf Gehäuseebene können Sie FlexAddress für Strukturen und Steckplätze aktivieren oder deaktivieren. FlexAddress ist jeweils für eine Struktur aktiviert, und dann werden die Steckplätze ausgewählt, die davon betroffen sein sollen. Sowohl Strukturen, als auch Steckplätze müssen für eine erfolgreiche FlexAddress-Konfiguration aktiviert sein.

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.

Befehlsmeldungen

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

Tabelle 15. FlexAddress-Befehle und -Ausgaben

Situation	Befehl	Output (Ausgabe)

SD-Karte im CMC-Modul ist an eine andere Service-Tag-Nummer gebunden.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)`
		
		`FlexAddress: bound to another chassis, svctag = <Service tag Number> SD card SN = <Valid flex address serial number>`

SD-Karte im CMC-Modul ist an die gleiche Service-Tag-Nummer gebunden.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)`
		
		`FlexAddress: bound`

SD-Karte im CMC-Modul ist an keine Service-Tag-Nummer gebunden.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)`
		
		`FlexAddress:not bound`

Die Funktion FlexAddress befindet sich aus irgendeinem Grunde (keine SD-Karte eingesetzt / beschädigte SD-Karte / Funktion deaktiviert / SD-Karte an anderes Gehäuse gebunden) nicht auf dem Gehäuse.	`$racadm setflexaddr [-f <fabricName> <slotState>]`
	
	`$racadm setflexaddr [-i <<slot#> <slotstate>]`
		`ERROR: Flexaddress feature is not active on the chassis`

Gastbenutzer versucht FlexAddress für Steckplätze/ Strukturen festzulegen	`$racadm setflexaddr [-f <fabricName> <slotState>]`
	
	`$racadm setflexaddr [-i <<slot#> <slotstate>]`
		`ERROR: Insufficient user privileges to perform operation`

Die Funktion FlexAddress bei eingeschaltetem Gehäuse deaktivieren.	`racadm feature -d -c flexaddress`	`ERROR: Unable to deactivate the feature`

Situation	Befehl	Output (Ausgabe)
		because the chassis is powered ON
Gastbenutzer versucht die Funktion auf dem Gehäuse zu deaktivieren.	racadm feature -d -c flexaddress	ERROR: Insufficient user privileges to perform operation
Ändern der FlexAddress-Einstellungen für einen Steckplatz/eine Struktur, während die Servermodule eingeschaltet sind.	$racadm setflexaddr -i 1 1	ERROR: Unable to perform the set operation because it affects a powered ON server
Flexaddress-Einstellungen auf Steckplatz oder Struktur ändern, wenn die CMC Enterprise-Lizenz nicht installiert ist.	$racadm setflexaddr -i<slotnum> <status> $racadm setflexaddr -f<FabricName> <status>	ERROR: SWC0242 : A required license is missing or expired. Obtain an appropriate license and try again, or contact your service provider for additional details. ANMERKUNG: Um dieses Problem zu beheben, müssen Sie eine **FlexAddress-Aktivierungs**-Lizenz aufweisen.

FlexAddress DELL SOFTWARE-LIZENZVEREINBARUNG

Dies ist ein rechtlich bindender Vertrag zwischen Ihnen, dem Benutzer, und Dell Products L.P oder Dell Global B.V. ("Dell"). Diese Vereinbarung erstreckt sich auf jede Software (zusammenfassend als „Software" bezeichnet), die mit dem Dell-Produkt geliefert wird und für die keine separate Lizenzvereinbarung zwischen Ihnen und dem Hersteller bzw. dem Eigentümer der Software besteht. Diese Vereinbarung ist nicht für den Verkauf von Software oder von anderem geistigen Eigentum bestimmt. Alle Eigentumsrechte und Rechte an geistigem Eigentum sind im Besitz des Herstellers oder Eigentümers der Software. Alle Rechte, die in dieser Vereinbarung nicht ausdrücklich übertragen werden, sind im Besitz des Herstellers oder Eigentümers der Software. Durch Öffnen bzw. Aufbrechen des Siegels am bzw. an den Softwarepaket(en), Installieren oder Herunterladen der Software oder Verwenden der Software, die bereits im Computer geladen oder im Produkt integriert ist, erkennen Sie die Bestimmungen dieser Vereinbarung an. Wenn Sie diesen Bestimmungen nicht zustimmen, geben Sie bitte die gesamte Software inklusive Begleitmaterial (Disketten, CDs, gedrucktes Material und Verpackungen) unverzüglich zurück, und löschen Sie die bereits geladene oder integrierte Software.

Sie sind berechtigt, eine Kopie der Software auf einem einzigen Computer zu installieren und zu verwenden. Wenn Sie über mehrere Lizenzen der Software verfügen, ist es Ihnen gestattet, so viele Kopien der Software gleichzeitig zu verwenden, wie Sie Lizenzen haben. Die Software wird auf einem Computer „verwendet", wenn sie in einen temporären Speicher geladen oder auf einem permanenten Speicher des Computers installiert ist. Die Installation auf einem Netzwerkserver nur zum Zweck der internen Verteilung stellt jedoch keine „Verwendung" dar, wenn (und nur wenn) Sie für jeden Computer,

an den die Software verteilt wird, über eine gesonderte Lizenz verfügen. Sie müssen sicherstellen, dass die Anzahl der Personen, die die auf einem Netzwerkserver installierte Software verwenden, nicht die Anzahl der vorhandenen Lizenzen übersteigt. Wenn mehr Personen die Software verwenden, die auf einem Netzwerkserver installiert ist, als Lizenzen vorhanden sind, müssen Sie erst so viele zusätzliche Lizenzen erwerben, bis die Anzahl der Lizenzen der Anzahl der Benutzer entspricht, bevor Sie weiteren Benutzern die Verwendung der Software gestatten dürfen. Als gewerblicher Kunde oder als Dell-Tochtergesellschaft gewähren Sie hiermit Dell oder einem von Dell bestimmten Vertreter das Recht, während der normalen Geschäftszeiten ein Audit der Softwareverwendung durchzuführen; außerdem erklären Sie sich damit einverstanden, Dell bei einem solchen Audit zu unterstützen und Dell alle Aufzeichnungen zur Verfügung zu stellen, die billigerweise mit der Verwendung der Software in Beziehung stehen. Das Audit beschränkt sich auf die Überprüfung der Einhaltung der Bestimmungen dieser Vereinbarung.

Die Software ist durch US-amerikanische Urheberrechtsgesetze und Bestimmungen internationaler Verträge geschützt. Sie sind berechtigt, eine Kopie der Software ausschließlich zu Sicherungs- oder Archivierungszwecken zu erstellen oder die Software auf eine einzige Festplatte zu übertragen, wenn Sie das Original ausschließlich zu Sicherungs- und Archivierungszwecken aufbewahren. Sie sind nicht berechtigt, die Software 240 bei Benutzung von FlexAddress and FlexAddress 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.

BESCHRÄNKTE RECHTE DER US-REGIERUNG

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.

Anzeigen von WWN/MAC-Adressinformationen

Sie können den WWW/MAC-Adressbestand von Netzwerkadaptern für die einzelnen Serversteckplätze oder für alle Server eines Gehäuses anzeigen. Folgendes ist in diesem Bestand enthalten:

- Fabric-Konfiguration

  ANMERKUNG:

  – Fabric A zeigt den Typ des installierten Eingabe/Ausgabe-Fabrics an. Wenn Fabric A aktiviert ist, zeigen die nicht bestückten Steckplätze gehäusezugewiesene MAC-Adressen für Fabric A an.

  – Der iDRAC-Management-Controller wird als Teil des Management-Fabrics betrachtet und zusammen mit den übrigen Fabrics angezeigt.

  – Ein Häkchen bei einer Komponente zeigt an, dass das Fabric für FlexAddress oder FlexAddressPlus aktiviert ist.
- Protokoll, das auf der NIC-Adapterschnittstelle verwendet wird., z. B. LAN, iSCSI, FCoE und so weiter.
- Fibre Channel World Wide Name (WWN) Konfiguration und MAC (Media Access Control)-Adressen eines Steckplatzes im Gehäuse.
- Zuweisungstyp für MAC-Adresse und derzeit aktiver Adresstyp – Serverzugewiesen, FlexAddress oder E/A-Identität. Ein grünes Häkchen zeigt den aktiven Adresstyp an (serverzugewiesen, gehäusezugewiesen oder Remote-zugewiesen).
- Status von NIC-Partitionen für Geräte, die Partitionierung unterstützen.

Sie können den WWN/MAC-Adressbestand unter Verwendung der Web-Schnittstelle oder der RACADM-CLI anzeigen. Je nach Schnittstelle können Sie die MAC-Adresse filtern und feststellen, welche WWN/MAC-Adresse eine Funktion oder Partition verwendet. Wenn für den Adapter NPAR aktiviert ist, können Sie anzeigen, welche Partitionen aktiviert oder deaktiviert sind.

Wenn Sie die Web-Schnittstelle verwenden, können Sie die WWN/MAC-Adressinformationen für bestimmte Steckplätze anzeigen, indem Sie die Seite **FlexAddress** verwenden (klicken Sie auf **Server-Übersicht → Steckplatz <x> → Setup → FlexAddress**). Die WWN/MAC-Adressinformationen für alle Steckplätze und Server können Sie unter Verwendung der Seite **WWN/MAC-Zusammenfassung** anzeigen (klicken Sie auf **Server-Übersicht → Eigenschaften → WWN/MAC**). Auf beiden Seiten können Sie die WWN/MAC-Adressinformationen entweder im grundlegenden oder im erweiterten Modus anzeigen:

- **Grundlegender Modus** – In diesem Modus können Sie Serversteckplatz, Fabric, Protokoll, WWN/MAC-Adressen und Partitionsstatus anzeigen. Es werden nur aktive MAC-Adressen im Feld „WWN/

MAC-Adresse“ angezeigt. Sie können die Ausgabe filtern, indem Sie nur bestimmte oder alle angezeigten Felder verwenden.

- **Erweiterter Modus** – In diesem Modus können Sie alle angezeigten Felder im grundlegenden Modus und alle MAC-Adresstypen anzeigen (serverzugewiesen, Flex Address und E/A-Identität). Sie können die Ausgabe filtern, indem Sie nur bestimmte oder alle angezeigten Felder verwenden.

Im grundlegenden Modus und im erweiterten Modus werden die WWN/MAC-Adressinformationen in einem minimierten Format angezeigt. Klicken Sie auf das + bei einem Steckplatz, oder klicken Sie auf **Alle erweitern/minimieren**, um die Informationen für einen bestimmten Steckplatz oder alle Steckplätze anzuzeigen.

Sie haben außerdem die Möglichkeit, die WWN/MAC-Adressinformationen für alle Server des Gehäuses in einen lokalen Ordner zu exportieren.

Weitere Informationen zu den Feldern finden Sie in der Online-Hilfe zu *CMC für Dell PowerEdge FX2/FX2s*.

Anzeigen von grundlegenden WWN/MAC-Adressinformationen unter Verwendung der Web-Schnittstelle

So können Sie WWN/MAC-Adressinformationen für die einzelnen Serversteckplätze oder alle Server in einem Gehäuse im grundlegenden Modus anzeigen:

1. Klicken Sie auf **Server-Übersicht → Eigenschaften → WWN/MAC.**

   Die Seite **WWN/MAC-Zusammenfassung** zeigt die WWN/MAC-Adressinformationen an.

   Klicken Sie alternativ auf **Server-Übersicht → Steckplatz <x> → Setup → FlexAddress**, um die WWN/MAC-Adressinformationen für einen bestimmten Serversteckplatz anzuzeigen. Die Seite **FlexAddress** wird angezeigt.
2. Klicken Sie in der Tabelle **WWN/MAC-Adressen** auf **Exportieren**, um die WWN/MAC-Adressen lokal zu speichern.
3. Klicken Sie auf das Symbol + bei einem Steckplatz, oder klicken Sie auf **Alle erweitern/minimieren**, um die Attribute für einen bestimmten Steckplatz oder alle Steckplätze in der Tabelle „WWN/MAC-Adressen“ zu erweitern oder zu minimieren.
4. Wählen Sie im Drop-Down-Menü **Ansicht** die Option **Grundlegend** aus, um die WWN/MAC-Adressattribute in der Strukturansicht anzuzeigen.
5. Wählen Sie im Drop-Down-Menü **Serversteckplatz** die Option **Alle Server** oder einen bestimmten Steckplatz aus, um die WWN/MAC-Adressattribute für alle Server bzw. nur für diejenigen in einem bestimmten Steckplatz anzuzeigen.
6. Wählen Sie im Drop-Down-Menü **Fabric** einen Fabric-Typ aus, um Details für alle oder für bestimmte Verwaltungstypen bzw. E/A-Fabrics für die Server anzuzeigen.
7. Wählen Sie im Drop-Down-Menü **Protokoll** die Option **Alle Protokolle** oder eines der aufgeführten Netzwerkprotokolle aus, um alle MACs bzw. die dem ausgewählten Protokoll zugeordnete MAC anzuzeigen.
8. Um die einer bestimmten MAC-Adresse zugeordneten Steckplätze zu filtern, geben Sie in das Feld **WWN/MAC-Adressen** die betreffende MAC-Adresse ein. Sie können die MAC-Adressen auch nur teilweise eingeben, um die zugeordneten Steckplätze anzuzeigen. Geben Sie z. B. `4A` ein, um die Steckplätze anzuzeigen, deren MAC-Adressen den Eintrag `4A` enthalten.
9. Wählen Sie im Drop-Down-Menü **Partitionsstatus** einen Status aus, um die Server mit dem ausgewählten Partitionsstatus anzuzeigen.

Wenn eine bestimmte Partition deaktiviert ist, wird die Zeile, in der die Partition angezeigt wird, grau unterlegt.

Weitere Informationen zu den Feldern finden Sie in der Online-Hilfe zu *CMC für Dell PowerEdge FX2/FX2s*.

Anzeigen von erweiterten WWN/MAC-Adressinformationen unter Verwendung der Web-Schnittstelle

So können Sie WWN/MAC-Adressinformationen für die einzelnen Serversteckplätze oder alle Server in einem Gehäuse im erweiterten Modus anzeigen:

1. Klicken Sie auf **Server-Übersicht** → **Eigenschaften** → **WWN/MAC.**

   Die Seite **WWN/MAC-Zusammenfassung** zeigt die WWN/MAC-Adressinformationen an.
2. Wählen Sie im Drop-Down-Menü **Ansicht** die Option **Erweitert** aus, um die WWN/MAC-Adressattribute in der ausführlichen Ansicht anzuzeigen.

   In der Tabelle **WWN/MAC-Adressen** werden Servers teckplatz, Fabric, Protokoll, WWN/MAC-Adressen, Zuweisungstyp für MAC-Adresse (Serverzugewiesen, FlexAddress oder E/A-Identität) und der Partitionsstatus aufgeführt. Der jeweils aktive Adresstyp wird anhand eines grünen Häkchens angezeigt (serverzugewiesen, gehäusezugewiesen oder Remote-zugewiesen). Ist bei einem Server FlexAddress oder E/A-Identität nicht aktiviert, wird der Status bei **FlexAddress (gehäusezugewiesen)** bzw. **E/A-Identität (Remote-zugewiesen)** mit **Nicht aktiviert** angezeigt.
3. Klicken Sie in der Tabelle **WWN/MAC-Adressen** auf **Exportieren**, um die WWN/MAC-Adressen lokal zu speichern.
4. Klicken Sie auf das Symbol  bei einem Steckplatz, oder klicken Sie auf **Alle erweitern/minimieren**, um die Attribute für einen bestimmten Steckplatz oder alle Steckplätze in der Tabelle „WWN/MAC-Adressen" zu erweitern oder zu minimieren.
5. Wählen Sie im Drop-Down-Menü **Serversteckplatz** die Option **Alle Server** oder einen bestimmten Steckplatz aus, um die WWN/MAC-Adressattribute für alle Server bzw. nur für diejenigen in einem bestimmten Steckplatz anzuzeigen.
6. Wählen Sie im Drop-Down-Menü **Fabric** einen Fabric-Typ aus, um Details für alle oder für bestimmte Verwaltungstypen bzw. E/A-Fabrics für die Server anzuzeigen.
7. Wählen Sie im Drop-Down-Menü **Protokoll** die Option **Alle Protokolle** oder eines der aufgeführten Netzwerkprotokolle aus, um alle MACs bzw. die dem ausgewählten Protokoll zugeordnete MAC anzuzeigen.
8. Geben Sie in das Feld **WWN/MAC-Adressen** eine bestimmte MAC-Adresse ein, um nur die Steckplätze anzuzeigen, die dieser MAC-Adresse zugeordnet sind. Sie können die MAC-Adressen auch nur teilweise eingeben, um die zugeordneten Steckplätze anzuzeigen. Geben Sie z. B. `4A` ein, um die Steckplätze anzuzeigen, deren MAC-Adressen den Eintrag `4A` enthalten.
9. Wählen Sie im Drop-Down-Menü **Partitionsstatus** einen Status aus, um die Server mit dem ausgewählten Partitionsstatus anzuzeigen.

   Wenn eine bestimmte Partition deaktiviert ist, wird der Status mit **Deaktiviert** angezeigt, und die Zeile, in der die Partition angezeigt wird, ist grau unterlegt.

Weitere Informationen zu den Feldern finden Sie in der *Online-Hilfe zu CMC für Dell PowerEdge FX2/FX2s*.

Anzeigen von WWN/MAC-Adressinformationen unter Verwendung von RACADM

Um die WWN/MAC-Adressinformationen für alle oder für bestimmte Server unter Verwendung von RACADM anzuzeigen, verwenden Sie die Unterbefehle **getflexaddr** und **getmacaddress**.

Um die FlexAddress für das gesamte Gehäuse anzuzeigen, verwenden Sie den folgenden RACADM-Befehl:

```
racadm getflexaddr
```

Um den FlexAddress-Status für einen bestimmten Steckplatz anzuzeigen, verwenden Sie den folgenden RACADM-Befehl:

```
racadm getflexaddr [-i <slot#>]
```

(wobei <*Steckplatz-Nr.*> ein Wert von 1 bis 4 ist)

Um die NDC- oder LOM-MAC-Adresse anzuzeigen, verwenden Sie den folgenden RACADM-Befehl:

```
racadm getmacaddress
```

Um die MAC-Adresse für das Gehäuse anzuzeigen, verwenden Sie den folgenden RACADM-Befehl:

```
racadm getmacaddress -m chassis
```

Um die iSCSI-MAC-Adresse für alle Server anzuzeigen, verwenden Sie den folgenden RACADM-Befehl:

```
racadm getmacaddress -t iscsi
```

Um die iSCSI-MAC-Adresse für einen bestimmten Server anzuzeigen, verwenden Sie den folgenden RACADM-Befehl:

```
racadm getmacaddress [-m <module> [-x]] [-t iscsi]
```

Um die benutzerdefinierte MAC- und WWN-Adresse anzuzeigen, verwenden Sie den folgenden RACADM-Befehl:

```
racadm getmacaddress -c io-identity
```

```
racadm getmacaddress -c io-identity -m server -2
```

Um die Ethernet- und iSCSI-MAC-Adressen aller LOMs oder Zusatzkarten anzuzeigen, verwenden Sie den folgenden RACADM-Befehl:

```
racadm getmacaddress -a
```

Um die konsolenzugewiesene MAC/WWN-Adresse aller LOMs oder Zusatzkarten anzuzeigen, verwenden Sie den folgenden RACADM-Befehl:

```
racadm getmacaddress -c all
```

Um die gehäusezugewiesene WWN/MAC-Adresse anzuzeigen, verwenden Sie den folgenden RACADM-Befehl:

```
racadm getmacaddress -c flexaddress
```

Um die MAC/WWN-Adresse aller LOMs oder Zusatzkarten anzuzeigen, verwenden Sie den folgenden RACADM-Befehl:

```
racadm getmacaddress -c factory
```

Weitere Informationen zu den Unterbefehlen **getflexaddr** und **getmacaddress** finden Sie im Referenzhandbuch *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Dell Chassis Management Controller für PowerEdge FX2/FX2s).

13

Verwalten von Strukturen

Das Gehäuse unterstützt zwei Fabric-Typen: Fabric A1 und Fabric A2, die von beiden E/A-Modulen verwendet werden und immer mit den integrierten Ethernet-Adaptern der Server verbunden sind.

ANMERKUNG: Im PowerEdge FX2s-Gehäuse bilden die Fabrics B und C die PCIe-Verbindung zu den PCIe Extension-Karten.

Die folgenden E/A-Module werden unterstützt:

- 1-GbE-Pass-Through
- 10-GbE-Pass-Through
- E/A-Aggregator (verfügbar für PowerEdge FX2/FX2s)

Beide Fabrics unterstützen nur Ethernet. Jeder Server-E/A-Adapter (LOM) kann je nach Funktion entweder 2 oder 4 Schnittstellen haben. Die Zusatzkarten-Steckplätze sind mit PCIe-Erweiterungskarten belegt, die mit PCIe-Karten (und nicht mit E/A-Modulen) verbunden sind.

ANMERKUNG: In der CMC-Befehlszeilenschnittstelle werden die EAMs mit der Konvention Schalter bezeichnet.

EAM-Funktionszustand überwachen

Weitere Informationen zur Überwachung des EAM-Funktionszustands finden Sie unter Informationen und Funktionszustand der EAMs anzeigen.

Netzwerkeinstellungen für EAM(s) konfigurieren

Sie können die Netzwerkeinstellungen der zur Verwaltung der EAM verwendeten Schnittstelle angeben. Für Ethernet-Switches wird die bandexterne Verwaltungsschnittstelle (IP-Adresse) konfiguriert. Die bandinterne Verwaltungsschnittstelle (das heißt VLAN1) wird nicht mittels dieser Schnittstelle konfiguriert.

Stellen Sie vor der Konfiguration der Netzwerkeinstellungen für EAM(s) sicher, dass das EAM eingeschaltet ist.

Um die Netzwerkeinstellungen für IOM in Gruppe A konfigurieren zu können, müssen Sie die Berechtigungen als Struktur A-Administrator aufweisen.

ANMERKUNG: Für Ethernet-Switches können weder die bandinternen (VLAN1) noch die bandexterne Verwaltungs-IP-Adressen gleich sein bzw. sich im gleichen Netzwerk befinden; dies führt dazu, dass die bandexterne IP-Adresse nicht vergeben wird. Beachten Sie die EAM-Dokumentation für die standardmäßige bandinterne Verwaltungs-IP-Adresse.

ANMERKUNG: Die Netzwerkeinstellungen des E/A-Moduls für Ethernet-Passthrough und Infiniband-Schalter dürfen nicht konfiguriert werden.

Konfigurieren der Netzwerkeinstellungen für EAM über die CMC-Webschnittstelle

So konfigurieren Sie die Netzwerksicherheitseinstellungen für E/A-Module:

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht**, dann auf **E/A-Modul-Übersicht**, und klicken Sie dann auf **Setup**. Alternativ, um die Netzwerkeinstellungen der verfügbaren E/A-Module **A1** und **A2** zu konfigurieren, klicken Sie auf **A1 Gigabit Ethernet** oder **A2 Gigabit Ethernet**, und klicken Sie dann auf **Setup**.

   Geben Sie auf der Seite **E/A-Modul-Netzwerkeinstellungen** die entsprechenden Daten ein, und klicken Sie dann auf „Anwenden".
2. Falls zugelassen, geben Sie das Stammkennwort, die SNMP RO Community-Zeichenkette und die SysLog Server IP-Adresse für das EAM ein. Weitere Informationen über die Feldbeschreibungen auf dieser Seite finden Sie in der *Online-Hilfe*.

   ANMERKUNG: Die auf den EAMs festgelegte IP-Adresse vom CMC wird nicht in die permanente Startkonfiguration des Switch übertragen. Um die IP-Adressenkonfiguration permanent zu speichern, müssen Sie den Befehl `connect switch` oder den RACADM-Befehl `racadm connect switch` eingeben oder eine direkte Schnittstelle zum GUI des EAMs verwenden, um diese Adresse in der Startkonfiguration zu speichern.
3. Klicken Sie auf **Anwenden**.

   Die Netzwerkeinstellungen sind für das IOM konfiguriert.

   ANMERKUNG: Falls zugelassen, können Sie die VLANs, Netzwerkeigenschaften und E/A-Schnittstellen auf die Standardkonfiguration zurückzusetzen..

Konfigurieren von Netzwerkeinstellungen für EAMs unter Verwendung von RACADM

Um die Netzwerkeinstellungen für ein EAM unter Verwendung von RACADM zu konfigurieren, stellen Sie das Datum und die Uhrzeit ein. Lesen Sie den Abschnitt zum deploy-Befehl im Referenzhandbuch *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Dell Chassis Management Controller für PowerEdge FX2/FX2s).

Sie können den Benutzernamen, das Kennwort und die SNMP-Zeichenkette für das EAM mithilfe des Befehls „RACADM bereitstellen" einstellen:

```
racadm deploy -m switch -u <username> -p <password>

racadm deploy -m switch -u -p <password> -v SNMPv2 <snmpCommunityString> ro

racadm deploy -a [server|switch] -u <username> -p <password>
```

Anzeigen des E/A-Modul-Uplink- und Downlinkstatus über die Webschnittstelle

ANMERKUNG: Diese Funktion ist nur für PowerEdge FX2/FX2s verfügbar.

Sie können den Uplink- und Downlinkstatus des Dell PowerEdge M E/A-Aggregators über die Webschnittstelle anzeigen. Gehen Sie dazu wie folgt vor:

1. Wählen Sie **Gehäuseübersicht → E/A-Modul-Übersicht**.

   Alle EAMs (1-2) erscheinen in der erweiterten Liste.
2. Klicken Sie auf das EAM (Steckplatz), das Sie anzeigen möchten.

   Es wird die Seite E/A-Modulstatus für das jeweilige EAM angezeigt. Die Tabellen „Uplink-Status E/A-Modul" und „Downlink-Status E/A-Modul" werden angezeigt. Diese Tabellen enthalten Informationen zu den Downlink-Ports (1-8) und zu den Uplink-Ports (9-12). Weitere Informationen hierzu finden Sie in der Online-Hilfe zu *CMC für Dell PowerEdge FX2/FX2s*.

Anzeigen von FCoE-Sitzungsinformationen des E/A-Moduls über die Webschnittstelle

Sie können die FCoE-Sitzungsinformationen des Dell PowerEdge M E/A-Aggregators über die Webschnittstelle anzeigen. Gehen Sie dazu wie folgt vor:

1. Wählen Sie **Gehäuseübersicht → E/A-Modul-Übersicht**.

   Alle EAMs (1–6) erscheinen in der erweiterten Liste.
2. Klicken Sie auf das EAM (Steckplatz), das Sie anzeigen möchten, und klicken Sie dann auf **Eigenschaften → FCoE**.

   Die Seite **FCoE E/A-Modul** für das jeweilige EAM wird angezeigt.
3. Wählen Sie im Drop-Down-Menü **Schnittstelle** die erforderliche Schnittstellennummer für das ausgewählte EAM aus, und klicken Sie auf „Sitzungen anzeigen". Die ausgewählte Option ruft die FCoE-Sitzungsinformationen für den Switch ab und zeigt diese in Form einer Tabelle an.

   Im Abschnitt **FCoE-Sitzungsinformationen** werden die FCoE-Sitzungsinformationen für den Switch angezeigt.

   ANMERKUNG: Der E/A-Aggregator zeigt außerdem die aktiven FCoE-Sitzungen an, wenn der Switch das Protokoll verwendet.

EAM auf Werkseinstellungen zurücksetzen

Sie können EAM mithilfe der Seite **E/A-Module bereitstellen** auf die Werkseinstellungen 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.

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: Diese Funktion wird nur auf dem **Dell PowerEdge E/A-Aggregator** 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-Aktualisierung" wird angezeigt. Sie können alternativ auch eine der folgenden Seiten aufrufen:
   - **Gehäuseübersicht → Aktualisieren**.
   - **Gehäuseübersicht → Gehäuse-Controller → Aktualisieren**.

   Die Seite Firmware-Aktualisierung mit einem Link für den Zugriff auf die Seite EAM-Firmware und Software, wird angezeigt.
2. Aktivieren Sie auf der Seite „EAM-Firmware-Aktualisierung" im Abschnitt „Firmware" das Kontrollkästchen in der Spalte „Aktualisieren" für das EAM, dessen Software Sie aktualisieren möchten, und klicken Sie auf **Firmware-Aktualisierung anwenden**. Alternativ können Sie, um die Software auf eine frühere Version zurückzusetzen, das Kontrollkästchen in der Spalte „Zurücksetzen" aktivieren.
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.

   ANMERKUNG: Die FTOS- oder EAM-Softwareversion wird im Format X-Y (A-B) angezeigt. Zum Beispiel 8-3 (1-4). Wenn die Rollback-Version des FTOS-Images ein altes Image ist, das die alte Version des Zeichenkettenformats 8-3-1-4 verwendet, dann wird die aktuelle Version als 8-3 (1-4) angezeigt.

14

Verwenden des VLAN-Managers

Sie können die VLAN-Einstellungen der EAMs mithilfe der Option **VLAN-Manager** zuweisen oder anzeigen.

ANMERKUNG: Diese Funktion wird nur auf dem Dell PowerEdge E/A-Aggregator unterstützt.

Zuweisen von VLANs zu EAMs

Virtuelle LANs (VLANs) für EAMs ermöglichen Ihnen, Benutzer aus Sicherheits- und anderen Gründen in verschiedene individuelle Netzwerksegmente 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.

Zum Zuweisen eines VLAN zu einem EAM wechseln Sie zu **Gehäuseübersicht** → **E/A-Modul-Übersicht** → **Setup** → **VLAN-Manager**.

Wählen Sie im Abschnitt **VLAN-Zuweisung** das E/A-Modul aus, und wählen Sie die Art der Konfiguration. Geben Sie außerdem den Port-Bereich und den Steckplatz ein.

Ändern oder bearbeiten Sie die VLANs, indem Sie sie aus der Liste im Drop-Down-Menü auswählen.

VLAN-Einstellungen für EAMs über die CMC-Webschnittstelle konfigurieren

So werden die VLAN-Einstellungen auf EAM(s) über die CMC-Webschnittstelle konfiguriert:

1. Wechseln Sie zu **E/A-Modul-Übersicht**, 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.
3. Wählen Sie im Abschnitt **Port-Bereich angeben** den Bereich von Strukturports aus, die dem/den ausgewählten EAM(s) zugewiesen werden sollen.
4. Wählen Sie die Option **Alle auswählen oder Auswahl aufheben** 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.
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.

   ANMERKUNG: Im Abschnitt „Zusammenfassung – VLANs aller Schnittstellen" werden Informationen zu den im Gehäuse vorhandenen EAMs sowie den zugewiesenen VLANs angezeigt. Klicken Sie auf **Speichern**, um eine csv-Datei mit 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 **Apply** (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. Wechseln Sie zu **E/A-Modul-Übersicht**, und klicken Sie auf **Setup → VLAN Manager**.

   Die Seite **VLAN-Manager** wird angezeigt. Der Abschnitt „Zusammenfassung, VLANs aller Schnittstellen" enthält Informationen zu den aktuellen VLAN-Einstellungen für die EAMs.
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. Wechseln Sie zu **E/A-Modul-Übersicht**, 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.

VLANs für EAMs über die CMC-Webschnittstelle entfernen

So entfernen Sie VLANs von EAM(s) über die CMC-Webschnittstelle:

1. Wechseln Sie zu **E/A-Modul-Übersicht**, und klicken Sie dann 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 entfernen** aus der Dropdown-Liste aus und klicken Sie auf **Anwenden**.
   Die den ausgewählten EAMs zugewiesenen VLANs werden entfernt.
   Die Meldung „Vorgang erfolgreich" wird angezeigt. Die aktuellen den EAMs 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:

ANMERKUNG: Die nicht gekennzeichneten VLANs können nicht auf eine VLAN-ID gesetzt werden, die bereits mit Tags versehen ist.

1. Wechseln Sie zu **E/A-Modul-Übersicht**, 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 EAM(s) zugewiesen werden sollen.
4. Wählen Sie die Option **Alle auswählen oder Auswahl aufheben** 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 EAM(s) auf die Standardkonfigurationen über die CMC-Webschnittstelle zurück:

1. Wechseln Sie zu **E/A-Modul-Übersicht**, 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 EAMs gemäß den Standardkonfigurationen zugewiesen.
   Die Meldung „Vorgang erfolgreich" wird angezeigt. Die aktuellen den EAMs zugewiesenen VLAN-Einstellungen werden im Feld VLAN-Zuweisung, Zusammenfassung angezeigt.

15

Energieverwaltung und -überwachung

Das PowerEdge FX2/FX2s-Gehäuse ist der energieeffizienteste Server auf dem Markt. Er ist für hocheffiziente Netzteile und Lüfter konzipiert, verfügt über ein optimiertes Layout, sodass die Luft leichter durch das System strömen kann, und verfügt im gesamten Gehäuse über energieoptimierte Komponenten. Das verbesserte Hardware-Design ist mit fortschrittlichen Stromverwaltungsfunktionen gekoppelt, die im CMC (Chassis Management Controller), in Netzteilen und im iDRAC integriert sind. Sie können damit die Stromeffizienz weiter verbessern.

Die Stromverwaltung bei der PowerEdge FX2/FX2s ist relativ anders als bei PowerEdge VRTX. Eine der Hauptveränderungen in der Methode der Stromverwaltung ist die Verwendung einer Closed Loop System Throttle (CLST), um die gewünschte Stromobergrenze des Gehäuses aufrecht zu erhalten. Der Zweck dieses Verfahrens ist die bessere Steuerung und Nutzung der verfügbaren Netzteileinheiten in vollem Umfang durch das Gehäuse.

Die Stromverwaltungsfunktionen des PowerEdge FX2/FX2s helfen Administratoren, das Gehäuse zu konfigurieren, um den Stromverbrauch zu reduzieren und die Stromverwaltung ggf. an die jeweilige Umgebung anzupassen.

Das PowerEdge FX2-/FX2s-Gehäuse verbraucht Wechselstrom und verteilt die Last auf der aktiven Netzteileinheit (PSU). Das System kann bis zu 3.371 Watt Wechselstrom übertragen, der Servermodulen und der damit verbundenen Gehäuse-Infrastruktur zugeteilt wird. Diese Kapazität variiert jedoch je nach der von Ihnen ausgewählten Stromredundanzregel.

Das PowerEdge FX2/FX2s-Gehäuse kann auf eine von drei Redundanzregeln konfiguriert werden, die das Verhalten der Netzteileinheit beeinflussen und bestimmen, wie der Gehäuse-Redundanzstatus Administratoren gemeldet wird.

Sie können die Energieverwaltung auch über die **OpenManage Power Center (OMPC)** steuern. Wenn die Energie über OMPC extern gesteuert wird, setzt CMC die Verwaltung der folgenden Aktivitäten fort:

- Redundanzregel
- Remote-Stromprotokollierung

OMPC verwaltet dann:

- Server-Stromversorgung
- Eingangsstromkapazität des Systems

ANMERKUNG: Die tatsächliche Stromzuteilung hängt von der Konfiguration und von der Auslastung ab.

Sie können die CMC-Webschnittstelle oder RACADM verwenden, um Stromsteuerungen auf CMC zu verwalten und zu konfigurieren:

- Anzeigen des Status des Gehäuses, der Server und der Netzteile.
- Strombudget und Redundanzregel für das Gehäuse konfigurieren

- Stromsteuerungsvorgänge (Einschalten, Ausschalten, System-Reset, Aus- und Einschalten) für das Gehäuse ausführen.

Redundanzregeln

Eine Redundanzregel ist ein konfigurierbarer Satz von Eigenschaften, die festlegen, wie der CMC den Strom im Gehäuse verwaltet. Die folgenden Redundanzregeln sind konfigurierbar:

- Netzredundanz
- Keine Redundanz
- Nur Redundanzwarnungen

Netzredundanzregeln

Zweck der Netzredundanzregel ist es, ein Gehäusesystem so zu aktivieren, dass es in einem Modus betrieben wird, in dem es Netzstromausfälle überbrücken kann. Diese Ausfälle können ihren Ursprung im Wechselstromnetz, in der Verkabelung oder in einer Netzteileinheit selbst haben. Wenn ein System für Netzredundanz konfiguriert wird, schließen Sie die Netzteile 1 und 2 an separate Stromnetze ein.

In diesem Modus stellt der CMC sicher, dass die Stromabnahme beibehalten wird, so dass das System ohne Einbußen weiterarbeiten kann, wenn das Stromnetz oder ein einzelnes Netzteil ausfällt. Voraussetzung für die Stromversorgung des Servers ist die Verfügbarkeit einer Netzteileinheit. Wenn Redundanz nicht aufrecht erhalten werden kann (z. B. wenn ein Netzteil entfernt wird oder ausfällt) werden Warnungen ausgelöst, und der Gehäusezustand wechselt zu **Kritisch**.

Die Regel Keine Redundanz

In diesem Modus sind beide Netzteile verfügbar und werden genutzt, es gibt jedoch keine Gewähr, dass ein Netzteil- oder Stromausfall keine Auswirkungen auf den Systembetrieb hat. Der Redundanzstatus des Gehäuses ist immer **Keine Redundanz**.

Die Regel Nur Redundanzwarnungen

Die Regel „Nur Redundanzwarnungen" erlaubt es der Server-Stromversorgung, die Kapazität beider Netzteileinheiten zu verwenden, wobei Warmeldungen bei Redundanzverlust auf Grundlage der aktuellen Bedingungen erfolgen. Redundanzverlust wird gemeldet, wenn ein Netzteil entfernt wird oder ausfällt, oder wenn der tatsächliche Stromverbrauch die Kapazität einer einzelnen Netzteileinheit überschreitet. Dies ist die Standardregel.

Netzteilfehler

Netzteilfehler werden, unabhängig von der ausgewählten Redundanzregel, immer gemeldet.

Standard-Redundanzkonfiguration

Nur Redundanzwarnungen ist die Standard-Redundanzkonfiguration für ein Gehäuse und zwei Netzteile.

Multi-Knoten-Schlitten-Anpassung

Der PowerEdge FM120 ist ein Schlitten mit mehreren Knoten und halber Breite, der vier Server mit den zugehörigen iDRAC mit unabhängigen Prozessoren aufnehmen kann. Er ist auf eine optimale Energie-Effizienz ausgelegt, und die Prozessoren können nicht entfernt werden. Die Prozessoren im PowerEdge FM120x4 nutzen die gleiche Infrastruktur für die Stromversorgung, zum Beispiel gemeinsame Strom- und Temperatursensoren für den gesamten Schlitten.

Überwachung der Gehäusestromgrenze

Das Open Manage Power Center (OMPC) kann verwendet werden, um den Stromverbrauch der Computer in einem Rechenzentrum zu überwachen und zu steuern. PowerEdge FX2-/FX2s aktiviert OMPC durch Festlegen einer Stromobergrenze für das Gehäuse sowie von Einschränkungen für die Einstellung der Stromobergrenze. Die unteren und oberen Grenzwerte der Stromobergrenze werden durch den CMC festgelegt und können nicht konfiguriert werden.

ANMERKUNG: Die untere Stromgrenze ist die erforderliche Mindestleistung für den Betrieb des Gehäuses unter Berücksichtigung der aktuellen Konfiguration. Die obere Stromgrenze stellt die maximale Leistung gemäß der aktuellen Redundanzregel dar.

Anzeige des Stromverbrauchsstatus

Der CMC zeigt den tatsächlichen Eingangsstromverbrauch für das gesamte System auf der Seite Stromverbrauchsstatus an.

Anzeigen von Stromverbrauchsstatus über die CMC-Webschnittstelle

Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht → Strom → Stromüberwachung**. Die Seite „Stromüberwachung" zeigt Stromfunktionszustand, Systemstromstatus, Stromstatistik in Echtzeit und Energiestatistik in Echtzeit an. Weitere Informationen finden Sie in der *Online-Hilfe*.

ANMERKUNG: Der Stromredundanzstatus wird auch unter Netzteile angezeigt.

Anzeigen des Stromverbrauchsstatus mithilfe von RACADM

So zeigen Sie den Stromverbrauchsstatus mithilfe von RACADM an:

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

```
racadm getpminfo
```

Strombudgetstatus über die CMC-Webschnittstelle anzeigen

Wechseln Sie zum Anzeigen des Strombudgetstatus unter Verwendung der CMC Web-Schnittstelle im linken Fenster zu **Gehäuse-Übersicht**, und klicken Sie auf **Strom → Budgetstatus**. Auf der Seite **Strombudgetstatus** wird die Regelkonfiguration des Systemstroms mit den Attributen **Systemeingangsstrom-Obergrenze**, **Redundanzregel**, Strombudgetdetails mit den Attributen **Maximale System-Eingangsstromkapazität**, **Eingangsredundanz-Reserve**, **Verfügbarer Strom für**

Servereinschaltung sowie die Gehäusestromversorgung mit den Details zur Netzteileinheit angezeigt. Weitere Informationen finden Sie in der Online-Hilfe zu *CMC für Dell PowerEdge FX2/FX2s*.

Stromverbrauchsstatus mithilfe von RACADM anzeigen

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

```
racadm getpbinfo
```

Weitere Informationen zum Befehl **getpbinfo**, einschließlich der Ausgabedetails finden Sie im Befehlsabschnitt **getpbinfo** im Referenzhandbuch *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Dell Chassis Management Controller für PowerEdge FX2/FX2s).

Redundanzstatus und allgemeiner Stromzustand

Der Redundanzstatus ist ein Faktor zur Bestimmung des allgemeinen Stromzustands. Wenn die Stromredundanzregel beispielsweise auf „Wechselstromredundanz" festgelegt wird, und der Redundanzstatus anzeigt, dass das System mit Redundanz arbeitet, ist der allgemeine Stromzustand in der Regel **OK**. Wenn jedoch die Bedingungen für den Betrieb mit Wechselstromredundanz nicht erfüllt werden können, ist der Redundanzstatus **Keine** und der allgemeine Stromzustand **Kritisch**. Dies liegt daran, dass das System nicht in der Lage ist, in Übereinstimmung mit der konfigurierten Stromredundanzregel zu arbeiten.

ANMERKUNG: Der CMC führt keine Vorabprüfung dieser Bedingungen durch, wenn Sie die Redundanzregel auf oder von „Netzredundanz" ändern. Das Konfigurieren der Redundanzregel kann demzufolge unverzüglich zu Redundanzverlust oder zu einer wiedererlangten Bedingung führen.

Stromverwaltung nach Entdeckung von Netzteilfehlern

Für den Fall, dass eine Netzteileinheit ausfällt oder entfernt wird, kann die Stromversorgung des Servers reduziert werden. In extremen Fällen können Server ausgeschaltet werden, um den Betrieb aufrecht zu erhalten. Das Konfigurieren und Aufrechterhalten der Netzredundanz vermeidet negative Auswirkungen auf die Server bei Ausfall einer einzelnen Netzteileinheit.

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 16. SEL-Ereignisse für Netzteiländerungen

Netzteilereignis	Systemereignisprotokoll (SEL)-Eintrag
Einfügen	Netzteil ist vorhanden.
Entfernung	Netzteil ist nicht vorhanden.
Wechselstromeingang	Die Stromzufuhr vom Netzteil wurde wiederhergestellt.

Wechselstrom-Eingangsverlust	Verlust der Stromzufuhr vom Netzteil.
Gleichstromausgabe hergestellt	Netzteil funktioniert normal.
Gleichstromausgabeverlust	Netzteil fehlerhaft.

Ereignisse, die mit Änderungen des Stromredundanzstatus zusammenhängen und Einträge im SEL verursachen, sind Redundanzverlust und Redundanzwiederherstellung für das Gehäuse, das für die Redundanzregel **Netzredundanz** oder für die Redundanzregel **Nur Redundanzwarnungen** konfiguriert ist. Die folgende Tabelle listet die SEL-Einträge auf, die mit Änderungen der Stromredundanzregeln zusammenhängen.

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

Strombudget und Redundanz konfigurieren

Sie können das Strombudget, die Redundanz und die dynamische Energie des gesamten Gehäuses (Gehäuse, Server, E/A-Modul, PCIe, CMC und Gehäuse-Infrastruktur) konfigurieren. Der Stromverwaltungsdienst optimiert den Stromverbrauch und weist den verschiedenen Modulen entsprechend den Anforderungen Strom zu.

Sie können Folgendes konfigurieren:

- Systemeingangsstrom-Obergrenze
- Redundanzregel
- Netzschalter des Gehäuses deaktivieren
- Max. Stromkonservierungsmodus
- Remote-Stromprotokollierung
- Remote-Stromverbrauchsprotokollierungszeitraum

Stromeinsparung und Strombudget

Wenn der Stromverbrauch die Systemeingangsstrom-Obergrenze überschreitet, wird die Stromversorgung der Server über die Netzteile reduziert, um die nominelle Ebene aufrecht zu erhalten.

Konfigurieren von Stromversorgungsbudget und Redundanz über die CMC-Webschnittstelle

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, müssen Sie die Berechtigung als **Gehäusekonfigurations-Administrator** besitzen.

So konfigurieren Sie das Strombudget

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht → Strom → Konfiguration**.
2. Wählen Sie auf der Seite **Budget/Redundanzkonfiguration** jede oder alle der folgenden Eigenschaften, Ihren Anforderungen entsprechend, aus. Weitere Informationen zu den Feldbeschreibungen finden Sie in der *Online-Hilfe*.
   - **Redundanzregel**
   - **Netzschalter des Gehäuses deaktivieren**

- **Max. Stromkonservierungsmodus**

3. Klicken Sie auf **Anwenden**, um die Änderungen zu speichern.

Strombudget und Redundanz unter Verwendung von RACADM konfigurieren

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, müssen Sie die Berechtigung als **Gehäusekonfigurations-Administrator** besitzen.

So aktivieren Sie die Redundanz und legen die Redundanzregel fest:

1. Öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC und melden Sie sich an.
2. Legen Sie die Eigenschaften nach Bedarf fest:
   - Um eine Redundanzregel auszuwählen, geben Sie Folgendes ein:
     ```
     racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy <value>
     ```
     wobei <*Wert*> 0 (Keine Redundanz), 1 (Wechselstromredundanz) und 3 (Nur Redundanzwarnungen) ist. Der Standardwert ist 3.

     Zum Beispiel legt der folgende Befehl die Redundanzregel wie folgt fest:

     ```
     racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy 1
     ```
   - Um einen Wechselstrombudgetwert festzulegen, geben Sie Folgendes ein:
     ```
     racadm config -g cfgChassisPower -o cfgChassisPowerCap <value>
     ```
     wobei <*Wert*> eine Zahl zwischen der aktuellen Gehäusebelastungslaufzeit und 3371 ist und die maximale Stromgrenze in Watt angibt. Die Standardeinstellung ist 3371.
     Der folgende Befehl setzt zum Beispiel das maximale Strombudget mit 3371 Watt fest:

     ```
     racadm config -g cfgChassisPower -o cfgChassisPowerCap 3371
     ```
   - Geben Sie zum Anzeigen der oberen und der unteren Grenze Folgendes ein:
     ```
     racadm getconfig -g cfgchassispower -o cfgchassispowercap <lower,upper>
     bound
     ```
     wobei <*untere, obere*> die untere Grenze und die obere Grenze ist.
     ```
     racadm config -g cfgChassisPower -o cfgChassisPowerCap 3000
     ```
   - Um den Modus für maximalen Stromverbrauch zu aktivieren, geben Sie Folgendes ein:
     ```
     racadm config -g cfgChassisPower -o cfgChassisMaxPowerConservationMode 1
     ```
   - Um den Normalbetrieb wiederherzustellen, geben Sie Folgendes ein:
     ```
     racadm config -g cfgChassisPower -o cfgChassisMaxPowerConservationMode 0
     ```
   - Geben Sie zur Aktivierung der Remote-Stromverbrauchsprotokollierungsfunktion den folgenden Befehl ein:
     ```
     racadm config -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingEnabled 1
     ```
   - Geben Sie zur Angabe des gewünschten Protokollierungszeitraums den folgenden Befehl ein:
     ```
     racadm config -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingInterval n
     ```
     wobei *n* 1-1440 Minuten sein kann.
   - Geben Sie zur Bestimmung dessen, ob die Remote-Stromverbrauchsprotokollierungsfunktion aktiviert ist den folgenden Befehl ein:
     ```
     racadm getconfig -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingEnabled
     ```
   - Geben Sie zur Bestimmung des Remote-Stromverbrauchsprotokollierungszeitraums den folgenden Befehl ein:
     ```
     racadm getconfig -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingInterval
     ```

Die Remote-Stromverbrauchsprotokollierungsfunktion hängt von den bereits konfigurierten Remote-Syslog-Hosts ab. Die Protokollierung auf einem oder mehreren Remote-Syslog-Hosts muss aktiviert sein, anderenfalls wird der Stromverbrauch nicht protokolliert. Dies kann entweder mittels der Web-GUI oder RACADM-CLI erfolgen. Weitere Informationen finden Sie in der Anleitung zur Remote-Syslog-Konfiguration.

- Um die 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 Referenzhandbuch *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Dell Chassis Management Controller für PowerEdge FX2/FX2s).

Stromsteuerungsvorgänge ausführen

Sie können den folgenden Stromsteuerungsvorgang für das Gehäuse, Server und die E/A-Module ausführen.

ANMERKUNG: Stromsteuerungsvorgänge wirken sich auf das gesamte Gehäuse aus.

Durchführen von Energieverwaltungsmaßnahmen am Gehäuse

Mit dem CMC können Sie im Remote-Zugriff verschiedene Stromverwaltungsmaßnahmen auf dem gesamten Gehäuse (Gehäuse, Server, E/A-Module und Netzteileinheiten) ausführen, z. B. ordnungsgemäßes Herunterfahren.

Energieverwaltungsmaßnahmen am Gehäuse über die Webschnittstelle durchführen

So führen Sie auf dem Gehäuse Stromsteuerungsvorgänge unter Verwendung der CMC-Webschnittstelle durch:

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht Strom → Steuerung**.
   Die Seite **Gehäuse-Stromsteuerung** wird angezeigt.
2. Wählen Sie eine der folgenden Stromsteuerungsoptionen aus.
   Weitere Informationen zu jeder Option finden Sie in der *Online-Hilfe*.
   - **System einschalten**
   - **System ausschalten**
   - **System aus- und wieder einschalten (Hardwareneustart)**
   - **Reset CMC (Warmstart)**
   - **Nicht-ordentliches Herunterfahren**
3. Klicken Sie auf **Anwenden**.
   Ein Dialogfeld wird eingeblendet, das Sie zur Bestätigung auffordert.
4. Klicken Sie auf **OK**, um die Energieverwaltungsmaßnahme auszuführen (z. B. das System zurückzusetzen).

Energieverwaltungsmaßnahmen am Gehäuse über RACADM durchführen

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

```
racadm chassisaction -m chassis <action>
```

wobei <*Maßnahme*> powerup, powerdown, powercycle, nongraceshutdown oder reset ist.

Stromsteuerungsvorgänge für mehrere Server unter Verwendung der CMC-Webschnittstelle ausführen

So führen Sie Stromsteuerungsvorgänge unter Verwendung der Webschnittstelle für mehrere Server durch:

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

   Die Seite **Energiesteuerung** wird angezeigt.
2. In der Spalte **Vorgänge** des Drop-Down-Menüs, Wählen Sie einen der nachfolgenden Stromsteuerungsvorgänge für die erforderlichen Server aus:
   - **Kein Vorgang**
   - **Ordentliches Herunterfahren**
   - **Server einschalten**
   - **Server ausschalten**
   - **Server zurücksetzen (Softwareneustart)**
   - **Server aus- und einschalten (Hardwareneustart)**

   Weitere Informationen zu den Optionen finden Sie in der *Online-Hilfe zu CMC für Dell PowerEdge FX2/FX2s*.
3. Klicken Sie auf **Apply** (Anwenden).

   Daraufhin werden Sie über ein Dialogfeld zur Bestätigung des Vorgangs aufgefordert.
4. Klicken Sie auf **OK**, um die Stromverwaltungsmaßnahme durchzuführen (z. B. den Server zurückzusetzen).

Stromsteuerungsvorgänge für ein E/A-Modul ausführen

Sie können im Remote-Zugriff ein E/A-Modul zurücksetzen oder einschalten.

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchzuführen, benötigen Sie **Administratorrechte für die Gehäusesteuerung**.

Stromsteuerungsvorgänge auf EAM unter Verwendung der CMC-Webschnittstelle ausführen

So führen Sie auf einem E/A-Modul Stromsteuerungsvorgänge aus:

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht → E/A-Modul-Übersicht → Strom**.
2. Wählen Sie auf der Seite **Stromsteuerung** für EAM aus dem Drop-Down-Menü den Vorgang aus, den Sie ausführen möchten (Aus- und einschalten).
3. Klicken Sie auf **Anwenden**.

Energieverwaltungsmaßnahmen am EAM über RACADM durchführen

Um auf einem EAM Stromsteuerungsvorgänge unter Verwendung von RACADM auszuführen, öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole zum CMC, melden Sie sich an und geben Sie Folgendes ein:

```
racadm chassisaction -m switch <action>
```

wobei <*Maßnahme*> den Vorgang anzeigt, den Sie ausführen möchten: Aus- und Einschalten.

Weitere Informationen über die RACADM-Befehle finden Sie im Referenzhandbuch *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-

Befehlszeilen-Referenzhandbuch für Dell Chassis Management Controller für PowerEdge FX2/FX2s) unter dell.com/support/manuals.

Konfigurieren des Schlitten-Netzschalters

Sie können den Schlitten-Netzschalter auf deaktivieren konfigurieren, sodass wenn Sie den Schlitten-Netzschalter drücken, dies keine Auswirkung hat. Wechseln Sie zum Konfigurieren des Schlitten-Netzschalters zu **Gehäuseübersicht → Server-Übersicht → Strom → Steuerung**

Aktivieren bzw. deaktivieren Sie im Abschnitt **Eigenschaften** das Kontrollkästchen, um den Netzschalter zu aktivieren bzw. zu deaktivieren.

ANMERKUNG: Diese Einstellung gilt nur für die im Gehäuse vorhandenen Multi-Knoten-Schlitten. Andere Schlitten sind davon nicht betroffen.

16

Anzeigen von PCIe-Steckplätzen

Die PowerEdge FX2-/FX2s-Gehäuse verfügen optional über acht PCIe-Steckplätze, wobei jeder davon einem bestimmten Schlitten zugewiesen ist. Standardmäßig werden alle PCIe-Steckplätzen zugeordnet. Die Zuweisung der PCIe-Steckplätze zu den Servern kann nicht geändert oder aufgehoben werden.

PCIe-Steckplatz	Zuordnung für PowerEdge FC630
PCIe-Steckplatz 1	4
PCIe-Steckplatz 2	4
PCIe-Steckplatz 3	2
PCIe-Steckplatz 4	2
PCIe-Steckplatz 5	3
PCIe-Steckplatz 6	3
PCIe-Steckplatz 7	1
PCIe-Steckplatz 8	1

ANMERKUNG: Die PCIe-Verwaltung wird nur für PowerEdge FX2s und nicht für PowerEdge FX2 unterstützt.

Weitere Informationen zum Verwalten von PCIe-Steckplätzen finden Sie in der *Online-Hilfe zu CMC für Dell PowerEdge FX2/FX2s*.

ANMERKUNG: Die agentenlose Überwachung ist für PCIe PERC- und Netzwerkkarten in den Gehäuse-PCIe-Steckplätzen nicht verfügbar. Die agentenlose Überwachung ist die Systemverwaltungslösung für Dell Server der 12. Generation, die vollständig bandextern und unabhängig von Betriebssystem-Agenten erfolgt. Mit der agentenlosen Überwachung können Sie den an die Server-Netzwerkgeräte (PERCs, Festplatten, Gehäuse usw.) angeschlossenen Speicher mit iDRAC überwachen, ohne einen Agenten auf dem verwalteten System oder auf der Management Station installieren zu müssen. Weitere Informationen zur agentenlosen Überwachung finden Sie im Whitepaper *Agent-free inventory and monitoring for storage and network devices in Dell PowerEdge 12G Servers* (Agentenlose Bestandsaufnahme und Überwachung von Speicher- und Netzwerkgeräten für Dell PowerEdge-Server der 12. Generation) im Dell TechCenter.

Anzeigen von PCIe-Steckplatz-Eigenschaften unter Verwendung der CMC Web-Schnittstelle

- Um die Informationen über alle acht PCIe-Steckplätze im linken Fensterbereich anzuzeigen, klicken Sie auf **Gehäuseübersicht → PCIe-Übersicht**. Klicken Sie auf das + , um alle Eigenschaften für den erforderlichen Steckplatz anzuzeigen.

- Um die Informationen eines PCIe-Steckplatzes anzuzeigen, klicken Sie auf **Gehäuseübersicht → PCIe-Steckplatz <Nummer> → Eigenschaften → Status**.

Anzeigen von PCIe-Steckplatz-Eigenschaften mit RACADM

Sie können die Zuweisung eines PCIe-Steckplatzes zu einem Server mithilfe der RACADM-Befehle anzeigen. Einige der Befehle werden hier aufgeführt. Weitere Informationen über RACADM-Befehle finden Sie im Referenzhandbuch *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (RACADM-Befehlszeilen-Referenzhandbuch für Dell Chassis Management Controller für PowerEdge FX2/FX2s) unter dell.com/support/manuals.

ANMERKUNG: Der PCIe-Kartenname wird nur angezeigt, wenn das BIOS den `POST`-Test im zugehörigen sSled abschließt. Bis dahin wird der Gerätename als **Unbekannt** angezeigt.

- Führen Sie zum Anzeigen der aktuellen Zuweisung der PCIe-Geräte zu Servern den folgenden Befehl aus:

  ```
  racadm getpciecfg -a
  ```

- Führen Sie zum Anzeigen der Eigenschaften für PCIe-Geräte mithilfe von FQDD den folgenden Befehl aus:

  ```
  racadm getpciecfg [-c <FQDD>]
  ```

  Um zum Beispiel die Eigenschaften von PCIe-Gerät 1 anzuzeigen, führen Sie den folgenden Befehl aus.

  ```
  racadm getpciecfg -c pcie.chassisslot.1
  ```

ANMERKUNG: Die PCIe-Karte kann nicht eingeschaltet werden, wenn die Mezzanine-Karte auf dem zugehörigen Schlitten nicht vorhanden ist.

17

Fehlerbehebung und Wiederherstellung

Dieser Abschnitt erklärt, wie Tasks unter Verwendung der CMC-Webschnittstelle ausgeführt werden, die sich auf die Wiederherstellung und Behebung eines Problems auf dem Remote-System beziehen.

- Gehäuseinformationen anzeigen.
- Ereignisprotokolle anzeigen.
- Konfigurationsinformationen, Fehlerstatus und Fehlerprotokolle sammeln.
- Diagnosekonsole verwenden.
- Strom auf einem Remote-System verwalten.
- Lifecycle Controller-Aufträge auf einem Remote-System verwalten.
- Komponenten zurücksetzen.
- Fehlerbehebung bei Network Time Protocol (NTP)-Problemen.
- Fehlerbehebung bei Netzwerkproblemen.
- Fehlerbehebung bei Warnmeldungsproblemen.
- Vergessenes Administratorkennwort zurücksetzen.
- Gehäusekonfigurationseinstellungen und Zertifikate speichern und wiederherstellen.
- Fehlercodes und -protokolle anzeigen.

Konfigurationsinformationen, Gehäusestatus und Protokolle über 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 fasst die folgenden RACADM-Befehle zusammen. Weitere Informationen zu `racdump` finden Sie im Referenzhandbuch *Dell Chassis Management*

Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide (RACADM-Befehlszeilen-Referenzhandbuch für Dell Chassis Management Controller für PowerEdge FX2/FX2s).

Untersystem	RACADM-Befehl
Allgemeine System-/RAC-Informationen	`getsysinfo`
Sitzungsinformationen	`getssninfo`
Sensorinformationen	`getsensorinfo`
Switches-Informationen (EA-Modul)	`getioinfo`
Mezzanine-Karteninformationen (Tochterkarte)	`getdcinfo`
Informationen zu allen Modulen	`getmodinfo`
Strombudgetinformationen	`getpbinfo`
NIC-Informationen (CMC-Modul)	`getniccfg`
Ablaufverfolgungsprotokollinformationen	`gettracelog`
RAC-Ereignisprotokoll	`getraclog`
System-Ereignisprotokoll	`getsel`

Herunterladen der SNMP-MIB-Datei Verwaltungsinformationsbasis

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

So laden Sie die CMC-SNMP-MIB-Datei Verwaltungsinformationsbasis über die Web-Schnittstelle herunter:

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht → Netzwerk → Dienste → SNMP**.
2. Klicken Sie im Abschnitt **SNMP-Konfiguration** auf **Speichern**, um die CMC-**MIB**-Datei auf Ihr lokales System herunterzuladen.

   Weitere Informationen zur SNMP-**MIB**-Datei finden Sie im *Dell OpenManage Server Administrator SNMP Reference Guide* (Dell OpenManage Server Administrator-SNMP-Referenzhandbuch) unter **dell.com/support/manuals**.

Erste Schritte, um Störungen an einem Remote-System zu beheben

Die folgenden Fragen werden häufig für die Fehlerbehebung bei Problemen auf hoher Ebene auf dem verwalteten System gestellt:

- Ist das System ein- oder ausgeschaltet?
- Wenn eingeschaltet, funktioniert das Betriebssystem, antwortet es nicht oder reagiert es nicht mehr?
- Wenn ausgeschaltet, wurde der Strom unerwartet ausgeschaltet?

Strombezogene Fehlerbehebung

Die folgenden Informationen sind Ihnen bei der Fehlerbehebung bei Netzteilen und bei der Stromversorgung hilfreich:

- **Problem:** Die **Stromredundanzregel** ist auf **Netzredundanz** eingestellt und es wurde ein Keine-Netzteilredundanz-Ereignis gemeldet.
  - **Lösung A:** Für diese Konfiguration muss das Netzteil auf Seite 1 (linker Steckplatz) und das Netzteil auf Seite 2 (rechter Steckplatz) im Gehäuse vorhanden und funktionsfähig sein. Außerdem muss die Kapazität jedes Netzteils ausreichen, um die gesamte Stromzuteilung für das Gehäuse zu unterstützen und die **Netzredundanz** aufrecht zu erhalten.
  - **Lösung B:** Prüfen Sie, ob alle Netzteile ordnungsgemäß an die beiden Wechselstromnetze angeschlossen sind: das Netzteil auf Seite 1 muss mit dem einen Wechselstromnetz verbunden sein, und das Netzteil auf Seite 2 muss mit dem anderen Wechselstromnetz verbunden sein. Beide Wechselstromnetze müssen funktionieren. Die **Netzredundanz** fällt aus, wenn eines der Wechselstromnetze nicht funktioniert.
- **Problem:** Der Zustand der Netzteileinheit wird als **Fehlgeschlagen (Kein Wechselstrom)** angezeigt, selbst wenn ein Netzkabel angeschlossen ist und der Stromverteiler ausreichenden Wechselstromausgang erzeugt.
  - **Lösung A:** Das Netzkabel prüfen und ersetzen. Prüfen und verifizieren Sie, dass der Stromverteiler, der Strom an das Netzteil liefert, ordnungsgemäß funktioniert. Falls der Fehler nach wie vor besteht, rufen Sie den Dell-Kundendienst an, um das Netzteil zu ersetzen.
  - **Lösung B:** Überprüfen Sie, ob die Netzteileinheit an dieselbe Spannung angeschlossen ist wie die anderen Netzteileinheiten. Wenn der CMC feststellt, dass eine Netzteileinheit mit einer anderen Spannung arbeitet, dann wird die Netzteileinheit ausgeschaltet und als „Fehlerhaft" markiert.
- **Problem:** 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.
- **Problem:** Verfügbare Leistung schwankt, selbst wenn die Gehäusekonfiguration nicht verändert wurde.
  - **Lösung:** CMC verfügt über dynamisches Lüfterleistungsmanagement, das Serverstromzuweisungen kurzzeitig verringert, wenn das Gehäuse im Bereich der benutzerseitig konfigurierten maximalen Leistungsgrenze (Spitze) betrieben wird; es bewirkt, dass den Lüftern Strom durch Verringerung von Serverleistung zugewiesen wird, so dass die Eingangsleistungsaufnahme unterhalb der **Eingangsleistungsgrenze des Systems** gehalten werden kann. Dieses Verhalten ist normal.
- **Problem:** 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-Sendeversuchs wird im CMC-Protokoll gespeichert. Zusätzliche Informationen, die die einzelnen Fehler beschreiben, werden im Ablaufverfolgungsprotokoll gespeichert. Da SNMP jedoch die Übermittlung von Traps nicht bestätigt, ist

es am besten, die Pakete auf dem verwalteten System mit Hilfe eines Netzwerkanalysators oder eines Hilfsprogramms wie snmputil von Microsoft zu verfolgen.

Ereignisprotokolle anzeigen

Sie können Hardware- und Gehäuseprotokolle für Informationen über systemkritische Ereignisse, die auf dem verwalteten System auftreten, anzeigen.

Hardwareprotokoll anzeigen

Der CMC erstellt ein Hardwareprotokoll von Ereignissen, die im Gehäuse auftreten. Sie können das Hardwareprotokoll über die Webschnittstelle und Remote-RACADM anzeigen.

ANMERKUNG: Um das Hardwareprotokoll zu löschen, müssen Sie die Berechtigung als **Administrator zum Löschen von Protokollen** besitzen.

ANMERKUNG: Sie können CMC so konfigurieren, dass E-Mail- oder SNMP-Traps gesendet werden, wenn spezifische Ereignisse auftreten.

Beispiele von Hardwareprotokolleinträgen

```
critical System Software event: redundancy lost Wed May 09 15:26:28 2007 normal
System Software event: log cleared was asserted Wed May 09 16:06:00 2007
warning System Software event: predictive failure was asserted Wed May 09
15:26:31 2007 critical System Software event: log full was asserted Wed May 09
15:47:23 2007 unknown System Software event: unknown event
```

Gehäuseprotokoll anzeigen

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

ANMERKUNG: Um das Gehäuseprotokoll zu löschen, müssen Sie die Berechtigungen als **Administrator zum Löschen von Protokollen** aufweisen.

Diagnosekonsole verwenden

Wenn Sie ein fortgeschrittener Benutzer oder ein Benutzer unter der Leitung des technischen Supports sind, können Sie Probleme im Zusammenhang mit der Gehäuse-Hardware unter Verwendung von CLI-Befehlen diagnostizieren.

ANMERKUNG: Um diese Einstellungen zu ändern, müssen Sie Berechtigungen als **Administrator für Debug-Befehle** haben.

So greifen Sie auf die Seite „Diagnosekonsole" zu:

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht → Fehlerbehebung → Diagnose**.
   Die Seite **Diagnosekonsole** wird angezeigt.
2. Geben Sie im Textfeld **Befehl** einen Befehl ein und klicken Sie auf **Senden.**
   Weitere Informationen zu den Befehlen finden Sie in der *Online-Hilfe*.

   Es wird eine Seite mit Diagnoseergebnissen eingeblendet.

Komponenten zurücksetzen

Sie können den CMC zurücksetzen oder Server virtuell neu einsetzen und somit bewirken, dass sie sich so verhalten, als seien sie herausgenommen und wieder eingesetzt worden.

ANMERKUNG: Zum Zurücksetzen von Komponenten müssen Sie die Berechtigung als **Debug-Befehl-Administrator** besitzen.

ANMERKUNG: Der virtuelle Neustart ist für die einzelnen Knoten des PowerEdge FM120x4 nicht verfügbar.

So setzen Sie die Komponenten bei Verwendung der CMC-Webschnittstelle zurück:

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht → Fehlerbehebung → Komponenten zurücksetzen**.

   Die Seite **Aktualisierbare Komponenten** wird angezeigt.
2. Klicken Sie zum Zurücksetzen des CMC im Abschnitt **CMC-Status** auf **CMC zurücksetzen**. Der vorhandene CMC wird neu gestartet.

Weitere Informationen finden Sie in der *Online-Hilfe zu CMC für Dell PowerEdge FX2/FX2s*.

Gehäusekonfiguration speichern oder wiederherstellen.

Dies ist eine lizenzierte Funktion. So führen Sie eine Speicherung oder Wiederherstellung einer Gehäusekonfiguration unter Verwendung der CMC Webschnittstelle durch:

ANMERKUNG: FlexAddress-Informationen, Serverprofile und der erweiterte Speicher können nicht mit der Gehäusekonfiguration gespeichert oder wiederhergestellt werden. Es wird empfohlen, wichtige Serverprofile separat vom Gehäuse auf einer Remote-Dateifreigabe oder als Kopie auf einer lokalen Workstation zu speichern. Weitere Informationen zu diesem Vorgang finden Sie im Abschnitt Hinzufügen oder Speichern eines Profils.

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht → Setup → Gehäuse-Backup**. Die Seite **Gehäuse-Backup** wird angezeigt. Klicken Sie auf **Speichern**, um die Gehäusekonfiguration zu speichern. Überschreiben Sie den Standarddateipfad (optional) und klicken Sie auf **OK**, um die Datei zu speichern. Der standardmäßige Sicherungsdateiname enthält die Service-Tag-Nummer des Gehäuses. Diese Sicherungsdatei kann später verwendet werden, um die Einstellungen und Zertifikate für dieses eine Gehäuse wiederherzustellen.
2. Klicken Sie zum Wiederherstellen der Gehäusekonfiguration im Abschnitt „Wiederherstellen“ auf **Durchsuchen**, geben Sie die Sicherungsdatei an, und klicken Sie dann auf **Wiederherstellen**.

   ANMERKUNG: CMC wird beim Wiederherstellen der Konfiguration nicht zurückgesetzt, jedoch kann es einige Zeit dauern, bis jedwede geänderte oder neue Konfiguration effektiv durch die CMC-Dienste durchgesetzt wird. Nach der erfolgreichen Fertigstellung werden alle aktuellen Sitzungen beendet.

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 danach noch immer keine Änderung auftritt, handelt es sich möglicherweise um ein Problem, das

untersucht werden muss. Der CMC kann seine Uhr möglicherweise aus folgenden Gründen nicht synchronisieren:

- Es könnte ein Problem mit den NTP-Server 1-, NTP-Server 2- und NTP-Server 3-Einstellungen vorliegen.
- Es wurden versehentlich ein ungültiger Hostname oder eine ungültige IP-Adresse eingegeben.
- Es könnte ein Netzwerkverbindungsproblem geben, das verhindert, dass der CMC mit den konfigurierten NTP-Servern kommunizieren kann.
- Es könnte ein DNS-Problem geben, das verhindert, dass NTP-Server-Hostnamen aufgelöst werden können.

Überprüfen Sie zur Behebung von Fehlern, die mit NTP in Verbindung stehen, die Informationen im CMC-Ablaufverfolgungsprotokoll. Dieses Protokoll enthält eine Fehlermeldung für NTP-bezogene Ausfälle. Falls der CMC sich nicht mit einem konfigurierten NTP-Server synchronisieren kann, dann ist CMC-Zeit mit der lokalen Systemuhr synchronisiert und das Ablaufverfolgungsprotokoll enthält einen Eintrag der folgenden Art:

```
Jan 8 20:02:40 cmc ntpd[1423]: synchronized to LOCAL(0), stratum 10
```

Sie können den ntpd-Status auch prüfen, indem Sie den folgenden racadm-Befehl eingeben:

```
racadm getractime –n
```

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

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

Um den Parameter zu ändern, geben Sie folgenden Befehl ein:

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpMaxDist 32
```

Nach Durchführung der Änderung deaktivieren Sie NTP, warten Sie 5-10 Sekunden und dann aktivieren Sie den NTP neu.

ANMERKUNG: NTP könnte drei zusätzliche Minuten benötigen, um neu zu synchronisieren.

Um NPT zu deaktivieren, geben Sie Folgendes ein:

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpEnable 0
```

Um NPT zu aktivieren, geben Sie Folgendes ein:

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpEnable 1
```

Wenn die NTP-Server richtig konfiguriert sind und dieser Eintrag im Ablaufverfolgungsprotokoll steht, dann bestätigt dies, dass sich der CMC nicht mit einem der konfigurierten NTP-Server synchronisieren kann.

Wenn die NTP-Server-IP-Adresse nicht konfiguriert ist, könnte ein Eintrag der folgenden Art vorhanden sein:

```
Jan 8 19:59:24 cmc ntpd[1423]: Cannot find existing interface for address
1.2.3.4 Jan 8 19:59:24 cmc ntpd[1423]: configuration of 1.2.3.4 failed
```

Falls eine NTP-Server-Einstellung mit einem ungültigen Hostnamen konfiguriert wurde, enthält das Ablaufverfolgungsprotokoll u. U. einen Eintrag der folgenden Art:

```
Aug 21 14:34:27 cmc ntpd_initres[1298]: host name not found: blabla Aug 21
14:34:27 cmc ntpd_initres[1298]: couldn't resolve `blabla', giving up on it
```

Weitere Informationen zur Eingabe des Befehls `gettracelog` zur Prüfung des Ablaufverfolgungsprotokolls unter Verwendung der CMC-Schnittstelle finden Sie unter „Diagnosekonsole verwenden".

LED-Farben und Blinkmuster interpretieren

Die LEDs im Gehäuse geben den folgenden Status einer Komponente an:

- Eine blinkende gelbe LED an einem Modul weist auf einen Fehler in diesem Modul hin.
- Blau blinkende LEDs können vom Benutzer konfiguriert und zur Identifikation genutzt werden. Weitere Informationen zur Konfiguration von finden Sie unter CMC_Stmp_Konfigurieren von LEDs zum Identifizieren von Komponenten im Gehäuse.

Tabelle 17. LED-Farbe und Blinkmuster

Komponente	LED-Farbe, Blinkmuster	Status
CMC		Eingeschaltet
		Firmware wird hochgeladen
		Ausgeschaltet
	Blau, beständig leuchtend	Aktiv
	Blau blinkend	Vom Benutzer aktivierte Modulidentifizierung
	Gelb, beständig leuchtend	Nicht verwendet
	Gelb blinkend	Fehler
Server		Eingeschaltet
		Firmware wird hochgeladen
		Ausgeschaltet
	Blau, beständig leuchtend	Server ist auf dem KVM ausgewählt
	Blau blinkend	Vom Benutzer aktivierte Modulidentifizierung
	Gelb, beständig leuchtend	Nicht verwendet
	Gelb blinkend	Fehler
	Blau, dunkel	Kein Fehler
E/A-Modul (Allgemein)	Grün, beständig leuchtend	Eingeschaltet
	Grün, blinkend	Firmware wird hochgeladen
	Grün, dunkel	Ausgeschaltet
	Blau, beständig leuchtend	Normal/übergeordneter Stapel

Komponente	LED-Farbe, Blinkmuster	Status
	Blau blinkend	Vom Benutzer aktivierte Modulidentifizierung
	Gelb, beständig leuchtend	Nicht verwendet
	Gelb blinkend	Fehler
	Blau, dunkel	Kein Fehler/untergeordneter Stapel
E/A (Passthrough)	Grün, beständig leuchtend	Eingeschaltet
	Grün, blinkend	Nicht verwendet
	Grün, dunkel	Ausgeschaltet
	Blau, beständig leuchtend	Normal
	Blau blinkend	Vom Benutzer aktivierte Modulidentifizierung
	Gelb, beständig leuchtend	Nicht verwendet
	Gelb blinkend	Fehler
	Blau, dunkel	Kein Fehler
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
PCI	Blau, dunkel	Eingeschaltet
	Blau blinkend	PCI-Identifizierung wird ausgeführt.
	Gelb blinkend	Fehler

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.

Problem durch Beobachtung der LEDs erkennen

Der CMC verfügt über eine LED-Farbe, um mithilfe von Farbänderungen Folgendes anzuzeigen:

Farbe	Beschreibung
Blau	Normaler Betrieb
Blau blinkend	ID (0,5 Sekunden Ein, 0,5 Sekunden Aus)
Gelb	Gehäusefehlerzusammenfassung
Gelb blinkend	Gehäusefehler mit gleichzeitiger ID

Wiederherstellungsinformationen über die serielle DB-9-Schnittstelle abrufen

Wenn die untere CMC-LED gelb leuchtet, stehen über die serielle DB-9-Schnittstelle, die sich an der Vorderseite des CMC befindet, Wiederherstellungsinformationen zur Verfügung.

So rufen Sie Wiederherstellungsinformationen ab:

1. Installieren Sie ein NULL-Modemkabel zwischen einem CMC-System und einem Client-Computer.
2. Öffnen Sie einen Terminalemulator Ihrer Wahl (z. B. HyperTerminal oder Minicom). Stellen Sie Folgendes ein,wenn Sie dazu aufgefordert werden: 8 Bit, keine Parität, keine Ablaufsteuerung, Baudrate 115200.

   Bei einem Kernspeicherfehler wird alle 5 Sekunden eine Fehlermeldung angezeigt.
3. Drücken Sie die Eingabetaste.

   Wenn die Eingabeaufforderung Wiederherstellung angezeigt wird, stehen zusätzliche Informationen zur Verfügung. Die Eingabeaufforderung zeigt die CMC-Steckplatznummer und den Fehlertyp an.

   Um die Ursache des Fehlers und die Syntax für einige Befehle anzuzeigen, geben Sie `recover` ein und dann drücken Sie die Taste <Eingabe>.

   Beispiele von Eingabeaufforderungen:

   ```
   recover1[self test] CMC self test failure
   ```

   ```
   recover1[Bad FW images] CMC has corrupted images
   ```

   - Wenn die Eingabeaufforderung auf einen Selbsttestfehler hinweist, befinden sich keine betriebsfähigen Komponenten auf dem CMC. Der CMC ist unbrauchbar und muss zu Dell zurückgesendet werden.
   - Wenn die Eingabeaufforderung **Beschädigte Firmware-Images** anzeigt, führen Sie die Tasks in Wiederherstellen von Firmware-Image 1 aus.

Firmware-Image wiederherstellen

Der CMC geht in den Wiederherstellungsmodus über, wenn ein normaler Start des CMC-Betriebssystems nicht möglich ist. Im Wiederherstellungsmodus steht ein kleiner Teilsatz an Befehlen zur Verfügung, mit denen Sie Flash-Geräte durch Hochladen der Firmware-Aktualisierungsdatei **fx2_cmc.bin** neu

programmieren können. Dies ist dieselbe Firmware-Image-Datei, die auch für normale Firmware-Aktualisierungen verwendet wird. Der Wiederherstellungsvorgang zeigt die laufende Aktivität an und startet am Ende das CMC-Betriebssystem.

Wenn Sie recover eingeben und dann bei der Eingabeaufforderung zur Wiederherstellung die Taste <Eingabe> drücken, werden der Wiederherstellungsgrund und die verfügbaren Unterbefehle angezeigt. Ein Beispiel einer Wiederherstellungsabfolge könnte folgendermaßen lauten:

```
recover getniccfg recover setniccfg 192.168.0.120 255.255.255.0 192.168.0.1
recover ping 192.168.0.100 recover fwupdate -g -a 192.168.0.100
```

ANMERKUNG: Schließen Sie das Netzwerkkabel an den RJ45 ganz links an.

ANMERKUNG: Im Wiederherstellungsmodus können Sie den CMC normalerweise nicht pingen, da kein aktiver Netzwerkstapel vorhanden ist. Mit dem Befehl `recover ping <TFTP-Server-IP>` können Sie den TFTP-Server pingen, um die LAN-Verbindung zu überprüfen. Möglicherweise müssen Sie auf einigen Systemen den Befehl `recover reset` nach `setniccfg` verwenden.

Fehlerbehebung bei Netzwerkproblemen

Mit dem internen CMC-Ablaufverfolgungsprotokoll können Sie CMC-Warnmeldungen und den CMC-Netzwerkbetrieb debuggen. Sie können auf das Protokoll unter Verwendung der CMC Web-Schnittstelle oder von RACADM zugreifen. Weitere Informationen zum gettracelog-Befehl finden Sie im Abschnitt zum `gettracelog`-Befehl im Referenzhandbuch *RACADM Command Line Reference Guide for iDRAC and CMC* (RACADM-Befehlszeilen-Referenzhandbuch für iDRAC 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.

Allgemeine Fehlerbehebung

Wenn nach Abschluss eines Vorgangs eine Bestätigungsmeldung angezeigt wird, z. B. nach dem Speichern eines Serverprofils, kann es dennoch vorkommen, dass die Maßnahme nicht wirksam ist.

Um dieses Problem zu beheben, prüfen Sie, ob die CMC-Dienstschnittstellen für SSH, Telnet, HTTP oder HTTPS Schnittstellen benutzen, die in der Regel vom Betriebssystem verwendet werden, z. B. die Schnittstelle 111. Wenn dies der Fall ist, ändern Sie die Einstellungen so, dass eine nicht reservierte Schnittstelle verwendet wird. Weitere Informationen über reservierte Ports finden Sie unter http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml.

18

Häufig gestellte Fragen

In diesem Abschnitt werden häufig gestellte Fragen zu den folgenden Themen aufgelistet:

- RACADM
- Remote-System verwalten und wiederherstellen
- Active Directory
- EAM

RACADM

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

```
racadm <subcommand> Transport: ERROR: (RC=-1)
```

Was bedeutet diese Meldung?

Ein anderer Befehl muss nur dann ausgegeben werden, nachdem CMC-Reset abgeschlossen ist.

Durch die Verwendung der RACADM-Unterbefehle wird manchmal ein oder mehrere der folgenden Fehler angezeigt:

- Lokale RACADM-Fehlermeldungen - Probleme wie Syntax, typografische Fehler und falsche Namen. Beispiel: `ERROR: <message>`

Verwenden Sie den RACADM-Unterbefehl `help`, um richtige Syntax- und Anwendungsinformationen anzuzeigen. Wenn Sie zum Beispiel einen Fehler im Löschen eines Gehäuseprotokolls haben, führen Sie den folgenden Unterbefehl aus.

```
racadm chassislog help clear
```

Fehlermeldungen, die sich auf den CMC beziehen – Probleme, bei denen der CMC keine Maßnahme durchführen kann. Die folgende Fehlermeldung wird angezeigt:

```
racadm command failed (racadm-Befehl fehlerhaft).
```

Um Informationen über ein Gehäuse anzuzeigen, geben Sie den folgenden Befehl ein.

```
racadm gettracelog
```

Während ich Firmware-RACADM verwendet habe, wechselt die Eingabeaufforderung zu „>“ und die Eingabeaufforderung „$“ wird nicht wieder angezeigt.

Wenn ein doppeltes Anführungszeichen (") oder ein einfaches Anführungszeichen (') nicht paarig als Teil des Befehls eingegeben wird, dann wechselt die Befehlszeile zur Aufforderung „>“ und stellt alle Befehle in die Warteschlange.

Um zur Eingabeaufforderung „$“ zurückzukehren, geben Sie <Strg>–d ein.

Eine Fehlermeldung `Not Found` wird beim Verwenden der Befehle `$ logout` und `$ quit` angezeigt.

Remote-System verwalten und wiederherstellen

Wenn ich auf die CMC-Schnittstelle zugreife, erhalte ich eine Sicherheitswarnung, die besagt, dass der Host-Name des SSL-Zertifikats nicht mit dem Host-Namen des CMC übereinstimmt.

Der CMC enthält ein Standard-CMC-Serverzertifikat zur Sicherung der Netzwerksicherheit für die Webschnittstelle und die Remote-RACADM-Funktionen. Wenn dieses Zertifikat verwendet wird, zeigt der Webbrowser eine Sicherheitswarnung an, weil das Standardzertifikat als CMC-Standardzertifikat ausgegeben wird, was nicht mit dem Host-Namen des CMC (z. B. IP-Adresse) übereinstimmt.

Um dieses Sicherheitsproblem zu beseitigen, laden Sie ein CMC-Serverzertifikat herunter, das auf die IP-Adresse des CMC ausgestellt ist. Wenn Sie die Zertifikatsignierungsanforderung (CSR) zur Ausgabe des Zertifikats erstellen, müssen Sie sicherstellen, dass der allgemeine Name (CN) des CSR der IP-Adresse des CMC (z. B. 192.168.0.120) oder dem eingetragenen DNS-CMC-Namen entspricht.

So stellen Sie sicher, dass die CSR dem eingetragenen DNS-CMC-Namen entspricht:

1. Klicken Sie im linken Fensterbereich auf **Gehäuseübersicht.**
2. Klicken Sie auf **Netzwerk**.
   Die Seite **Netzwerkkonfiguration** wird angezeigt.
3. Wählen Sie die Option **CMC auf DNS registrieren**.
4. Geben Sie einen CMC-Namen in das Feld **DNS-CMC-Name** ein.
5. Klicken Sie auf **Änderungen anwenden**.

Warum sind die Remote-RACADM- und webbasierten Dienste nach einer Eigenschaftsänderung nicht verfügbar?

Es kann etwa eine Minute dauern, bis die Remote-RACADM-Dienste und die Webschnittstelle nach einem Reset des CMC-Webservers wieder verfügbar sind.

Der CMC-Webserver führt nach den folgenden Ereignissen einen Reset durch:

- Änderung der Netzwerkkonfiguration oder Netzwerksicherheitseigenschaften über die CMC-Webschnittstelle.
- Die Eigenschaft cfgRacTuneHttpsPort wird geändert (einschließlich der Änderung durch eine config -f-<Konfigurationsdatei>).
- Bei Verwendung von `racresetcfg` oder Wiederherstellen einer Gehäusekonfigurationssicherung.
- CMC wird zurückgesetzt.
- Ein neues SSL-Serverzertifikat wird hochgeladen.

Warum registriert mein DNS-Server meinen CMC nicht?

Einige DNS-Server registrieren nur Namen mit höchstens 31 Zeichen.

Wenn ich auf die CMC-Webschnittstelle zugreife, erhalte ich eine Sicherheitswarnung, die aussagt, dass das SSL-Zertifikat durch eine nicht vertrauenswürdige Zertifizierungsstelle ausgegeben wurde.

Der CMC enthält ein Standard-CMC-Serverzertifikat zur Sicherung der Netzwerksicherheit für die Webschnittstelle und die Remote-RACADM-Funktionen. Dieses Zertifikat wurde nicht von einer

vertrauenswürdigen Zertifizierungsstelle ausgestellt. Um dieses Sicherheitsproblem zu beseitigen, laden Sie ein CMC-Serverzertifikat von einer vertrauenswürdigen Zertifizierungsstelle (z. B. Thawte oder Verisign) hoch.

Warum wird die folgende Meldung aus unbekannten Gründen angezeigt?

Remote-Zugriff: SNMP-Authentifizierungsfehler

Als Teil der Ermittlung versucht IT Assistant, die **Get**- und **Set**-Community-Namen des Geräts zu überprüfen. Im IT Assistant ist der **Get-Community-Name = public** und der **Set-Community-Name = private**. Standardmäßig ist der Community-Name für den CMC-Agenten „public". Wenn IT Assistant eine Set-Aufforderung sendet, erstellt der CMC-Agent den SNMP-Authentifizierungsfehler, da er nur Aufforderungen von **Community = public** akzeptiert.

Ändern des CMC-Community-Namens mit RACADM. Um den CMC Community-Namen zu sehen, verwenden Sie den folgenden Befehl:

```
racadm getconfig -g cfgOobSnmp
```

Um den CMC Community-Namen anzugeben, verwenden Sie den folgenden Befehl:

```
racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <community name>
```

Um die Erzeugung von SNMP-Authentifizierungs-Traps zu verhindern, geben Sie Community-Namen ein, die vom Agenten akzeptiert werden. Da der CMC nur einen Community-Namen zulässt, geben Sie den gleichen Get- und Set-Community-Namen für das IT Assistant-Ermittlungs-Setup ein.

Active Directory

Unterstützt Active Directory CMC-Anmeldung über mehrfache Strukturen?

Ja. Der Abfragealgorithmus des CMC-Active Directory unterstützt mehrere Strukturen in einer Gesamtstruktur.

Funktioniert die Anmeldung am CMC unter Verwendung des Active Directory im gemischten Modus (d. h. die Domänen-Controller der Gesamtstruktur führen verschiedene Betriebssysteme aus, wie z. B. Microsoft Windows 2000 oder Windows Server 2003)?

Ja. Im gemischten Modus müssen sich alle Objekte, die vom CMC-Abfrageverfahren verwendet werden, (unter Benutzer, RAC-Geräteobjekt und Zuordnungsobjekt) in derselben Domäne befinden.

Das Dell-erweiterte Active Directory-Benutzer- und Computer-Snap-In überprüft den Modus und beschränkt Benutzer, um Objekte über Domänen hinweg zu erstellen (nur im gemischten Mischmodus).

Unterstützt die Verwendung des CMC mit Active Directory mehrfache Domänenumgebungen?

Ja. Die Domänen-Gesamtstrukturfunktionsebene muss sich im Native-Modus oder Windows-2003-Modus befinden. Außerdem müssen die Gruppen unter Zuordnungsobjekt, RAC-Benutzerobjekten und RAC-Geräteobjekten (einschließlich Zuordnungsobjekt) Universal-Gruppen sein.

Können diese Dell-erweiterten Objekte (Dell-Zuordnungsobjekt, Dell RAC-Gerät und Dell-Berechtigungsobjekt) in verschiedenen Domänen sein?

Das Zuordnungsobjekt und das Berechtigungsobjekt müssen sich in derselben Domäne befinden. Beim Dell-erweiterten Active Directory-Benutzer- und -Computer-Snap-In können Sie diese zwei Objekte nur in derselben Domäne erstellen. Andere Objekte können sich in verschiedenen Domänen befinden.

Gibt es Beschränkungen der Domänen-Controller SSL-Konfiguration?

Ja. Alle SSL-Zertifikate für Active Directory-Server in der Gesamtstruktur müssen von dem gleichen, von der root-Zertifizierungsstelle signierten, Zertifikat signiert werden, da der CMC nur erlaubt, ein einziges von einer vertrauenswürdigen Zertifizierungsstelle signiertes SSL-Zertifikat, hochzuladen.

Die Webschnittstelle startet nicht nach dem Erstellen und Hochladen eines neuen RAC-Zertifikats.

Wenn Sie Zertifikatsdienste von Microsoft verwenden, um das RAC-Zertifikat zu erstellen, haben Sie beim Erstellen des Zertifikats möglicherweise versehentlich Benutzerzertifikat ausgewählt anstatt Webzertifikat.

Generieren Sie zur Wiederherstellung eine CSR, erstellen Sie ein neues Webzertifikat von Microsoft Certificate Services und laden Sie es dann durch Ausführen der folgenden RACADM-Befehle hoch:

```
racadm sslcsrgen [-g] [-f {filename}]

racadm sslcertupload -t 1 -f {web_sslcert}
```

EAM

Nach einer Konfigurationsänderung zeigt CMC manchmal die IP-Adresse als 0.0.0.0. an.

Sie müssen die **Aktualisierungs**schaltfläche betätigen, um zu sehen, ob die IP-Adresse im Switch korrekt festgelegt wurde. Wurden IP/Maske/Gateway fehlerhaft festgelegt, wird der Switch die IP-Adresse nicht vergeben und zu 0.0.0.0 in allen Feldern zurückkehren.

Häufige Fehler sind:

- Einstellen der bandexternen IP-Adresse auf die gleiche Adresse oder im gleichen Netzwerk wie die bandinterne Verwaltungs-IP-Adresse.
- Eingabe einer ungültigen Subnetzmaske.
- Einstellen des Standard-Gateway auf eine Adresse, die sich nicht in einem Netzwerk befindet, welches direkt mit dem Switch verbunden ist.

Ereignis- und Fehlermeldungen

Warum wird nach dem Zurückstufen der CMC-Firmware von der neuesten CMC-Version auf eine frühere Version im Gehäuseprotokoll die folgende Nachricht für einige der Protokolle angezeigt?

```
USR8513 - MessageID missing from message registry.
```

Die angezeigte Meldung ist neu in der aktuellen Firmware und kann von früheren Versionen nicht interpretiert werden. Weitere Informationen zur Meldungs-ID finden Sie im Referenzhandbuch für Ereignisse und Fehler *Event and Error Messages Reference Guide* unter OpenManage Software auf der Seite **www.dell.com/openmanagemanuals**.