Dell Chassis Management Controller Firmware Version 2.10, Benutzerhandbuch

Anmerkungen und Vorsichtshinweise

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

VORSICHTSHINWEIS: Mit einem VORSICHTSHINWEIS werden Sie auf eine potenziell gefährliche Situation hingewiesen, die zu Sachschäden, Verletzungen oder zum Tod führen könnte.

August 2009

Zurück zum Inhaltsverzeichnis

CMC mit Microsoft Active Directory verwenden

Dell Chassis Management Controller Firmware Version 2.10, Benutzerhandbuch

Ein Verzeichnisdienst führt eine allgemeine Datenbank aller Informationen, die für die Steuerung von Netzwerkbenutzern, Computern, Druckern usw. erforderlich sind. Wenn Ihr Unternehmen die Microsoft® Active Directory®-Dienstsoftware verwendet, können Sie die Software so konfigurieren, dass Zugriff auf den CMC gewährt wird. Dies ermöglicht Ihnen, CMC-Benutzerberechtigungen für vorhandene Benutzer in der Active Directory-Software hinzuzufügen und zu kontrollieren.

ANMERKUNG: Die Verwendung von Active Directory zur Erkennung von CMC- Benutzern wird auf den Betriebssystemen Microsoft Windows® 2000 und Windows Server® 2003 unterstützt. Active Directory über IPv6 wird nur unter Windows 2008 unterstützt.

Active Directory-Schemaerweiterungen

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

- Das erweiterte Lösungsschema, das Active Directory-Objekte nutzt, wurde durch Dell definiert.
- Die Standardschemalösung, die nur Active Directory-Gruppenobjekte verwendet.

Erweitertes Schema vs. Standardschema

Wenn Sie Active Directory verwenden, um den Zugang zum CMC zu konfigurieren, müssen Sie entweder das erweiterte Schema oder die Standardschema-Lösung wählen.

Bei der erweiterten Schemalösung:

- Alle Zugriffssteuerungsobjekte werden im Active Directory verwahrt.
- Konfiguration des Benutzerzugriffs auf verschiedene CMCs mit verschiedenen Berechtigungsebenen ermöglicht maximale Flexibilität.

Bei der Standardschemalösung:

- Es ist keine Schema-Erweiterung erforderlich, weil das Standardschema nur Active Directory-Objekte verwendet.
- Die Konfiguration vom Active Directory aus ist einfach.

Erweiterte Schema-Übersicht

Das Active Directory mit erweitertem Schema kann auf zwei Arten aktiviert werden:

- Mit der CMC-Webschnittstelle. Anleitungen hierzu finden Sie unter Konfiguration des CMC mit der Schema-Erweiterung des Active Directory und der Internet-Schnittstelle.
- Mit dem RACADM CLI-Hilfsprogramm. Anleitungen hierzu finden Sie unter CMC mit dem erweiterten Schema von Active Directory und RACADM konfigurieren.

Active Directory-Schemaerweiterungen

Bei den Active Directory-Daten handelt es sich um eine dezentrale Datenbank von Attributen und Klassen. Das Active Directory-Schema enthält die Regeln, die

den Typ der Daten bestimmen, die der Datenbank hinzugefügt werden können bzw. darin enthalten sind.

Ein Beispiel einer Klasse, die in der Datenbank gespeichert wird, ist die Benutzerklasse. Benutzerklassenattribute können den Vornamen, Nachnamen, Telefonnummer usw. des Benutzers umfassen.

Sie können die Active Directory-Datenbank erweitern, indem Sie Ihre eigenen einzigartigen Attribute und Klassen hinzufügen, um umgebungsspezifische Bedürfnisse Ihres Unternehmens zu lösen. Dell hat das Schema erweitert, um die erforderlichen Änderungen zur Unterstützung der Remote-Verwaltungsauthentifizierung und -autorisierung einzuschließen.

Jedes Attribut bzw. jede Klasse, das/die zu einem vorhandenen Active Directory-Schema hinzugefügt wird, muss mit einer eindeutigen ID definiert werden. Um auf dem gesamten Markt eindeutige IDs zu wahren, führt Microsoft eine Datenbank mit Active Directory Object Identifiers (OIDs). Um das Schema in Microsofts Active Directory zu erweitern, hat Dell eindeutige OIDs, eindeutige Namenserweiterungen und eindeutig verknüpfte Attribut-IDs für Dell-spezifische Attribute und Klassen eingeführt:

Dell-Erweiterung: dell

Grund-OID von Dell: 1.2.840.113556.1.8000.1280

RAC-LinkID-Bereich: 12070–2079

Übersicht der RAC-Schema-Erweiterungen

Dell stellt eine Gruppe von Eigenschaften bereit, die Sie konfigurieren können. Das von Dell erweiterte Schema enthält Zuordnungs-, Geräte- und Berechtigungseigenschaften.

Diese Zuordnungseigenschaft verknüpft Benutzer oder Gruppen mit einem spezifischen Satz Berechtigungen mit einem oder mehreren RAC-Geräten. Dieses Modell gibt dem Administrator höchste Flexibilität über die verschiedenen Kombinationen von Benutzern, RAC-Berechtigungen und RAC-Geräten auf dem Netzwerk, ohne zu viel Komplexität hinzuzufügen.

Active Directory - Objektübersicht

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

Jedoch darf jedes Zuordnungsobjekt nur mit einem Berechtigungsobjekt verbunden werden bzw. darf jedes Zuordnungsobjekt Benutzer, Benutzergruppen oder RAC-Geräteobjekte nur mit einem Berechtigungsobjekt verbinden. Dieses Beispiel ermöglicht dem Administrator, die Berechtigungen jedes Benutzers auf spezifischen CMCs zu steuern.

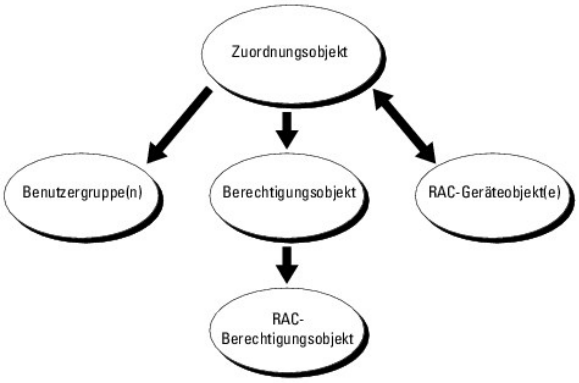
Das RAC-Geräteobjekt ist die Verknüpfung zur RAC-Firmware für die Abfrage des Active Directory auf Authentifizierung und Autorisierung. Wenn dem Netzwerk ein RAC hinzugefügt wird, muss der Administrator den RAC und sein Geräteobjekt mit seinem Active Directory-Namen so konfigurieren, dass Benutzer mit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

Abbildung 7-1 zeigt, dass das Zuordnungsobjekt die Verbindung bereitstellt, die für die gesamte Authentifizierung und Autorisierung erforderlich ist.

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

Sie können eine beliebige Anzahl an Zuordnungsobjekten erstellen. Sie müssen jedoch mindestens ein Zuordnungsobjekt erstellen und für jedes RAC (CMC) im Netzwerk, das Sie in Active Directory integrieren möchten, ein RAC-Geräteobjekt haben.

Abbildung 7-1. Typisches Setup für Active Directory-Objekte

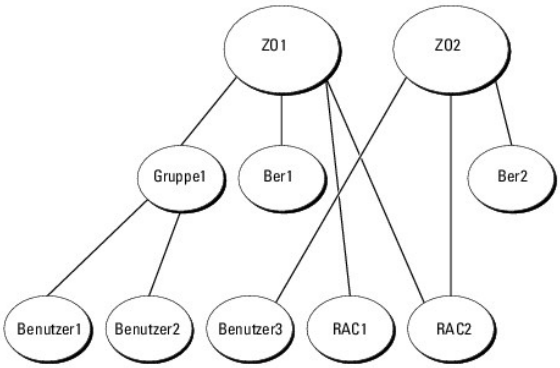


Das Zuordnungsobjekt lässt ebenso viele oder wenige Benutzer und/oder Gruppen sowie RAC-Geräteobjekte zu. Das Zuordnungsobjekt enthält jedoch nur ein Berechtigungsobjekt pro Zuordnungsobjekt. Das Zuordnungsobjekt verbindet die "Benutzer", die "Berechtigungen" auf den RACs (CMCs) haben.

Außerdem können Sie Active Directory-Objekte in einer einzelnen Domäne oder in mehreren Domänen konfigurieren. Z. B. haben Sie zwei CMCs (RAC1 und RAC2) und drei vorhandene Active Directory-Benutzer (Benutzer1, Benutzer2 und Benutzer3). Sie wollen Benutzer1 und Benutzer2 eine Administratorberechtigung für beide CMCs geben und Benutzer3 eine Anmeldungsberechtigung für die RAC2-Karte. Abbildung 7-2 zeigt, wie Sie die Active Directory-Objekte in diesem Szenario einrichten können.

Wenn Sie Universalgruppen von unterschiedlichen Domänen hinzufügen, erstellen Sie ein Zuordnungsobjekt mit Universalreichweite. Die durch das Dell Schema Extender-Dienstprogramm erstellten Standardzuordnungsobjekte sind lokale Domänengruppen und arbeiten nicht mit Universalgruppen anderer Domänen.

Abbildung 7-2. Active Directory-Objekte in einer einzelnen Domäne einrichten



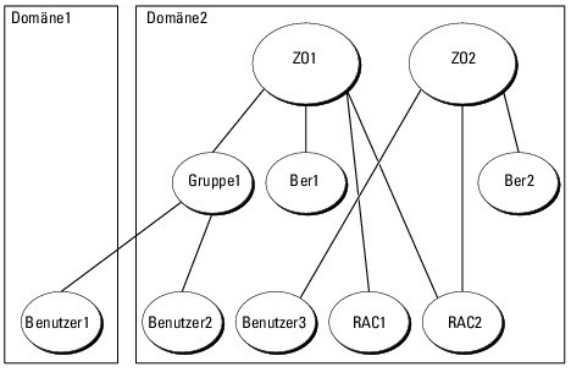
So konfigurieren Sie die Objekte für das Einzeldomänenszenario:

1. Erstellen Sie zwei Zuordnungsobjekte.
2. Erstellen Sie zwei RAC-Geräteobjekte, RAC1 und RAC2, die die zwei CMCs darstellen.
3. Erstellen Sie zwei Berechtigungsobjekte, Ber1 und Ber2, wobei Ber1 alle Berechtigungen (Administrator) und Ber2 Anmeldungsberechtigung hat.
4. user1 und user2 in Group1 gruppieren.
5. Fügen Sie Gruppe1 als Mitglieder im Zuordnungsobjekt 1 (A01), Ber1 als Berechtigungsobjekte in A01, und RAC1, RAC2 als RAC-Geräte in A01 hinzu.
6. Fügen Sie User3 als Mitglied im Zuordnungsobjekt 2 (A02), Ber2 als Berechtigungsobjekte in A02, und RAC2 als RAC-Geräte in A02 hinzu.

Für eine detaillierte Anleitung, siehe "CMC-Benutzer und -Berechtigungen zum Active Directory hinzufügen".

Abbildung 7-3 gibt ein Beispiel von Active Directory-Objekten in mehreren Domänen an. Dieses Szenario weist zwei CMCs (RAC1 und RAC2) und drei vorhandene Active Directory-Benutzer (Benutzer1, Benutzer2 und Benutzer3) auf. Benutzer1 ist in Domäne1 und Benutzer2 und Benutzer3 sind in Domäne2. In diesem Fallbeispiel konfigurieren Sie Benutzer1 und Benutzer2 mit Administratorrechten für beide CMCs, und konfigurieren Sie Benutzer3 mit Anmeldungsberechtigungen an der RAC2-Karte.

Abbildung 7-3. Active Directory-Objekte in mehreren Domänen einrichten



So konfigurieren Sie die Objekte für das Mehrdomänenszenario:

1. Stellen Sie sicher, dass die Gesamtstrukturfunktionen der Domäne im systemeigenen oder im Windows 2003-Modus sind.
2. Erstellen Sie zwei Zuordnungsobjekte, A01 (mit universellem Bereich) und A02 in jeder Domäne.

   Abbildung 7-3 zeigt die Objekte in Domäne2.
3. Erstellen Sie zwei RAC-Geräteobjekte, RAC1 und RAC2, die die zwei CMCs darstellen.
4. Erstellen Sie zwei Berechtigungsobjekte, Ber1 und Ber2, wobei Ber1 alle Berechtigungen (Administrator) und Ber2 Anmeldungsberechtigung hat.
5. user1 und user2 in Group1 gruppieren. Die Gruppenreichweite von Gruppe1 muss universell sein.
6. Fügen Sie Gruppe1 als Mitglieder im Zuordnungsobjekt 1 (A01), Ber1 als Berechtigungsobjekte in A01, und RAC1, RAC2 als RAC-Geräte in A01 hinzu.
7. Fügen Sie User3 als Mitglied im Zuordnungsobjekt 2 (A02), Ber2 als Berechtigungsobjekte in A02, und RAC2 als RAC-Geräte in A02 hinzu.

Erweitertes Schema von Active Directory konfigurieren um auf Ihren CMC zuzugreifen

Bevor Sie mit Active Directory auf den CMC zugreifen, konfigurieren Sie die Active Directory-Software und den CMC:

1. Erweitern Sie das Active Directory-Schema (s. "Erweiterung des Active Directory-Schemas").
2. Erweitern Sie das Snap-in von Active Directory-Benutzern und -Computern (s. "Dell Erweiterung zum Active Directory-Benutzer und -Computer-Snap- In installieren").
3. Fügen Sie dem Active Directory CMC-Benutzer und ihre Berechtigungen hinzu (siehe "CMC-Benutzer und -Berechtigungen zum Active Directory hinzufügen").
4. SSL auf allen Domänen-Controllern aktivieren.
5. Konfigurieren Sie die Active Directory-Eigenschaften des CMC über die CMC-Webschnittstelle oder das RACADM (siehe "Konfiguration des CMC mit der Schema-Erweiterung des Active Directory und der Internet- Schnittstelle" oder "CMC mit dem erweiterten Schema von Active Directory und RACADM konfigurieren").

Erweiterung des Active Directory-Schemas

Mit der Erweiterung des Active Directory-Schemas werden dem Active Directory-Schema eine Dell-Organisationseinheit, Schemaklassen und -attribute sowie Beispielberechtigungen und Zuordnungsobjekte hinzugefügt. Bevor Sie das Schema erweitern, vergewissern Sie sich, dass Sie Schema-Admin-Berechtigung auf dem Schema Master Flexible Single Master Operation (FSMO)-Rollenbesitzer der Domänengesamtstruktur haben.

Sie können das Schema mit einer der folgenden Methoden erweitern:

- Dell Schema Extender-Dienstprogramm
- LDIF-Script-Datei

Die Dell-Organisationseinheit wird dem Schema nicht hinzugefügt, wenn Sie die LDIF-Skriptdatei verwenden.

Die LDIF-Dateien und Dell Schema Extender befinden sich auf der DVD Dell Systems Management Tools and Documentation in den folgenden jeweiligen Verzeichnissen:

- **<DVD-Laufwerk>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\<Installationstyp>\LDIF Files**
- **<DVD-Laufwerk>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_ Tools\<Installationstyp>\Schema Extender**

Lesen Sie zur Verwendung der LDIF-Dateien die Anleitungen in der Infodatei im Verzeichnis **LDIF_Files**. Eine Anleitung zur Verwendung des Dell Schema Extenders, um das Active Directory Schema zu erweitern, siehe Dell Schema Extender verwenden.

Sie können den Schema Extender bzw. die LDIF-Dateien von einem beliebigen Standort kopieren und ausführen.

Dell Schema Extender verwenden

VORSICHTSHINWEIS: Das Dell Schema Extender-Dienstprogramm verwendet die Datei SchemaExtenderOem.ini. Um sicherzustellen, dass das Dell Schemaerweiterungs-Dienstprogramm richtig funktioniert, modifizieren Sie den Namen dieser Datei nicht.

1. Klicken Sie auf dem **Willkommen**-Bildschirm auf **Weiter**.
2. Lesen Sie die Warnung und vergewissern Sie sich, dass Sie sie verstehen, und klicken Sie dann auf Weiter.
3. Wählen Sie **Aktuelle Anmeldeinformationen verwenden** aus, oder geben Sie einen Benutzernamen und ein Kennwort mit Schema- Administratorrechte ein.
4. Klicken Sie auf **Weiter**, um den Dell Schema Extender auszuführen.
5. Klicken Sie auf **Fertig stellen**.

Das Schema wird erweitert. Um die Schema-Erweiterung zu überprüfen, verwenden Sie die Microsoft Verwaltungskonsole (MMC) und das Active Directory Schema-Snap-In, um die Existenz der folgenden Elemente zu überprüfen:

- Klassen (siehe Tabelle 7-1 bis Tabelle 7-6)
- Eigenschaften – siehe Tabelle 7-7

Weitere Informationen über das Aktivieren und die Verwendung von Active Directory-Schema-Snap-In im MCC erhalten Sie in Ihrer Microsoft-Dokumentation.

Tabelle 7-1. Klassendefinitionen für dem Active Directory hinzugefügte Klassen Verzeichnisschema

Klassenname	Zugewiesene Objekt-Identifikationsnummer (OID)
dellRacDevice	1.2.840.113556.1.8000.1280.1.1.1.1
dellAssociationObject	1.2.840.113556.1.8000.1280.1.1.1.2
dellRACPrivileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Tabelle 7-2. dellRacDevice Class

OID	1.2.840.113556.1.8000.1280.1.1.1.1
Beschreibung	Stellt das Dell RAC-Gerät dar. Das RAC-Gerät muss als dellRacDevice im Active Directory konfiguriert werden. Mit dieser Konfiguration kann der CMC Lightweight Directory Access Protocol (LDAP)-Abfragen an das Active Directory senden.
Klassentyp	Strukturklasse
SuperClasses	dellProduct
Attribute	**dellSchemaVersion**

	dellRacType

Tabelle 7-3. dellAssociationObject Class

OID	1.2.840.113556.1.8000.1280.1.1.1.2
Beschreibung	Repräsentiert das Dell-Zuordnungsobjekt. Das Zuordnungsobjekt ist die Verbindung zwischen Benutzern und Geräten.
Klassentyp	Strukturelle Klasse
SuperClasses	Gruppe
Attribute	**dellProductMembers** **dellPrivilegeMember**

Tabelle 7-4. dellRAC4Privileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Beschreibung	Definiert Autorisierungsrechte (Berechtigungen) für das CMC-Gerät.
Klassentyp	Erweiterungsklasse
SuperClasses	Keine
Attribute	**dellIsLoginUser** **dellIsCardConfigAdmin** **dellIsUserConfigAdmin** **dellIsLogClearAdmin** **dellIsServerResetUser** **dellIsTestAlertUser** **dellIsDebugCommandAdmin** **dellPermissionMask1** **dellPermissionMask2**

Tabelle 7-5. dellPrivileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Beschreibung	Container-Klasse für die Dell Berechtigungen (Autorisierungsrechte).
Klassentyp	Strukturelle Klasse
SuperClasses	Benutzer
Attribute	**dellRAC4Privileges**

Tabelle 7-6. dellProduct Class

OID	1.2.840.113556.1.8000.1280.1.1.1.5
Beschreibung	Die Hauptklasse, von der alle Dell-Produkte abgeleitet werden.
Klassentyp	Strukturelle Klasse
SuperClasses	Computer
Attribute	**dellAssociationMembers**

Tabelle 7-7. Liste von Attributen, die dem Active Directory-Schema hinzugefügt wurden

Zugewiesener OID/Syntax-Objektkennzeichner	Einzelbewertung
Attribut: dellPrivilegeMember Beschreibung: Liste mit dellPrivilege-Objekten, die zu diesem Attribut gehören.	-
OID: 1.2.840.113556.1.8000.1280.1.1.2.1	FALSE

Eindeutiger Name: (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
Attribut: dellProductMembers Beschreibung: Liste mit dellRacDevices-Objekten, die zu dieser Rolle gehören. Dieses Attribut ist die Vorwärtsverbindung zur dellAssociationMembers-Rückwärtsverbindung. Link-ID: 12070	-
OID: 1.2.840.113556.1.8000.1280.1.1.2.2 Eindeutiger Name: (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
Attribut: dellIsCardConfigAdmin Beschreibung: TRUE, wenn der Benutzer Kartenkonfigurationsrechte auf dem Gerät hat.	-
OID: 1.2.840.113556.1.8000.1280.1.1.2.4 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut: dellIsLoginUser Beschreibung: TRUE, wenn der Benutzer Anmeldungsrechte auf dem Gerät hat.	-
OID: 1.2.840.113556.1.8000.1280.1.1.2.3 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut: dellIsCardConfigAdmin Beschreibung: TRUE, wenn der Benutzer Kartenkonfigurationsrechte auf dem Gerät hat.	-
OID: 1.2.840.113556.1.8000.1280.1.1.2.4 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut: dellIsUserConfigAdmin Beschreibung: TRUE, wenn der Benutzer Benutzerkonfigurationsrechte auf dem Gerät hat.	-
OID: 1.2.840.113556.1.8000.1280.1.1.2.5 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut: dellIsLogClearAdmin Beschreibung: TRUE, wenn der Benutzer Administratorrechte zum Löschen von Protokollen auf dem Gerät hat.	-
OID: 1.2.840.113556.1.8000.1280.1.1.2.6 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut: dellIsServerResetUser Beschreibung: TRUE, wenn der Benutzer Server-Reset-Rechte auf dem Gerät hat.	-
OID: 1.2.840.113556.1.8000.1280.1.1.2.7 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut: dellIsTestAlertUser Beschreibung: TRUE, wenn der Benutzer Rechte für Warnungstests für Benutzer auf dem Gerät hat.	-
OID: 1.2.840.113556.1.8000.1280.1.1.2.10 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut: dellIsDebugCommandAdmin Beschreibung: TRUE, wenn der Benutzer Debug-Befehlsadministratorenrechte auf dem Gerät hat.	-
OID: 1.2.840.113556.1.8000.1280.1.1.2.11 Boolesch (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut: dellSchemaVersion Beschreibung: Die aktuelle Schemaversion wird verwendet, um das Schema zu aktualisieren.	-
OID: 1.2.840.113556.1.8000.1280.1.1.2.12 Case Ignore String(LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
Attribut: dellRacType	-

Beschreibung: Dieses Attribut ist der aktuelle RAC-Typ für das DellRacDevice-Objekt und die rückwärts gerichtete Verknüpfung zur Vorwärtsverknüpfung von dellAssociationObjectMembers.	
OID: 1.2.840.113556.1.8000.1280.1.1.2.13 Case Ignore String(LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
Attribut: dellAssociationMembers Beschreibung: Die Liste von dellAssociationObjectMembers, die zu diesem Produkt gehören. Dieses Attribut ist das Rückwärtslink zum Attribut dellProductMembers. Link-ID: 12071	-
OID: 1.2.840.113556.1.8000.1280.1.1.2.14 Eindeutiger Name (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
Attribut: dellPermissionsMask1	
OID: 1.2.840.113556.1.8000.1280.1.6.2.1 Integer (LDAPTYPE_INTEGER)	
Attribut: dellPermissionsMask2	
OID: 1.2.840.113556.1.8000.1280.1.6.2.2 Integer (LDAPTYPE_INTEGER)	

Dell Erweiterung zum Active Directory-Benutzer und -Computer-Snap-In installieren

Wenn Sie das Schema im Active Directory erweitern, müssen Sie auch die Active Directory-Benutzer und das Computer-Snap-In erweitern, so dass der Administrator RAC-Geräte (CMC), Benutzer und Benutzergruppen, RAC-Zuordnungen und RAC-Berechtigungen verwalten kann.

Wenn Sie die Systemverwaltungssoftware auf der DVD *Dell Systems Management Tools and Documentation* installieren, können Sie das Snap-In erweitern, indem Sie während des Installationsverfahrens die Option **Dell-Erweiterung zum Snap-In von Active Directory-Benutzern und -Computern** auswählen. Das Schnellinstallationshandbuch zu Dell OpenManage-Software enthält zusätzliche Anleitungen zur Installation von Systemverwaltungssoftware.

Weitere Informationen zum Active Directory-Benutzer und -Computer-Snap-In finden Sie in der Microsoft-Dokumentation.

Administratorpaket installieren

Sie müssen das Administrator-Pack auf jedem System installieren, das die Active Directory-CMC-Objekte verwaltet. Wenn Sie das Administratorpaket nicht installieren, können Sie das Dell RAC-Objekt nicht im Container anzeigen.

Snap-In von Active Directory-Benutzer und -Computer öffnen

So öffnen Sie die Active Directory-Benutzer und Computer-Snap-In:

1. Wenn Sie auf dem Domänen-Controller angemeldet sind, klicken Sie auf **Start Admin-Hilfsprogramme→ Active Directory-Benutzer und - Computer**.

   Wenn Sie nicht auf dem Domänen-Controller angemeldet sind, muss das entsprechende Microsoft-Administratorpaket auf dem lokalen System installiert sein. Um dieses Administratorpaket zu installieren, klicken Sie auf **Start→ Ausführen**, geben Sie `MMC` ein und drücken Sie auf Eingabe.

   Die Microsoft-Verwaltungskonsole (MMC) wird eingeblendet.

2. Klicken Sie im Fenster **Konsole 1** auf Datei (oder auf Konsole bei Systemen, auf denen Windows 2000 ausgeführt wird).
3. Klicken Sie auf **Snap-In hinzufügen/entfernen**.
4. Wählen Sie Active Directory-Benutzer- und Computer -Snap-In aus und klicken Sie auf Hinzufügen.
5. Klicken Sie auf **Schließen** und dann auf **OK**.

CMC-Benutzer und -Berechtigungen zum Active Directory hinzufügen

Mit dem Dell Erweiterten Active Directory-Benutzer- und Computer-Snap-In können Sie CMC-Benutzer und -Berechtigungen hinzuzufügen, indem Sie RAC-, Zuordnungs- und Berechtigungsobjekte erstellen. Um jeden Objekttyp hinzuzufügen, müssen Sie Folgendes ausführen:

1. RAC-Geräteobjekt erstellen
2. Berechtigungsobjekt erstellen
3. Zuordnungsobjekt erstellen
4. Einem Zuordnungsobjekt Objekte hinzufügen

RAC-Geräteobjekt erstellen

1. Klicken Sie im Fenster **Console Root** (MCC) mit der rechten Maustaste auf einen Container.
2. Wählen Sie **Neu→ Dell RAC-Objekt** aus.

   Das Fenster **Neues Objekt** wird geöffnet.
3. Tippen Sie einen Namen für das neue Objekt ein. Der Name muss mit dem CMC-Namen übereinstimmen, den Sie in Schritt 8a von "Konfiguration des CMC mit der Schema-Erweiterung des Active Directory und der Internet-Schnittstelle" eingeben werden.
4. Wählen Sie **RAC-Geräteobjekt** aus.
5. Klicken Sie auf OK.

Berechtigungsobjekt erstellen

ANMERKUNG: Ein Berechtigungsobjekt muss in derselben Domäne wie das zugehörige Zuordnungsobjekt erstellt werden.

1. Klicken Sie im Fenster **Console Root** (MMC) mit der rechten Maustaste auf einen Container.
2. Wählen Sie **Neu→ Dell RAC-Objekt** aus.

   Das Fenster **Neues Objekt** wird geöffnet.
3. Tippen Sie einen Namen für das neue Objekt ein.
4. Wählen Sie **Berechtigungsobjekt** aus.
5. Klicken Sie auf OK.
6. Klicken Sie mit der rechten Maustaste auf das Berechtigungsobjekt, das Sie erstellt haben, und wählen Sie **Eigenschaften** aus.
7. Klicken Sie auf die Registerkarte **RAC-Berechtigungen**, und wählen Sie die Berechtigungen aus, die der Benutzer aufweisen soll. Für weitere Informationen über CMC-Benutzerberechtigungen, siehe "Benutzertypen".

Zuordnungsobjekt erstellen

Das Zuordnungsobjekt wird von einer Gruppe abgeleitet und muss einen Gruppentyp enthalten. Die Zuordnungsreichweite legt den Sicherheitsgruppentyp für das Zuordnungsobjekt fest. Wenn Sie ein Zuordnungsobjekt erstellen, müssen Sie die Zuordnungsreichweite wählen, die sich auf den Typ der Objekte bezieht, die hinzugefügt werden sollen.

Wenn z. B. **Universal** ausgewählt wird, bedeutet dies, dass Zuordnungsobjekte nur verfügbar sind, wenn die Active Directory-Domäne im systemspezifischen Modus oder einem höheren Modus arbeitet.

1. Klicken Sie im Fenster **Console Root** (MMC) mit der rechten Maustaste auf einen Container.
2. Wählen Sie **Neu→ Dell RAC-Objekt** aus.

   Hierdurch wird das Fenster **Neues Objekt** geöffnet.
3. Tippen Sie einen Namen für das neue Objekt ein.
4. Wählen Sie **Zuordnungsobjekt**.
5. Wählen Sie den Wirkungsbereich für das **Zuordnungsobjekt**.
6. Klicken Sie auf OK.

Objekte zu einem Zuordnungsobjekt hinzufügen

Durch die Verwendung des Fensters **Zuordnungsobjekt-Eigenschaften** können Sie Benutzer oder Benutzergruppen, Berechtigungsobjekte und RAC-Geräte oder RAC-Gerätegruppen zuordnen. Wenn das System Windows 2000 oder höher ausführt, müssen Sie universale Gruppen verwenden, damit sich Benutzer- oder RAC-Objekte über Domänen erstrecken.

Sie können Gruppen von Benutzern und RAC-Geräte hinzufügen. Die Verfahren zum Erstellen von Dell-bezogenen Gruppen und nicht-Dell-bezogenen Gruppen sind identisch.

Benutzer oder Benutzergruppen hinzufügen

1. Klicken Sie mit der rechten Maustaste auf das **Zuordnungsobjekt** und wählen Sie **Eigenschaften**.
2. Wählen Sie die Registerkarte **Benutzer** und klicken Sie auf **Hinzufügen**.
3. Geben Sie den Namen des Benutzers oder der Benutzergruppe ein und klicken Sie auf **OK**.

Klicken Sie auf die Registerkarte **Berechtigungsobjekt**, um das Berechtigungsobjekt der Zuordnung hinzuzufügen, die die Berechtigungen des Benutzers bzw. der Benutzergruppe bei Authentifizierung eines RAC-Geräts definiert. Einem Zuordnungsobjekt kann nur ein Berechtigungsobjekt hinzugefügt werden.

Berechtigungen hinzufügen

1. Wählen Sie die Registerkarte Berechtigungsobjekt und klicken Sie auf Hinzufügen.
2. Geben Sie den Berechtigungsobjektnamen ein und klicken Sie auf OK.

Klicken Sie auf die Registerkarte **Produkte**, um der Zuordnung ein RAC-Gerät oder mehrere RAC-Geräte hinzuzufügen. Die zugeordneten Geräte geben die an das Netzwerk angeschlossenen RAC-Geräte an, die für die festgelegten Benutzer oder Benutzergruppen verfügbar sind. Mehrere RAC-Geräte können einem Zuordnungsobjekt hinzugefügt werden.

RAC-Geräte oder RAC-Gerätegruppen hinzufügen

RAC-Geräte oder RAC-Gerätegruppen hinzufügen:

1. Wählen Sie das Register **Produkte** aus und klicken Sie auf **Hinzufügen**.
2. Geben Sie den Namen des RAC-Geräts oder der RAC-Gerätegruppe ein und klicken Sie auf OK.
3. Im Fenster Eigenschaften klicken Sie auf Anwenden und dann auf OK.

Konfiguration des CMC mit der Schema-Erweiterung des Active Directory und der Internet-Schnittstelle

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf **Chassis** (Gehäuse).
3. Klicken Sie auf die Registerkarte **Netzwerk/Sicherheit** und dann auf das **Active Directory-Unterregister**. Die Seite **Active Directory-Hauptmenü** wird angezeigt.
4. Wählen Sie die Optionsschaltfläche **Konfigurieren** aus, und klicken Sie dann auf **Weiter**. Die Seite Active Directory-Konfiguration und Verwaltung wird aufgerufen.
5. Im Abschnitt Allgemeine Einstellungen:
   a. Wählen Sie das Kontrollkästchen **Active Directory aktivieren** aus, um es zu markieren.
   b. Geben Sie den **Root-Domänennamen** ein. Der **Root-Domänenname** ist der vollständig qualifizierte Root-Domänenname der Gesamtstruktur.

   ANMERKUNG: Der Root-Domänenname muss ein gültiger Domänenname sein, für den die Namenskonvention *x.y* verwendet wird, wobei *x* eine ASCII- Zeichenkette aus 1 - 256 Zeichen ohne Leerstellen zwischen den Zeichen und *y* ein gültiger Domänentyp wie com, edu, gov, int, mil, net oder org ist.

   c. Geben Sie die **Zeitüberschreitung**szeit in Sekunden ein. Konfigurationsbereich: 15 - 300 Sekunden. Standardeinstellung: 90 Sekunden.
6. Optional: Wenn der geleitete Abruf den Domänen-Controller und den globalen Katalog durchsuchen soll, wählen Sie das Kontrollkästchen AD-Server für Suche durchsuchen (optional) aus, und dann:

a. Geben Sie im Textfeld Domänen-Controller den Server ein, auf dem der Active Directory-Dienst installiert ist.

b. Geben Sie im Textfeld Globaler Katalog den Standort des globalen Katalogs auf dem Active Directory-Domänen-Controller ein. Der globale Katalog ist eine Ressource zum Durchsuchen einer Active Directory-Gesamtstruktur.

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

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

ANMERKUNG: Domänen-Controller und Server des globalen Katalogs, die nicht korrekt für alle Domänen und Anwendungen konfiguriert sind, könnten zu unerwarteten Ereignissen bei der Funktionsweise der vorhandenen Anwendungen/Domänen führen.

7. Wählen Sie die Optionsschaltfläche **Erweitertes Schema verwenden** im Bereich Auswahl des Active Directory-Schemas aus.

8. Im Abschnitt Erweiterte Schemaeinstellungen:

   a. Geben Sie den **CMC-Namen** ein. Der CMC-Name identifiziert die CMC-Karte im Active Directory eindeutig. Der CMC-Name muss dem allgemeinen Namen des neuen CMC-Objekts entsprechen, das Sie in Ihrem Domänen-Controller erstellt haben. Der CMC-Name muss eine ASCII Zeichenkette mit 1 bis 256 Zeichen ohne Leerstellen sein.

   b. Geben Sie den **CMC-Domänennamen** ein (z. B. `cmc.com`). Der CMC-Domänenname ist der DNS-Name (Zeichenkette) der Domäne, bei der sich das Active Directory-CMC-Objekt befindet. Der Name muss ein gültiger Domänenname sein und aus *x.y* bestehen, wobei *x* eine ASCII-Zeichenkette mit 1 bis 256 Zeichen ohne Leerstellen und *y* ein gültiger Domänentyp wie com, edu, gov, int, mil, net, org ist.

9. Klicken Sie auf Anwenden, um die Einstellungen zu speichern.

ANMERKUNG: Sie müssen Ihre Einstellungen anwenden, bevor Sie mit dem nächsten Schritt fortfahren, in dem Sie zu einer anderen Seite wechseln. Wenn Sie die Einstellungen nicht anwenden, verlieren Sie die eingegebenen Einstellungen, wenn Sie zur nächsten Seite wechseln.

10. Klicken Sie auf **Zurück zum Active Directory Hauptmenü**.

11. Wählen Sie die Optionsschaltfläche AD-Zertifikat hochladen aus, und klicken Sie dann auf **Weiter**. Die Seite Zertifikat hochladen wird aufgerufen.

12. Geben Sie im Textfeld den Dateipfad des Zertifikats ein oder klicken Sie auf Durchsuchen, um die Zertifikatdatei auszuwählen.

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

Die SSL-Zertifikate für den Domänen-Controller müssen von der root-Zertifizierungsstelle signiert werden. Das von der root-Zertifizierungsstelle signierte Zertifikat muss bei der Management Station verfügbar sein, die auf den CMC zugreift.

13. Klicken Sie auf Anwenden. Der CMC-Webserver wird automatisch erneut starten, nachdem Sie auf **Anwenden** klicken.

14. Melden Sie sich erneut bei der CMC-Webschnittstelle an.

15. Wählen Sie in der Systemstruktur **Gehäuse** aus, klicken Sie auf die Registerkarte **Netzwerk/Sicherheit** und anschließend auf die Unterregisterkarte **Netzwerk**. Die Seite **Netzwerkkonfiguration** wird eingeblendet.

16. Wenn **DHCP verwenden (für NIC-IP-Adresse)** aktiviert (markiert) ist, wählen Sie eine der folgenden Vorgehensweisen:

    - Wählen Sie **DHCP zum Abrufen von DNS-Serveradressen verwenden** aus, um die DNS-Server-Adressen zu aktivieren, die automatisch vom DHCP-Server abgerufen werden sollen, oder
    - konfigurieren Sie manuell eine DNS-Server-IP-Adresse, indem Sie das Kontrollkästchen **DHCP zum Abrufen von DNS-Serveradressen verwenden** frei lassen und dann die IP-Adresse des primären und alternativen DNS-Servers in die entsprechenden Felder eingeben.

17. Klicken Sie auf **Änderungen übernehmen**.

Die CMC-Funktionskonfiguration für das erweiterte Schema von Active Directory ist abgeschlossen.

CMC mit dem erweiterten Schema von Active Directory und RACADM konfigurieren

Verwendung der folgenden Befehle, um die CMC-Active Directory-Funktion mit erweitertem Schema mit Hilfe der RACADM CLI, anstatt der webbasierten Schnittstelle, zu konfigurieren.

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

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1
```

```
racadm config -g cfgActiveDirectory -o cfgADType 1
```

```
racadm config-g cfgActiveDirectory-o cfgADRacDomain <vollständig qualifizierter CMC-Domänenname>
```

```
racadm config -g cfgActiveDirectory -o cfgADRootDomain <vollständig qualifizierter root-Domänenname>
```

```
racadm config-g cfgActiveDirectory-o cfgADRacName <CMC allgemeiner Name>
```

```
racadm sslcertupload -t 0x2 -f <ADS-root-Zertifizierungsstellenzertifikat> -r
```

ANMERKUNG: Sie können diesen Befehl nur über Remote-RACADM verwenden.

```
racadm sslcertdownload-t 0x1-f <CMC-SSL-Zertifikat>
```

ANMERKUNG: Sie können diesen Befehl nur über Remote-RACADM verwenden.

Optional: Wenn Sie ein LDAP oder einen Server des globalen Katalogs festlegen möchten, statt die Server zu verwenden, die vom DNS-Server zur Suche nach einem Benutzernamen zurückgegeben wurden, geben Sie den folgenden Befehl ein, um die Option Server festlegen zu aktivieren:

```
racadm config -g cfgActiveDirectory -o cfgADSpecifyServerEnable 1
```

ANMERKUNG: Wenn Sie die Option Server festlegen verwenden, wird der Host-Name in dem von der Zertifizierungsstelle signierten Zertifikat nicht mit dem Namen des angegebenen Servers abgeglichen. Dies ist besonders nützlich, wenn Sie ein CMC-Administrator sind, weil es Ihnen hierdurch möglich ist, sowohl einen Host-Namen als auch eine IP-Adresse einzugeben.

Nachdem Sie die Option Server festlegen aktiviert haben, können Sie einen LDAP-Server und globalen Katalog mit IP-Adressen oder vollständig qualifizierten Domänennamen (FQDNs) der Server festlegen. Die FQDNs bestehen aus den Host-Namen und Domänennamen der Server.

Geben Sie zur Angabe eines LDAP-Servers Folgendes ein:

```
racadm config -g cfgActiveDirectory -o cfgADDomainController <AD-Domänen-Controller-IP-Adresse>
```

Um einen Server anzugeben, der den globalen Katalog enthält, geben Sie Folgendes ein:

```
racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog <AD-IP-Adresse des globalen Katalogs>
```

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

ANMERKUNG: Sie können eine Liste von LDAP-Servern oder von Servern, die den globalen Katalog enthalten, angeben, indem Sie ein Kommatrennungsformat anwenden. Der CMC ermöglicht Ihnen, bis zu drei IP-Adressen oder Host-Namen festzulegen.

ANMERKUNG: LDAPs, die nicht korrekt für alle Domänen und Anwendungen konfiguriert sind, könnten zu unerwarteten Ereignissen bei der Arbeitsweise der vorhandenen Anwendungen/Domänen führen.

2. Legen Sie einen DNS-Server anhand einer der folgenden Optionen fest:

   - Wenn DHCP auf dem CMC aktiviert wird und Sie die vom DHCP-Server automatisch abgefragte DNS-Adresse verwenden wollen, geben Sie den folgenden Befehl ein:

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

   - Wenn DHCP auf dem CMC deaktiviert ist oder wenn DHCP aktiviert, Sie aber Ihre DNS-IP-Adresse manuell eingeben wollen, geben Sie die folgenden Befehle ein:

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

```
racadm config -g cfgLanNetworking -o cfgDNSServer1 <primäre DNS-IP-Adresse>

racadm config -g cfgLanNetworking -o cfgDNSServer2 <sekundäre DNS-IP-Adresse>
```

Die Funktionskonfiguration des erweiterten Schemas ist abgeschlossen.

Übersicht des Standardschema-Active Directory

Bei Verwendung des Standardschemas für die Active Directory-Integration ist die Konfiguration sowohl auf dem Active Directory als auch auf dem CMC erforderlich.

Auf der Seite des Active Directory wird ein Standardgruppenobjekt als Rollengruppe verwendet. Ein Benutzer, der Zugang zum CMC hat, wird ein Mitglied der Rollengruppe sein.

Um diesem Benutzer Zugriff auf eine spezifische CMC-Karte zu gewähren, müssen der Rollengruppenname und sein Domänenname auf der spezifischen CMC-Karte konfiguriert werden. Im Unterschied zur Lösung des erweiterten Schemas, sind die Rollen- und Berechtigungsstufen auf jeder CMC-Karte und nicht im Active Directory definiert. Es können bis zu fünf Rollengruppen in jedem CMC konfiguriert und definiert werden. Tabelle 5-19 zeigt die Zugriffsstufe der Rollengruppen, und Tabelle 7-8 zeigt die standardmäßigen Einstellungen der Rollengruppen.

Abbildung 7-4. Konfiguration von CMC mit Active Directory und Standardschema

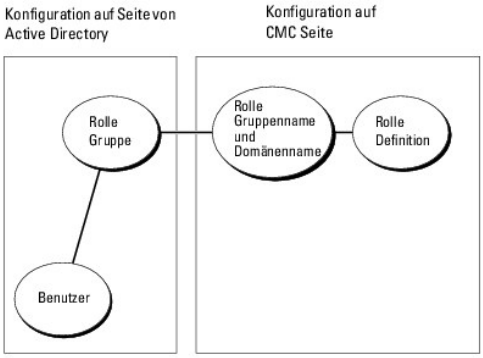


Tabelle 7-8. Standardeinstellungsberechtigungen der Rollengruppe

Rollengruppe	Standardberechtigung Stufe	Gewährte Berechtigungen	Bitmaske
1	Keine	• Benutzer: CMC-Anmeldung • Gehäusekonfigurations-Administrator • Benutzerkonfigurations-Administrator • Administrator zum Löschen von Protokollen • Gehäusesteuerungs-Administrator (Strombefehle) • Superbenutzer • Server Administrator • Warnungstests für Benutzer • Debug-Befehlsbenutzer • Architektur A-Administrator • Architektur B-Administrator • Architektur C-Administrator	0x00000fff
2	Keine	• Benutzer: CMC-Anmeldung • Administrator zum Löschen von Protokollen • Gehäusesteuerungs-Administrator (Strombefehle) • Server Administrator • Warnungstests für Benutzer • Architektur A-Administrator	0x000000f9

		• Architektur B-Administrator • Architektur C-Administrator	
3	Keine	Benutzer: CMC-Anmeldung	0x00000001
4	Keine	Keine zugewiesenen Berechtigungen	0x00000000
5	Keine	Keine zugewiesenen Berechtigungen	0x00000000

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

ANMERKUNG: Weitere Informationen über CMC-Benutzerberechtigungen erhalten Sie unter Benutzertypen.

Das Standardschema-Active Directory kann auf zwei Arten aktiviert werden:

- Mit der CMC-Webschnittstelle. Siehe Konfigurieren von CMC Mit dem Standardschema von Active Directory und der Internet-Schnittstelle".
- Mit dem RACADM-CLI-Hilfsprogramm. Siehe CMC mit dem Standardschema von Active Directory und RACADM konfigurieren".

Standardschema von Active Directory konfigurieren um auf Ihren CMC zuzugreifen

Sie müssen die folgenden Schritte ausführen, um das Active Directory zu konfigurieren, bevor ein Active Directory-Benutzer auf den CMC zugreifen kann:

1. Öffnen Sie auf einem Active Directory-Server (Domänen-Controller) das Active Directory-Benutzer- und -Computer-Snap-In.
2. Erstellen Sie eine Gruppe oder wählen Sie eine bestehende Gruppe aus. Der Name der Gruppe und der Name dieser Domäne müssen entweder mit der Webschnittstelle oder mittels RACADM auf dem CMC konfiguriert werden.

   Für weitere Informationen, siehe "Konfigurieren von CMC Mit dem Standardschema von Active Directory und der Internet-Schnittstelle" oder "CMC mit dem Standardschema von Active Directory und RACADM konfigurieren".
3. Fügen Sie den Active Directory-Benutzer als ein Mitglied der Active Directory-Gruppe hinzu, um auf den CMC zuzugreifen.

Konfigurieren von CMC Mit dem Standardschema von Active Directory und der Internet-Schnittstelle

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur Gehäuse aus.
3. Klicken Sie auf die Registerkarte **Netzwerk/Sicherheit** und dann auf die Unterregisterkarte **Active Directory**. Die Seite **Active Directory- Hauptmenü** wird angezeigt.
4. Wählen Sie die Option **Konfigurieren** aus, und klicken Sie dann auf **Weiter**. Die Seite Active Directory-Konfiguration und Verwaltung wird aufgerufen.
5. Im Abschnitt Allgemeine Einstellungen:
   a. Wählen Sie das Kontrollkästchen **Active Directory aktivieren** aus.
   b. Geben Sie den **Root-Domänennamen** ein. Der **Root-Domänenname** ist der vollständig qualifizierte Root-Domänenname der Gesamtstruktur.

      ANMERKUNG: Der Root-Domänenname muss ein gültiger Domänenname sein, für den die Namenskonvention *x.y* verwendet wird, wobei *x* eine ASCII- Zeichenkette aus 1 - 256 Zeichen ohne Leerstellen zwischen den Zeichen und *y* ein gültiger Domänentyp wie com, edu, gov, int, mil, net oder org ist.

   c. Geben Sie die **Zeitüberschreitung**szeit in Sekunden ein. Konfigurationsbereich: 15 - 300 Sekunden. Standardeinstellung: 90 Sekunden
6. Optional: Wenn der geleitete Abruf den Domänen-Controller und den globalen Katalog durchsuchen soll, wählen Sie das Kontrollkästchen AD- Server für Suche durchsuchen (optional) aus, und gehen Sie dann folgendermaßen vor:
   a. Geben Sie im Textfeld Domänen-Controller den Server ein, auf dem der Active Directory-Dienst installiert ist.
   b. Geben Sie im Textfeld Globaler Katalog den Standort des globalen Katalogs auf dem Active Directory-Domänen-Controller ein. Der globale Katalog ist eine Ressource zum Durchsuchen einer Active Directory-Gesamtstruktur.
7. Klicken Sie im Abschnitt Active Directory-Schemaauswahl auf **Standardschema verwenden**.
8. Klicken Sie auf Anwenden, um Ihre Einstellungen zu speichern.

   ANMERKUNG: Sie müssen Ihre Einstellungen anwenden, bevor Sie mit dem nächsten Schritt fortfahren, in dem Sie zu einer anderen Seite wechseln. Wenn Sie die Einstellungen nicht anwenden, verlieren Sie die eingegebenen Einstellungen, wenn Sie zur nächsten Seite wechseln.
9. Klicken Sie im Abschnitt Standardschemaeinstellungen auf eine Rollengruppe. Die Seite Rollengruppe konfigurieren wird aufgerufen.

10. Geben Sie den **Gruppennamen** ein. Der Gruppenname identifiziert die Rollengruppe im Active Directory, das mit der CMC-Karte verbunden ist.

11. Geben Sie die **Gruppendomäne** ein. Die **Gruppendomäne** ist der vollständig qualifizierte root-Domänenname der Gesamtstruktur.

12. Wählen Sie auf der Seite Rollengruppenberechtigungen die Berechtigungen für die Gruppe aus.

    Wenn Sie einige der Berechtigungen modifizieren, wird die vorhandene Rollengruppenberechtigung (Administrator, Hauptbenutzer oder Gastbenutzer) entweder zur benutzerdefinierten Gruppe oder zur entsprechenden Rollengruppenberechtigung wechseln. Siehe Tabelle 5-19.

13. Klicken Sie auf **Anwenden**, um die Einstellungen der Rollengruppe zu speichern.

14. Klicken Sie auf **Zurück zur Active Directory-Konfiguration und - Verwaltung**.

15. Klicken Sie auf **Zurück zum Active Directory Hauptmenü**.

16. Laden Sie das von der Zertifizierungsstelle signierte root-Zertifikat Ihrer Domänengesamtstruktur auf den CMC.

    a. Wählen Sie das Kontrollkästchen **Active Directory- Zertifizierungsstellenzertifikat hochladen** aus, und klicken Sie dann auf **Weiter**.

    b. Geben Sie auf der Seite **Zertifikat hochladen** den Dateipfad des Zertifikats ein oder durchsuchen Sie die Zertifikatsdatei.

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

    Die SSL-Zertifikate für die Domänen-Controller müssen von dem von der root-Zertifizierungsstelle signierten Zertifikat signiert werden. Das von der root-Zertifizierungsstelle signierte Zertifikat muss bei der Management Station verfügbar sein, die auf den CMC zugreift.

    c. Klicken Sie auf Anwenden. Der CMC-Webserver startet automatisch neu, nachdem Sie auf **Anwenden** klicken.

17. Melden Sie sich ab und dann beim CMC an, um die CMC Active Directory-Funktionskonfiguration abzuschließen.

18. Wählen Sie in der Systemstruktur Gehäuse aus.

19. Klicken Sie auf die Registerkarte **Netzwerk/Sicherheit.**

20. Klicken Sie auf die Unterregisterkarte **Netzwerk**. Die Seite **Netzwerkkonfiguration** wird eingeblendet.

21. Wenn **DHCP verwenden (für NIC-IP-Adresse)** unter **Netzwerkeinstellungen** ausgewählt ist, wählen Sie **DHCP zum Abrufen der DNS-Serveradresse verwenden** aus.

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

22. Klicken Sie auf **Änderungen übernehmen**.

    Die Funktionskonfiguration von CMC Standardschema von Active Directory ist abgeschlossen.

CMC mit dem Standardschema von Active Directory und RACADM konfigurieren

Verwenden Sie die folgenden Befehle, um den CMC mit dem Standardschema von Active Directory unter Verwendung von RACADM CLI zu konfigurieren.

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

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1

racadm config -g cfgActiveDirectory -o cfgADType 2

racadm config -g cfgActiveDirectory -o cfgADRootDomain <vollständig qualifizierter root-Domänenname>

racadm config -g cfgStandardSchema -i <Index> -o cfgSSADRoleGroupName <allgemeiner Name der Rollengruppe>

racadm config -g cfgStandardSchema -i <Index> -o cfgSSADRoleGroupDomain <voll qualifizierter Domänenname>
```

```
racadm config -g cfgStandardSchema -i <Index> -o cfgSSADRoleGroupPrivilege <Bitmaskenwert für spezifische Benutzerberechtigungen>
```

```
racadm sslcertupload -t 0x2 -f <ADS-root-CA-Zertifikat>
```

```
racadm sslcertdownload -t 0x1 -f <RAC-SSL-Zertifikat>
```

ANMERKUNG: Bitmasken-Zahlenwerte sind in Tabelle 3-1 im Kapitel "Datenbankeigenschaften" im Dell Chassis Management Controller Administrator-Referenzhandbuch zu finden.

2. Legen Sie einen DNS-Server anhand einer der folgenden Optionen fest:

   - Wenn DHCP auf dem CMC aktiviert wird und Sie die vom DHCP-Server automatisch abgefragte DNS-Adresse verwenden wollen, geben Sie den folgenden Befehl ein:

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

   - Wenn DHCP auf dem CMC deaktiviert ist oder Sie Ihre DNS-IP-Adresse manuell eingeben wollen, geben Sie die folgenden Befehle ein:

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

     ```
     racadm config -g cfgLanNetworking -o cfgDNSServer1 <primäre DNS-IP-Adresse>
     ```

     ```
     racadm config -g cfgLanNetworking -o cfgDNSServer2 <sekundäre DNS-IP-Adresse>
     ```

Häufig gestellte Fragen

Tabelle 7-9 listet häufig gestellte Fragen und Antworten zur Verwendung von Active Directory mit dem CMC auf.

Tabelle 7-9. CMC mit Active Directory verwenden: Häufig gestellte Fragen

Frage	Antwort
Kann ich mich beim CMC anmelden, indem ich Active Directory über mehrfache Strukturen verwende?	Ja. Der Abfragealgorithmus des CMC-Active Directory unterstützt mehrere Strukturen in einer einzelnen 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 alle, durch das CMC-Abfrageverfahren verwendeten, Objekte (unter dem Benutzer, RAC-Geräteobjekt und Zuordnungsobjekt) in derselben Domäne sein. Das Dell-erweiterte Active Directory Users and Computers Snap-In überprüft den Modus und beschränkt Benutzer, um Objekte über Domänen hinweg zu erstellen, wenn es im Mischmodus ist.
Unterstützt die Verwendung von CMC mit Active Directory mehrfache Domänenumgebungen?	Ja. Die Domänen-Gesamtstrukturstufe muss im einheitlichen Modus oder Windows-2003-Modus sein. Außerdem müssen die Gruppen unter Zuordnungsobjekt, RAC-Benutzerobjekten und RAC-Geräteobjekten (einschließlich Zuordnungsobjekt) universale 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 in derselben Domäne sein. Beim Dell-erweiterten Snap-In 'Active Directory Users and Computers' müssen Sie diese zwei Objekte in derselben Domäne erstellen. Andere Objekte können sich in verschiedenen Domänen befinden.
Gibt es Beschränkungen bei der SSL-Konfiguration der Domänen-Controller?	Ja. Alle SSL-Zertifikate für Active Directory-Server in der Gesamtstruktur müssen von dem gleichen, von der root-Zertifizierungsstelle signierten, Zertifikat signiert werden, da der CMC nur erlaubt, ein einziges von einer vertrauenswürdigen Zertifizierungsstelle signiertes SSL-Zertifikat, hochzuladen.
Ich habe ein neues RAC-Zertifikat erstellt und hochgeladen und jetzt startet die Webschnittstelle nicht.	Wenn Sie Zertifikatsdienste von Microsoft verwenden, um das RAC-Zertifikat zu erstellen, haben Sie beim Erstellen des Zertifikats möglicherweise versehentlich **Benutzerzertifikat** ausgewählt anstatt **Webzertifikat**. Generieren Sie zur Wiederherstellung eine CSR, erstellen Sie dann ein neues Webzertifikat von Microsoft Certificate Services und laden Sie es mit Hilfe der folgenden RACADM-Befehle hoch:

	racadm sslcsrgen [-g] [-f {Dateiname}] racadm sslcertupload -t 1 -f {web_sslcert}
Was kann ich tun, wenn ich mich mittels Active Directory-Authentifizierung nicht beim CMC anmelden kann? Wie kann ich das Problem beheben?	1. Stellen Sie sicher, dass Sie während einer Anmeldung den korrekten Benutzerdomänennamen anstelle des NetBIOS-Namens verwenden. 2. Wenn Sie ein lokales CMC-Benutzerkonto haben, melden Sie sich mit Ihren lokalen Anmeldeinformationen beim CMC an. Nachdem Sie angemeldet sind, führen Sie die folgenden Schritte aus: a. Stellen Sie sicher, dass Sie das Kästchen **Active Directory aktivieren** auf der CMC Active Directory-Konfigurationsseite markiert haben. b. Stellen Sie sicher, dass die DNS-Einstellung auf der CMC-Netzwerkkonfigurationsseite richtig ist. c. Stellen Sie sicher, dass Sie das Active Directory-Zertifikat von dem von Ihrer Active Directory-root-Zertifizierungsstelle signierten Zertifikat zum CMC geladen haben. d. Überprüfen Sie die SSL-Zertifikate der Domänen-Controller, um sicherzustellen, dass sie nicht abgelaufen sind. e. Stellen Sie sicher, dass **CMC-Name**, **Root-Domänenname** und **CMC-Domänenname** mit Ihrer Active Directory-Umgebungskonfiguration übereinstimmen. f. Stellen Sie sicher, dass das CMC-Kennwort maximal 127 Zeichen aufweist. Während der CMC Kennwörter von bis zu 256 Zeichen unterstützt, unterstützt Active Directory nur Kennwörter, die maximal 127 Zeichen lang sind.

Einfache Anmeldung konfigurieren

Microsoft® Windows® 2000, Windows XP, Windows Server® 2003, Windows Vista® und Windows Server 2008 können Kerberos (ein Netzwerk-Authentifizierungsprotokoll) als Authentifizierungsmethode verwenden und Benutzern, die sich bei der Domäne angemeldet haben, automatische oder einfache Anmeldung für nachfolgende Anwendungen wie Exchange ermöglichen.

Beginnend mit CMC Version 2.10 kann der CMC Kerberos verwenden, um zwei zusätzliche Authentifizierungsmechanismen, einfache Anmeldung und Smart Card-Anmeldung, zu unterstützen. Bei der einfachen Anmeldung verwendet der CMC die Anmeldeinformationen des Clientsystems, die im Betriebssystem zwischengespeichert werden, nachdem Sie sich mit einem gültigen Active Directory®-Konto angemeldet haben.

ANMERKUNG: Die Auswahl einer Anmeldemethode legt keine Richtlinienattribute hinsichtlich anderer Anmeldeschnittstellen, z. B. SSH, fest. Sie müssen sonstige Richtlinienattribute für andere Anmeldeschnittstellen ebenfalls setzen. Falls Sie alle anderen Anmeldeschnittstellen deaktivieren möchten, navigieren Sie zur Seite **Dienste** und deaktivieren Sie alle (oder bestimmte) Anmeldeschnittstellen.

Systemanforderungen

Zu Verwendung der Kerberos-Authentifizierung muss Ihr Netzwerk Folgendes enthalten:

- DNS-Server
- Microsoft Active Directory®-Server

  ANMERKUNG: HINWEIS: Falls Sie Active Directory unter Windows 2003 verwenden, müssen Sie sicherstellen, dass die neuesten Service-Packs auf dem Clientsystem installiert sind. Falls Sie Active Directory unter Windows 2008 verwenden, müssen Sie sicherstellen, dass SP1 sowie die folgenden Hotfixes installiert sind.
  Windows6.0-KB951191-x86.msu für das Dienstprogramm KTPASS. Ohne dieses Patch erzeugt das Dienstprogramm *fehlerhafte* Keytab-Dateien.
  Windows6.0-KB957072-x86.msu für Verwendung von GSS_API- und SSL- Transaktionen während einer LDAP-Bindung.
- Kerberos-Schlüsselverteilungscenter – KDC (mit der Active Directory Server-Software)
- DHCP-Server (empfohlen)
- Die DNS-Server-Reverse-Zone muss einen Eintrag für den Active Directory-Server und den CMC enthalten.

Clientsysteme

- Für die 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 die einfache Anmeldung und Smart Card-Anmeldung muss das Clientsystem ein Teil der Active Directory-Domäne und des Kerberosbereichs sein.

CMC

- Der CMC muss Firmwareversion 2.10 oder neuer aufweisen.
- Jeder CMC muss ein Active Directory-Konto haben.
- Der CMC muss ein Teil der Active Directory-Domäne und des Kerberosbereichs sein.

Einstellungen konfigurieren

Vorbedingungen

- Der Kerberosbereich und das Kerberos-Schlüsselverteilungscenter (KDC) für Active Directory (AD) wurden eingerichtet (ksetup).
- Gewährleisten Sie eine robuste NTP- und DNS-Infrastruktur zur Vermeidung von Problemen mit Clock-Drift und Reverse-Lookup.
- Die CMC-Standardschema-Rollengruppe mit autorisierten Mitgliedern

Active Directory konfigurieren

Konfigurieren Sie im Dialogfeld **CMC-Eigenschaften** im Optionsabschnitt **Konten** diese Einstellungen:

- **Konto wird für Delegierungszwecke vertraut** – Der CMC verwendet derzeit keine weitergeleiteten Anmeldeinformationen, wenn diese Option ausgewählt ist. Sie können diese Option abhängig von anderen Dienstanforderungen auswählen oder nicht auswählen.
- **Konto ist vertraulich und kann nicht delegiert werden** – Sie können diese Option abhängig von anderen Dienstanforderungen auswählen oder nicht auswählen.
- **DES-Verschlüsselungstypen für dieses Konto verwenden**– Wählen Sie diese Option aus.
- **Keine Kerberos-Vorauthentifizierung erforderlich** – Wählen Sie diese Option nicht aus.

Führen Sie das Dienstprogramm ktpass (Teil von Microsoft Windows) auf dem Domänen-Controller (Active Directory-Server) aus, auf dem Sie den CMC einem Benutzerkonto in Active Directory zuordnen möchten. Beispiel:

```
C:\>ktpass -princ HTTP/cmcname.domain_name.com@REALM_NAME.COM -mapuser dracname -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -pass * -out
c:\krbkeytab
```

ANMERKUNG: `cmcname.domainname.com` muss gemäß RFC in Kleinbuchstaben und der REALM-Name `@REALM_NAME` muss in Großbuchstaben angegeben werden. Darüber hinaus unterstützt der CMC den DES-CBC-MD5-Typ von Kryptographie für Kerberos-Authentifizierung.

Dieses Verfahren erstellt eine Keytab-Datei, die Sie zum CMC hochladen müssen.

ANMERKUNG: Das Keytab enthält einen Verschlüsselungsschlüssel und muss an einem sicheren Ort aufbewahrt werden. Weitere Informationen zum Dienstprogramm ktpass finden Sie auf der Microsoft-Website unter: **technet2.microsoft.com/windowsserver/en/library/64042138-9a5a-4981-84e9- d576a8db0d051033.mspx?mfr=true**.

Konfiguration des CMC-Moduls:

ANMERKUNG: Die in diesem Abschnitt beschriebenen Konfigurationsschritte gelten nur für den Webzugriff des CMC.

Konfigurieren Sie den CMC zu Verwendung von Standardschema-Rollengruppen, die in Active Directory eingerichtet sind. Weitere Informationen finden Sie unter "Standardschema von Active Directory konfigurieren um auf Ihren CMC zuzugreifen".

Kerberos-Keytab-Datei hochladen

Die Kerberos-Keytab-Datei liefert die CMC-Benutzername-Kennwort-Anmeldeinformationen für das KDC (Kerberos Data Center), das wiederum Zugriff auf das Active Directory ermöglicht. Jeder CMC im Kerberosbereich muss beim Active Directory registriert sein und eine eindeutige Keytab-Datei aufweisen.

So laden Sie die Keytab-Datei hoch:

1. Wechseln Sie zu **Remote-Zugriff**→ Register **Konfiguration**→ Unterregister **Active Directory**.
2. Wählen Sie **Kerberos-Keytab hochladen** aus und klicken Sie auf **Weiter**.
3. Wechseln Sie auf der Seite **Kerberos-Keytab-Hochladen** zu dem Ordner, in dem die Keytab-Datei gespeichert ist und klicken Sie auf **Anwenden**.

   Wenn der Vorgang beendet ist, wird ein Nachrichtenfenster eingeblendet, das anzeigt, ob der Upload erfolgreich oder fehlerhaft war.
4. Wenn die Keytab-Datei erfolgreich hochgeladen wurde, klicken Sie auf **Zurück zum Active Directory Hauptmenü**.

Einfache Anmeldung aktivieren

1. Wechseln Sie zur Registerkarte **Chassis Management Controller – Netzwerksicherheit** und Unterregisterkarte **Active Directory**, und wählen Sie **Active Directory konfigurieren** aus.
2. Wählen Sie auf der Seite **Active Directory-Konfiguration und Verwaltung** Folgendes aus:
   - Einfache Anmeldung – diese Option ermöglicht die Anmeldung beim CMC unter Verwendung der zwischengespeicherten Anmeldeinformationen, die bei der Anmeldung beim Active Directory verwendet wurden.

   ANMERKUNG: Alle bandexternen Befehlszeilenschnittstellen, einschließlich Secure Shell (SSH), Telnet, Seriell und Remote-RACADM, bleiben für diese Option unverändert.
3. Klicken Sie am unteren Seitenrand auf **Anwenden**.

Sie können das Active Directory mit Kerberos-Authentifizierung testen, indem Sie die Testfunktion des CLI-Befehls verwenden.

Geben Sie Folgendes ein:

```
testfeature -f adkrb -u <Benutzer>@<Domäne>
```

wobei 'Benutzer' für ein gültiges Active Directory-Benutzerkonto steht.

Wenn der Befehl erfolgreich ist, bedeutet das, dass der CMC Kerberos-Anmeldeinformationen beschaffen und auf das Active Directory-Konto des Benutzers zugreifen kann. Wenn der Befehl nicht erfolgreich ist, müssen Sie den Fehler beseitigen und den Befehl wiederholen. Weitere Informationen finden Sie im *Chassis Management Controller Administrator-Referenzhandbuch* unter **support.dell.com\manuals**.

Browser für einfache Anmeldung konfigurieren

Einfache Anmeldung wird von Internet Explorer Version 6.0 und neuer und Firefox Version 3.0 und neuer unterstützt.

ANMERKUNG: Die folgenden Anweisungen gelten nur, wenn der CMC die einfache Anmeldung mit Kerberos-Authentifizierung verwendet.

Internet Explorer

1. Wählen Sie in Internet Explorer **Extras**→ **Internetoptionen** aus.
2. Wählen Sie auf der Registerkarte **Sicherheit** unter **Wählen Sie eine Zone aus, um deren Sicherheitseinstellungen festzulegen** die Option **Lokales Intranet** aus.
3. Klicken Sie auf **Sites**.

   Das Dialogfeld **Lokales Intranet** wird angezeigt.
4. Klicken Sie auf **Advanced** (Erweitert).

   Das Dialogfeld **Lokales Intranet – Erweiterte Einstellungen** wird angezeigt.

5. Geben Sie im Feld **Diese Website zur Zone hinzufügen** den Namen des CMC und dessen Domäne ein und klicken Sie auf **Hinzufügen**.

   ANMERKUNG: Sie können einen Platzhalter (*) verwenden, um alle Geräte/Benutzer in dieser Domäne anzugeben.

Mozilla Firefox

1. Geben Sie in Firefox **about:config** in die Adressleiste ein.

   ANMERKUNG: Wenn der Browser die Warnung **This might void your warranty** (Das kann Ihre Garantie unwirksam machen) anzeigt, klicken Sie auf **I'll be careful. I promise** (Ich werde vorsichtig sein, ich verspreche es).

2. Im Textfeld **Filter** geben Sie `negotiate` (verhandeln) ein.

   Der Browser zeigt eine Liste bevorzugter Namen an, die alle das Wort "negotiate" enthalten.

3. Doppelklicken Sie in der Liste auf **network.negotiate-auth.trusted-uris**.
4. Geben Sie im Dialogfeld **Enter string value** (Zeichenfolgewert eingeben) den Domänennamen des CMC ein und klicken Sie auf **OK**.

Anmelden beim CMC unter Verwendung der einfachen Anmeldung

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

1. Melden Sie sich unter Verwendung Ihres Netzwerkkontos beim Clientsystem an.
2. Greifen Sie auf die CMC-Webseite zu. Verwenden Sie:

   https://<*cmcname.domain-name*>

   Beispiel: `cmc-6G2WXF1.cmcad.lab`

   wobei `cmc-6G2WXF1` der CMC-Name ist

   und `cmcad.lab´` der Domänenname.

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

   Die Seite **CMC – einfache Anmeldung** wird angezeigt.

3. Klicken Sie auf **Anmelden**.

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

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

Smart Card-Zweifaktor-Authentifizierung konfigurieren

Für herkömmliche Authentifizierungsschemata werden der Benutzername und das Kennwort zum Authentifizieren von Benutzern verwendet. Bei der Zweifaktor-Authentifizierung wird andererseits eine höhere Sicherheitsstufe geboten, indem Benutzer aufgefordert werden, ein Kennwort oder eine PIN sowie eine physische Karte mit einem privaten Schlüssel oder einem digitalen Zertifikat anzugeben. Kerberos, ein Netzwerk-Authentifizierungsprotokoll, verwendet diesen Zweifaktor-Authentifizierungsmechanismus und ermöglicht es Systemen, ihre Authentizität zu beweisen. Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista und Windows Server 2008 verwenden Kerberos als bevorzugte Authentifizierungsmethode. Beginnend mit CMC Version

2.10 Version kann der CMC Kerberos verwenden, um Smart Card-Anmeldung zu unterstützen.

ANMERKUNG: Die Auswahl einer Anmeldemethode legt keine Richtlinienattribute hinsichtlich anderer Anmeldeschnittstellen, z. B. SSH, fest. Sie müssen sonstige Richtlinienattribute für andere Anmeldeschnittstellen ebenfalls setzen. Falls Sie alle anderen Anmeldeschnittstellen deaktivieren möchten, navigieren Sie zur Seite **Dienste** und deaktivieren Sie alle (oder bestimmte) Anmeldeschnittstellen.

Systemanforderungen

Die "Systemanforderungen" für Smart Card entsprechen denen für einfache Anmeldung.

Einstellungen konfigurieren

Die "Vorbedingungen" für Smart Card entsprechen denen für einfache Anmeldung.

Active Directory konfigurieren

1. Richten Sie den Kerberosbereich und das Kerberos- Schlüsselverteilungscenter (KDC) für Active Directory ein, falls diese Komponenten noch nicht konfiguriert sind (ksetup).

   ANMERKUNG: Gewährleisten Sie eine robuste NTP- und DNS-Infrastruktur zur Vermeidung von Problemen mit Clock-Drift und Reverse-Lookup.

2. Erstellen Sie Active Directory-Benutzer für jeden CMC und konfigurieren Sie Kerberos-DES-Verschlüsselung, jedoch nicht Vorauthentifizierung.
3. Registrieren Sie die CMC-Benutzer mit Ktpass beim Schlüsselverteilungscenter (dies erzeugt auch einen Schlüssel zum Hochladen auf den CMC).

Konfiguration des CMC-Moduls:

ANMERKUNG: Die in diesem Abschnitt beschriebenen Konfigurationsschritte gelten nur für den Webzugriff des CMC.

Konfigurieren Sie den CMC zu Verwendung von Standardschema-Rollengruppen, die in Active Directory eingerichtet sind. Weitere Informationen finden Sie unter "Standardschema von Active Directory konfigurieren um auf Ihren CMC zuzugreifen".

Kerberos-Keytab-Datei hochladen

Die Kerberos-Keytab-Datei liefert die CMC-Benutzername-Kennwort-Anmeldeinformationen für das KDC (Kerberos Data Center), das wiederum Zugriff auf das Active Directory ermöglicht. Jeder CMC im Kerberosbereich muss beim Active Directory registriert sein und eine eindeutige Keytab-Datei aufweisen.

So laden Sie die Keytab-Datei hoch:

1. Wechseln Sie zu **Remote-Zugriff**→ Register **Konfiguration**→ Unterregister **Active Directory**.
2. Wählen Sie **Kerberos-Keytab hochladen** aus und klicken Sie auf **Weiter**.
3. Wechseln Sie auf der Seite **Kerberos-Keytab-Hochladen** zu dem Ordner, in dem die Keytab-Datei gespeichert ist und klicken Sie auf **Anwenden**.

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

4. Wenn die Keytab-Datei erfolgreich hochgeladen wurde, klicken Sie auf **Zurück zum Active Directory Hauptmenü**.

Smart Card-Authentifizierung aktivieren

1. Wechseln Sie zu Registerkarte **Chassis Management Controller – Netzwerksicherheit**→ und Unterregisterkarte **Active Directory**Æ und wählen Sie **Active Directory konfigurieren** aus.
2. Wählen Sie auf der Seite **Active Directory-Konfiguration und Verwaltung** Folgendes aus:
   - Smart Card – diese Option erfordert das Einführen einer Smart Card in den Leser und die Eingabe der PIN-Nummer.

ANMERKUNG: Alle bandexternen Befehlszeilenschnittstellen, einschließlich Secure Shell (SSH), Telnet, Seriell und Remote-RACADM, bleiben für diese Option unverändert.

3. Klicken Sie am unteren Seitenrand auf **Anwenden**.

Sie können das Active Directory mit Kerberos-Authentifizierung testen, indem Sie die Testfunktion des CLI-Befehls verwenden.

Geben Sie Folgendes ein:

`testfeature -f adkrb -u <Benutzer>@<Domäne>`

wobei 'Benutzer' für ein gültiges Active Directory-Benutzerkonto steht.

Wenn der Befehl erfolgreich ist, bedeutet das, dass der CMC Kerberos-Anmeldeinformationen beschaffen und auf das Active Directory-Konto des Benutzers zugreifen kann. Wenn der Befehl nicht erfolgreich ist, müssen Sie den Fehler beseitigen und den Befehl wiederholen. Weitere Informationen finden Sie im *Chassis Management Controller Administrator-Referenzhandbuch*.

Browser für Smart Card-Anmeldung konfigurieren

Mozilla Firefox

CMC 2.10 unterstützt Smart Card-Anmeldung über Firefox-Browser nicht.

Internet Explorer

Stellen Sie sicher, dass der Internet-Browser zum Herunterladen von Active-X-Plug-ins konfiguriert ist.

Anmeldung beim CMC mit Smart Card

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

1. Melden Sie sich unter Verwendung Ihres Netzwerkkontos beim Clientsystem an.
2. Greifen Sie auf die CMC-Webseite zu. Verwenden Sie:

   https://<*cmcname.domain-name*>

   Beispiel: `cmc-6G2WXF1.cmcad.lab`

   wobei `cmc-6G2WXF1` der CMC-Name ist

   und `cmcad.lab` der Domänenname.

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

Die Seite **CMC – einfache Anmeldung** wird eingeblendet. Sie werden aufgefordert, die Smart Card einzuführen.

3. Führen Sie die Smart Card in den Leser ein und klicken Sie auf **OK**.

Das **PIN-Popup-**Dialogfeld wird angezeigt.

4. Geben Sie die PIN ein und klicken Sie auf **OK**.

Fehlerbehebung Smart Card-Anmeldung

Die folgenden Tipps helfen beim Debuggen einer Smart Card, auf die nicht zugegriffen werden kann.

Das ActiveX Plug-in kann das Smart Card-Laufwerk nicht erkennen.

Stellen Sie sicher, dass die Smart Card auf dem Microsoft Windows-Betriebssystem unterstützt wird. Windows unterstützt eine beschränkte Anzahl von Cryptographic Service Providers (CSP) für die Smart Card.

Tipp: Sie können generell überprüfen, ob die Smart Card-CSPs auf einem bestimmten Client vorhanden sind, indem Sie die Smart Card bei der Windows-Anmeldung (Strg-Alt-Entf) in das Laufwerk einlegen, um zu sehen, ob Windows die Smart Card erkennt und das PIN-Dialogfeld einblendet.

Falsche Smart Card-PIN

Prüfen Sie, ob die Smart Card aufgrund übermäßiger Versuche mit einer falschen PIN gesperrt worden ist. In solchen Fällen kann Ihnen der Aussteller der Smart Card in der Organisation helfen, eine neue Smart Card zu erwerben.

Anmeldung beim CMC als Active Directory-Benutzer nicht möglich.

Wenn Sie sich als Active Directory-Benutzer nicht beim CMC anmelden können, versuchen Sie sich einzuloggen, ohne die Smart Card-Anmeldung zu aktivieren. Sie haben auch die Möglichkeit, die Smart Card-Anmeldung über den lokalen RACADM zu deaktivieren, indem Sie die folgenden Befehle verwenden:

```
racadm config -g cfgActiveDirectory -o cfgADSCLEnable 0
```

```
racadm config -g cfgActiveDirectory -o cfgADSSOEnable 0
```

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

CMC zur Verwendung von Befehlszeilenkonsolen konfigurieren

Dell Chassis Management Controller Firmware Version 2.10, Benutzerhandbuch

Dieser Abschnitt enthält Informationen über die Funktionen der CMC-Befehlszeilenkonsole (bzw. serielle/Telnet-/Secure Shell-Konsole) und erklärt, wie man das System einrichtet, sodass Systemverwaltungsmaßnahmen über die Konsole ausgeführt werden können. Informationen zur Verwendung der RACADM-Befehle im CMC über die Befehlszeilenkonsole finden Sie unter "RACADM-Befehlszeilenschnittstelle verwenden".

Funktionen der Befehlszeilenkonsole auf dem CMC

Der CMC unterstützt die folgenden Funktionen von seriellen, Telnet- und SSH-Konsolen:

- Eine serielle Client-Verbindung und bis zu vier gleichzeitige Telnet-Client-Verbindungen
- Bis zu vier gleichzeitige Secure Shell- (SSH-) Client-Verbindungen)
- RACADM-Befehlsunterstützung
- Integrierter **connect**-Befehl zum Anschließen an die serielle Konsole von Servern und E/A-Modulen; auch als racadm connect-Befehl verfügbar
- Befehlszeilenbearbeitung und Protokoll
- Sitzungszeitüberschreitungssteuerung auf allen Konsole-Schnittstellen

---

Verwendung einer seriellen, Telnet- oder SSH-Konsole

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

Tabelle 3-1. CMC-Befehlszeilenbefehle

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

Telnet-Konsole mit dem CMC verwenden

Bis zu vier Telnet-Client-Systeme und vier SSH-Clients können zu jeder gegebenen Zeit angeschlossen werden.

Wenn auf Ihrer Verwaltungsstation Windows XP oder Windows 2003 ausgeführt wird, tritt möglicherweise ein Problem mit den Zeichen in einer CMC-Telnet-

Sitzung auf. Dieses Problem kann als eingefrorene Anmeldung auftreten, bei der die Eingabetaste nicht reagiert und die Eingabeaufforderung für das Kennwort nicht angezeigt wird.

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

SSH mit dem CMC verwenden

SSH ist eine Befehlszeilensitzung, die über die gleichen Merkmale wie eine Telnet-Sitzung verfügt, allerdings mit Sitzungsverhandlung und -verschlüsselung für eine verbesserte Sicherheit. Der CMC unterstützt SSH Version 2 mit Kennwortauthentifizierung. SSH ist beim CMC standardmäßig aktiviert.

ANMERKUNG: Der CMC unterstützt SSH-Version 1 nicht.

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

ANMERKUNG: OpenSSH sollte unter Windows von einem VT100 oder ANSI- Terminalemulator ausgeführt werden. Das Ausführen von OpenSSH an der Windowseingabeaufforderung ergibt keine volle Funktionalität (d. h. einige Tasten reagieren nicht, und keine Grafiken werden angezeigt). Führen Sie für Linux SSH- Client-Dienste aus, um über beliebige Shells eine Verbindung zum CMC herzustellen.

Vier gleichzeitige SSH-Sitzungen werden jeweils zu einer vorgegebenen Zeit unterstützt. Die Sitzungszeitüberschreitung wird von der Eigenschaft `cfgSsnMgtSshIdleTimeout` gesteuert (siehe Kapitel über Datenbankeigenschaften im *Dell Chassis Management Controller Administrator-Referenzhandbuch*) oder von der Seite Dienstverwaltung der Webschnittstelle (siehe "Dienste konfigurieren").

CMC unterstützt auch Authentifizierung mit öffentlichem Schlüssel (PKA) über SSH. Diese Authentifizierungsmethode verbessert SSH-Skripting-Automatisierung durch Beseitigung des Bedarfs, Benutzer-ID/Kennwort einzubetten bzw. Anforderungen auszugeben. Weitere Informationen finden Sie unter "Verwendung von RACADM zum Konfigurieren der Authentifizierung mit öffentlichem Schlüssel über SSH".

SSH auf dem CMC aktivieren

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

Anleitungen zum Aktivieren von SSH-Verbindungen beim CMC unter Verwendung von RACADM sind im Abschnitt config-Befehl und im Abschnitt cfgSerial-Datenbankeigenschaft im *Dell Chassis Management Controller Administrator-Referenzhandbuch* zu finden. Eine Anleitung zum Aktivieren von SSH-Verbindungen beim CMC anhand der Webschnittstelle finden Sie unter "Dienste konfigurieren".

SSH-Schnittstelle ändern

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

```
racadm config -g cfgRacTuning -o cfgRacTuneSshPort <Anschlussnummer>
```

Weitere Informationen über die Eigenschaften `cfgSerialSshEnable` und `cfgRacTuneSshPort` sind im Kapitel über Datenbankeigenschaften im *Dell Chassis Management Controller Administrator-Referenzhandbuch* zu finden.

Die CMC-SSH-Umsetzung unterstützt mehrfache Verschlüsselungs-Schemata, wie in Tabelle 3-2 dargestellt.

Tabelle 3-2. Verschlüsselungsschemata

Schematyp	Schema

Asymmetrische Verschlüsselung	Diffie-Hellman DSA/DSS 512-1024 (zufällige) Bits pro NIST-Spezifizierung
Symmetrische Verschlüsselung	• AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
Meldungsintegrität	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
Authentifizierung	Kennwort

Frontblende für iKVM-Verbindung aktivieren

Für Informationen und Anleitungen zur Verwendung des iKVM-Fronblendenanschlusses, siehe "Frontblende aktivieren oder deaktivieren".

Terminalemulationssoftware konfigurieren

Ihr CMC unterstützt eine serielle Textkonsole einer Verwaltungsstation, auf der einer der folgenden Typen der Terminalemulationssoftware ausgeführt wird:

- Linux Minicom
- Hilgraeve HyperTerminal Private Edition (Version 6.3)

Um Ihre Art der Terminalsoftware zu konfigurieren, führen Sie die folgenden Schritte aus.

Konfigurieren von Linux Minicom

Minicom ist ein serielles Schnittstellenzugriffdienstprogramm für Linux. Die folgenden Schritte beziehen sich auf die Konfiguration von Minicom-Version 2.0. Andere Minicom-Versionen können geringfügig abweichen, erfordern jedoch dieselben grundlegenden Einstellungen. Verwenden Sie die Informationen in "Erforderliche Minicom-Einstellungen" zur Konfiguration anderer Minicom-Versionen.

Minicom Version 2.0 konfigurieren

ANMERKUNG: Für beste Ergebnisse stellen Sie die Eigenschaft **cfgSerialConsoleColumns** so ein, dass sie der Anzahl der Spalten entspricht. Beachten Sie, dass die Eingabeaufforderung zwei Zeichen beansprucht. Geben Sie zum Beispiel für ein 80-Spalten-Terminalfenster Folgendes ein: `racadm config -g cfgSerial -o cfgSerialConsoleColumns 80`.

1. Wenn Sie keine Minicom-Konfigurationsdatei haben, fahren Sie mit dem nächsten Schritt fort.

   Wenn Sie eine Minicom-Konfigurationsdatei haben, geben Sie `minicom <Minicom-Konfigurationsdateiname>` ein und fahren Sie mit Schritt 14 fort.

2. Geben Sie bei der Linux-Eingabeaufforderung `minicom -s` ein.
3. Wählen Sie die Option **Seriellen Anschluss einrichten** aus, und drücken Sie die Eingabetaste.
4. Drücken Sie <a> und wählen Sie dann das entsprechende serielle Gerät aus (Beispiel: **/dev/ttyS0**).
5. Drücken Sie <e> und stellen Sie dann die Option **Bps/Par/Bits** auf **115200 8N1**.
6. Drücken Sie <f> und stellen Sie dann die **Hardware-Datenflusssteuerung** auf **Ja** und die **Software-Datenflusssteuerung** auf **Nein**.

   Um das Menü **Seriellen Anschluss einrichten** zu beenden, drücken Sie die Eingabetaste.

7. Wählen Sie **Modem und Wählen** aus, und drücken Sie die Eingabetaste.
8. Drücken Sie im Menü **Modem-Wählen und Parameter-Setup** die Rücktaste, um die Einstellungen **init**, **reset**, **connect** und **hangup** zu löschen, sodass Sie leer sind.
9. Drücken Sie auf Eingabetaste, um jeden leeren Wert zu speichern.
10. Wenn alle angegebenen Felder gelöscht sind, drücken Sie die Eingabetaste, um das Menü **Modem-Wählen und Parameter-Setup** zu beenden.
11. Wählen Sie **Setup als config_name speichern** aus und drücken Sie die Eingabetaste.
12. Wählen Sie **Minicom beenden** aus und drücken Sie die Eingabetaste.
13. An der Befehls-Shell-Eingabeaufforderung geben Sie `minicom <Minicom-Konfigurationsdateiname>` ein
14. Drücken Sie <Strg+a>, <x>, <Eingabe>, um Minicom zu beenden.

Stellen Sie sicher, dass das Minicom-Fenster eine Anmeldeaufforderung anzeigt. Wenn die Anmeldeaufforderung angezeigt wird, wurde Ihre Verbindung erfolgreich hergestellt. Sie können sich jetzt anmelden und auf die CMC-Befehlszeilenschnittstelle zugreifen.

Erforderliche Minicom-Einstellungen

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

Tabelle 3-3. Minicom-Einstellungen

Einstellung der Beschreibung	Erforderliche Einstellung
Bit/s/Par/Bit	115200 8N1
Hardware-Datenflusssteuerung	Ja
Software-Datenflusssteuerung	Nein
Terminalemulation	ANSI
Modemwahl- und Parameter-Einstellungen	Löschen Sie die Einstellungen **init**, **reset**, **connect** und **hangup**, sodass sie leer sind

---

Verbindung zu Servern oder Modulen mit dem connect-Befehl herstellen

Der CMC kann eine Verbindung herstellen, um die serielle Konsole von Servern oder E/A-Modulen umzuleiten. Für Server kann die Umleitung der seriellen Konsole auf verschiedene Arten erzielt werden:

- über die CMC-Befehlszeile mit dem connect- oder racadm connect-Befehl. Weitere Informationen über connect finden Sie beim Abschnitt über den Befehl **racadm connect** im *Dell Chassis Management Controller Administrator-Referenzhandbuch*.
- mit der seriellen Konsolenumleitungsfunktion der iDRAC-Webschnittstelle.
- mit der iDRAC-Seriell über LAN (SOL)-Funktionalität.

Bei einer seriellen, Telnet- oder SSH-Konsole unterstützt der CMC den Befehl connect, um eine serielle Verbindung zu einem Server oder EAMs herzustellen. Die serielle Serverkonsole umfasst sowohl die BIOS-Boot- und Setup-Bildschirme als auch die serielle Betriebssystemkonsole. Für E/A-Module ist die serielle Schaltkonsole verfügbar.

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

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

ANMERKUNG: Wenn ein EAMl Konsolenumleitung nicht unterstützt, wird beim Befehl connect eine leere Konsole angezeigt. Wenn Sie in diesem Fall zur CMC- Konsole zurückkehren möchten, geben Sie die Escape-Sequenz ein. Die standardmäßige Konsolen-Escape-Sequenz ist <Strg>\.

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

```
connect switch-n
```

wobei n eine EAM-Kennung a1, a2, b1, b2, c1, und c2 ist.

EAMse werden A1, A2, B1, B2, C1 und C2 bezeichnet. (Beachten Sie Abbildung 10-1 für eine Illustration der Positionierung der EAMs im Gehäuse.) Wenn Sie sich beim **connect**-Befehl auf die EAMs beziehen, werden die EAMs Weichen zugewiesen, wie in Tabelle 3-4 dargestellt.

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

Bezeichnung des E/A-Moduls	Switch
A1	Switch-a1
A2	Switch-a2
B1	Switch-b1
B2	Switch-b2
C1	Switch-c1
C2	Switch-c2

ANMERKUNG: Es kann nur eine EAM-Verbindung pro Gehäuse zu einem bestimmten Zeitpunkt aktiv sein.

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

Um eine Verbindung zu einer seriellen Konsole eines verwalteten Servers herzustellen, verwenden Sie den Befehl connect server-n, wobei -n die Steckplatznummer des Servers ist. Sie können auch den Befehl racadm connect server-n verwenden. Wenn Sie mit der Option -b eine Verbindung zu einem Server aufbauen, wird eine binäre Datenübertragung vorausgesetzt und das Escape-Zeichen wird deaktiviert. Wenn der iDRAC nicht verfügbar ist, sehen Sie die Fehlermeldung `No route to host (Keine Route zum Host)`.

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

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

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

BIOS des verwalteten Servers für die serielle Konsolenumleitung konfigurieren

Es ist erforderlich, mit dem iKVM (siehe "Server mit iKVM verwalten") eine Verbindung zum verwalteten Server herzustellen oder über die iDRAC-Web-GUI (siehe *iDRAC-Benutzerhandbuch* unter **support.dell.com/manuals**) eine VKVM-Sitzung aufzubauen und die folgenden Schritte durchzuführen:

Die serielle Kommunikation ist im BIOS standardmäßig ausgeschaltet. Um die Daten der Hosttextkonsole zu 'Seriell über LAN' umzuleiten, müssen Sie die Konsolenumleitung über COM1 aktivieren. So ändern Sie die BIOS-Einstellung:

1. Starten Sie den verwalteten Server.
2. Drücken Sie <F2>, um das BIOS-Setup-Dienstprogramm während des POST aufzurufen.
3. Scrollen Sie zu Serielle Kommunikation herunter, und drücken Sie die Eingabetaste. Im Popup-Dialogfeld wird die Liste der seriellen Kommunikation mit den folgenden Optionen angezeigt:
   - Aus
   - Ein ohne Konsolenumleitung
   - Ein mit Konsolenumleitung über COM1

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

Windows für serielle Konsolenumleitung konfigurieren

Es ist keine Konfiguration erforderlich für Server unter den Microsoft® Windows Server®-Versionen, beginnend mit Windows Server 2003. Windows erhält Informationen vom BIOS und aktiviert die spezielle Verwaltungskonsole (SAC) auf COM1.

Linux während des Starts für die Umleitung der seriellen Konsole konfigurieren

Die folgenden Schritte beziehen sich speziell auf den Linux GRand Unified Bootloader (GRUB). Ähnliche Änderungen wären erforderlich, um einen anderen Bootloader zu verwenden.

ANMERKUNG: Beim Konfigurieren des Client-VT100-Emulationsfensters stellen Sie das Fenster bzw. die Anwendung, die die umgeleitete Konsole anzeigt, auf 25 Reihen x 80 Spalten ein, um eine ordnungsgemäße Textanzeige sicherzustellen, Andernfalls werden einige Textbildschirmanzeigen möglicherweise nicht richtig dargestellt werden.

Die Datei **/etc/grub.conf** muss wie folgt bearbeitet werden:

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

```
serial -unit=1 -speed=57600
terminal -timeout=10 serial
```

2. Hängen Sie zwei Optionen an die Kernel-Zeile an:

```
kernel..... console=ttyS1,57600
```

3. Wenn **/etc/grub.conf** eine splashimage-Direktive enthält, kommentieren Sie sie aus.

Im folgenden Beispiel sind die Änderungen zu sehen, die in diesem Verfahren beschrieben werden.

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes
# to this file
# NOTICE:  You do not have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /, e.g.
#          root (hd0,0)
#          kernel /boot/vmlinuz-version ro root= /dev/sdal
#          initrd /boot/initrd-version.img
#
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz

serial --unit=1 --speed=57600
terminal --timeout=10 serial

title Red Hat Linux Advanced Server (2.4.9-e.3smp)
   root (hd0,0)
   kernel /boot/vmlinuz-2.4.9-e.3smp ro root= /dev/sda1 hda=ide-scsi console=ttyS0 console= ttyS1,57600
   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 s
   initrd /boot/initrd-2.4.9-e.3.im

(# grub.conf, erstellt durch
#
# Beachten Sie, dass grub nach dem Vornehmen von Änderungen nicht erneut ausgeführt werden muss.
# zu dieser Datei
# HINWEIS:  Sie haben keine /boot-Partition.  Dies bedeutet, dass
#          alle Kernel und initrd-Pfade relativ zu / sind, z. B.
#          root (hd0,0)
#          kernel /boot/vmlinuz-version ro root= /dev/sdal
#          initrd /boot/initrd-version.img
#
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz
```

```
serial -unit=1 -speed=57600
terminal -timeout=10 serial

Titel 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
Titel Red Hat Linux Advanced Server-up (2.4.9-e.3)
   root (hd0,00)
   kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s
   initrd /boot/initrd-2.4.9-e.3.im)
```

Verwenden Sie bei der Verarbeitung der Datei **/etc/grub.conf** die folgenden 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 dem seriellen COM2-Anschluss 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


(#
# inittab  Diese Datei beschreibt, wie der INIT- Prozess
#          konfiguriert werde sollte für ein bestimmtes
#          Betriebsniveau.
#
# Autor:  Miquel van Smoorenburg
#          Geändert für RHS Linux von Marc Ewing und
#          Donnie Barnes
#
# Standard-Ausführungsstufe. Die von RHS verwendeten Ausführungsstufen lauten:
#   0 - Halt (NICHT initdefault einstellen)
#   1 - Einzelbenutzermodus
#   2 - Multibenutzer, ohne NFS (wie 3, wenn Sie kein
#       Netzwerk haben)
#   3 - Voller Multibenutzer-Modus
#   4 - Nicht verwendet
#   5 - X11
#   6 - Neu starten (NICHT initdefault einstellen)
#
id:3:initdefault:

# Systeminitialisierung.
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



# Auf jeder Ausführungsstufe auszuführende Befehle.
ud::once:/sbin/update

# Trap STRG-ALT-ENTF
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# Wenn die USV Stromausfall anzeigt, davon ausgehen, dass einige
# Minuten Strom verbleiben. Planen Sie ein Herunterfahren in 2 Minuten.
# Es wird hierbei natürlich angenommen, dass Strom anliegt und die
# USV angeschlossen ist und korrekt funktioniert.
pf::powerfail:/sbin/shutdown -f -h +2 "Stromausfall; System fährt herunter"
# Wenn Strom wiederhergestellt wurde, bevor das Herunterfahren eingeleitet wurde, brechen Sie ab.
pr:12345:powerokwait:/sbin/shutdown -c "Strom wiederhergestellt; Herunterfahren abgebrochen"



# gettys in Standard-Ausführungsstufen ausführen
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

# xdm in Ausführungsstufe 5 ausführen
```

```
# xdm ist jetzt ein separater Dienst
x:5:respawn:/etc/X11/prefdm -nodaemon
```

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

- Fügen Sie eine neue Zeile mit dem Namen des seriellen tty für COM2 hinzu:

```
ttyS1
```

Das folgende Beispiel zeigt eine Beispieldatei mit der neuen Zeile.

```
vc/1
vc/2
vc/3
vc/4
vc/5
vc/6
vc/7
vc/8
vc/9
vc/10
vc/11
tty1
tty2
tty3
tty4
tty5
tty6
tty7
tty8
tty9
tty10
tty11
ttyS1
```

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Glossar

Dell Chassis Management Controller Firmware Version 2.10, Benutzerhandbuch

Active Directory

Active Directory ist ein zentralisiertes, standardisiertes System zur Automatisierung der Netzwerkverwaltung von Benutzerdaten, Sicherheit und verteilten Ressourcen und macht die Zusammenarbeit mit anderen Verzeichnissen möglich. Active Directory ist besonders für dezentrale Netzwerkumgebungen ausgelegt.

ARP

Address Resolution Protocol (Adressenauflösungsprotokoll), eine Methode, die Ethernet-Adresse eines Hosts aus seiner Internet-Adresse ermittelt.

ASCII

American Standard Code for Information Interchange (US-Standardcode für Informationsaustausch). Eine Codedarstellung zur Anzeige oder zum Drucken von Buchstaben, Zahlen und anderen Zeichen.

BIOS

Basic Input/Output System (Grundlegendes Eingabe-/Ausgabesystem), der Teil der Systemsoftware, der die Schnittstelle niedrigster Ebene zu Peripheriegeräten angibt und der die erste Stufe des Systemstartprozesses steuert, einschließlich der Installierung des Betriebssystems in den Speicher.

Blade

Ein eigenständiger Server, gestaltet für hoch-dichte Einbaugehäuse.

Bus

Eine Reihe von Leitern, über die verschiedene Funktionseinheiten in einem Computer verbunden sind. Busse werden nach dem Typ der transportierten Daten benannt, wie Datenbus, Adressbus oder PCI-Bus.

CA

Eine Zertifizierungsstelle ist ein Geschäftsunternehmen, das in der IT -Branche dafür anerkannt ist, hohe Standards der zuverlässigen Abschirmung, Identifizierung und anderer wichtiger Sicherheitskriterien einzuhalten. Beispiele von CAs schließen Thawte und VeriSign ein. Nachdem die CA Ihr CSR empfangen hat, werden die in der CSR enthaltenen Informationen eingesehen und überprüft. Wenn der Bewerber den Sicherheitsstandards der CA genügt, wird für den Bewerber ein Zertifikat ausgestellt, das den Bewerber bei Übertragungen über Netzwerke oder über das Internet eindeutig identifiziert.

CD

Compact Disc

CLI

Befehlszeilenoberfläche

CMC

Der Dell Chassis Management Controller, stellt Remote-Verwaltungsfähigkeiten und Stromregelungsfunktionen für Dell PowerEdge-Systeme bereit.

DHCP

Dynamic Host Configuration Protocol (Dynamisches Host-Konfigurationsprotokoll), ein Mittel zur dynamischen Zuweisung von IP-Adressen an Computer in einem lokalen Netzwerk.

DLL

Bibliothek für dynamisches Verbinden, eine Bibliothek von kleinen Programmen, von denen eins, wenn erforderlich, durch ein größeres Programm gerufen werden kann, das im System läuft. Die kleineren Funktionen ermöglichen dem größeren Programm mit einem bestimmten Gerät, wie Drucker oder Scanner, zu kommunizieren.

DNS

Domänennamensystem

erweitertes Schema

Eine mit Active Directory verwendete Lösung, um Benutzerzugriff auf den CMC zu bestimmen; verwendet von Dell definierte Active Directory-Objekte.

FQDN

Fully Qualified Domain Name (Vollqualifizierter Domänenname), ein Domänenname, der den absoluten Standort eines Moduls in der Hierarchie der DNS-Struktur angibt. Microsoft® Active Directory® unterstützt nur einen FQDN bis zu maximal 64 Bytes.

FSMO

Flexible Single Master Operation (flexibler, einzelner, übergeordneter Vorgang), eine Domänen-Controller-Aufgabe von Microsoft Active Directory, die die Atomarität eines Erweiterungsvorgangs gewährleistet.

GB1

Der Uplink-Port des Gehäuses

GMT

Greenwich Mean Time (Mittlere Greenwich-Zeit). GMT ist die allgemeine Standardzeitzone für jeden Ort der Welt. GMT stellt nominell die mittlere Sonnenzeit entlang des durch das Greenwich Observatory außerhalb Londons, Großbrittanien verlaufenden Nullmeridians (0 Längengrad) dar.

GUI

Grafische Benutzeroberfläche, die eine Anzeigenoberfläche eines Computers darstellt, in der Elemente wie z. B. Fenster, Dialogfelder und Schaltflächen verwendet werden, im Gegensatz zu einer Befehlsaufforderungsschnittstelle, in der alle Eingaben und Anzeigen als Text dargestellt werden.

Hardwareprotokoll

Ein vom CMC erstellter Eintrag an Ereignissen, die mit Hardware im Gehäuse in Beziehung stehen.

ICMP

Internet Control Message Protocol (Internetsteuerungs-Meldungsprotokoll), eine Methode, mit der Betriebssysteme Fehlermeldungen senden können.

ID

Abkürzung für Identifier (Bezeichner), wird normalerweise als Bezeichnung für einen Benutzer-Bezeichner (Benutzer-ID) oder Objekt-Bezeichner (Objekt-ID) verwendet.

iDRAC

Der Dell Integrated Remote Access Controller, eine Systemverwaltungs-Hardware und Softwarelösung, die Fernzugriff-Verwaltungsfähigkeiten, Wiederherstellung bei abgestürzten Systemen sowie Stromsteuerungsfunktionen für Dell PowerEdge-Systeme bietet.

iKVM

Avocent® Integriertes KVM-Weichenmodul; ein optionales, an das Gehäuse anschließbares, "plug-and-play"-fähiges Modul, das lokalen Tastatur-, Maus- und Bildschirmzugriff auf die 16 Server im Gehäuse ermöglicht sowie die zusätzliche Option der Dell CMC-Konsole, die die Verbindung zum aktiven CMC im Gehäuse herstellt.

IOMINF

E/A-Infrastrukturgerät

IP

Internetprotokoll. IP ist die Netzwerkschicht für TCP/IP. IP ermöglicht Paket-Routing, Fragmentierung und Reorganisation.

IPMB

Intelligent Platform Management Bus; wird bei der Systemverwaltungstechnologie verwendet.

Kbps oder kBit/s

Kilobit pro Sekunde, eine Datentransferrate.

LAN

Local Area Network (lokales Netzwerk)

LDAP

Lightweight Directory Access Protocol (Lightweight-Verzeichniszugriffsprotokoll)

LED

Light-Emitting Diode (Leuchtdiode)

LOM

Local Area Network on Motherboard (Lokales Netzwerk auf der Hauptplatine)

MAC

Akronym für Media Access Control (Medienzugriffssteuerung), wobei es sich um eine Netzwerkunterschicht zwischen einem Netzwerkknoten und der physikalischen Netzwerkschicht handelt.

MAC-Adresse

Media Access Control Address (Medienzugriffssteuerungs-Adresse) ist eine eindeutige Adresse, die in den physischen Komponenten einer NIC integriert ist.

Management Station

Ein System, das im Remote-Zugriff auf den CMC zugreift.

Mbps oder MBit/s

Megabit pro Sekunde, wobei es sich um eine Datentransferrate handelt.

MC

Mezzanine-Karte

Microsoft Active Directory

Ein zentralisiertes und standardisiertes System, das Netzwerkverwaltung von Benutzerdaten, Sicherheit und verteilten Ressourcen automatisiert, und Interoperation mit anderen Verzeichnissen aktiviert. Active Directory ist besonders für dezentrale Netzwerkumgebungen ausgelegt.

NIC

Network Interface Card (Netzwerkschnittstellenkarte), eine Adapterplatine, die in einem Computer eingebaut ist, um eine physische Verbindung zu einem Netzwerk herzustellen.

Nicht-Beständiges Protokoll

Ein Protokoll, das gelöscht wird, wenn der CMC neu startet.

OID

Object Identifier (Objektkennung)

OSCAR

On Screen Configuration and Reporting (Bildschirmkonfiguration und -berichterstattung), eine grafische Benutzeroberfläche, die für den iKVM-Zugang verwendet wird.

PCI

Abkürzung für Peripheral Component Interconnect (Verbindung peripherer Komponenten), eine Standardschnittstellen- und Bustechnologie zum Anschluss von Peripheriegeräten an ein System und zur Kommunikation mit diesen Peripheriegeräten.

POST

Akronym für Power-On Self-Test (Einschaltselbsttest), eine Folge von Diagnosetests, die automatisch beim Einschalten eines Systems ausgeführt werden.

RAC

Remote-Access-Controller

RAM

Random-Access Memory (Speicher mit wahlfreiem Zugriff). Der RAM-Speicher ist ein lesbarer und beschreibbarer Allzweckspeicher in Systemen.

RAM-Platte

Ein speicherresidentes Programm, das ein Festplattenlaufwerk emuliert.

ROM

Read-Only Memory (Nur-Lesen Speicher), Daten können aus dem Speicher gelesen, jedoch nicht in den Speicher geschrieben werden.

RPM

Red Hat Package Manager, ein Paketverwaltungssystem für das Linux-Betriebssystem Red Hat Enterprise. RPM verwaltet die Installation von Softwarepaketen. Es ist einem Installationsprogramm ähnlich.

SEL

Systemereignis- oder Hardwareprotokoll

SMTP

Simple Mail Transfer Protocol (einfaches Mailübertragungsprotokoll), wird verwendet zum Übertragen elektronischer Mails zwischen Systemen—meist über ein Ethernet.

SNMP

Simple Network Management Protokoll, ausgelegt für die Verwaltung von Knoten in einem IP -Netzwerk. iDRACs sind SNMP-verwaltete Geräte (Knoten).

SNMP-Trap

Eine vom CMC erzeugte Meldung (Ereignis), die Informationen über Statusänderungen auf dem verwalteten System oder über mögliche Hardwarestörungen enthält.

SSH

Secure Shell, ein Netzwerkprotokoll, das den Datenaustausch zwischen zwei Computern über einen sicheren Kanal ermöglicht.

SSL

Secure Sockets Layer, ein Protokoll, das eine sichere Datenübertragung über Netzwerke bereitstellt.

Standardschema

Eine mit Active Directory verwendete Lösung, um Benutzerzugriff auf den CMC zu bestimmen; verwendet nur Active Directory-Gruppenobjekte.

STK

Der Stacking-Port des Gehäuses

TCP/IP

Abkürzung für Transmission Control Protocol/Internet Protocol (Übertragungssteuerungsprotokoll/Internetprotokoll), das den Standard-Ethernetprotokollsatz repräsentiert, der die Protokolle der Netzwerkschicht und der Übertragungsschicht enthält.

TFTP

Abkürzung für Trivial File Transfer Protocol (Trivial-Dateiübertragungsprotokoll), ein einfaches Dateiübertragungsprotokoll, das zum Herunterladen von Startcode auf datenträgerlose Geräte oder Systeme verwendet wird.

UDP

User Datagram Protocol (Protokoll für Benutzerdatagramme)

USB

Universal Serial Bus, ein serieller Bus-Standard für Geräteschnittstellen.

USV

Uninterruptible Power Supply (unterbrechungsfreie Stromversorgung)

UTC

Universal Coordinated Time. *Siehe* GMT.

Verzögerungszeit (OSCAR-Benutzeroberfläche)

Die Anzahl von Sekunden, bevor das OSCAR-Hauptdialogfeld angezeigt wird, nachdem die Taste <DRUCK> gedrückt wird.

vKVM

Virtual Keyboard-Video-Mouse Console (virtuelle Tastatur-Video-Maus-Konsole)

VLAN

Akronym für Virtual Local Area Network (virtuelles lokales Netzwerk)

VNC

Virtual Network Computing (virtueller Netzwerkcomputerbetrieb)

VT-100

Abkürzung für Video Terminal 100, das von den meisten allgemeinen Terminal-Emulationsprogrammen verwendet wird.

WAN

Wide Area Network (Weitbereichsnetz)

WWN

World Wide Name, ein eindeutiger Wert, der Fibre Channel-Knoten in der Bitübertragungsschicht repräsentiert.

Zertifikatsignierungsanforderung (CSR)

Eine digitale Anfrage an eine Zertifizierungsstelle nach einem sicheren Serverzertifikat.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Dell Chassis Management Controller Firmware Version 2.10, Benutzerhandbuch

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

VORSICHTSHINWEIS: Mit einem VORSICHTSHINWEIS werden Sie auf eine potenziell gefährliche Situation hingewiesen, die zu Sachschäden, Verletzungen oder zum Tod führen könnte.

_____

August 2009

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

FlexAddress verwenden

Dell Chassis Management Controller Firmware Version 2.10, Benutzerhandbuch

Die FlexAddress-Funktion ist ein optionales Upgrade, das Servermodulen ermöglicht, die werkseitig zugewiesenen "World Wide Name" und "Media Access Control" (WWN/MAC)-Netzwerkkennungen durch vom Gehäuse bereitgestellte WWN/MAC zu ersetzen.

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

FlexAddress versetzt den CMC in die Lage, WWN/MAC-IDs an einen konkreten Steckplatz zu übergeben und die werkseitigen IDs aufzuheben. Wird das Servermodul ausgetauscht, bleiben die Steckplatz-basierten WWN/MAC-IDs erhalten. Diese Funktion eliminiert die Notwendigkeit, die Netzwerkverwaltungsinstrumente für das Ethernet und die SAN-Ressourcen wegen eines neuen Servermoduls neu zu konfigurieren.

Außerdem tritt der Vorgang des Aufhebens nur ein, wenn ein Servermodul in ein FlexAddress-aktiviertes Gehäuse eingesetzt wird; es werden keine dauerhaften Änderungen am Servermodul vorgenommen. Wird ein Servermodul in ein Gehäuse eingesetzt, das FlexAddress nicht unterstützt, werden die werkseitigen WWN/MAC-IDs verwendet.

Vor der Installation von FlexAddress können Sie den MAC-Adressenbereich, der auf einer FlexAddress-Funktionskarte enthalten ist, feststellen indem Sie die SD-Karte in einen USB-Speicherkartenleser einsetzen und die Datei pwwn_mac.xml betrachten. Diese Klartext-XML-Datei auf der SD-Karte wird ein XML-Segment, mac_start, beinhalten, das die hexadezimale MAC-Start-Adresse für diesen einzigartigen MAC-Adressbereich enthält. Das Segment mac_count ist die Gesamtzahl der MAC-Adressen, die die SD-Karte zuweist. Der gesamte zugewiesen MAC-Bereich kann wie folgt bestimmt werden:

<mac_start> + 0xCF (208 - 1) = mac_end

wobei 208 mac_count ist und die Formel lautet
<mac_start> + <mac_count> - 1 = <mac_end>

Zum Beispiel: (starting_mac)00188BFFDCFA + 0xCF =(ending_mac)00188BFFDDC9.

ANMERKUNG: Sperren Sie die SD-Karte vor dem Einsetzen in den USB- Speicherkartenleser, um versehentliche Änderungen des Inhalts zu verhindern. Die SD-Karte *muss gesperrt* sein, bevor Sie sie in den CMC einsetzen.

Aktivierung von FlexAddress

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

Komponente	Minimale erforderte Version
Ethernet Mezzanine-Karte - Broadcom M5708t, 5709, 5710	Startcode-Firmware 4.4.1 oder später iSCSI-Startfirmware 2.7.11 oder später PXE Firmware 4.4.3 oder später
FC Mezzanine-Karte - QLogic QME2472, FC8	BIOS 2.04 oder später
FC Mezzanine-Karte - Emulex LPe1105-M4, FC8	BIOS 3.03a3 und Firmware 2.72A2 oder später
Servermodul BIOS	PowerEdge M600 – BIOS 2.02 oder später

	PowerEdge M605 – BIOS 2.03 oder später PowerEdge M805 PowerEdge M905 PowerEdge M610 PowerEdge M710
PowerEdgeM600/M605 LAN auf der Hauptplatine (LAN on motherboard; LOM)	Startcode-Firmware 4.4.1 oder später iSCSI-Startfirmware 2.7.11 oder später
iDRAC	Version 1.50 oder später für PowerEdge *xx*0*x* Systeme Version 2.10 oder später für PowerEdge *xx*1*x* Systeme
CMC	Version 1.10 oder später

ANMERKUNG: Alle Systeme, die später als Juni 2008 bestellt wurden, haben korrekte Firmwareversionen.

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

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

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

Beachten Sie auch das Dokument Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification für Anleitungen zur SD-Karteninstallation.

ANMERKUNG: Die SD-Karte enthält eine FlexAddress-Funktion. Auf der SD-Karte befindliche Daten sind verschlüsselt und dürfen auf keine Weise vervielfältigt oder verändert werden, da dies die Systemfunktion beeinträchtigen und zu Fehlfunktionen führen könnte.

ANMERKUNG: Die SD-Karte kann nur für ein einzelnes Gehäuse verwendet werden. Wenn Sie mehrere Gehäuse haben, ist es notwendig weitere SD-Karten zu erwerben.

Die Aktivierung der FlexAddress-Funktion findet automatisch bei Neustart des CMC mit der installierten SD-Funktionskarte statt; diese Aktivierung bindet diese Funktion an das Gehäuse. Wenn Sie eine SD-Karte auf einem redundanten CMC installiert haben, wird die Aktivierung der FlexAddress-Funktion erst stattfinden, nachdem Sie den redundanten CMC zum aktiven gemacht haben. Beachten Sie auch das Dokument Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification für Information dazu, wie man einen redundanten CMC aktiv macht.

Wenn der CMC neu startet, bestätigen Sie den Aktivierungsprozess, indem Sie die Schritte im nächsten Abschnitt, "Bestätigung FlexAddress-Aktivierung", ausführen.

Bestätigung FlexAddress-Aktivierung

Um die korrekte Aktivierung von FlexAddress sicherzustellen, können RACADM-Befehle verwendet werden, um die SD-Funktionskarte und die FlexAddress-Aktivierung zu bestätigen.

Verwenden Sie den folgenden RACADM-Befehl, um die SD-Funktionskarte und ihren Status zu bestätigen:

```
racadm featurecard -s
```

Die folgende Tabelle listet die Statusmeldungen auf, die durch den Befehl zurückgegeben werden auf.

Tabelle 6-1. Statusmeldungen, geliefert durch den Befehl featurecard -s

Statusmeldung	Aktionen
Keine Funktionskarte eingesetzt.	Prüfen Sie den CMC um sicherzustellen, dass die SD-Karte korrekt eingesetzt wurde. Stellen Sie in einer redundanten CMC-Konfiguration sicher, dass der CMC mit der installierten SD-Funktionskarte der aktive CMC ist und nicht der Standby-CMC.
Die eingesetzte Funktionskarte ist gültig und enthält die folgenden FlexAddress-Funktion(en): Die Funktionskarte ist an dieses Gehäuse gebunden.	Keine Aktion erforderlich.
Die eingesetzte SD-Karte ist gültig und enthält die folgende(n) FlexAddress-Funktion(en): Die Funktionskarte ist an ein anderes Gehäuse gebunden, svctag = ABC1234, SD-Karte SN = 01122334455	Entfernen Sie die SD-Karte; finden und installieren Sie die SD-Karte für das aktuelle Gehäuse.
Die eingesetzte Funktionskarte ist gültig und enthält die folgenden Funktion(en) FlexAddress: Die Funktionskarte ist an kein Gehäuse gebunden.	Die Funktionskarte kann in ein anderes Gehäuse eingesetzt oder für das aktuelle Gehäuse neu reaktiviert werden. Um sie für das aktuelle Gehäuse zu reaktivieren, geben Sie racadm racreset ein, bis das CMC-Modul mit der installierten SD-Karte aktiv wird.

Verwenden Sie den folgenden RACADM-Befehl, um alle aktivierten Funktionen dieses Gehäuses anzuzeigen.

```
racadm feature -s
```

Der Befehl liefert folgende Statusmeldung:

```
Feature = FlexAddress

Date Activated (Aktivierungsdatum) = 8 April 2008 - 10:39:40

Feature installed from SD-card SN = 01122334455
```

Gibt es keine aktiven Funktionen auf dem Gehäuse, wird der Befehl folgende Meldung liefern:

```
racadm feature -s

No features active on the chassis (Keine Funktionen auf dem Gehäuse aktiviert.)
```

Weitere Informationen über die RACADM-Befehle finden Sie in den Abschnitten feature- und featurecard-Befehl im *Dell Chassis Management Controller Administrator-Referenzhandbuch*.

Deaktivierung von FlexAddress

Die Funktion FlexAddress kann deaktiviert werden und die SD-Karte kann mittels eines RACADM-Befehls auf einen Zustand vor der Installation zurückgesetzt werden. Es gibt keine Deaktivierungsfunktion in der Webschnittstelle. Die Deaktivierung versetzt die SD-Karte zurück in ihren Originalzustand, mit dem sie für ein anderes Gehäuse installiert und aktiviert werden kann.

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

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

Deaktivierung von FlexAddress

Verwenden Sie den folgenden RACADM-Befehl zur Deaktivierung der Funktion FlexAddress und zur Wiederherstellung der SD-Karte:

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

Der Befehl liefert folgende Statusmeldung bei erfolgreicher Ausführung:

```
feature FlexAddress is deactivated on the chassis successfully. (Die Funktion FlexAddress wurde erfolgreich für das Gehäuse deaktiviert.)
```

Wurde das Gehäuse vor der Ausführung nicht heruntergefahren, wird der Befehl mit folgender Fehlermeldung fehlschlagen:

```
ERROR: Unable to deactivate the feature because the chassis is powered ON (FEHLER: Nicht möglich die Funktion zu deaktivieren, da das Gehäuse eingeschaltet ist.)
```

Weitere Informationen über den Befehl finden Sie im Abschnitt zum feature-Befehl im *Dell Chassis Management Controller Administrator-Referenzhandbuch*.

FlexAddress mittels CLI konfigurieren

ANMERKUNG: Sie müssen beides aktivieren, Steckplatz und Architektur, sodass die Gehäuse-zugewiesene MAC-Adresse auf den iDRAC übertragen wird.

ANMERKUNG: Sie können den Status von FlexAddress auch über die grafische Benutzeroberfläche einsehen. Weitere Informationen finden Sie unter "FlexAddress".

Sie können die Befehlszeilenschnittstelle nutzen, um FlexAddress auf Architekturbasis zu aktivieren oder zu deaktivieren. Zusätzlich können Sie die Funktion Steckplatz-basiert aktivieren/deaktivieren. Nachdem Sie die Funktion auf Architekturbasis aktiviert haben, können sie die zu aktivierenden Steckplätze auswählen. Ist zum Beispiel nur Architektur-A aktiviert, werden alle aktivierten Steckplätze FlexAddress nur für die Architektur-A aktiviert haben. In allen anderen Architekturen werden die werkseitigen WWN/MAC-IDs des Servers verwendet. Diese Funktion funktioniert nur, wenn die Architektur aktiviert und der Server ausgeschaltet ist.

Aktivierte Steckplätze sind für alle aktivierten Architekturen FlexAddress-fähig. So ist es zum Beispiel nicht möglich, Architektur-A und -B zu aktivieren und FlexAddress auf Steckplatz 1 nur für Architektur-A, nicht aber für Architektur-B, zu aktivieren.

Verwenden Sie den folgenden RACADM-Befehl zum Aktivieren/Deaktivieren von Architekturen:

```
racadm setflexaddr [-f <ArchitekturName> <Status>]
```

```
<Architekturname> = A, B, C oder iDRAC
```

```
<Status> = 0 oder 1
```

Wobei 0 deaktiviert und 1 aktiviert bedeuten.

Verwenden Sie den folgenden RACADM-Befehl zum Aktivieren/Deaktivieren von Steckplätzen:

```
racadm setflexaddr [-i <Steckplatz#> <Status>]
```

```
<Steckplatz#> = 1 bis 16
```

```
<Status> = 0 oder 1
```

Wobei 0 deaktiviert und 1 aktiviert bedeuten.

Weitere Informationen über den Befehl finden Sie im Abschnitt setflexaddr-Befehl im *Dell Chassis Management Controller Administrator-Referenzhandbuch*.

Weiterführende Konfiguration von FlexAddress für Linux

Wenn Sie von einer Server-zugewiesenen MAC-ID zu einer Gehäuse-zugewiesenen MAC-ID auf Linux-basierten Betriebssystemen wechseln, sind zusätzliche Konfigurationsschritte nötig:

- SUSE Linux Enterprise Server 9 und 10: Sie müssen u. U. YAST (Yet another Setup Tool) auf den Linux-System laufen lassen, um ihre Netzwerkgeräte zu konfigurieren, und dann die Netzwerkdienste neu starten.
- Red Hat® Enterprise Linux® 4(RHEL) und RHEL 5: Sie müssen Kudzu laufen lassen, ein Hilfsprogramm zur Erkennung und Konfiguration neuer/geänderter Hardware im System. Kudzu präsentiert das Hardware Discovery Menu (Hardwareerkennung), das die MAC-Adressänderung erkennt, wenn Hardware entfernt und durch neue Hardware ersetzt wird.

Anzeigen des FlexAddress-Status mittels CLI

Sie können die Befehlszeilenschnittstelle nutzen, um Statusinformationen zu FlexAddress anzuzeigen. Sie können Statusinformationen für das gesamte Gehäuse oder für einen bestimmten Steckplatz anzeigen lassen. Die angezeigten Informationen beinhalten:

- Architekturkonfiguration
- FlexAddress aktiviert/deaktiviert
- Steckplatznummer und -name
- Gehäuse-zugewiesene und Server-zugewiesene Adressen
- Verwendete Adressen

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

```
racadm getflexaddr
```

Um den FlexAddress-Status für einen bestimmten Steckplatz anzuzeigen:

```
racadm getflexaddr [-i <Steckplatz#>]
```

```
<Steckplatz#> = 1 bis 16
```

Unter "FlexAddress mittels CLI konfigurieren" finden Sie weitere Details zur FlexAddress-Konfiguration. Weitere Informationen über den Befehl finden Sie im Abschnitt getflexaddr-Befehl im *Dell Chassis Management Controller Administrator-Referenzhandbuch*.

FlexAddress mittels GUI konfigurieren

Wake-On-LAN mit FlexAddress verwenden

Wenn die FlexAddress-Funktion zum ersten Mal auf einem Servermodul bereitgestellt wird, erfordert dies ein Herunterfahren und erneutes Hochfahren, damit FlexAddress in Kraft tritt. FlexAddress auf Ethernet-Geräten wird vom BIOS des Systemmoduls programmiert. Damit das BIOS des Servermoduls die Adresse programmieren kann, muss es in Betrieb sein, was erfordert, dass das Servermodul eingeschaltet ist. Ist die Herunter-/Hochfahrprozedur abgeschlossen, sind

die Gehäuse-zugewiesenen MAC-IDs für die Wake-On-LAN (WOL)-Funktion verfügbar.

Fehlerbehebung FlexAddress

Dieser Abschnitt enthält Informationen zur Fehlerbehebung für FlexAddress.

1. Was wird passieren, wenn eine Funktionskarte entfernt wird?

   Nichts wird passieren. Funktionskarten können entfernt und gelagert oder im System belassen werden.

2. Was wird passieren, wenn eine Funktionskarte, die in einem Gehäuse verwendet wurde, entfernt und in ein anderes Gehäuse gesteckt wird?

   Die Webbenutzeroberfläche wird folgenden Fehler melden:

   This feature card was activated with a different chassis. It must be removed before accessing the FlexAddress feature. (Diese Funktionskarte wurde auf einem anderen Gehäuse aktiviert. Sie muss vor einem Zugriff auf die Funktion FlexAddress entfernt werden.)

   Current Chassis Service Tag (Aktuelle Gehäuse-Service-Tag-Nummer) = XXXXXXX

   Feature Card Chassis Service Tag (Gehäuse-Service-Tag-Nummer der Funktionskarte) = YYYYYYY

   Folgender Eintrag wird dem CMC-Protokoll hinzugefügt:

   cmc <Datum Zeitstempel> : feature 'FlexAddress@XXXXXXX' not activated; chassis ID= 'YYYYYYY'

3. Was passiert, wenn die Funktionskarte entfernt und eine Karte, die FlexAddress nicht unterstützt, eingesetzt wird?

   Es wird keine Aktivierung oder Änderung der Karte stattfinden. Die Karte wird vom CMC ignoriert. In dieser Situation wird der Befehl $racadm featurecard -s folgende Meldung liefern:

   No feature card inserted (Keine Funktionskarte eingesetzt.)

   ERROR: can't open file (FEHLER: kann Datei nicht öffnen)

4. Was passiert mit einer ans Gehäuse gebundenen Funktionskarte, wenn die Gehäuse-Service-Tag-Nummer neu programmiert wird?

   - Wenn die Original-Funktionskarte im aktiven CMC auf diesem oder einem beliebigen anderen Gehäuse vorhanden ist, zeigt die Webschnittstelle einen Fehler an mit der Angabe:

     This feature card was activated with a different chassis. It must be removed before accessing the FlexAddress feature. (Diese Funktionskarte wurde auf einem anderen Gehäuse aktiviert. Sie muss vor einem Zugriff auf die Funktion FlexAddress entfernt werden.)

     Current Chassis Service Tag (Aktuelle Gehäuse-Service-Tag-Nummer) = XXXXXXX

     Feature Card Chassis Service Tag (Gehäuse-Service-Tag-Nummer der Funktionskarte) = YYYYYYY

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

   - Die FlexAddress-Funktion bleibt auf dem ursprünglich gebundenen Gehäuse aktiviert. Die Funktion *Bindung dieses Gehäuses* wird das neue Service-Tag aktualisiert.

- Was ist, wenn ich zwei Funktionskarten in meinem redundanten CMC- System installiert habe? Erhalte ich eine Fehlermeldung?

  Die Funktionskarte im aktiven CMC wird aktiv und im Gehäuse installiert sein. Die zweite Karte wird vom CMC ignoriert.

6. Hat die SD-Karte einen Schreibschutz?

   Ja, hat sie. Bevor Sie die SD-Karte in das CMC-Modul installieren, bestätigen Sie, dass sich die Schreibschutzsperre in der "Entsperr"-Position befindet. Die FlexAddress-Funktion kann nicht aktiviert werden, wenn die SD-Karte schreibgeschützt ist. In dieser Situation gibt der Befehl $racadm feature -s folgende Meldung zurück:

   ```
   No features active on the chassis. ERROR: read only file system (Keine Funktionen auf dem Gehäuse aktiviert. FEHLER: schreibgeschütztes Dateisystem)
   ```

7. Was passiert, wenn keine SD-Karte im aktiven CMC-Modul steckt?

   Der Befehl $racadm featurecard -s wird folgende Meldung liefern:

   ```
   No feature card inserted (Keine Funktionskarte eingesetzt.)
   ```

8. Was passiert mit meiner FlexAddress-Funktion, wenn das Server-BIOS von Version 1.xx auf Version 2.xx aktualisiert wird?

   Das Servermodul muss heruntergefahren werden, bevor es mit FlexAddress verwendet werden kann. Nachdem die Server-BIOS-Aktualisierung abgeschlossen wurde, erhält das Servermodul solange keine gehäuseseitigen Adressen, bis der Server aus- und wieder eingeschaltet wurde.

9. Was geschieht, wenn ein Gehäuse mit einem einzelnen CMC auf Firmware vor der Version 1.10 heruntergestuft wird?

   - Die FlexAddress-Funktion und die Konfiguration werden aus dem Gehäuse entfernt.
   - Die Funktionskarte, die zum Aktivieren der Funktion auf diesem Gehäuse verwendet wurde, bleibt unverändert und an das Gehäuse gebunden. Wenn die CMC-Firmware des Gehäuses nachfolgend auf 1.10 oder später aktualisiert wird, wird die FlexAddress-Funktion durch Wiedereinführen der Original-Funktionskarte (falls erforderlich), Zurücksetzen des CMC (falls Funktionskarte nach Abschluss der Firmwareaktualisierung eingeführt wurde) und Neukonfigurieren der Funktion reaktiviert.

10. Wenn Sie in einem Gehäuse mit redundanten CMCs eine CMC-Einheit durch eine mit einer Firmware vor Version 1.10 ersetzen, muss die folgende Prozedur verwendet werden, um sicherzustellen, dass die derzeitige FlexAddress-Funktion und die Konfiguration NICHT entfernt werden.

    a. Versichern Sie sich, dass der aktive CMC auf Firmwareversion 1.10 oder höher läuft.

    b. Entfernen Sie den Stand-by-CMC und setzen Sie den neuen CMC ein.

    c. Aktualisieren Sie die Firmware des neuen Standby-CMC über den aktiven CMC auf Version 1.10 oder höher.

ANMERKUNG: Wenn Sie die Standby-CMC-Firmware nicht auf Version 1.10 oder höher aktualisieren und es findet ein Failover statt, wird die Funktion FlexAddress nicht konfiguriert, und Sie müssen die Funktion reaktivieren und neu konfigurieren.

11. Die SD-Karte war nicht im Gehäuse, als ich den Deaktivierungsbefehl auf der FlexAddress ausführte. Wie stelle ich die SD-Karte jetzt wieder her?

    Das Problem ist, dass die SD-Karte nicht zur Installation von FlexAddress auf einem anderen Gehäuse verwendet werden kann, wenn sie sich nicht im CMC befand, als FlexAddress deaktiviert wurde. Um die Nutzung der Karte wiederherzustellen, führen Sie die Karte wieder in einen CMC in dem Gehäuse ein, das damit gebunden ist, installieren Sie FlexAddress neu und deaktivieren Sie FlexAddress erneut.

12. Ich habe eine SD-Karte sowie sämtliche Firmware/Software- Aktualisierungen korrekt installiert. Ich sehe, dass FlexAddress aktiv ist, kann aber auf der Serververteilungsseite nichts zum Verteilen erkennen? Was stimmt nicht?

    Das ist ein Problem des Browser-Cache; Schließen Sie den Browser und starten Sie ihn erneut.

13. Was geschieht mit FlexAddress, wenn ich meine Gehäusekonfiguration mit dem RACADM-Befehl racresetcfg zurücksetzen muss?

    Die FlexAddress-Funktion bleibt aktiviert und einsatzbereit. Alle Architekturen und Steckplätze werden als Standard ausgewählt.

    ANMERKUNG: Es wird dringend empfohlen, dass Sie das Gehäuse herunterfahren, bevor Sie den RACADM-Befehl racresetcfg verwenden.

Befehlsmeldungen

In der folgenden Tabelle werden RACADM-Befehle und -ausgaben für häufig vorkommende FlexAddress-Situationen aufgelistet.

Tabelle 6-2. FlexAddressbefehle und -ausgaben

Situation	Befehl	Ausgabe
SD-Karte im aktiven CMC-Modul ist an eine andere Service-Tag-Nummer gebunden.	$racadm featurecard -s	The feature card inserted is valid and contains the following feature(s) (Die eingesetzte Funktionskarte ist ungültig und enthält die folgende(n) Funktion (en)) FlexAddress: The feature card is bound to another chassis, (Die Funktionskarte ist an ein anderes Gehäuse gebunden,) svctag = J310TF1 SD card SN = 0188BFFE03A
SD-Karte im aktiven CMC-Modul ist an die gleiche Service-Tag-Nummer gebunden.	$racadm featurecard -s	The feature card inserted is valid and contains the following feature(s) (Die eingesetzte Funktionskarte ist ungültig und enthält die folgende(n) Funktion (en)) FlexAddress: The feature card is bound to this chassis (Die Funktionskarte ist an dieses Gehäuse gebunden)
SD-Karte im aktiven CMC-Modul ist an keine Service-Tag-Nummer gebunden.	$racadm featurecard -s	The feature card inserted is valid and contains the following feature(s) (Die eingesetzte Funktionskarte ist ungültig und enthält die folgende(n) Funktion (en)) FlexAddress: The feature card is not bound to any chassis (Die Funktionskarte ist an kein Gehäuse gebunden)
Die Funktion FlexAddress ist auf dem Gehäuse aus irgendeinem Grunde (keine SD-Karte eingesetzt/ beschädigte SD-Karte/ Funktion deaktiviert/ SD-Karte an anderes Gehäuse gebunden) nicht aktiv.	$racadm setflexaddr [-f <ArchitekturName> <SteckplatzStatus>] ODER $racadm setflexaddr [-i <Steckplatz#> <SteckplatzStatus>]	ERROR: Flexaddress feature is not active on the chassis (FEHLER: Die Funktion FlexAddress ist nicht auf dem Gehäuse aktiviert)
Gastbenutzer versucht FlexAddress für Steckplätze/Architekturen zu vergeben	$racadm setflexaddr [-f <ArchitekturName> <SteckplatzStatus>] $racadm setflexaddr [-i <Steckplatz#> <SteckplatzStatus>]	ERROR: Insufficient user privileges to perform operation (FEHLER: Unzureichende Benutzerrechte, zur Ausführung der Operation)
Die Funktion FlexAddress bei eingeschaltetem Gehäuse deaktivieren	$racadm feature -d -c flexaddress	ERROR: Unable to deactivate the feature because the chassis is powered ON (FEHLER: Nicht möglich die Funktion zu deaktivieren, da das Gehäuse eingeschaltet ist.)
Gastbenutzer versucht die Funktion auf dem Gehäuse zu deaktivieren	$racadm feature -d -c flexaddress	ERROR: Insufficient user privileges to perform operation (FEHLER: Unzureichende Benutzerrechte, zur Ausführung der Operation)
Änder der FlexAddress-Einstellungen für eine(n) Steckplatz/Architektur, während die Servermodule eingeschaltet sind.	$racadm setflexaddr -i 1 1	ERROR: Unable to perform the set operation because it affects a powered ON server (FEHLER: die Einstell-Operation kann nicht vorgenommen werden, da sie einen eingeschalteten Server betrifft.)

FlexAddress DELL SOFTWARE-LIZENZVERTRAG

Dies ist ein rechtsgültiger Vertrag zwischen Ihnen, dem Benutzer, und Dell Products, L.P. oder Dell Global B.V. ("Dell"). Dieser Vertrag erstreckt sich auf jede Software (zusammenfassend als Software" bezeichnet), die mit dem Dell-Produkt geliefert wird und für die kein getrennter Lizenzvertrag zwischen Ihnen und dem Hersteller bzw. Eigentümer der Software besteht. Dieser Vertrag 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 diesem Vertrag 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 dieses Vertrages 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 dieser Vertragsbestimmungen.

Die Software ist durch US-amerikanische Urheberrechtsgesetze und Bestimmungen internationaler Verträge geschützt. Sie sind berechtigt, eine einzige Kopie der Software ausschließlich zu Sicherungs- oder Archivierungszwecken zu erstellen oder die Software auf eine einzige Festplatte zu übertragen, wenn Sie das Original ausschließlich zu Sicherungs- und Archivierungszwecken aufbewahren. Sie sind nicht berechtigt, die Software durch Vermietung oder Leasing zu veräußern oder die schriftlichen Begleitmaterialien zu kopieren; Sie sind jedoch berechtigt, die Software mit sämtlichen Begleitmaterialien dauerhaft als Teil eines Verkaufs des Dell-Produkts zu übertragen, vorausgesetzt, Sie behalten keine Kopien zurück, und die Empfängerin bzw. der Empfänger stimmt den Bestimmungen dieses Vertrages zu. Jede Übertragung muss die neueste Aktualisierung und alle früheren Versionen enthalten. Sie sind nicht berechtigt, die Software zurückzuentwickeln, zu dekompilieren oder zu disassemblieren. Wenn das Paket, das mit dem Computer geliefert wird, CDs, 3,5-Zoll- und/oder 5,25-Zoll-Disketten enthält, dürfen Sie nur die Datenträger verwenden, die für Ihren Computer geeignet sind. Sie sind nicht berechtigt, die Disketten auf einem anderen Computer zu verwenden oder sie durch Verleih, Vermietung, Leasing oder Übertragung anderen Benutzern zugänglich zu machen, es sei denn, dieser Vertrag gewährt Ihnen dieses Recht.

BESCHRÄNKTE GARANTIE

Dell garantiert, dass die Software für einen Zeitraum von neunzig (90) Tagen ab Erhalt bei normalem Gebrauch frei von Material- und Verarbeitungsfehlern ist. Diese Garantie ist auf Ihre Person beschränkt und nicht übertragbar. Jegliche konkludente Garantie ist ab dem Erhalt der Software auf neunzig (90) Tage beschränkt. Da einige Staaten oder Rechtsordnungen die Begrenzung der Gültigkeitsdauer von konkludenten Garantien nicht gestatten, gilt die vorstehende Einschränkung für Sie möglicherweise nicht. Die gesamte Haftung von Dell und seinen Lieferanten und Ihr ausschließlicher Anspruch beschränkt sich auf (a) Rückerstattung des Kaufpreises der Software oder (b) den Ersatz von Datenträgern, die der vorstehenden Garantie nicht genügen, sofern diese unter Angabe einer Rücksendegenehmigungsnummer an Dell geschickt werden, wobei Sie das Risiko und die Kosten tragen. Diese eingeschränkte Garantie gilt nicht, wenn Disketten durch einen Unfall oder durch falsche und unsachgemäße Anwendung beschädigt wurden oder an ihnen von anderen Parteien als Dell Reparaturen oder Veränderungen vorgenommen wurden. Der Garantiezeitraum für Ersatzdisketten ist auf die verbleibende ursprüngliche Garantiedauer oder dreißig (30) Tage beschränkt, je nachdem welcher der beiden Zeiträume länger ist.

Dell kann NICHT garantieren, dass die Software Ihren Anforderungen entspricht oder die Software ohne Unterbrechung bzw. fehlerfrei funktioniert. Sie übernehmen selbst die Verantwortung für die Auswahl der Software, um die von Ihnen gewünschten Ergebnisse zu erzielen, und für die Verwendung sowie die Ergebnisse, die durch den Gebrauch der Software erzielt werden.

DELL LEHNT AUCH IM NAMEN SEINER LIEFERANTEN ALLE ANDEREN AUSDRÜCKLICHEN ODER KONKLUDENTEN GARANTIEN FÜR DIE SOFTWARE SOWIE DIE GESAMTEN BEILIEGENDEN GEDRUCKTEN MATERIALIEN AB, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF JEGLICHE KONKLUDENTEN GARANTIEN FÜR MARKTGÄNGIGE QUALITÄT UND TAUGLICHKEIT FÜR EINEN BESTIMMTEN ZWECK. Diese beschränkte Garantie verleiht Ihnen bestimmte Rechte; möglicherweise haben Sie weitere Rechte, die je nach Staat, Land oder Rechtsordnung unterschiedlich sein können.

DELL HAFTET NICHT FÜR DIREKTE ODER INDIREKTE SCHÄDEN (DIES GILT UNTER ANDEREM AUCH OHNE BESCHRÄNKUNG FÜR FOLGESCHÄDEN JEGLICHER ART, FÜR SCHÄDEN DURCH ENTGANGENE GEWINNE, BETRIEBSUNTERBRECHUNGEN, VERLUST VON GESCHÄFTSDATEN ODER SONSTIGE PEKUNIÄRE VERLUSTE), DIE AUS DER VERWENDUNG ODER DER FEHLENDEN MÖGLICHKEIT, DIE SOFTWARE ZU VERWENDEN, ENTSTEHEN, AUCH WENN AUF DIE MÖGLICHKEIT DES ENTSTEHENS SOLCHER SCHÄDEN HINGEWIESEN WURDE. In einigen Staaten oder Gerichtsbarkeiten ist ein Ausschluss oder eine Beschränkung der Haftung für Folgeschäden oder beiläufig entstandene Schäden nicht zulässig, deshalb gilt die oben aufgeführte Beschränkung für Sie möglicherweise nicht.

Open-Source-Software

Ein Teil dieser CD enthält eventuell Open-Source-Software, die Sie gemäß den Bedingungen der spezifischen Lizenz verwenden können, unter der die Open-

Source-Software veröffentlicht wird.

Die Veröffentlichung dieser Open-Source-Software erfolgt in der Hoffnung, dass sie Ihnen von Nutzen sein wird, WIRD JEDOCH OHNE MÄNGELGEWÄHR" ZUR VERFÜGUNG GESTELLT, OHNE IRGENDEINE AUSDRÜCKLICHE ODER IMPLIZITE GARANTIE, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE IMPLIZITE GARANTIE FÜR MARKTREIFE ODER DIE VERWENDBARKEIT FÜR EINEN BESTIMMTEN ZWECK. DELL, DIE URHEBERRECHTSINHABER ODER BETEILIGTE HAFTEN IN KEINER WEISE FÜR DIREKTE, INDIREKTE, BESONDERE, VERSCHÄRFTE, ZUFALLS- ODER FOLGESCHÄDEN (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZGÜTERN ODER -DIENSTEN, ENTGANGENE NUTZUNG ODER GEWINNE, DATENVERLUSTE BZW. BETRIEBSUNTERBRECHUNG), DIE SICH AUS DER VERWENDUNG DIESER SOFTWARE ERGEBEN, UND ZWAR UNABHÄNGIG DAVON, WIE DIESE VERURSACHT WERDEN BZW. AUF WELCHER HAFTUNGSTHEORIE SIE BASIEREN UND OB SIE AUF VERTRAG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER UNERLAUBTER HANDLUNG (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF FAHRLÄSSIGKEIT) BERUHEN. DIES GILT SELBST DANN, WENN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE.

U.S. STAATLICH BESCHRÄNKTE RECHTE

Die Software und Dokumentation sind commercial items" (Handelswaren) gemäß Definition in 48 C.F.R. (Code of Federal Regulations) 2.101, bestehend aus "kommerzieller Computersoftware" und "kommerzielle Computersoftwaredokumentation", wie verwendet in 48 C.F.R. 12,212. im Einklang mit 48 C.F.R. 12,212 und 48 C.F.R. 227,7202-1 bis 227,7202-4, jegliche U.S. Regierungs-Endnutzer beziehen die Software und die Dokumentation ausschließlich mit den hierin festgelegten Rechten. Vertragsnehmer bzw. Hersteller ist Dell Products, L.P., One Dell Way, Round Rock, Texas 78682.

ALLGEMEIN

Dieser Lizenzvertrag gilt bis zu seiner Kündigung. Er gilt gemäß oben genannten Bedingungen oder wenn Sie gegen irgendeine der Bestimmungen verstoßen, als gekündigt. Im Fall der Vertragskündigung sind Sie verpflichtet, die Software und das Begleitmaterial sowie sämtliche Kopien davon zu vernichten. Dieser Vertrag unterliegt dem Recht des Staates Texas. Jede Bestimmung dieses Vertrages ist unabhängig von den anderen Bestimmungen gültig. Wenn es sich herausstellt, dass eine Bestimmung des vorliegenden Vertrages nicht durchsetzbar ist, so wird die Gültigkeit und Durchsetzbarkeit der übrigen Bestimmungen und Bedingungen davon nicht berührt. Dieser Vertrag 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 diesen Vertrag zu verzichten. Da in einigen Rechtsordnungen diese Verzichtserklärung nicht rechtsgültig ist, gilt die Verzichtserklärung für Sie möglicherweise nicht. Sie bestätigen hiermit, dass Sie diesen Vertrag gelesen und verstanden haben, dass Sie sich an die vorgenannten Bestimmungen halten und dass dieser Vertrag hinsichtlich der Software die vollständige und exklusive Vertragsvereinbarung zwischen Ihnen und Dell darstellt.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

iKVM-Modul verwenden

Dell Chassis Management Controller Firmware Version 2.10, Benutzerhandbuch

---

Übersicht

Das Lokalzugriffs-KVM-Modul für Ihr Dell M1000e-Servergehäuse wird als Avocent® Integrated KVM Switch-Modul bezeichnet bzw. iKVM. Das iKVM ist ein analoger Tastatur-, Video- und Maus-Switch, der in das Gehäuse eingesteckt wird. Es ist ein optionales, hot-plug-fähiges Modul für das Gehäuse, das einen lokalen Tastatur-, Maus- und Videozugriff auf die Server im Gehäuse und auf die aktive Befehlszeile des CMC bereitstellt.

iKVM-Benutzeroberfläche

Das iKVM verwendet die graphische Benutzeroberfläche OSCAR® (On Screen Configuration and Reporting), die über eine Schnelltaste aktiviert wird. OSCAR ermöglicht Ihnen, einen der Server oder die Dell CMC-Befehlszeile auszuwählen, auf den/die Sie über die lokale Tastatur oder Maus bzw. die lokale Anzeige zugreifen möchten.

Es ist nur eine iKVM-Sitzung pro Gehäuse zulässig.

Sicherheit

Die OSCAR-Benutzeroberfläche ermöglicht Ihnen, Ihr System mit einem Bildschirmschonerkennwort zu schützen. Nach einer benutzerdefinierten Zeit wird der Bildschirmschonermodus aktiviert und der Zugriff verhindert, bis das richtige Kennwort zum Reaktivieren von OSCAR eingegeben wird.

Suchen

Mit OSCAR können Sie eine Liste mit Servern auswählen, die in der ausgewählten Reihenfolge angezeigt werden, während sich OSCAR im Scan-Modus befindet.

Serveridentifikation

Der CMC weist allen Servern im Gehäuse Steckplatznamen zu. Obwohl Sie mit der OSCAR-Benutzerschnittstelle von einer mehrstufigen Verbindung aus den Servern Namen zuweisen können, haben die vom CMC zugewiesenen Namen Vorrang. Neue Namen, die Sie Servern mit OSCAR zuweisen, werden überschrieben.

Der CMC identifiziert einen Steckplatz, indem er ihm einen eindeutigen Namen zuweist. Informationen zum Ändern von Steckplatznamen mit der CMC-Webschnittstelle finden Sie unter "Steckplatznamen bearbeiten". Informationen zum Ändern eines Steckplatznamens mit RACADM finden Sie im Abschnitt setslotname im *Dell Chassis Management Controller Administrator-Referenzhandbuch*.

Grafik

Die iKVM-Videoverbindungen unterstützen Video-Bildschirmauflösungen von 640 x 480 bei 60 Hz bis zu 1280 x 1024 bei 60 Hz.

Plug-and-Play

Das iKVM unterstützt Plug-and-Play des Bildschirmdatenkanals (DDC), was die Videomonitorkonfiguration automatisiert und mit dem VESA DDC2B-Standard konform ist.

FLASH-aktualisierbar

Die iKVM-Firmware kann über die CMC-Webschnittstelle oder mit dem RACADM-Befehl **fwupdate** aktualisiert werden. Weitere Informationen finden Sie unter "iKVM vom CMC aus verwalten".

Physische Verbindungsschnittstellen

Sie können eine Verbindung zu einem Server oder zur CMC-CLI-Konsole über das iKVM von der Frontblende des Gehäuses, von einer analogen Konsolenschnittstelle (ACI) und von der rückseitigen Abdeckung des Gehäuses aus herstellen.

ANMERKUNG: Die Anschlüsse auf dem Bedienfeld an der Vorderseite des Gehäuses wurden speziell für das iKVM konzipiert, das optional ist. Falls Sie das iKVM nicht haben, können Sie die Anschlüsse am vorderen Bedienfeld nicht verwenden.

iKVM-Verbindungsprioritäten

Es ist nur eine iKVM-Verbindung auf einmal verfügbar. Das iKVM weist jedem Verbindungstyp eine Prioritätsreihenfolge zu; wenn mehrere Verbindungen vorhanden sind, ist somit nur eine Verbindung verfügbar und die anderen sind deaktiviert.

Die Prioritätsreihenfolge für iKVM-Verbindungen lautet folgendermaßen:

1. Vorderseite
2. ACI
3. Rückseitige Abdeckung

Wenn beispielsweise iKVM-Verbindungen bei der Frontblende und ACI bestehen, bleibt die Frontblendenverbindung aktiv, während die ACI-Verbindung deaktiviert wird. Wenn ACI- und rückseitige Verbindungen bestehen, hat die ACI-Verbindung Vorrang.

Mehrstufen über die ACI-Verbindung

Das iKVM lässt mehrstufige Verbindungen mit Servern und der CMC-Befehlszeilenkonsole des iKVM zu, entweder lokal über einen Remote-Konsolen-Switch-Anschluss oder im Remote-Zugriff über die Dell RCS®-Software. Das iKVM unterstützt ACI-Verbindungen von den folgenden Produkten aus:

- 180AS, 2160AS, 2161DS*, 2161DS-2 oder 4161DS Dell Remote Console Switches
- Avocent AutoView®-Switch-System
- Avocent DSR®-Switch-System
- Avocent AMX®-Switch-System

* Unterstützt die Dell CMC-Konsolenverbindung nicht.

ANMERKUNG: Das iKVM unterstützt auch eine ACI-Verbindung zu Dell 180ES und 2160ES, doch ist der Stufenaufbau nicht nahtlos. Diese Verbindung erfordert einen USB-zu-PS2-SIP (Sitzungsinitiationsprotokoll).

OSCAR verwenden

In diesem Abschnitt erhalten Sie eine Übersicht über die OSCAR-Benutzeroberfläche.

Navigationsgrundlagen

Tabelle 9-1 beschreibt die Navigation in der OSCAR-Benutzeroberfläche unter Verwendung von Tastatur und Maus.

Tabelle 9-1. OSCAR-Tastatur- und Mausnavigation

Taste oder Tastenfolge	Ergebnis
• <Druck>-<Druck> • <Umsch>-<Umsch> • <Alt>-<Alt> • <Strg>-<Strg>	OSCAR kann über jede dieser Tastenfolgen aufgerufen werden, abhängig von Ihren Einstellungen zur OSCAR-Aufrufung. Sie können zwei, drei oder alle dieser Tastenfolgen aktivieren, indem Sie das jeweilige Kontrollkästchen im Bereich OSCAR aufrufen des Hauptdialogfeldes auswählen und anschließend auf OK klicken.
<F1>	Öffnet den Hilfe-Bildschirm für das aktuelle Dialogfeld.
<Esc>	Schließt das aktuelle Dialogfeld, ohne die Änderungen zu speichern, und kehrt zum vorhergehenden Dialogfeld zurück. Im Haupt-Dialogfeld schließt man mit der Taste <Esc> die OSCAR-Benutzeroberfläche und kehrt zum ausgewählten Server zurück. In einem Nachrichtenfenster wird damit das Popup-Fenster geschlossen, und man kehrt zum aktuellen Dialogfeld zurück.
<Alt>	Öffnet Dialogfelder, wählt bzw. aktiviert Optionen und führt Maßnahmen aus, wenn in Verbindung mit unterstrichenen Buchstaben oder gekennzeichneten Zeichen verwendet.
<Alt>+<X>	Schließt das aktuelle Dialogfeld und kehrt zum vorhergehenden Dialogfeld zurück.
<Alt>+<O>	Wählt die OK-Schaltfläche aus und kehrt dann zum vorhergehenden Dialogfeld zurück.
<Eingabetaste>	Führt einen Switch-Vorgang im Haupt-Dialogfeld durch und beendet OSCAR.
Einfachklick, <Eingabe>	In einem Textfeld: wählt den Text zum Bearbeiten aus und aktiviert die Tasten Nach links und Nach rechts, um den Cursor zu bewegen. Drücken Sie erneut die <Eingabetaste>, um den Bearbeitungsmodus zu beenden.
<Druck>, <Rücktaste>	Wechselt zur vorhergehenden Auswahl zurück, wenn keine weiteren Tastenanschläge ausgeführt wurden.
<Druck>, <Alt>+<0>	Trennt umgehend die Verbindung eines Benutzers zu einem Server; es ist kein Server ausgewählt. Status-Flag zeigt Frei an. (Diese Maßnahme gilt nur für =<0> auf der Tastatur und nicht auf dem numerischen Tastenblock.)
<Druck>, <Pause>	Schaltet umgehend den Bildschirmschonermodus ein und verhindert den Zugriff auf die spezifische Konsole, falls sie kennwortgeschützt ist.
Tasten Nach oben/Nach unten	Bewegt den Cursor in Listen von Zeile zu Zeile.
Tasten Nach rechts/Nach links	Bewegt den Cursor beim Bearbeiten eines Textfeldes innerhalb der Spalten.
<Pos1>/<Ende>	Bewegt den Cursor ganz nach oben (Pos1) oder unten (Ende) in einer Liste.
<Entf>	Löscht Zeichen in einem Textfeld.
Nummerntasten	Eingabe über die Tastatur oder den numerischen Tastenblock.
<Feststelltaste>	Deaktiviert. Verwenden Sie zum Ändern der Schreibweise (Groß- oder Kleinschreibung) die <Umsch>-Taste.

OSCAR konfigurieren

Tabelle 9-2 beschreibt die Funktionen, die über das Setup-Menü von OSCAR für das Konfigurieren der Server zur Verfügung stehen.

Tabelle 9-2. OSCAR-Setup-Menüfunktionen

Funktion	Zweck
Menü	Ändert die Serverauflistung zwischen numerisch nach Steckplatz und alphabetisch nach Name.
Sicherheit	• Legt ein Kennwort fest, um den Zugriff auf Server einzuschränken. • Aktiviert einen Bildschirmschoner und legt eine Inaktivitätszeit fest, bevor der Bildschirmschoner aufgerufen und der Bildschirmschonermodus aktiviert wird.
Flag	Ändert Anzeige, Zeitmessung, Farbe oder Standort der Status-Flag.
Language (Sprache)	Ändert die Sprache aller OSCAR-Bildschirme.
Broadcast	Richtet die gleichzeitige Steuerung mehrerer Server mittels Tastatur- und Mausmaßnahmen ein.
Suchen	Richtet ein benutzerdefiniertes Suchmuster für bis zu 16 Server ein.

So rufen Sie das Setup-Dialogfeld auf:

1. Betätigen Sie die Taste <Druck> (PrintScreen), um die OSCAR- Benutzerschnittstelle aufzurufen. Das Dialogfeld Main (Hauptfenster) wird geöffnet.
2. Klicken Sie auf Setup. Das Setup-Dialogfeld wird aufgerufen.

Anzeigeverhalten ändern

Ändern Sie im Menü-Dialogfeld die Anzeigereihenfolge von Servern, und legen Sie eine Bildschirmverzögerungszeit für OSCAR fest.

So rufen Sie das Menü-Dialogfeld auf:

1. Drücken Sie <Druck>, um OSCAR zu starten. Das Dialogfeld Main (Hauptfenster) wird geöffnet.
2. Klicken Sie auf Setup und anschließend auf Menü. Das Dialogfeld Menu (Menü) wird geöffnet.

So wählen Sie die standardmäßige Anzeigereihenfolge von Servern im Haupt-Dialogfeld aus:

1. Wählen Sie Name aus, um die Server alphabetisch nach Namen sortiert anzuzeigen.

   oder

   Markieren Sie die Option Slot (Schacht), um die Server in Reihenfolge der Schachtnummern anzuzeigen.
2. Klicken Sie auf OK.

So weisen Sie eine oder mehrere Tastenfolgen für die OSCAR-Aktivierung zu:

1. Wählen Sie im Menü OSCAR aufrufen eine Tastenfolge aus.
2. Klicken Sie auf OK.

Die Standardtaste zum Aktivieren von OSCAR ist <Druck>.

So legen Sie eine Anzeigeverzögerungszeit für OSCAR fest:

1. Geben Sie die Anzahl der Sekunden ein (0 bis 9), mit der die Anzeige von OSCAR verzögert werden soll, nachdem Sie auf <Druck> gedrückt haben. Bei der Eingabe von <0> wird OSCAR ohne Verzögerung gestartet.
2. Klicken Sie auf OK.

Das Festlegen einer Verzögerungszeit für die Anzeige von OSCAR ermöglicht Ihnen, einen Soft-Switch durchzuführen. Um einen Soft-Switch auszuführen, siehe "Soft-Switch ausführen".

Status-Flag steuern

Die Status-Flag wird auf Ihrem Desktop angezeigt, wo der Name des ausgewählten Servers oder der Status des ausgewählten Steckplatzes zu sehen ist. Konfigurieren Sie mit dem Dialogfeld Flag die Flag, um diese nach Server anzuzeigen oder Flag-Farbe, -Transparenz, -Anzeigezeit und -Standort auf dem Desktop zu ändern.

Tabelle 9-3. OSCAR-Status-Flags

Flag	Beschreibung
	Flag-Typ nach Name
	Flag, die angibt, dass die Verbindung des Benutzers bei allen Systemen abgebrochen wurde
	Flag, die angibt, dass der Broadcast-Modus aktiviert ist

So rufen Sie das Flag-Dialogfeld auf:

1. Drücken Sie auf die Taste <Druck>. Das Dialogfeld Main (Hauptfenster) wird geöffnet.
2. Klicken Sie auf Setup und anschließend auf Flag. Das Dialogfeld Flag wird aufgerufen.

So legen Sie fest, wie die Status-Flag angezeigt wird:

1. Wählen Sie Angezeigt aus, damit die Flag die ganze Zeit über angezeigt wird, oder Angezeigt und zeitlich bestimmt, um die Flag nur fünf Sekunden lang nach dem Umschalten einzublenden.

   ANMERKUNG: Wenn Sie Zeitlich bestimmt allein auswählen, wird die Flag nicht angezeigt.

2. Wählen Sie eine Flag-Farbe aus dem Abschnitt Anzeigefarbe aus. Es stehen Schwarz, Rot, Blau und Lila zur Auswahl.
3. Wählen Sie im Anzeigemodus die Option Opak für eine durchgängige Farb-Flag aus oder Transparent, damit der Desktop durch die Flag zu sehen ist.
4. So platzieren Sie die Status-Flag auf dem Desktop:
   a. Klicken Sie auf Position festlegen. Die Flag Position festlegen wird aufgerufen.
   b. Klicken Sie mit der linken Maustaste auf die Titelleiste und ziehen Sie sie an den gewünschten Speicherort auf dem Desktop.
   c. Klicken Sie mit der rechten Maustaste, um zum Dialogfeld Flag zurückzukehren.

ANMERKUNG: Änderungen an der Flag-Position werden erst gespeichert, wenn Sie im Dialogfeld Flag auf OK klicken.

5. Klicken Sie auf OK, um die Einstellungen zu speichern.

Um zu beenden, ohne zu speichern, klicken Sie auf ☒.

Server mit iKVM verwalten

Das iKVM ist eine analoge Switch-Matrix, die bis zu 16 Server unterstützt. Der iKVM-Switch verwendet die OSCAR-Benutzeroberfläche, um Server auszuwählen und zu konfigurieren. Zusätzlich beinhaltet das iKVM eine Systemeingabe, um eine CMC-Befehlszeilenkonsolenverbindung zum CMC herzustellen.

Peripheriegerätekompatibilität und -unterstützung

Das iKVM ist mit folgenden Peripheriegeräten kompatibel:

- Standardmäßige PC-USB-Tastaturen mit den Layouts QWERTY, QWERTZ, AZERTY und Japanisch 109.
- VGA-Monitore mit DDC-Unterstützung.

- Standardmäßige USB-Zeigegeräte.
- USB 1.1-Hubs mit eigener Stromversorgung, die am lokalen USB-Anschluss des iKVM angeschlossen sind.
- Mit Strom versorgte USB 2.0-Hubs, die an der Frontblendenkonsole des Dell M1000e-Gehäuses angeschlossen sind.

ANMERKUNG: Es können mehrere Tastaturen und Mäuse am lokalen iKVM-USB- Anschluss verwendet werden. Das iKVM führt die Eingabesignale zusammen. Wenn gleichzeitige Eingabesignale von mehreren USB-Tastaturen oder -Mäusen vorhanden sind, kann dies unvorhergesehene Ergebnisse zur Folge haben.

ANMERKUNG: Die USB-Verbindungen sind ausschließlich für unterstützte Tastaturen, Mäuse und USB-Hubs konzipiert. Das iKVM unterstützt keine Daten übertragen von anderen USB-Geräten.

Anzeigen und Auswählen von Servern

Verwenden Sie das Haupt-Dialogfeld von OSCAR, um Server über das iKVM anzuzeigen, zu konfigurieren und zu verwalten. Sie können Ihre Server nach Name oder Steckplatz anzeigen. Die Schachtnummer ist die Nummer des Gehäuseschachts, in dem der Server installiert ist. Die Schachtnummer eines Servers wird in der Spalte Slot (Schacht) angezeigt.

ANMERKUNG: Die Dell CMC-Befehlszeile nimmt Steckplatz 17 in Anspruch. Beim Auswählen dieses Steckplatzes wird die CMC-Befehlszeile angezeigt, in der Sie RACADM-Befehle ausführen oder eine Verbindung zur seriellen Konsole von Servern oder E/A-Modulen herstellen können.

ANMERKUNG: Servernamen und Schachtnummern werden vom CMC-Modul zugewiesen.

So öffnen Sie das Dialogfeld Main (Hauptfenster):

Betätigen Sie die Taste <Druck> (PrintScreen), um die OSCAR-Benutzerschnittstelle aufzurufen. Das Dialogfeld Main (Hauptfenster) wird geöffnet.

oder

Wenn ein Kennwort zugewiesen ist, wird das Dialogfeld Password (Kennwort) angezeigt. Das Passwort eingeben und auf OK klicken. Das Dialogfeld Main (Hauptfenster) wird geöffnet.

Für weitere Informationen über das Einstellen eines Kennwortes, siehe "Konsolensicherheit einstellen".

ANMERKUNG: Es gibt vier Optionen zum Aufrufen von OSCAR. Sie können eine oder alle dieser Tastenfolgen aktivieren, indem Sie das jeweilige Kontrollkästchen im Bereich OSCAR aufrufen des Hauptdialogfeldes auswählen und anschließend auf OK klicken.

Status der Server anzeigen

Der Status der Server im Gehäuse wird in den rechten Spalten des HauptDialogfelds angezeigt. In der folgenden Tabelle werden die Statussymbole beschrieben.

Tabelle 9-4. Statussymbole der OSCAR-Benutzeroberfläche

Symbole	Beschreibung
	(Grüner Punkt.) Server ist online.
	(Rotes X.) Server ist offline oder nicht im Gehäuse.
	(Gelber Punkt.) Server ist nicht verfügbar.
	(Grün A oder B.) Server wird über den Benutzerkanal genutzt, der mit den folgenden Buchstaben gekennzeichnet ist: A=rückseitige Abdeckung, B=Frontblende.

Server auswählen

Wählen Sie über das Haupt-Dialogfeld Server aus. Wenn Sie einen Server auswählen, konfiguriert das iKVM die Tastatur und Maus mit den ordnungsgemäßen Einstellungen für diesen Server neu.

- So wählen Sie Server aus:

  Doppelklicken Sie auf den Servernamen oder die Steckplatznummer.

  oder

  Wenn die Anzeigereihenfolge der Serverliste nach Steckplatz ist (d. h. die Schaltfläche Steckplatz ist gedrückt), geben Sie die Steckplatznummer ein, und drücken Sie auf <Eingabe>.

  oder

  Wenn die Serverliste nach dem Namen sortiert ist (d. h. die Schaltfläche Name ist gedrückt), geben Sie die ersten Zeichen des Servernamens ein, machen Sie ihn eindeutig und drücken Sie zweimal auf <Eingabe>.

- So wählen Sie den vorhergehenden Server aus:

  Drücken Sie auf die Taste <Druck> und anschließend auf die <Rücktaste>. Mit dieser Tastenkombination wird zwischen der vorhergehenden und aktuellen Verbindung umgeschaltet.

- So unterbrechen Sie die Verbindung eines Benutzers zu einem Server:

  Drücken Sie auf die Taste <Druck>, um OSCAR aufzurufen, und klicken Sie dann auf Unterbrechen.

  oder

  Drücken Sie die Taste <Druck> und anschließend <Alt><0>. Dadurch wird ein freier Zustand ohne ausgewählten Server bewahrt. Die Status-Flag auf dem Desktop (falls aktiv) zeigt "Frei" an. Siehe Status-Flag steuern".

Soft-Switch ausführen

Bei einem Soft-Switch wird mittels einer Schnelltastenfolge zwischen Servern umgeschaltet. Um per Soft-Switching zu einem Server zu wechseln, drücken Sie die Taste Druck (PrintScreen), und geben Sie die ersten Zeichen des Namens bzw. der Nummer des gewünschten Servers ein. Falls Sie zuvor eine Verzögerungszeit (die Anzahl der Sekunden, bevor das Hauptdialogfeld nach Drücken von <Druck> aufgerufen wird) festgelegt haben und die Tastenfolgen drücken, bevor diese Zeit abgelaufen ist, wird die OSCAR-Benutzeroberfläche nicht angezeigt.

So konfigurieren Sie OSCAR für einen Soft-Switch:

1. Betätigen Sie die Taste <Druck> (PrintScreen), um die OSCAR- Benutzerschnittstelle aufzurufen. Das Dialogfeld Main (Hauptfenster) wird geöffnet.
2. Klicken Sie auf Setup und anschließend auf Menü. Das Dialogfeld Menu (Menü) wird geöffnet.
3. Wählen Sie Name oder Steckplatz für die Anzeige-/Sortiertaste aus.
4. Geben Sie im Feld Anzeigeverzögerungszeit die gewünschte Verzögerungszeit (in Sekunden) ein.
5. Klicken Sie auf OK.

So führen Sie einen Soft-Switch zu einem Server aus:

- Um einen Server auszuwählen, drücken Sie auf die Taste <Druck>.

  Wenn die Anzeigereihenfolge der Serverliste gemäß Ihrer Auswahl unter Schritt 3 diejenige nach Steckplatz ist (d. h. die Schaltfläche Steckplatz ist gedrückt), geben Sie die Steckplatznummer ein, und drücken Sie die <Eingabetaste>.

  oder

  Wenn die Serverliste gemäß Ihrer Auswahl unter Schritt 3 nach dem Namen sortiert ist (d. h. die Schaltfläche Name ist gedrückt), geben Sie die ersten Zeichen des Servernamens ein, um ihn eindeutig zu machen und drücken Sie zwei Mal die <Eingabetaste>.

- Um zum vorhergehenden Server zurückzuschalten, drücken Sie auf <Druck> und dann die <Rücktaste>.

Videoverbindungen

Das iKVM hat Videoanschlüsse an der Frontblende und der rückseitigen Abdeckung des Gehäuses. Die Verbindungssignale an der Frontblende haben Vorrang vor denen der rückseitigen Abdeckung. Wenn ein Monitor an der Frontblende angeschlossen ist, geht die Videoverbindung nicht weiter an die rückseitige Abdeckung; es wird eine OSCAR-Meldung angezeigt, die angibt, dass die KVM- und ACI-Verbindungen der rückseitigen Abdeckung deaktiviert sind. Wenn der Monitor deaktiviert wird (d. h. er wird von der Frontblende entfernt oder durch einen CMC-Befehl deaktiviert), wird die ACI-Verbindung aktiv, während das KVM der rückseitigen Abdeckung deaktiviert bleibt. (Informationen über Verbindungsprioritäten finden Sie unter "iKVM-Verbindungsprioritäten".)

Informationen zum Aktivieren/Deaktivieren der Frontblendenanschlüsse finden Sie unter "Frontblende aktivieren oder deaktivieren".

Verdrängungswarnung

Normalerweise hat sowohl ein Benutzer, der über das iKVM, als auch ein anderer Benutzer, der über die iDRAC-GUI-Konsolenumleitungsfunktion mit derselben Serverkonsole verbunden ist, Zugriff auf die Konsole, und beide können gleichzeitig Eingaben vornehmen.

Um dieses Szenario zu vermeiden, kann der Remote-Benutzer vor dem Starten der GUI-Konsolenumleitung die lokale Konsole in der iDRAC-Webschnittstelle deaktivieren. Der lokale iKVM-Benutzer sieht die OSCAR-Meldung, dass die Verbindung in einer festgelegten Zeitspanne verdrängt wird. Der lokale Benutzer sollte seine Arbeit fertig stellen, bevor die iKVM-Verbindung zum Server abgebrochen wird.

Für den iKVM-Benutzer steht keine Verdrängungsfunktion zur Verfügung.

ANMERKUNG: Wenn ein Remote-iDRAC-Benutzer das lokale Video für einen bestimmten Server deaktiviert hat, sind das Video, die Tastatur und die Maus des Servers nicht für das iKVM verfügbar. Der Serverzustand ist mit einem gelben Punkt im OSCAR-Menü markiert, um anzuzeigen, dass er für die lokale Nutzung gesperrt bzw. nicht verfügbar ist (siehe "Status der Server anzeigen").

Konsolensicherheit einstellen

OSCAR ermöglicht Ihnen, Sicherheitseinstellungen auf der iKVM-Konsole zu konfigurieren. Sie können einen Bildschirmschonermodus einrichten, der aktiviert wird, wenn die Konsole für eine bestimmte Zeitspanne nicht genutzt wird. Nach dem Aktivieren bleibt die Konsole gesperrt, bis Sie eine beliebige Taste drücken oder die Maus bewegen. Geben Sie das Kennwort des Bildschirmschoners ein, um fortzufahren.

Sperren Sie mit Hilfe des Dialogfelds Sicherheit Ihre Konsole mit einem Kennwortschutz, legen Sie Ihr Kennwort fest bzw. ändern Sie es oder aktivieren Sie den Bildschirmschoner.

ANMERKUNG: Falls das iKVM-Kennwort verloren geht oder vergessen wird, können Sie es über die CMC-Webschnittstelle oder RACADM auf die iKVM-Werkseinstellung zurücksetzen. Siehe Verlorenes oder vergessenes Kennwort löschen".

Sicherheitsdialogfeld aufrufen

1. Drücken Sie auf die Taste <Druck>. Das Dialogfeld Main (Hauptfenster) wird geöffnet.
2. Klicken Sie auf Setup und dann auf Sicherheit. Das Dialogfeld Sicherheit wird angezeigt.

Kennwort festlegen oder ändern

1. Klicken Sie einmal und drücken Sie auf <Eingabe> oder doppelklicken Sie auf das Feld Neu.
2. Geben Sie im Feld Neu das neue Kennwort ein, und drücken Sie dann auf <Eingabe>. Bei Kennwörtern wird zwischen Groß- und Kleinschreibung unterschieden und sie müssen zwischen 5 und 12 Zeichen lang sein. Sie müssen mindestens einen Buchstaben und eine Zahl enthalten. Erlaubte Zeichen sind A-Z, a-z, 0-9, Leerstelle und Bindestrich.
3. Geben Sie im Feld Wiederholen das Kennwort erneut ein und drücken Sie dann die <Eingabetaste>.
4. Klicken Sie auf OK, wenn Sie nur das Kennwort ändern möchten; schließen Sie danach das Dialogfeld.

Konsole mit Kennwort schützen

1. Legen Sie das Kennwort, wie im vorhergehenden Verfahren beschrieben, fest.
2. Wählen Sie das Feld Bildschirmschoner aktivieren aus.
3. Geben Sie die Anzahl der Minuten für die Inaktivitätszeit (von 1 bis 99) ein, mit welcher der Kennwortschutz und die Bildschirmschoneraktivierung verzögert werden sollen.
4. Bei Modus: Wenn Ihr Monitor ENERGY STAR®-konform ist, wählen Sie Energie aus; wählen Sie andernfalls Anzeige aus.

ANMERKUNG: Wenn der Modus auf Energie gesetzt wird, versetzt das Gerät den Monitor in den Energiesparmodus. Dies sieht man normalerweise daran, dass der Monitor ausgeschaltet wird und die grüne LED- Betriebsanzeige durch ein gelbes Licht ersetzt wird. Wird der Modus auf Anzeige gesetzt, springt die OSCAR-Flag für die Dauer des Tests auf dem Bildschirm hin und her. Bevor der Test startet, wird in einem Warnungs- Popup-Feld die folgende Meldung angezeigt: "Der Energiemodus kann einen Monitor, der nicht ENERGY STAR-konform ist, beschädigen. Nach dem Start kann der Test jedoch umgehend per Maus oder Tastatur beendet werden."

VORSICHTSHINWEIS: Monitore, die nicht Energy Star-kompatibel sind, können bei Verwendung des Energie-Modus beschädigt werden.

5. Optional: Um den Bildschirmschonertest zu aktivieren, klicken Sie auf Test. Das Dialogfeld Bildschirmschonertest wird angezeigt. Klicken Sie auf OK, um den Test zu starten.

Der Test dauert 10 Sekunden. Nach Abschluss kehren Sie zum Dialogfeld Sicherheit zurück.

Anmeldung

1. Drücken Sie <Druck>, um OSCAR zu starten. Das Dialogfeld Kennwort wird aufgerufen.
2. Geben Sie das Kennwort ein und klicken Sie dann auf OK. Das Hauptdialogfeld wird angezeigt.

Automatische Abmeldung einstellen

Sie können OSCAR so einstellen, dass nach einer Phase der Inaktivität ein automatisches Abmelden auf einem Server erfolgt.

1. Klicken Sie im Haupt-Dialogfeld auf Setup und anschließend auf Sicherheit.
2. Geben Sie im Feld Inaktivitätszeit die Zeitspanne ein, in der Sie mit einem Server verbunden sein wollen, bevor er die Verbindung automatisch trennt.
3. Klicken Sie auf OK.

Kennwortschutz von Konsole entfernen

1. Klicken Sie im Hauptdialogfeld auf Setup und anschließend auf Sicherheit.
2. Klicken Sie im Dialogfeld Sicherheit einmal, und drücken Sie auf <Eingabe>, oder doppelklicken Sie auf das Feld Neu.
3. Lassen Sie das Feld Neu frei, und drücken Sie auf <Eingabe>.
4. Klicken Sie einmal und drücken Sie auf <Eingabe>, oder doppelklicken Sie auf das Feld Wiederholen.
5. Lassen Sie das Feld Wiederholen frei, und drücken Sie auf <Eingabe>.
6. Klicken Sie auf OK, wenn Sie lediglich das Kennwort löschen möchten.

Bildschirmschonermodus ohne Kennwortschutz aktivieren

ANMERKUNG: Falls die Konsole kennwortgeschützt ist, müssen Sie zuerst den Kennwortschutz entfernen. Folgen Sie den Schritten im vorhergehenden Verfahren, bevor Sie die unteren Schritte durchführen.

1. Wählen Sie Bildschirmschoner aktivieren aus.
2. Geben Sie die Anzahl der Minuten (zwischen 1 und 99) ein, die vergehen soll, bevor der Bildschirmschoner aktiviert wird.
3. Wählen Sie Energie aus, wenn Ihr Monitor ENERGY STAR-konform ist; wählen Sie ansonsten Anzeige aus.

VORSICHTSHINWEIS: Monitore, die nicht Energy Star-kompatibel sind, können bei Verwendung des Energie-Modus beschädigt werden.

4. Optional: Um den Bildschirmschonertest zu aktivieren, klicken Sie auf Test. Das Dialogfeld Bildschirmschonertest wird angezeigt. Klicken Sie auf OK, um den Test zu starten.

Der Test dauert 10 Sekunden. Nach Abschluss kehren Sie zum Dialogfeld Sicherheit zurück.

ANMERKUNG: Durch das Aktivieren des Bildschirmschonermodus wird die Verbindung des Benutzers zu einem Server getrennt, und es ist kein Server mehr ausgewählt. Die Status-Flag zeigt Frei an.

Bildschirmschonermodus beenden

Um den Bildschirmschonermodus zu beenden und zum Haupt-Dialogfeld zurückzukehren, drücken Sie auf eine beliebige Taste oder bewegen Sie die Maus.

So schalten Sie den Bildschirmschoner aus:

1. Deaktivieren Sie im Dialogfeld Sicherheit das Feld Bildschirmschoner aktivieren.
2. Klicken Sie auf OK.

Um den Bildschirmschoner umgehend einzuschalten, drücken Sie die Taste <Druck> und dann <Pause>.

Verlorenes oder vergessenes Kennwort löschen

Wenn das iKVM-Kennwort verloren geht oder vergessen wird, können Sie es auf den iKVM-Werksstandard zurücksetzen und anschließend das Kennwort ändern. Sie können das Kennwort entweder über die CMC-Webschnittstelle oder RACADM zurücksetzen.

So setzen Sie ein verloren gegangenes oder vergessenes iKVM-Kennwort mit der CMC-Webschnittstelle zurück:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie im Gehäuse-Untermenü iKVM aus.
3. Klicken Sie auf die Registerkarte Setup. Die Seite iKVM Configuration (iKVM-Konfiguration) wird angezeigt.
4. Klicken Sie auf Standardwerte wiederherstellen.

Sie können nun die Standardeinstellung des Kennworts über OSCAR ändern. Siehe "Kennwort festlegen oder ändern".

Um ein verloren gegangenes oder vergessenes Kennwort mit RACADM zurückzusetzen, öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole zum CMC, melden sich an und geben Folgendes ein:

```
racadm racresetcfg -m kvm
```

ANMERKUNG: Der Befehl racresetcfg setzt die Einstellungen Frontblende aktivieren und Dell CMC-Konsole aktivieren zurück, wenn sie von den Standardwerten abweichen.

Weitere Informationen über den Unterbefehl racresetcfg finden Sie im Abschnitt "racresetcfg" im *Dell Chassis Management Controller Firmware Version 2.0 Administrator-Referenzhandbuch*.

Sprache ändern

Ändern Sie mit dem Dialogfeld Sprache die Sprache des OSCAR-Texts in eine der unterstützten Sprachen. Der Text ändert auf allen OSCAR-Bildschirmen umgehend in die ausgewählte Sprache.

So ändern Sie die OSCAR-Sprache:

1. Drücken Sie auf die Taste <Druck>. Das Dialogfeld Main (Hauptfenster) wird geöffnet.
2. Klicken Sie auf Setup und anschließend auf Sprache. Das Dialogfeld Sprache wird aufgerufen.
3. Klicken Sie auf die Optionsschaltfläche für die gewünschte Sprache und anschließend auf OK.

Versionsinformationen anzeigen

Verwenden Sie das Dialogfeld Version, um die iKVM-Firmware- und Hardwareversion anzuzeigen und die Sprach- und Tastaturkonfiguration zu identifizieren.

So zeigen Sie Versionsinformationen an:

1. Drücken Sie auf die Taste <Druck>. Das Dialogfeld Main (Hauptfenster) wird geöffnet.
2. Klicken Sie auf Befehl und dann auf Versionen anzeigen. Das Dialogfeld Version wird angezeigt.

   In der oberen Hälfte des Dialogfelds Version werden die Subsystemversionen im Gerät angezeigt.
3. Klicken Sie auf ☒, oder drücken Sie auf <Esc>, um das Dialogfeld Version zu schließen.

System scannen

Im Scan-Modus scannt das iKVM automatisch von Steckplatz zu Steckplatz (Server zu Server). Sie können bis zu 16 Server scannen, indem Sie die Server angeben, die gescannt werden sollen, sowie die Anzahl der Sekunden, während denen jeder Server angezeigt wird.

So fügen Sie der Scan-Liste Server hinzu:

1. Drücken Sie auf die Taste <Druck>. Das Dialogfeld Main (Hauptfenster) wird geöffnet.
2. Klicken Sie auf Setup und dann auf Suchen. Das Dialogfeld Suchen wird aufgerufen, in dem alle Server im Gehäuse aufgelistet werden.
3. Wählen Sie das Kontrollkästchen neben den Servern aus, die gescannt werden sollen.

   oder

   Doppelklicken Sie auf den Servernamen oder den Steckplatz.

   oder

   Drücken Sie auf die Taste <Alt > und die Nummer des Servers, der gescannt werden soll. Es können bis zu 16 Server ausgewählt werden.
4. Geben Sie im Feld Zeit die Anzahl der Sekunden ein (zwischen 3 und 99), die iKVM abwarten soll, bevor der Scan zum nächsten Server der Folge übergeht.
5. Klicken Sie auf die Schaltfläche Hinzufügen/Entfernen und anschließend auf OK.

So entfernen Sie einen Server aus der Scan-Liste:

1. Wählen Sie im Dialogfeld Suchen das Kontrollkästchen neben dem zu entfernenden Server aus.

oder

Doppelklicken Sie auf den Servernamen oder den Steckplatz.

oder

Klicken Sie auf die Schaltfläche Löschen, um alle Server aus der Scan-Liste zu entfernen.

2. Klicken Sie auf die Schaltfläche Hinzufügen/Entfernen und anschließend auf OK.

So starten Sie den Scan-Modus:

1. Drücken Sie auf die Taste <Druck>. Das Dialogfeld Main (Hauptfenster) wird geöffnet.
2. Klicken Sie auf Befehle. Das Dialogfeld Befehl wird aufgerufen.
3. Wählen Sie das Feld Scan aktivieren aus.
4. Klicken Sie auf OK. Es wird eine Meldung angezeigt, die angibt, dass die Maus und die Tastatur zurückgesetzt wurden.
5. Klicken Sie auf ☒, um das Nachrichtenfenster zu schließen.

So brechen Sie den Scan-Modus ab:

1. Wenn OSCAR geöffnet ist und das Haupt-Dialogfeld angezeigt wird, wählen Sie einen Server aus der Liste aus.

oder

Ist OSCAR nicht geöffnet, bewegen Sie die Maus, oder drücken Sie eine beliebige Taste auf der Tastatur. Der Scan-Vorgang wird beim derzeit ausgewählten Server gestoppt.

oder

Drücken Sie auf die Taste <Druck>. Das Haupt-Dialogfeld wird angezeigt; wählen Sie einen Server aus der Liste aus.

2. Klicken Sie auf die Schaltfläche Befehle. Das Dialogfeld Befehle wird aufgerufen.
3. Deaktivieren Sie das Kästchen Scan aktivieren.

Broadcast zu Servern

Sie können mehrere Server eines Systems gleichzeitig steuern, um sicherzustellen, dass alle ausgewählten Server die gleiche Eingabe erhalten. Sie können Tastenanschläge und/oder Mausbewegungen unabhängig voneinander senden lassen.

ANMERKUNG: Sie können einen Broadcast an bis zu 16 Server gleichzeitig ausführen lassen.

So führen Sie einen Broadcast an Server durch:

1. Drücken Sie auf die Taste <Druck>. Das Dialogfeld Main (Hauptfenster) wird geöffnet.
2. Klicken Sie auf Setup und anschließend auf Broadcast. Das Dialogfeld Broadcast wird angezeigt.

ANMERKUNG: Tastenanschläge senden: Wenn Sie Tastenanschläge verwenden, muss der Tastaturzustand bei allen Servern, die einen Broadcast empfangen, identisch sein, damit die Tastenanschläge auf identische Weise interpretiert werden können. Genauer gesagt müssen die Modi <Feststelltaste> und <Num-Taste> bei allen Tastaturen gleich sein. Während das iKVM versucht, Tastenanschläge gleichzeitig an die ausgewählten Server zu senden, ist es möglich, dass einige Server die Übertragung hemmen und dadurch verzögern.

ANMERKUNG: Mausbewegungen senden: Damit die Maus korrekt funktioniert, müssen alle Server über den gleichen Maustreiber, Desktop (z. B. identisch platzierte Symbole) und Grafikauflösungen verfügen. Auch die Maus muss sich bei allen Bildschirmen an genau der gleichen Position befinden. Da diese Betriebszustände extrem schwierig zu erzielen sind, kann der Broadcast von Mausbewegungen an mehrere Server unberechenbare Ergebnisse nach sich ziehen.

3. Aktivieren Sie die Maus und/oder die Tastatur für die Server, welche die Broadcast-Befehle erhalten sollen, indem Sie die jeweiligen Kontrollkästchen auswählen.

   oder

   Drücken Sie die Tasten Nach oben oder Nach unten, um den Cursor zu einem Zielserver zu bewegen. Drücken Sie dann <Alt><K>, um das Tastaturfeld auszuwählen, und/oder <Alt><M>, um das Mausfeld auszuwählen. Wiederholen Sie diesen Vorgang für weitere Server.

4. Klicken Sie auf OK, um die Einstellungen zu speichern und zum Dialogfeld Setup zurückzukehren. Klicken Sie auf ☒ , oder drücken Sie auf <Esc>, um zum Haupt-Dialogfeld zurückzukehren.
5. Klicken Sie auf Befehle. Das Dialogfeld Befehle wird aufgerufen.
6. Klicken Sie auf das Feld Broadcast aktivieren, um Broadcasts zu aktivieren. Das Dialogfeld Broadcast-Warnung wird angezeigt.
7. Klicken Sie auf OK, um den Broadcast zu aktivieren.

   Um den Vorgang abzubrechen und zum Dialogfeld Befehle zurückzukehren, klicken Sie auf ☒ , oder drücken Sie auf <Esc>.

8. Wenn Broadcasts aktiviert sind, geben Sie die Informationen ein und/oder führen Sie die Mausbewegungen aus, die von der Management Station gesendet werden sollen. Nur Server aus der Liste sind verfügbar.

So schalten Sie Broadcasts aus:

Deaktivieren Sie im Dialogfeld Befehle das Kontrollkästchen Broadcast aktivieren.

---

iKVM vom CMC aus verwalten

Frontblende aktivieren oder deaktivieren

Um den Zugriff auf das iKVM von der Frontblende mit RACADM zu aktivieren oder zu deaktivieren, öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole zum CMC, melden sich an und geben folgendes ein:

```
racadm config -g cfgKVMInfo -o cfgKVMFrontPanelEnable <Wert>
```

wobei <*Wert*> 1 (aktivieren) oder 0 (deaktivieren) ist.

Weitere Informationen über den Unterbefehl config finden Sie im Abschnitt "config" im *Dell Chassis Management Controller Administrator-Referenzhandbuch*.

So aktivieren oder deaktivieren Sie den Zugriff auf das iKVM über die Webschnittstelle von der Frontblende aus:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur iKVM aus. Die Seite iKVM Status (iKVM-Status) wird angezeigt.
3. Klicken Sie auf die Registerkarte Setup. Die Seite iKVM Configuration (iKVM-Konfiguration) wird angezeigt.
4. Wählen Sie zur Aktivierung das Kontrollkästchen Frontblende USB/Video aktiviert aus.

   Entfernen Sie zum Deaktivieren das Häkchen aus dem Kontrollkästchen Frontblende USB/Video aktiviert.

5. Klicken Sie auf Apply (Übernehmen), um die Einstellung zu speichern.

Dell CMC-Konsole über iKVM aktivieren.

Um dem iKVM den Zugriff auf die Dell CMC-Konsole mit RACADM zu ermöglichen, öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole zum CMC, melden sich an und geben folgendes ein:

```
racadm config -g cfgKVMInfo -o cfgKVMAccessToCMCEnable 1
```

So aktivieren Sie die Dell-CMC-Konsole über die Webschnittstelle:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur iKVM aus. Die Seite iKVM Status (iKVM-Status) wird angezeigt.
3. Klicken Sie auf die Registerkarte Setup. Die Seite iKVM Configuration (iKVM-Konfiguration) wird angezeigt.
4. Wählen Sie das Kontrollkästchen Zugang zu CMC-CLI über iKVM zulassen aus.
5. Klicken Sie auf Apply (Übernehmen), um die Einstellung zu speichern.

iKVM-Status und -Eigenschaften anzeigen

Das Lokalzugriffs-KVM-Modul für das Dell M1000e-Servergehäuse heißt Avocent® Integrated KVM Switch Modul oder iKVM. Der Funktionszustand des mit dem Gehäuse verbundenen iKVM kann auf der Seite Gehäuseeigenschaftszustand im Abschnitt Gehäuse-Grafiken eingesehen werden.

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

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Die Seite Gehäusezustand wird angezeigt. Der rechte Abschnitt von Gehäuse-Grafiken zeigt die Rückansicht des Gehäuses und enthält den Funktionszustand des iKVM. Der iKVM-Funktionszustand wird durch die Farbe der iKVM-Grafik angezeigt:
   - Grün - iKVM ist vorhanden, wird mit Strom versorgt und kommuniziert mit dem CMC. Es gibt keine Anzeichen eines unerwünschten Zustands.
   - Bernstein - iKVM wird erkannt, wird oder wird nicht mit Strom versorgt oder kommuniziert oder kommuniziert nicht mit dem CMC; ein ungünstiger Zustand könnte vorhanden sein.
   - Grau - iKVM wird erkannt und nicht mit Strom versorgt. Es kommuniziert nicht mit dem CMC und es gibt keine Anzeichen eines ungünstigen Zustands.
3. Bewegen Sie den Cursor über die iKVM-Grafik und ein entsprechender Texthinweis oder Bildschirmtipp wird angezeigt. Der Texthinweis liefert zusätzliche Informationen zu diesem iKVM.
4. Die iKVM-Grafik ist mit der entsprechenden GUI-Seite des CMC verknüpft, um sofort die Navigation zur Seite iKVM-Status zu ermöglichen.

Weitere Informationen zum iKVM finden Sie unter "iKVM-Modul verwenden".

Um den Zustand des iKVM einzusehen, nutzen Sie die Seite iKVM Status:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur iKVM aus. Die Seite iKVM-Status wird aufgerufen.

Tabelle 9-5 beschreibt die Informationen, die auf der Seite iKVM-Status zu finden sind.

Bauteil	Beschreibung
Vorhandensein	Zeigt an, ob das iKVM-Modul Vorhanden oder Nicht vorhanden ist.
Stromzustand	Zeigt den iKVM-Stromstatus an: Ein, Aus oder - (Nicht vorhanden).
Name	Zeigt den Produktnamen des iKVM an.
Hersteller	Zeigt den Hersteller des iKVM an.
Teilenummer	Zeigt die Teilenummer des iKVM an. Die Teilenummer ist eine vom Hersteller eindeutig identifizierbare Nummer.
Firmware-Version	Zeigt die iKVM-Firmware-Version an.
Hardwareversion	Zeigt die iKVM-Hardware-Version an.
Frontblende angeschlossen	Zeigt an, ob der Monitor mit dem Frontblenden-VGA-Anschluss verbunden ist (Ja oder Nein). Diese Informationen werden dem CMC zur Verfügung gestellt, damit er bestimmen kann, ob ein lokaler Benutzer Zugriff auf das Gehäuse von der Frontblende aus hat.
Rückseite angeschlossen	Zeigt an, ob der Monitor mit dem rückseitigen VGA-Anschluss verbunden ist (Ja oder Nein). Diese Informationen werden dem CMC zur Verfügung gestellt, damit er bestimmen kann, ob ein lokaler Benutzer Zugriff auf das Gehäuse von der Rückseite aus hat.
Reihenanschluss Verbunden	iKVM unterstützt nahtlose Rangunterteilung mit externen iKVM-Anwendungen von Dell und Avocent, die eingebaute Hardware verwenden. Wenn das iKVM abgestuft wird, kann auf die Server im Gehäuse durch die Bildschirmanzeige des externen KVM-

	Schalters zugegriffen werden, von denen aus iKVM abgestuft wird.
Frontblenden-USB/Video aktiviert	Zeigt an, ob der Frontblenden-VGA-Anschluss aktiviert ist (Ja oder Nein).
Zugriff von iKVM auf CMC zulassen	Zeigt an, ob die CMC-Befehlskonsole durch iKVM aktiviert ist (Ja oder Nein).

Aktualisieren der iKVM-Firmware

Die iKVM-Firmware kann mit der CMC-Webschnittstelle oder RACADM aktualisiert werden.

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

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf Chassis (Gehäuse).
3. Klicken Sie auf die Registerkarte Update (Aktualisieren). Die Seite Aktualisierbare Komponenten wird angezeigt.
4. Klicken Sie auf den Namen des iKVM-Moduls. Die Seite Firmware Update (Firmware-Aktualisierung) wird eingeblendet.
5. Im Feld Firmware-Abbild geben Sie den Pfad zur Firmware-Abbilddatei auf Ihrer Managementstation oder dem gemeinsam genutzten Netzwerk ein oder klicken Sie Durchsuchen, um zum Dateispeicherort zu navigieren.

ANMERKUNG: Der Standardname des iKVM-Firmware-Abbildes ist ikvm.bin; der Dateiname des iKVM-Firmware-Abbildes kann jedoch vom Benutzer verändert werden.

6. Klicken Sie auf Firmware-Aktualisierung beginnen. Ein Dialogfeld fordert Sie auf die Aktion zu bestätigen.
7. Klicken Sie auf Yes (Ja), um fortzufahren. Der Abschnitt Fortschritt der Firmware-Aktualisierung bietet Statusinformationen zur Firmwareaktualisierung. Ein Statusindikator wird auf der Seite während des Aktualisierungsvorganges angezeigt. Die Dauer der Dateiübertragung kann abhängig von der Verbindungsgeschwindigkeit stark variieren. Wenn der interne Aktualisierungsprozess beginnt, wird die Seite laufend aktualisiert und zeigt den Firmwareaktualisierungs-Timer an. Zusätzliche Informationen:
   - Verwenden Sie während der Dateiübertragen nicht den Button Aktualisieren und navigieren nicht Sie zu einer anderen Seite.
   - Um den Prozess abzubrechen, klicken Sie auf Dateiübertrag und Aktualisierung abbrechen - diese Option ist nur während der Dateiübertragung verfügbar.
   - Der Status der Aktualisierung wird im Feld Aktualisierungsstatus angezeigt; diese Feld wird automatisch während der Dateiübertragung aktualisiert. Bestimmte älter Browser unterstützen diese automatischen Aktualisierungen nicht. Um das Feld Aktualisierungszustand manuell zu aktualisieren, klicken Sie auf Aktualisieren.

ANMERKUNG: Die Aktualisierung für das iKVM kann bis zu einer Minute dauern.

Wenn die Aktualisierung abgeschlossen ist, wird das iKVM zurückgesetzt und die neue Firmware wird aktualisiert und auf der Seite Aktualisierbare Komponenten angezeigt.

Um die iKVM-Firmware mit RACADM zu aktualisieren, öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole zum CMC, melden Sie sich an und geben Sie Folgendes ein:

```
racadm fwupdate -g -u -a <TFTP-Server-IP-Adresse> -d <Dateipfad/Dateiname> -m kvm
```

Zum Beispiel:

```
racadm fwupdate -gua 192.168.0.10 -d ikvm.bin -m kvm
```

Weitere Informationen über den Unterbefehl fwupdate finden Sie im Abschnitt fwupdate im *Dell Chassis Management Controller Administrator-Referenzhandbuch*.

Fehlerbehebung

ANMERKUNG: Wenn eine aktive Konsolenumleitungssitzung vorhanden ist und ein Monitor mit niedriger Auflösung an der iKVM angeschlossen wird, wird die Serverkonsolenauflösung eventuell zurückgesetzt, wenn der Server auf der lokalen Konsole ausgewählt wird. Wenn der Server ein Linux-Betriebssystem ausführt, kann eine X11-Konsole auf dem lokalen Monitor eventuell nicht angezeigt werden. Durch Drücken auf <Strg><Alt><F1> auf

der iKVM wird Linux auf eine Textkonsole geschaltet.

Tabelle 9-6. Fehlerbehebung beim iKVM

Problem	Wahrscheinliche Ursache und Lösung
Die Meldung "Benutzer wurde durch die CMC-Steuerung deaktiviert" wird auf dem Monitor angezeigt, der an der Frontblende angeschlossen ist.	Die Frontblendenverbindung wurde vom CMC deaktiviert. Sie können die Frontblende entweder mit der CMC-Webschnittstelle oder RACADM aktivieren. So aktivieren Sie die Frontblende über die Webschnittstelle: 1. Melden Sie sich bei der CMC-Webschnittstelle an. 2. Wählen Sie in der Systemstruktur iKVM aus. 3. Klicken Sie auf die Registerkarte Setup. 4. Wählen Sie das Kontrollkästchen Frontblenden-USB/Video aktiviert aus. 5. Klicken Sie auf Apply (Übernehmen), um die Einstellung zu speichern. Um die Frontblende mit RACADM zu aktivieren, öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole zum CMC, melden Sie sich an und geben Sie Folgendes ein: `racadm config -g cfgKVMInfo - o cfgKVMAccesToCMCEnable 1`
Der Zugriff auf die rückseitige Abdeckung funktioniert nicht.	Die Frontblendeneinstellung ist durch den CMC aktiviert, und an der Frontblende ist gegenwärtig ein Monitor angeschlossen. Es ist nur eine Verbindung zu einem Zeitpunkt zulässig. Die Frontblendenverbindung hat Vorrang vor ACI und der rückseitigen Abdeckung. Weitere Informationen über Verbindungsprioritäten finden Sie unter "iKVM-Verbindungsprioritäten".
Die Meldung "Benutzer wurde deaktiviert, da ein weiteres Gerät derzeit Priorität hat" wird auf dem Monitor angezeigt, der an der rückseitigen Abdeckung angeschlossen ist.	Es ist ein Netzwerkkabel am iKVM ACI-Anschluss und an einem sekundären KVM-Gerät angeschlossen. Es ist nur eine Verbindung zu einem Zeitpunkt zulässig. Die ACI-Verbindung hat Vorrang vor dem Monitoranschluss an der rückseitigen Abdeckung. Die Prioritätsreihenfolge ist Frontblende, ACI und dann rückseitige Abdeckung.
Die gelbe iKVM-LED blinkt.	Es gibt drei mögliche Ursachen: Es liegt ein Problem mit dem iKVM vor, für welches das iKVM eine Neuprogrammierung erfordert. Um das Problem zu beheben, folgen Sie den Anweisungen zur Aktualisierung der iKVM-Firmware (siehe "Aktualisieren der iKVM-Firmware"). Das iKVM programmiert die CMC-Konsolenschnittstelle neu. In diesem Fall ist die CMC-Konsole vorübergehend nicht verfügbar und wird durch einen gelben Punkt in der OSCAR-Benutzeroberfläche dargestellt. Dieser Vorgang dauert bis zu 15 Minuten. Die iKVM-Firmware hat einen Hardwarefehler festgestellt. Weitere Informationen entnehmen Sie dem iKVM-Status. So zeigen Sie den iKVM-Status mithilfe der Webschnittstelle an: 1. Melden Sie sich bei der CMC-Webschnittstelle an. 2. Wählen Sie in der Systemstruktur iKVM aus. Um die iKVM-Firmware mit RACADM anzuzeigen, öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole zum CMC, melden Sie sich an und geben Sie Folgendes ein: `racadm getkvminfo`
Das iKVM wird über den ACI-Anschluss an einen externen KVM-Switch abgestuft, wobei jedoch sämtliche Einträge für die ACI-Verbindungen unverfügbar sind. Alle Zustände weisen einen gelben Punkt in der OSCAR-Benutzeroberfläche auf.	Der Frontblendenanschluss ist aktiviert, und es ist ein Monitor daran angeschlossen. Da die Frontblende Vorrang vor allen anderen iKVM-Anschlüssen hat, sind die ACI-Anschlüsse und die Anschlüsse der rückseitigen Abdeckung deaktiviert. Um die ACI-Anschlussverbindung zu aktivieren, müssen Sie zuerst den Frontblendenzugriff deaktivieren oder den Monitor entfernen, der an der Frontblende angeschlossen ist. Die OSCAR-Einträge des externen KVM-Switch werden aktiv und verfügbar. So deaktivieren Sie die Frontblende unter Verwendung der Webschnittstelle: 1. Melden Sie sich bei der CMC-Webschnittstelle an. 2. Wählen Sie in der Systemstruktur iKVM aus. 3. Klicken Sie auf die Registerkarte Setup. 4. Entfernen Sie zum Deaktivieren das Häkchen aus dem Kontrollkästchen Frontblende USB/Video aktiviert. 5. Klicken Sie auf Apply (Übernehmen), um die Einstellung zu speichern. Um die Frontblende mit RACADM zu deaktivieren, öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole zum CMC, melden Sie sich an und geben Sie Folgendes ein:

	`racadm config -g cfgKVMInfo - o cfgKVMFrontPanelEnable 0`
Im OSCAR-Menü zeigt die Dell-CMC-Verbindung ein rotes X an, und ein Verbindungsaufbau zum CMC ist nicht möglich.	Es gibt zwei mögliche Ursachen: Die Dell-CMC-Konsole wurde deaktiviert. In diesem Fall können Sie sie entweder über die CMC-Webschnittstelle oder RACADM aktivieren. So aktivieren Sie die Dell-CMC-Konsole über die Webschnittstelle: 1. Melden Sie sich bei der CMC-Webschnittstelle an. 2. Wählen Sie in der Systemstruktur iKVM aus. 3. Klicken Sie auf die Registerkarte Setup. 4. Wählen Sie das Kontrollkästchen Zugang zu CMC-CLI über iKVM zulassen aus. 5. Klicken Sie auf Apply (Übernehmen), um die Einstellung zu speichern. Um die Dell CMC-Verbindung mit RACADM zu aktivieren, öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole zum CMC, melden Sie sich an und geben Sie Folgendes ein: `racadm config -g cfgKVMInfo - o cfgKVMAccessToCMCEnable 1` Der CMC ist nicht verfügbar, da er initialisiert wird, zum Standby-CMC wechselt oder eine Neuprogrammierung durchführt. Warten Sie in diesem Falle einfach ab, bis der CMC die Initialisierung abgeschlossen hat.
Der Steckplatzname für einen Server wird in OSCAR als "Initialisiert" angezeigt, und er kann nicht ausgewählt werden.	Entweder führt der Server eine Initialisierung durch, oder iDRAC auf diesem Server hatte einen Fehler bei der Initialisierung. Warten Sie zuerst 60 Sekunden. Falls der Server weiterhin initialisiert wird, wird der Steckplatzname angezeigt, sobald die Initialisierung abgeschlossen ist. Sie können dann den Server auswählen. Falls OSCAR nach 60 Sekunden weiterhin angibt, dass der Steckplatz eine Initialisierung durchführt, nehmen Sie den Server aus dem Gehäuse heraus und setzen Sie ihn wieder ein. Diese Maßnahme ermöglicht iDRAC, eine Neuinitialisierung durchzuführen.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Installation und Setup des CMC

Dell Chassis Management Controller Firmware Version 2.10, Benutzerhandbuch

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 folgenden Schritte zum Konfigurieren des CMC:

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

Zusätzlich können Sie Informationen über die Installation und Konfiguration einer redundanten CMC-Umgebung unter "Die redundante CMC-Umgebung verstehen" abrufen.

Bevor Sie beginnen

Laden Sie die neueste Version der CMC-Firmware von Dells Support-Website unter **support.dell.com** herunter, bevor Sie die CMC-Umgebung einrichten.

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

CMC-Hardware installieren

Da der CMC im Gehäuse vorinstalliert ist, ist keine Installation erforderlich. Informationen zum Einstieg mit dem auf dem System installierten CMC finden Sie unter "Remote-Zugriffssoftware auf einer Management Station installieren".

Sie können einen zweiten CMC installieren und diesen als Standby-CMC zum primären CMC ausführen. Weitere Informationen zur Verwendung der CMC finden Sie unter "Die redundante CMC-Umgebung verstehen".

Remote-Zugriffssoftware auf einer Management Station installieren

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

Falls Sie Remote-RACADM von Ihrer Management Station aus verwenden möchten, müssen Sie die Komponente unter Verwendung der Dell Systems Management Tools and Documentation DVD installieren. Ihr System enthält die DVD Dell Systems Management Tools and Documentation. Diese DVD enthält die folgenden Dell OpenManage-Komponenten:

- DVD-Stammverzeichnis - Enthält das Dell Systems Build and Update-Hilfsprogramm
- SYSMGMT - Enthält die Systemmanagement-Softwareprodukte einschließlich des Dell OpenManage Server Administrators
- docs - Enthält die Dokumentation für Systeme, Softwareprodukte zur Systemverwaltung, Peripheriegeräte und RAID-Controller.

- SERVICE - Enthält die Hilfsprogramme, die Sie benötigen, um Ihr System zu konfigurieren, und liefert die neuesten Diagnosen sowie Dell-optimierte Treiber für Ihr System

Informationen zur Installation von Dell OpenManage-Softwarekomponenten finden Sie im verfügbaren Dell OpenManage-Installation und Sicherheit-Benutzerhandbuch auf der DVD oder unter support.dell.com.

RACADM auf einer Linux-Verwaltungsstation installieren

1. Melden Sie sich als root beim System an, auf dem das unterstützte Red Hat® Enterprise Linux®- oder SUSE® Linux Enterprise Server- Betriebssystem ausgeführt wird und wo Sie die Managed System- Komponenten installieren wollen.
2. Legen Sie die DVD Dell Systems Management Tools and Documentation in das DVD-Laufwerk ein.
3. Laden Sie die DVD anhand des Befehls mount oder eines ähnlichen Befehls an einen gewünschten Speicherort, falls notwendig.

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

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

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

5. Um Hilfe zum RACADM-Befehl zu erhalten, geben Sie nach der Eingabe der vorherigen Befehle `racadm help` ein. Weitere Informationen zu RACADM finden Sie unter "RACADM-Befehlszeilenschnittstelle verwenden".

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, beispielsweise:

```
racadm getconfig -f <Dateiname>
```

RACADM von einer Linux Management Station deinstallieren

1. Melden Sie sich mit root beim System an, auf dem die Funktionen der Management Station deinstalliert werden sollen.
2. Verwenden Sie den rpm-Abfragebefehl, um zu bestimmen, welche Version der DRAC-Hilfsprogramme installiert ist. Verwenden Sie den Befehl `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. Eine Liste unterstützter Internet-Browser befindet sich auf der *Dell Systems Software Support Matrix* auf der Support-Website von Dell unter **support.dell.com / manuals**.

Der für den CMC und die Management Station verwendete Browser muss sich in demselben Netzwerk befinden, welches sich *Verwaltungsnetzwerk* nennt. Je nach Sicherheitsanforderungen kann das Verwaltungsnetzwerk ein eigenständiges Hochsicherheitsnetzwerk sein.

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

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

Proxy-Server

Wenn Sie mit einem Proxyserver browsen und dieser keinen Zugriff auf das Verwaltungsnetzwerk hat, können Sie die Verwaltungsnetzwerkadressen der Ausnahmeliste des Browsers hinzufügen. Dies weist den Browser an, den Proxyserver beim Zugriff auf das Verwaltungsnetzwerk zu deaktivieren.

Internet Explorer

Bearbeiten Sie die Ausnahmeliste im Internet Explorer anhand der folgenden Schritte:

1. Starten Sie den Internet Explorer.
2. Klicken Sie auf **Werkzeuge→ Internetoptionen** und klicken Sie dann auf **Verbindungen**.
3. Klicken Sie im Abschnitt **LAN-Einstellungen** auf **LAN-Einstellungen.**
4. Klicken Sie im Abschnitt **Proxyserver** auf **Erweitert.**
5. Fügen Sie im Abschnitt **Ausnahmen** die Adressen für die CMCs und iDRACs im Verwaltungsnetzwerk unter Verwendung des Semikolons als Trennzeichen der Liste hinzu. Sie können DNS-Namen und Platzhalter in Ihren Einträgen verwenden.

Mozilla Firefox

So bearbeiten Sie die Ausnahmeliste in Mozilla Firefox Version 3.0:

1. Starten Sie Firefox.
2. Klicken Sie auf **Extras→ Optionen** (für Windows) oder klicken Sie auf **Bearbeiten→ Einstellungen** (für Linux)**.**
3. Klicken Sie auf **Erweitert** und dann auf die Registerkarte **Netzwerk**.
4. Klicken Sie auf **Einstellungen.**
5. Wählen Sie **Manuelle Proxykonfiguration** aus, und fügen Sie dann im Feld **Kein Proxy für** 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.

Microsoft® Phishing-Filter

Wenn der Microsoft Phishing-Filter im Internet Explorer 7 auf dem Verwaltungssystem aktiviert ist und der CMC nicht über einen Internetzugang verfügt, können beim Zugreifen auf den CMC Verzögerungen von mehreren Sekunden auftreten, wenn Sie den Browser oder eine andere Oberfläche, wie z. B. die Remote-RACADM-Oberfläche, verwenden. Folgen Sie diesen Schritten, um den Phishing-Filter zu deaktivieren:

1. Starten Sie den Internet Explorer.
2. Klicken Sie auf **Werkzeuge→ Phishing-Filter** und dann auf **Phishing- Filter-Einstellungen**.
3. Aktivieren Sie das Kontrollkästchen **Phishing-Filter deaktivieren**.
4. Klicken Sie auf **OK**.

Zertifikatsperrliste (CRL) abrufen

Wenn der CMC über keinen Internetzugang verfügt, deaktivieren Sie die Abruffunktion der Zertifikatsperrliste (CRL) im Internet Explorer. Diese Funktion überprüft, ob ein Server, wie z. B. der CMC-Webserver, ein Zertifikat verwendet, das sich in einer Liste mit gesperrten Zertifikaten befindet, die aus dem Internet abgerufen wurden. Wenn kein Zugriff auf das Internet möglich ist, kann diese Funktion zu Verzögerungen von mehreren Sekunden führen, wenn Sie mit dem Browser oder einer Befehlszeilenschnittstelle, wie z. B. Remote-RACADM, auf den CMC zugreifen.

Folgen Sie diesen Schritten, um das Abrufen der CRL zu deaktivieren:

1. Starten Sie den Internet Explorer.
2. Klicken Sie auf **Werkzeuge→ Internetoptionen** und klicken Sie dann auf **Erweitert**.
3. Gehen Sie mit der Bildlaufleiste zum Abschnitt Sicherheit und deaktivieren Sie **Auf gesperrte Zertifikate von Herausgebern überprüfen**.
4. 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.

Folgen Sie diesen Schritten, um die Option **Verschlüsselte Seiten nicht auf der Festplatte speichern** zu aktivieren:

1. Starten Sie den Internet Explorer.
2. Klicken Sie auf **Werkzeuge→ Internetoptionen** und klicken Sie dann auf **Erweitert**.
3. Scrollen Sie zum Abschnitt Sicherheit und aktivieren Sie **Verschlüsselte Seiten nicht auf der Festplatte speichern**.

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 ausgeführt wird. Für den Internet Explorer muss der Browser so konfiguriert sein, dass Animationen wiedergegeben werden können, was standardmäßig so eingestellt ist.

Folgen Sie diesen Schritten, um den Internet Explorer so zu konfigurieren, dass Animationen wiedergegeben werden können:

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

Ursprünglichen Zugriff auf den CMC einrichten

Um den CMC im Remote-Zugriff zu verwalten, verbinden Sie den CMC mit dem Verwaltungsnetzwerk, und konfigurieren Sie dann die CMC-Netzwerkeinstellungen. Weitere Informationen über die Konfiguration der CMC-Netzwerkeinstellungen finden Sie unter "CMC-Netzwerk konfigurieren". Diese ursprüngliche Konfiguration weist die TCP/IP-Netzwerkbetriebsparameter zu, die den Zugriff auf den CMC aktivieren.

Sobald der CMC mit dem Verwaltungsnetzwerk verbunden ist, erfolgen alle externen Zugriffe auf den CMC und die iDRACs über den CMC. Umgekehrt erfolgt der Zugriff auf die verwalteten Server über Netzwerkanschlüsse zu E/A-Modulen (EAMs). Dies ermöglicht, dass Anwendungsnetzwerk und Verwaltungsnetzwerk voneinander getrennt sind.

ANMERKUNG: Dell empfiehlt dringend, das Verwaltungsnetzwerk im von iDRAC und CMC verwendeten Gehäuse vom Produktionsnetzwerk zu isolieren/separieren. Das Mischen von Verwaltungs- und Produktionsanwendungsverkehr auf diesem Verwaltungsnetzwerk könnte Engpässe/Überlastung verursachen, was zu CMC- und iDRAC-Kommunikationsverzögerungen führt. Die Verzögerungen können unvorhersehbares Gehäuseverhalten verursachen, zum Beispiel: CMC zeigt iDRAC als offline an, obwohl iDRAC läuft, was wiederum anderes unerwünschtes Verhalten hervorrufen kann. Falls physisches Isolieren des Verwaltungsnetzwerks nicht praktikabel ist, besteht die Option, CMC- und iDRAC-Verkehr in ein separates VLAN zu isolieren. Die CMC- und die einzelnen iDRAC-Netzwerkschnittstellen können mit dem Befehl `racadm setniccfg` für die Verwendung eines VLAN konfiguriert werden. Weitere Informationen finden Sie im *Dell Chassis Management Controller Administrator-Referenzhandbuch*.

Wenn Sie ein Gehäuse haben, verbinden Sie den CMC und, falls vorhanden, den Standby-CMC mit dem Verwaltungsnetzwerk. Wenn Sie mehr als ein Gehäuse haben, können Sie zwischen einer Basisverbindung, bei der jeder CMC mit dem Verwaltungsnetzwerk verbunden ist, oder einer linear verkabelten Gehäuseverbindung wählen, bei der die Gehäuse in Serie angeschlossen sind und nur einer mit dem Verwaltungsnetzwerk verbunden ist. Der Basisverbindungstyp verwendet mehrere Schnittstellen im Verwaltungsnetzwerk und bietet höhere Redundanz. Der linear verkabelte Verbindungstyp verwendet weniger Schnittstellen im Verwaltungsnetzwerk, schafft jedoch Abhängigkeiten zwischen den CMCs, wodurch sich die Redundanz des Systems verringert.

CMC-Basisnetzwerkverbindung

Um eine höchstmögliche Redundanz zu erzielen, verbinden Sie jeden CMC mit dem Verwaltungsnetzwerk. Wenn sich in einem Gehäuse nur ein CMC befindet, stellen Sie eine Verbindung mit dem Verwaltungsnetzwerk her. Wenn das Gehäuse über einen redundanten CMC im sekundären CMC-Steckplatz verfügt, stellen Sie zwei Verbindungen mit dem Verwaltungsnetzwerk her.

Jeder CMC hat zwei RJ-45 Ethernetanschlüsse, gekennzeichnet mit GB1 (der Uplink-Port) und STK (der Stacking-Port). Bei einer Basisverkabelung verbinden Sie die GB1-Schnittstelle mit dem Verwaltungsnetzwerk und belassen die STK-Schnittstelle unbenutzt.

VORSICHTSHINWEIS: Anschließen des STK-Anschlusses an das Verwaltungsnetzwerk kann unvorhersehbare Ergebnisse verursachen.

in Reihe verkabelte CMC-Netzwerkverbindung

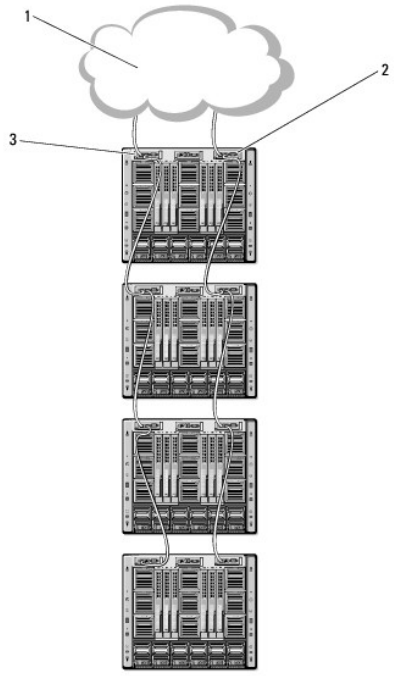
Wenn in einem Rack mehrere Gehäuse vorhanden sind, können Sie die Anzahl an Verbindungen mit dem Verwaltungsnetzwerk verringern, indem Sie bis zu vier Gehäuse miteinander in Reihe verkabeln. Wenn jedes der vier Gehäuse einen redundanten CMC enthält, können Sie durch eine Reihen-Verkabelung die Anzahl an erforderlichen Verwaltungsnetzwerkanschlüssen von acht auf zwei reduzieren. Wenn jedes Gehäuse nur über einen CMC verfügt, können Sie die Anzahl an erforderlichen Anschlüssen von vier auf einen reduzieren.

Wenn Sie Gehäuse in Reihe miteinander verkabeln, ist GB1 die "Uplink"-Schnittstelle und STK die "nachgelagerte" Schnittstelle. Eine GB1-Schnittstelle muss mit dem Verwaltungsnetzwerk verbunden sein oder mit der STK-Schnittstelle des CMC in einem Gehäuse, der näher am Netzwerk liegt. Die STK-Schnittstelle darf nur mit einer GB1-Schnittstelle weiter unten in Reihe verbunden sein.

Die CMCs im primären CMC-Steckplatz und im sekundären CMC-Steckplatz müssen jeweils separate Reihen bilden.

Abbildung 2-1 zeigt die Kabelanordnung für vier in Reihe verkabelte Gehäuse, wobei sich die CMCs in den jeweils primären und sekundären Steckplätzen befinden.

Abbildung 2-1. In Reihe verkabelte CMC-Netzwerkverbindung



1	Verwaltungsnetzwerk	2	sekundärer CMC
3	primärer CMC		

Folgen Sie diesen Schritten, um bis zu vier Gehäuse in Reihe zu verkabeln:

1. Verbinden Sie die GB1-Schnittstelle des primären CMC im ersten Gehäuse mit dem Verwaltungsnetzwerk.
2. Verbinden Sie die GB1-Schnittstelle des primären CMC im zweiten Gehäuse mit der STK-Schnittstelle des primären CMC im ersten Gehäuse.
3. Wenn ein drittes Gehäuse vorhanden ist, verbinden Sie dessen GB1- Schnittstelle vom primären CMC mit der STK-Schnittstelle des primären CMC im zweiten Gehäuse.
4. Wenn ein viertes Gehäuse vorhanden ist, verbinden Sie dessen GB1- Schnittstelle vom primären CMC mit der STK-Schnittstelle des primären CMC im dritten Gehäuse.
5. Wenn redundante CMCs im Gehäuse vorhanden sind, verbinden Sie diese nach demselben Muster.

VORSICHTSHINWEIS: Die STK-Schnittstelle von CMCs darf niemals mit dem Verwaltungsnetzwerk verbunden werden. Sie kann nur mit der GB1-Schnittstelle an einem anderen Gehäuse verbunden werden. Einen STK-Anschluss mit dem Managementnetzwerk zu verbinden, kann das Netzwerk zerstören und einen Datenverlust zur Folge haben.

ANMERKUNG: Verbinden Sie niemals einen primären CMC mit einem sekundären CMC.

ANMERKUNG: Wird ein CMC zurückgesetzt, dessen STK-Schnittstelle mit einem anderen CMC in der Reihe verbunden ist, kann das Netzwerk für weiter unten in der Reihe angeschlossene CMCs unterbrochen werden. Die "untergeordneten" CMCs geben eventuell Meldungen aus, die darauf hinweisen, dass keine Netzwerkverbindung mehr besteht und dass möglicherweise auf die redundanten CMCs umgeschaltet wird.

CMC-Netzwerk konfigurieren

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

Sie können die ursprüngliche Netzwerkkonfiguration des CMC durchführen, bevor oder nachdem der CMC über eine IP-Adresse verfügt. Die Konfiguration der ursprünglichen CMC-Netzwerkeinstellungen, bevor Sie über eine IP-Adresse verfügen, kann über eine der folgenden Schnittstellen erfolgen:

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

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

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

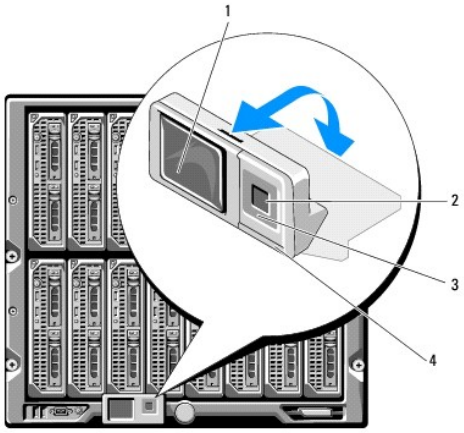
Netzwerkbetrieb mit dem LCD-Konfigurationsassistent konfigurieren

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

Die LCD-Anzeige befindet sich in der unteren linken Ecke an der Gehäusevorderseite.

Abbildung 2-2 stellt das LCD-Bedienfeld dar.

Abbildung 2-2. LCD-Anzeige



1	LCD-Bildschirm	2	Auswahltaste (Markieren")
3	Scrolltasten (4)	4	LED-Statusanzeige

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

Eine LED-Statusanzeige auf dem LCD-Bedienfeld zeigt den Gesamtfunktionszustand des Gehäuses und seiner Komponenten an.

- Beständig leuchtendes Blau zeigt einen guten Funktionszustand an.
- Blinkendes Gelb zeigt an, dass sich mindestens eine Komponente in einem fehlerhaften Betriebszustand befindet.
- Blinkendes Blau ist ein ID-Signal, das zur Identifikation eines einzelnen Gehäuses in einer Gruppe von Gehäusen verwendet wird.

Auf dem LCD-Bildschirm navigieren

Die rechte Seite des LCD-Bedienfelds enthält fünf Schaltflächen: vier Pfeiltasten (nach oben, unten, links und rechts) und eine Taste in der Mitte.

- *Um zwischen Bildschirmen zu wechseln*, verwenden Sie die Pfeiltasten nach rechts (nächster) und nach links (vorhergehender). Während Sie den Konfigurationsassistent verwenden, können Sie jederzeit zum vorherhegenden Bildschirm zurückkehren.
- *Um auf einem Bildschirm über die Bildlaufleiste zwischen Optionen zu wechseln*, verwenden Sie die Pfeiltasten nach unten und nach oben.
- *Um auf einem Bildschirm ein Element auszuwählen und zu speichern* und zum nächsten Bildschirm zu wechseln, verwenden Sie die Taste in der Mitte.

Weitere Informationen über die Verwendung des LCD-Bedienfeldes finden Sie im Abschnitt "LCD-Bedienfeld" im *Dell Chassis Management Controller Administrator-Referenzhandbuch*.

LCD-Konfigurationsassistent verwenden

1. Sofern noch nicht geschehen, schalten Sie den Netzschalter des Gehäuses ein.

   Der LCD-Bildschirm zeigt während des Einschaltens eine Reihe von Initialisierungsbildschirmen an. Wenn der Bildschirm Spracheinstellungen einsatzbereit ist, wird er angezeigt.

2. Wählen Sie Ihre Sprache mit den Pfeiltasten aus und drücken Sie dann die mittlere Schaltfläche, um **Annehmen/Ja** auszuwählen, und drücken Sie die mittlere Schaltfläche erneut.
3. Der Bildschirm Gehäuse zeigt die folgende Frage an: Gehäuse konfigurieren?
   a. Klicken Sie auf die mittlere Schaltfläche, um mit dem Bildschirm CMC-Netzwerkeinstellungen fortzufahren. Siehe Schritt 4.
   b. Um das Menü **Gehäuse konfigurieren** zu beenden, wählen Sie das Symbol NEIN aus und drücken Sie die mittlere Schaltfläche. Siehe Schritt 9.
4. Klicken Sie auf die mittlere Schaltfläche, um mit dem Bildschirm CMC- Netzwerkeinstellungen fortzufahren.
5. Wählen Sie mit der Pfeiltaste nach unten die Netzwerkgeschwindigkeit aus (10 MBit/s, 100 MBit/s, Automatisch (1 GBit/s)).

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

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

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

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

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

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

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

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

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

Dynamisches Host-	Der CMC ruft die IP-Konfiguration (IP-Adresse, -Maske und -Gateway) automatisch von einem DHCP-Server im

Konfigurationsprotokoll (DHCP)	Netzwerk ab. Dem CMC im Netzwerk wird eine eindeutige IP-Adresse zugewiesen. Klicken Sie auf die mittlere Schaltfläche, wenn Sie die DHCP-Option ausgewählt haben. Der Bildschirm iDRAC konfigurieren? wird angezeigt; gehen Sie zu Schritt 10.
Statisch	Sie geben die IP-Adresse, das Gateway und die Subnetzmaske in die gleich darauf eingeblendeten Bildschirme ein. Wenn Sie die Option Statisch ausgewählt haben, drücken Sie die Taste in der Mitte, um mit dem nächsten Bildschirm CMC-Netzwerkeinstellungen fortzufahren. Dann: a. Bestimmen Sie die Statische IP-Adresse, indem Sie mit den Pfeiltasten nach rechts und nach links zwischen den Positionen wechseln und mit den Pfeiltasten nach oben und nach unten eine Nummer für jede Position auswählen. Wenn die Festlegung der statischen IP-Adresse abgeschlossen ist, drücken Sie auf die Taste in der Mitte, um fortzufahren. b. Bestimmen Sie die Subnetzmaske, und drücken Sie dann auf die Taste in der Mitte. c. Bestimmen Sie den Gateway und drücken Sie dann auf die Taste in der Mitte. Der Bildschirm Netzwerk-Zusammenfassung wird angezeigt. Im Bildschirm Netzwerk-Zusammenfassung sind die von Ihnen eingegebenen Einstellungen zur statischen IP-Adresse, zur Subnetzmaske und zum Gateway aufgeführt. Überprüfen Sie die Einstellungen auf Richtigkeit. Für eine korrekte Einstellung, navigieren Sie zur linken Pfeiltaste und drücken Sie dann die mittlere Schaltfläche, um zum Bildschirm für diese Einstellung zurückzukehren. Nachdem Sie eine Korrektur vorgenommen haben, drücken Sie auf die Taste in der Mitte. d. Wenn Sie die Richtigkeit der von Ihnen eingegebenen Einstellungen bestätigt haben, drücken Sie auf die Taste in der Mitte. Der Bildschirm DNS registrieren? wird angezeigt.

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

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

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

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

10. Geben Sie an, ob Sie einen iDRAC konfigurieren möchten:
    - Nein: Fahren Sie mit Schritt 13 fort.
    - Ja: Drücken Sie auf die Taste in der Mitte.
11. Wählen Sie das Internet-Protokoll (IPv4, IPv6 oder beide) aus, das Sie für die Blades verwenden möchten.

Dynamisches Host-Konfigurationsprotokoll (DHCP)	iDRAC ruft die IP-Konfiguration (IP-Adresse, -Maske und -Gateway) automatisch von einem DHCP-Server im Netzwerk ab. Dem iDRAC im Netzwerk wird eine eindeutige IP-Adresse zugewiesen. Drücken Sie die mittlere Schaltfläche.
Statisch	Sie geben die IP-Adresse, das Gateway und die Subnetzmaske in die gleich darauf eingeblendeten Bildschirme ein. Wenn Sie die Option Statisch ausgewählt haben, drücken Sie die Taste in der Mitte, um mit dem nächsten Bildschirm iDRAC-Netzwerkeinstellungen fortzufahren. Dann: a. Bestimmen Sie die Statische IP-Adresse, indem Sie mit den Pfeiltasten nach rechts und nach links zwischen den Positionen wechseln und mit den Pfeiltasten nach oben und nach unten eine Nummer für jede Position auswählen. Diese Adresse ist die statische IP des iDRAC, der sich im ersten Steckplatz befindet. Die statische IP-Adresse jedes nachfolgenden iDRAC wird als Steckplatznummer-Inkrement dieser IP-Adresse berechnet. Wenn die Festlegung der statischen IP-Adresse abgeschlossen ist, drücken Sie auf die Taste in der Mitte, um fortzufahren. b. Bestimmen Sie die Subnetzmaske, und drücken Sie dann auf die Taste in der Mitte. c. Bestimmen Sie den Gateway und drücken Sie dann auf die Taste in der Mitte.

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

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

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

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

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

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

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

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

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

Über ein Netzwerk auf den CMC zugreifen

Nachdem Sie die CMC-Netzwerkeinstellungen konfiguriert haben, können Sie über die folgenden Schnittstellen im Remote-Verfahren auf den CMC zugreifen:

- Webschnittstelle
- Telnet-Konsole
- SSH
- Remote-RACADM

Telnet ist über eine der anderen Schnittstellen aktiviert; Telnet ist nicht so sicher, wie die anderen Schnittstellen und ist daher standardmäßig deaktiviert.

Tabelle 2-1 beschreibt jede CMC-Netzwerkschnittstelle.

Tabelle 2-1. CMC-Schnittstellen

Schnittstelle	Beschreibung
Webschnittstelle	Ermöglicht Remote-Zugriff auf den CMC über eine grafische Benutzeroberfläche. Die Webschnittstelle ist in die CMC-Firmware integriert und der Zugriff erfolgt von einem unterstützten Webbrowser über die NIC-Schnittstelle auf der Management Station. Eine Liste der unterstützten Webbrowser finden Sie in der *Dell Systems Software Support Matrix* auf der Dell Support-Website unter **support.dell.com / manuals**.
Remote-RACADM-Befehlszeilenschnittstelle	Ermöglicht den Remote-Zugriff auf den CMC von einer Management Station über eine Befehlszeilenschnittstelle (CLI). Remote-RACADM verwendet die Option **racadam -r** mit der IP-Adresse des CMC, um Befehle auf dem CMC auszuführen.
Telnet	Ermöglicht Befehlszeilen-Zugriff auf den CMC über das Netzwerk. Die RACADM-Befehlszeilenschnittstelle und der **connect**-Befehl, der zum Herstellen einer Verbindung zur seriellen Konsole eines Servers oder E/A-Moduls verwendet wird, sind über die CMC-Befehlszeile verfügbar. **ANMERKUNG:** Telnet ist ein ungesichertes Protokoll, das alle Daten, einschließlich Kennwörtern, in Klartext überträgt. Verwenden Sie bei Übertragung vertraulicher Informationen die SSH-Schnittstelle.
SSH	Bietet dieselben Fähigkeiten wie Telnet durch Verwendung einer verschlüsselten Transportschicht für höhere Sicherheit.

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

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

Eine Liste der unterstützten Webbrowser finden Sie in der *Dell Systems Software Support Matrix* auf der Dell Support-Website unter **support.dell.com / manuals**. Informationen für den Zugriff auf den CMC mit einem unterstützten Webbrowser finden Sie unter "Auf die CMC-Webschnittstelle zugreifen". Informationen über Dell OpenManage IT Assistant finden Sie unter "Remote-Zugriffssoftware auf einer Management Station installieren".

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

Um auf die CMC-Befehlszeile mit Telnet oder SSH zuzugreifen, lesen Sie bitte "CMC zur Verwendung von Befehlszeilenkonsolen konfigurieren".

Weitere Informationen über die Verwendung von RACADM finden Sie unter "RACADM-Befehlszeilenschnittstelle verwenden".

Weitere Informationen über die Verwendung der Befehle **connect** oder racadm connect zum Verbindungsaufbau mit den Servern und E/A-Modulen finden Sie unter "Verbindung zu Servern oder Modulen mit dem connect-Befehl herstellen".

Installieren oder Aktualisieren der CMC-Firmware

Herunterladen der CMC-Firmware

Bevor Sie mit der Firmware-Aktualisierung beginnen, laden Sie die neueste Firmware von Dells Support-Website unter **support.dell.com** herunter und speichern diese auf dem lokalen System.

Die folgenden Software-Komponenten sind in Ihrem CMC-Firmware-Paket enthalten:

- Kompilierte CMC-Firmware-Codes und -Daten
- Webschnittstelle JPEG und weitere Dateien mit Benutzeroberflächendaten
- Standard-Konfigurationsdateien

ANMERKUNG: Während der Aktualisierung von CMC-Firmware laufen einige oder alle Lüftereinheiten im Gehäuse mit 100%iger Kapazität. Dies ist normal.

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

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

Sie können den RACADM-Befehl **getsysinfo** (siehe Abschnitt getsysinfo-Befehl im *Dell Chassis Management Controller Administrator-Referenzhandbuch*) oder die Seite **Gehäusezusammenfassung** (siehe "Aktuelle Firmware-Versionen anzeigen") verwenden, um die aktuellen Firmwareversionen der CMCs in Ihrem Gehäuse anzuzeigen.

Wenn Sie über einen Standby-CMC verfügen, sollten Sie beide CMCs gleichzeitig in einem Vorgang aktualisieren. Nachdem der Standby-CMC aktualisiert wurde, tauschen Sie die CMC-Rollen miteinander aus, sodass der neu aktualisierte CMC als primärer CMC und der CMC mit der alten Firmware als Standby fungiert. (Hilfe zum Rollentausch finden Sie im Abschnitt zum cmcchangeover-Befehl im Dell Chassis Management Controller Firmware Administrator-Referenzhandbuch.) Damit können Sie überprüfen, ob die Aktualisierung erfolgreich war und die neue Firmware einwandfrei funktioniert, bevor Sie die Firmware für den zweiten CMC aktualisieren. Nachdem beide CMCs aktualisiert worden sind, können Sie den Befehl **cmcchangeover** verwenden, um die vorhergehenden Rollen der CMCs wiederherzustellen.

CMC-Firmware über die Webschnittstelle aktualisieren

Anleitungen zur Verwendung der Webschnittstelle, um die CMC-Firmware zu aktualisieren, finden Sie unter "CMC-Firmware aktualisieren".

Aktualisieren der CMC-Firmware über RACADM

Anweisungen zur Verwendung des RACADM-Unterbefehls **fwupdate** zur Aktualisierung der CMC-Firmware finden Sie im Abschnitt fwupdate-Befehl im *Dell Chassis Management Controller Administrator-Referenzhandbuch*.

CMC-Eigenschaften konfigurieren

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

Weitere Informationen über die Verwendung der Webschnittstelle finden Sie unter "Auf die CMC-Webschnittstelle zugreifen". Weitere Informationen über die Verwendung der RACADM-Befehle finden Sie unter "RACADM-Befehlszeilenschnittstelle verwenden".

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

Strombudget konfigurieren

Der CMC bietet einen Strombudgetdienst, mit dem Sie Strombudget, Redundanz sowie eine dynamische Stromversorgung für das Gehäuse konfigurieren können.

Mit dem Stromverwaltungsdienst kann der Stromverbrauch optimiert und den verschiedenen Modulen je nach Bedarf Strom zugewiesen werden.

Weitere Informationen über die Stromverwaltung des CMC finden Sie unter "Stromverwaltung".

Anleitungen zum Konfigurieren des Strombudgets und anderer Energieeinstellungen über die Webschnittstelle finden Sie unter "Strombudget konfigurieren".

CMC-Netzwerkeinstellungen konfigurieren

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

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

- RACADM – siehe "Mehrere CMCs in mehreren Gehäusen konfigurieren"

ANMERKUNG: Wird der CMC in einer Linux-Umgebung eingesetzt, finden Sie entsprechende Informationen unter "RACADM auf einer Linux-Verwaltungsstation installieren".

- Webschnittstelle – siehe "CMC-Netzwerkeigenschaften konfigurieren"

Benutzer hinzufügen und konfigurieren

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

Anleitungen zum Hinzufügen und Konfigurieren von Benutzern mit öffentlichem Schlüssel (Public Key) für den CMC unter Verwendung von RACADM finden Sie unter "Verwendung von RACADM zum Konfigurieren der Authentifizierung mit öffentlichem Schlüssel über SSH". Anleitungen zum Hinzufügen und Konfigurieren von Benutzern unter Verwendung der Webschnittstelle finden Sie unter "CMC-Benutzer hinzufügen und konfigurieren".

Anleitungen zur Verwendung von Active Directory mit Ihrem CMC finden Sie unter "CMC mit Microsoft Active Directory verwenden".

Hinzufügen von SNMP- und E-Mail-Warnungen

Sie können den CMC so konfigurieren, dass bei bestimmten Gehäuseereignissen SNMP- und/oder E-Mail-Warnungen erzeugt werden. Weitere Informationen finden Sie unter "Konfiguration von SNMP-Alarmen" und "Konfiguration von E-Mail-Alarmen".

Remote-Syslog konfigurieren

Die Funktion *Remote-Syslog* wird entweder über die CMC-GUI oder über den racadm-Befehl aktiviert/konfiguriert. Zu den Konfigurationsoptionen gehören der Syslog-Servername (bzw. die IP-Adresse) und der UDP-Anschluss, der vom CMC verwendet wird, um die Protokolleinträge weiterzuleiten. Sie können in der Konfiguration bis zu 3 verschiedene Syslog-Serverziele angeben. Remote-Syslog ist ein zusätzliches Protokollziel für den CMC. Nach der Konfiguration von Remote-Syslog wird jeder neue vom CMC erzeugte Protokolleintrag an die Ziele weitergeleitet.

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

So konfigurieren Sie die CMC-Dienste:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie auf die Registerkarte **Netzwerk/Sicherheit**.
3. Klicken Sie auf die Unterregisterkarte Dienste. Die Seite Dienste wird angezeigt.

Weitere Informationen über das Konfigurieren des Remote-Syslog finden Sie unter Tabelle 5-27.

Die redundante CMC-Umgebung verstehen

Sie können einen Standby-CMC installieren, der dann eingesetzt wird, wenn der primäre CMC ausfällt.

Ausfallsicherungen können auftreten, wenn:

- Der RACADM-Befehl **cmcchangeover** ausgeführt wird. (Siehe Abschnitt über den cmcchangeover-Befehl im *Dell Chassis Management Controller Administrator-Referenzhandbuch*.)
- Der RACADM-Befehl racreset auf dem aktiven CMC ausgeführt wird. (Siehe Abschnitt über den racreset-Befehl im *Dell Chassis Management Controller Administrator-Referenzhandbuch*.)
- Setzen Sie den aktiven CMC über die Webschnittstelle zurück. (Siehe Option Reset CMC für Stromsteuerungsvorgänge, die unter "Durchführen von Energieverwaltungsmaßnahmen am Gehäuse" beschrieben wird.)
- Das Netzwerkkabel vom aktiven CMC entfernt wird.
- Der aktive CMC vom Gehäuse entfernt wird.
- Ein CMC-Firmware-Flash auf dem aktiven CMC initiiert wird.
- der primäre CMC nicht mehr funktioniert

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

Info zum Standby-CMC

Der Standby-CMC ist mit dem aktiven CMC identisch und spiegelt diesen stets wider. Sowohl der aktive als auch der Standby-CMC müssen mit derselben Firmware-Revision installiert werden. Bei unterschiedlichen Firmware-Revisionen meldet das System eine herabgesetzte Redundanz.

Der Standby-CMC übernimmt dieselben Einstellungen und Eigenschaften des primären CMC. Sie müssen darauf achten, dass immer dieselbe Firmware-Version auf beiden CMCs aktualisiert wird. Konfigurationseinstellungen müssen auf dem Standby-CMC jedoch nicht dupliziert werden.

ANMERKUNG: Weitere Informationen zur Installation eines Standby-CMC finden Sie im Hardware-Benutzerhandbuch. Für Anleitungen zur Installation der CMC- Firmware auf Ihrem Standby-CMC, folgenden Sie den Anweisungen in "Installieren oder Aktualisieren der CMC-Firmware".

Auswahlverfahren des primären CMC

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

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

Funktionszustand eines redundanten CMC abrufen

Sie können den Funktionszustand eines Standby-CMC über die Webschnittstelle anzeigen. Weitere Information über den Zugriff auf den CMC-Funktionszustand über die Internetschnittstelle finden Sie unter "Gehäuse- und Komponenten-Funktionszustand anzeigen".

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Verwaltung der E/A-Architektur

Dell Chassis Management Controller Firmware Version 2.10, Benutzerhandbuch

Das Gehäuse kann bis zu sechs E/A-Module (EAMs) fassen, die entweder Switch- oder Passthrough-Module sein können.

Diese EAMs werden in drei Gruppen unterteilt: A, B und C. Jede Gruppe besitzt zwei Steckplätze: Steckplatz 1 und Steckplatz 2. Die Steckplätze sind auf der Geräterückseite von links nach rechts mit Buchstaben gekennzeichnet: A1 | B1 | C1 | C2 | B2 | A2. Jeder Server verfügt über Steckplätze für zwei Mezzanine-Karten (MCs) zum Anschließen an EAMs. Die MC und das entsprechende EAM müssen dieselbe Architektur aufweisen.

Das Gehäuse unterstützt drei Architektur- oder Protokolltypen. Alle EAMs und MCs in einer Gruppe müssen dieselben oder kompatible Architekturtypen aufweisen.

- EAMs der **Gruppe A** sind immer mit den integrierten Ethernet-Adaptern des Servers verbunden. Der Architekturtyp von Gruppe A ist immer Ethernet.
- Für Gruppe B sind die EAM-Steckplätze dauerhaft mit dem ersten MC (Mezzanine-Karte)-Steckplatz in jedem Servermodul verbunden.
- Für Gruppe C sind die EAM-Steckplätze dauerhaft mit dem zweiten MC (Mezzanine-Karte)-Steckplatz in jedem Servermodul verbunden.

Jede MC kann zwei externe Links unterstützen. Von der ersten MC ist der erste Link beispielsweise permanent mit dem EAM in Steckplatz 1 von Gruppe B verbunden, und der zweite Link ist permanent mit dem EAM in Steckplatz 2 von Gruppe B verbunden.

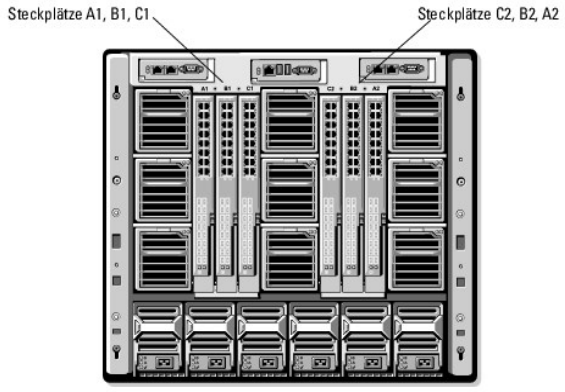
ANMERKUNG: In der CMC-CLI wird über die folgende Konvention auf EAMs Bezug genommen, switch-n:
A1=switch-1, A2=switch-2, B1=switch-3, B2=switch-4, C1=switch-5
und C2=switch-6.

Architekturverwaltung

Architekturverwaltung hilft bei der Vermeidung von elektrischen, Konfigurations- oder Konnektivitätsproblemen aufgrund der Installation eines EAMs oder einer MC, welche einen Architekturtypen hat, der nicht mit dem bekannten Architekturtypen des Gehäuses kompatibel ist. Ungültige Hardwarekonfigurationen können zu elektrischen oder funktionalen Problemen des Gehäuses oder seiner Komponenten führen. Die Architekturverwaltung verhindert, dass der Netzstrom bei ungültigen Konfigurationen eingeschaltet wird.

Abbildung 10-1 zeigt den Standort der EAMs im Gehäuse. Der Standort der einzelnen EAMs im Gehäuse wird durch die Gruppennummer (A, B oder C) und die Steckplatznummer (1 oder 2) angezeigt. Am Gehäuse sind die Steckplatznamen der EAMs mit A1, A2, B1, B2, C1 und C2 gekennzeichnet.

Abbildung 10-1. Rückansicht eines Gehäuses mit ausgewiesenen EAM-Standorten



Der CMC erstellt im Hardwareprotokoll und in den CMC-Protokollen Einträge zu ungültigen Hardwarekonfigurationen.

Zum Beispiel:

- Eine mit einem Fibre Channel-EAM verbundene Ethernet-MC ist eine ungültige Konfiguration. Eine Ethernet-MC, die sowohl mit einem Ethernet-Switch als auch mit einem Ethernet-Passthrough-EAM verbunden ist, die in der gleichen EAM-Gruppe installiert sind, ist eine gültige Verbindung.
- Ein Fibre Channel-Passthrough-EAM und ein Fibre Channel-Switch-EAM in den Steckplätzen B1 und B2 ist eine gültige Konfiguration, wenn die ersten MCs auf allen Servern ebenso Fibre Channels sind. In diesem Fall werden die EAMe und die Server über den CMC eingeschaltet. Einige Arten von Fibre Channel-Redundanzsoftware unterstützt diese Konfiguration jedoch möglicherweise nicht; nicht alle gültigen Konfigurationen sind zwangsläufig auch unterstützte Konfigurationen.

ANMERKUNG: Architekturbestätigung für Server-MCs wird nur ausgeführt, wenn das Gehäuse eingeschaltet ist. Wenn das Gehäuse nur im Standby läuft, bleiben die iDRACs auf den Servermodulen ausgeschaltet und können somit den MC- Architekturtyp des Servers nicht angeben. Der MC-Architekturtyp wird möglicherweise erst auf der CMC-Benutzeroberfläche angegeben, wenn der iDRAC auf dem Server eingeschaltet wird.

Ungültige Konfigurationen

Es gibt drei Typen ungültiger Konfigurationen:

- Eine ungültige MC-Konfiguration liegt vor, wenn sich eine neu installierte MC-Architektur von der vorhandenen EAM-Architektur unterscheidet.
- Eine ungültige EAM-MC-Konfiguration liegt vor, wenn eine neu installierte EAM-Architektur und die vorhandenen MC-Architekturen nicht übereinstimmen oder nicht miteinander kompatibel sind.
- Eine ungültige EAM-EAM-Konfiguration liegt vor, wenn ein neu installiertes EAM im Vergleich zu einem EAM, das bereits in der Gruppe installiert ist, einen unterschiedlichen oder inkompatiblen Architekturtyp aufweist.

Ungültige Konfiguration der Mezzanine-Karte (MC)

Eine ungültige MC-Konfiguration liegt vor, wenn die MC eines einzelnen Servers vom entsprechenden EAM nicht unterstützt wird. In diesem Fall können alle anderen Server im Gehäuse ausgeführt werden, aber der Server mit der nicht übereinstimmenden MC-Karte kann nicht eingeschaltet werden.

Ungültige Konfiguration der Mezzanine-Karte (MC)

Das nicht übereinstimmende EAM wird im ausgeschalteten Zustand belassen. Der CMC fügt den CMC- und Hardwareprotokollen einen Eintrag mit der ungültigen Konfiguration hinzu und gibt den Namen des EAMs an. Der CMC veranlasst auch, dass die Fehler-LED des fehlerhaften EAMs blinkt. Wenn der CMC zum Versenden von Warnungen konfiguriert ist, wird für dieses Ereignis eine E-Mail- und/oder SNMP-Warnung gesendet.

Informationen zu den CMC- und Hardwareprotokollen finden Sie unter "Ereignisprotokolle anzeigen".

Ungültige EAM-EAM-Konfiguration

Der CMC sorgt dafür, dass ein neu installiertes EAM in ausgeschaltetem Zustand bleibt, veranlasst, dass die Fehler-LED des EAMs blinkt und erstellt in den CMC- und Hardwareprotokollen Einträge zu der mangelnden Übereinstimmung.

Für Informationen zu den CMC- und Hardwareprotokollen, siehe "Ereignisprotokolle anzeigen".

Neues Einschalt-Szenario

Wenn der Netzstecker des Gehäuses eingesteckt und das Gehäuse eingeschaltet ist, haben die EAMe Priorität vor den Servern. Das erste EAM jeder Gruppe wird vor den anderen eingeschaltet. Zu diesem Zeitpunkt wird deren Architekturtyp nicht verifiziert. Wenn sich im ersten Steckplatz einer Gruppe kein EAM befindet, wird das Modul im zweiten Steckplatz dieser Gruppe eingeschaltet. Wenn sich in beiden Steckplätzen EAMe befinden, wird das Modul im zweiten Steckplatz im Hinblick auf Konsistenz mit dem im ersten verglichen.

Nachdem sich die EAMe eingeschaltet haben, schalten sich die Server ein, und der CMC überprüft die Server auf Architekturkonsistenz.

Ein Passthrough-Modul und ein Switch sind dann in derselben Gruppe zugelassen, wenn deren Architektur identisch ist. Switches und Passthrough-Module können in derselben Gruppe existieren, auch wenn Sie von unterschiedlichen Herstellern stammen.

EAM-Funktionszustand überwachen

Der Funktionszustand aller Server kann auf zwei Arten eingesehen werden: im Abschnitt Gehäuse-Grafiken auf der Seite Gehäusezustand oder auf der Seite Serverzustand. Die Seite Gehäuse-Grafiken bietet einen grafischen Überblick über die im Gehäuse installierten EAMs.

Um den Funktionszustand der EAMs mittel Gehäuse-Grafiken anzuzeigen:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Die Seite Gehäusezustand wird angezeigt. Die rechte Sektion der Gehäuse-Grafiken stellt die Rückansicht des Gehäuses dar und enthält den Funktionszustand aller EAMs. Der EAM-Funktionszustand wird durch die Farbe des EAM-Symbols angegeben:
   - Grün - EAM wird erkannt, mit Strom versorgt und kommuniziert mit dem CMC; es gibt keine Anzeichen eines ungünstigen Zustands.
   - Bernstein - EAM wird erkannt, kann jedoch mit Strom versorgt sein, oder nicht, kann mit dem CMC kommunizieren oder nicht; ein ungünstiger Zustand könnte vorhanden sein.
   - Grau - EAM wird erkannt und nicht mit Strom versorgt. Es kommuniziert nicht mit dem CMC und es gibt keine Anzeichen eines ungünstigen Zustands.
3. Bewegen Sie den Cursor über eine einzelne EAM-Grafik und ein entsprechender Texthinweis oder Bildschirmtipp wird angezeigt. Der Texthinweis liefert zusätzliche Informationen zu diesem EAM.
4. Die EAM-Grafik ist mit der entsprechenden Seite im CMC GUI verknüpft, um sofort die Navigation zur Seite EAMe -Status für dieses EAM zu ermöglichen.

Um den Status für alle EAMe einzusehen, verwenden Sie bitte die Seite EAMe-Status:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie im Menü Chassis (Gehäuse) der Systemstruktur den Eintrag I/O Module (EAM).
3. Klicken Sie auf die Registerkarte Eigenschaften.
4. Klicken Sie auf die Unterregisterkarte Status. Die Seite E/A Module- Status wird angezeigt. Tabelle 10-1 enthält Beschreibungen zu den Informationen auf der Seite E/A Module-Status.

Bauteil	**Beschreibung**		
Steckplatz	Zeigt den Standort des E/A Moduls im Gehäuse nach Gruppennummer (A, B oder C) und Steckplatznummer (1 oder 2) an. Steckplatznamen: A1, A2, B1, B2, C1 oder C2.		
Vorhanden	Zeigt an, ob das EAM vorhanden ist (Ja oder Nein).		
Funktionszustand		OK	Zeigt an, dass das EAM vorhanden ist und mit dem CMC kommuniziert. Im Falle eines Fehlers bei der Datenübertragung zwischen dem CMC und dem Server kann der CMC den Funktionszustand für das EAM nicht abrufen oder anzeigen.
		Zur Information	Zeigt Informationen zum EAM an, wenn keine Änderung im Funktionszustand (OK, Warnung, Schwerwiegend) aufgetreten ist.
		Warnung	Zeigt an, dass Warnungen ausgestellt wurden und Korrekturmaßnahmen ergriffen werden müssen. Wenn keine Korrekturmaßnahmen ergriffen werden, könnte dies zu kritischen oder schwerwiegenden Fehlern führen, die Auswirkungen auf die Integrität des EAMs haben können. Beispiele von Betriebszuständen, die Warnungen verursachen: Mangelnde Übereinstimmung der EAM-Architektur mit der Architektur der Mezzanine-Karte des Servers; ungültige EAM-Konfiguration, wobei das neu installierte EAM nicht mit dem vorhandenen EAM auf derselben Gruppe übereinstimmt.
		Schwerwiegend	Zeigt an, dass mindestens eine Fehlerwarnung ausgegeben wurde. Ein schwerwiegender Zustand weist auf einen Systemfehler im EAM hin, und es müssen sofort Korrekturmaßnahmen ergriffen werden. Beispiele von Betriebszuständen, die einen schwerwiegenden Zustand verursachen: Fehler im EAM erkannt; EAM wurde entfernt.

	ANMERKUNG: Alle Änderungen des Funktionszustands werden sowohl im Hardware- als auch im CMC-Protokoll aufgezeichnet. Weitere Informationen finden Sie unter "Ereignisprotokolle anzeigen".	
Architektur	Zeigt den Architekturtyp für das EAM an: Gigabit Ethernet, 10GE XAUI, 10GE KR, 10GE XAUI KR, FC 4 GBit/s, FC 8 GBit/s, SAS 3 GBit/s, SAS 6 GBit/s, Infiniband SDR, Infiniband DDR, Infiniband QDR, PCIe Bypass Generation 1, PCIe Bypass Generation 2. **ANMERKUNG:** Um EAM-Nichtübereinstimmungen innerhalb derselben Gruppe zu verhindern, ist es äußerst wichtig, dass Sie die Architekturtypen der EAMs im Gerät kennen. Für Informationen zur E/A- Architektur, siehe "Verwaltung der E/A-Architektur".	
Name	Zeigt den EAM-Produktnamen an.	
EAM-Verwaltungskonsole starten		Wenn das Symbol für ein bestimmtes E/A Modul vorhanden ist, kann man darauf klicken um die EAM-Verwaltungskonsole für dieses E/A Modul in einem neuen Fenster oder einer neuen Registerkarte des Browsers zu starten. **ANMERKUNG:** Diese Option ist nur für die verwalteten Switch- E/A Module verfügbar. Sie ist nicht für Passthrough-E/A Module oder nicht verwaltete Infiniband-Switches verfügbar. **ANMERKUNG:** Wenn ein EAM nicht zugreifbar ist, weil es ausgeschaltet ist, seine LAN-Schnittstelle deaktiviert ist oder dem Modul keine gültige IP-Adresse zugewiesen ist, wird die Option Launch IOM GUI (GUI des EAM starten) für dieses EAM nicht angezeigt. **ANMERKUNG:** Sie werden aufgefordert sich bei der E/A Modul Verwaltungsschnittstelle anzumelden. **ANMERKUNG:** Die IP-Adresse des E/A Moduls kann mit der CMC-GUI konfiguriert werden (s. Beschreibung in "Konfigurieren der Netzwerkeinstellungen für ein einzelnes EAM.").
Rolle	Wenn E/A Module miteinander verbunden werden, zeigt die Rolle die Stack-Zugehörigkeit der E/A Module an. Mitglied bedeutet, dass das Modul Teil eines Stack-Satzes ist. Besitzer bedeutet, dass das Modul ein primärer Zugangspunkt ist.	
Stromstatus	Zeigt den Stromstatus des EAMs an: Ein, Aus oder - (Nicht vorhanden).	
Service-Tag-Nummer	Zeigt die Service-Tag-Nummer für das EAM an. Die Service-Tag-Nummer ist eine eindeutige Kennung von Dell für Support und Wartung. Alle Änderungen des Funktionszustands werden sowohl im Hardware- als auch im CMC-Protokoll aufgezeichnet. Weitere Informationen finden Sie unter "Ereignisprotokolle anzeigen". **ANMERKUNG:** Passthroughs haben keine Service-Tag-Nummern. Nur Switch-Module haben Service-Tag-Nummern.	

Anzeigen des Funktionszustands eines einzelnen EAMs

Die Seite E/A Modulstatus (zu unterscheiden von der Seite E/A Module-Status) gibt eine Übersicht zu einem einzelnen EAM an.

So zeigen Sie den Funktionszustand eines einzelnen EAMs an:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Erweitern Sie im Systemverzeichnisbaum das Verzeichnis E/A Module. Es werden alle EAMe (1–6) in der erweiterten Liste der E/A Module angezeigt.
3. Klicken Sie auf das EAM, das Sie in der Liste der E/A Module in der Systemstruktur anzeigen möchten.
4. Klicken Sie auf die Unterregisterkarte Status. Die Seite E/A Module- Status wird angezeigt.

Tabelle 10-2 enthält Beschreibungen zu den Informationen auf der Seite E/A Modulstatus.

Bauteil	Beschreibung		
Standort	Zeigt den Standort des E/A Moduls im Gehäuse nach Gruppennummer (A, B oder C) und Steckplatznummer (1 oder 2) an. Steckplatznamen: A1, A2, B1, B2, C1 oder C2.		
Name	Zeigt den Namen des EAM an.		
Vorhanden	Zeigt an, ob das EAM vorhanden ist (Ja oder Nein).		
Funktionszustand		OK	Zeigt an, dass das EAM vorhanden ist und mit dem CMC kommuniziert. Im Falle eines Fehlers bei der Datenübertragung zwischen dem CMC und dem Server kann der CMC den Funktionszustand für das EAM nicht abrufen oder anzeigen.
		Zur Information	Zeigt Informationen zum EAM an, wenn keine Änderung im Funktionszustand (OK, Warnung, Schwerwiegend) aufgetreten ist. Beispiele von Betriebszuständen, die den Status "Zur Information" erzeugen: EAM erkannt; ein Benutzer hat das Aus- und Einschalten des EAMs angefordert.
		Warnung	Zeigt an, dass Warnungen ausgestellt wurden und Korrekturmaßnahmen ergriffen werden müssen. Wenn keine Korrekturmaßnahmen ergriffen werden, könnte dies zu kritischen oder schwerwiegenden Fehlern führen, die Auswirkungen auf die Integrität des EAMs haben können. Beispiele von Betriebszuständen, die Warnungen verursachen: Mangelnde Übereinstimmung der EAM-Architektur mit der Architektur der Mezzanine-Karte des Servers; ungültige EAM-Konfiguration, wobei das neu

			installierte EAM nicht mit dem existierenden EAM auf derselben Gruppe übereinstimmt.
		Schwerwiegend	Zeigt an, dass mindestens eine Fehlerwarnung ausgegeben wurde. Ein schwerwiegender Zustand weist auf einen Systemfehler im EAM hin, und es müssen sofort Korrekturmaßnahmen ergriffen werden. Beispiele von Betriebszuständen, die einen schwerwiegenden Zustand verursachen: Fehler im EAM erkannt; EAM wurde entfernt.
	ANMERKUNG: Alle Änderungen des Funktionszustands werden sowohl im Hardware- als auch im CMC-Protokoll aufgezeichnet. Informationen zur Einsicht der Protokolle finden Sie unter "Hardwareprotokoll anzeigen" und "CMC-Protokoll anzeigen".		
Stromstatus	Zeigt den Stromstatus des EAMs an: Ein, Aus oder - (Nicht vorhanden).		
Service-Tag-Nummer	Zeigt die Service-Tag-Nummer für das EAM an. Die Service-Tag-Nummer ist eine eindeutige Kennung von Dell für Support und Wartung.		
Architektur	Zeigt den Architekturtyp für das EAM an: Gigabit Ethernet, 10GE XAUI, 10GE KR, 10GE XAUI KR, FC 4 GBit/s, FC 8 GBit/s, SAS 3 GBit/s, SAS 6 GBit/s, Infiniband SDR, Infiniband DDR, Infiniband QDR, PCIe Bypass Generation 1, PCIe Bypass Generation 2. **ANMERKUNG:** Um EAM-Nichtübereinstimmungen innerhalb derselben Gruppe zu verhindern, ist es äußerst wichtig, dass Sie die Architekturtypen der EAMs im Gerät kennen. Für Informationen zur E/A-Architektur, siehe "Verwaltung der E/A-Architektur".		
MAC-Adresse	Zeigt die MAC-Adresse für das EAM an. Die MAC-Adresse ist eine eindeutige Adresse, die einem Gerät vom Hardwarehersteller zu Identifikationszwecken zugewiesen ist. **ANMERKUNG:** Passthroughs haben keine MAC-Adressen. Nur Switch-Module haben MAC-Adressen.		
Rolle	Zeigt die Stack-Zugehörigkeit eines EAMs an, wenn Module miteinander verbunden sind: • Mitglied - das Modul ist Teil eines Stack-Satzes. • Master - das Modul ist ein primärer Zugangspunkt.		

Konfigurieren der Netzwerkeinstellungen für ein einzelnes EAM.

Auf der Seite E/A Module-Setup können die Netzwerkeinstellungen für die Verwaltung der EAM verwendeten Schnittstelle angegeben werden. Für Ethernet-Switches wird der Port zur Band-externen Verwaltung (IP Adresse) konfiguriert. Der bandinterne Verwaltungsport (das heißt VLAN1) wird nicht mittels dieser Schnittstelle konfiguriert.

ANMERKUNG: Um Einstellungen auf der Seite E/A Module-Konfiguration zu ändern, müssen Sie zur Konfiguration der EAMs der Gruppe A Architektur-A-Administratorrechte besitzen; Architektur-B-Administratorrechte für die Konfiguration von EAMs in Gruppe B; oder Architektur-C-Administratorrechte zum Konfigurieren von EAMs in Gruppe C.

ANMERKUNG: Für Ethernet-Switches können weder die bandinterne (VLAN1), noch die bandexterne Verwaltungs-IP-Adresse die gleichen sein bzw. sich im gleichen Netzwerk befinden; dies führt dazu, dass die bandexterne IP-Adresse nicht vergeben wird. Beachten Sie die EAM-Dokumentation für die standardmäßige bandinterne Verwaltungs-IP-Adresse.

ANMERKUNG: Lediglich jene EAMs, die im Gehäuse vorhanden sind, werden angezeigt.

ANMERKUNG: Versuchen Sie nicht, E/A Modul-Netzwerkeinstellungen für Ethernet-Passthrough-Module oder Infiniband-Switches zu konfigurieren.

Um die Netzwerkeinstellungen für ein einzelnes EAM zu konfigurieren:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Erweitern Sie im Systemverzeichnisbaum das Verzeichnis E/A Module. Klicken Sie auf die Unterregisterkarte Einstellungen. Es wird die Seite Configure I/O Modules Network Settings (Konfiguration der E/A Module-Netzwerkeinstellungen) angezeigt.
3. Um die Netzwerkeinstellungen für E/A Module zu konfigurieren, tippen/wählen Sie Werte für die folgenden Eigenschaften und klicken dann auf Anwenden.

ANMERKUNG: Es können nur EAMs konfiguriert werden, die eingeschaltet sind.

ANMERKUNG: Die auf den EAMs festgelegte IP-Adresse vom CMC wird nicht in die permanente Hochfahr-Konfiguration der Switch übertragen. Um die konfigurierte IP-Adresse dauerhaft zu speichern, müssen Sie den Befehl connect switch -n oder den RACADM-Befehl racadm connect switch -n eingeben oder eine direkte Schnittstelle zum GUI des EAM verwenden, um diese Adresse in der Start-Konfiguration zu speichern.

Bauteil	Beschreibung
Steckplatz	Zeigt den Standort des EAMs im Gehäuse nach Gruppennummer (A, B oder C) und nach Steckplatznummer (1 oder 2) an. Steckplatznamen: A1, A2, B1, B2, C1 oder C2. (Der Wert für den Steckplatz kann nicht geändert werden.)
Name	Zeigt den EAM-Produktnamen an. (Der EAM-Name kann nicht geändert werden.)
Stromzustand	Zeig den Stromzustand des EAMs an. (Der Stromzustand kann auf dieser Seite nicht geändert werden.)
DHCP aktiviert	Hierdurch kann das EAM automatisch vom Server des dynamischen Host-Konfigurationsprotokolls (DHCP) eine IP-Adresse anfordern und abrufen.

	Standardeinstellung: Markiert (aktiviert). Wenn diese Option ausgewählt ist, ruft das EAM die IP-Konfiguration (IP-Adresse, Subnetzmaske, und Gateway) automatisch von einem DHCP-Server in Ihrem Netzwerk ab. **ANMERKUNG:** Wenn diese Funktion aktiviert ist, werden IP- Adresse, das Gateway und die Subnetzmasken-Eigenschaftsfelder (direkt an diese Option angrenzend) deaktiviert und sämtliche kürzlich eingegebenen Werte für diese Eigenschaften ignoriert. Ist diese Option ausgewählt, müssen Sie eine gültige IP-Adresse, das Gateway und die Subnetzmaske in die entsprechenden Textfelder gleich nach dieser Option manuell eingeben.
IP-Adresse	Gibt die IP-Adresse für die EAM-Netzwerkschnittstelle an.
Subnetzmaske	Gibt die Subnetzmaske für die EAM-Netzwerkschnittstelle an.
Gateway	Gibt den Gateway für die EAM-Netzwerkschnittstelle an.

Fehlerbehebung der EAM-Netzwerkeinstellungen

Die folgende Liste enthält Elemente zur Fehlerbehebung für die EAM-Netzwerkeinstellungen.

- Der CMC kann die IP-Adresseinstellung zu schnell nach einer Konfigurationsänderung auslesen; er wird 0.0.0.0 anzeigen, nach dem Klick auf Anwenden. Sie müssen die Aktualisierungsschaltfläche drücken, um zu sehen, ob die IP-Adresse in der Weiche korrekt gesetzt wurde.
- Wurden die Einstellungen der IP/Maske/Gateway fehlerhaft durchgeführt, wird die Weiche die IP-Adresse nicht vergeben und zu 0.0.0.0 in allen Feldern zurückkehren. Allgemeine 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 nicht in einem Netzwerk ist, das direkt mit dem Switch verbunden ist.

Für weitere Informationen zu EAM-Netzwerkeinstellungen, beachten Sie bitte das Dokument "Dell PowerConnect M6220 Switch" mit wichtigen Informationen und das White Paper "Dell PowerConnect 6220 Series Port Aggregator".

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Übersicht

Dell Chassis Management Controller Firmware Version 2.10, Benutzerhandbuch

Der Dell™ Chassis Management Controller (CMC) ist eine hotplug-fähige Hardware- und Softwarelösung zur Systemverwaltung, die Remote-Verwaltungsfähigkeiten und Stromsteuerungsfunktionen für Dell PowerEdge™ M1000e-Gehäusesysteme bietet.

Sie können den CMC so konfigurieren, dass E-Mail-Warnungen oder SNMP-Trap-Warnungen versendet werden, wenn Warnungen oder Fehler in Bezug auf Temperaturen, Hardwarefehlkonfigurationen, Stromausfälle und Lüftergeschwindigkeiten vorliegen.

Der CMC, der einen eigenen Mikroprozessor und Speicher hat, wird vom modularen Gehäuse, an das er angeschlossen ist, mit Strom versorgt.

Für erste Schritte mit dem CMC schlagen Sie unter "Installation und Setup des CMC" nach.

Was ist neu in dieser Version?

Diese Version von CMC unterstützt die folgenden Funktionen:

- IPv6 – CMC unterstützt jetzt das IPv6-Protokoll.

  Das IPv6 Ready Logo Committee hat den Auftrag, die Testspezifikationen für IPv6-Übereinstimmung und Interoperabilität-Tests zu definieren, um Selbsttest-Werkzeuge zu ermöglichen, die das "IPv6 Ready Logo" bereitstellen. CMC und iDRAC sind für das Phase-2 IPv6 Ready Logo zertifiziert. Die Logo-ID ist 02-C-000378 (Dell PowerEdge M1000e). Informationen über das IPv6 Ready Logo-Programm finden Sie unter **www.ipv6ready.org**.

- VLAN-Tagging – Der CMC und die iDRACs unterstützen jetzt die Möglichkeit, den Netzwerkverkehr einem virtuellen LAN (VLAN) zuzuordnen.
- Einfache Anmeldung für Active Directory-Konten – Einfache Anmeldung ermöglicht Benutzern, die mit Microsoft® Active Directory® auf ihren lokalen Systemen authentifiziert sind, die Anmeldeinformationen automatisch auf die CMC-Internet-Benutzeroberfläche anzuwenden.
- Zweifaktor-Authentifizierung mit Smart Card – Bietet höhere Sicherheit – eine Smart Card plus PIN zur Authentifizierung eines Benutzers anstelle eines einfachen Kennworts.
- Authentifizierung mit öffentlichem Schlüssel (PKA) über SSH – Verbessert SSH-Skripting-Automatisierung durch Beseitigung des Bedarfs, Benutzer-ID/Kennwort einzubetten bzw. Anforderungen auszugeben.
- Energieverwaltungsverbesserungen – Flexible Netzteilredundanzmodi: 1+1, 2+1 und 3+1. Zusätzliche fehlertolerante Wechselstromredundanzmodi: 1+1, 2+2 und 3+3.
- Zusätzliche Fehlerberichtsoptionen – Das iDRAC-Systemereignisprotokoll wird auf der Seite **Blade-Status** angezeigt und beseitigt den Bedarf, sich beim iDRAC anzumelden, um die Ereignisse anzuzeigen. Zudem werden CMC-Ereignisse jetzt auch auf einem Remote-Syslog-Server eingetragen.
- Option Remote-Dateifeigabe für virtuelle Datenträger – Ordnet ein Freigabelaufwerk im Netzwerk über den CMC einem oder mehreren Blades zu, um ein Betriebssystem bereitzustellen oder zu aktualisieren.
- Möglichkeit, SEL-Einträge für Server vom CMC zu lesen und zu löschen.

CMC-Verwaltungsfunktionen

Der CMC enthält die folgenden Verwaltungsfunktionen:

- Redundante CMC Umgebung.

- Registrierung des dynamischen Domänennamensystems (DDNS) für IPv4 und IPv6.
- Remote-Systemverwaltung und -überwachung über SNMP, eine Webschnittstelle, iKVM oder eine Telnet-/SSH-Verbindung.
- Unterstützung der Microsoft® Active Directory®-Authentifizierung - Zentralisiert CMC-Benutzer-IDs und Kennwörter im Active Directory anhand des Standardschemas oder eines Erweiterten Schemas.
- Überwachung - Zugriff auf Systeminformationen und Komponentenstatus.
- Zugriff auf Systemereignisprotokolle - Bietet Zugriff auf das Hardwareprotokoll und CMC-Protokoll.
- Firmware-Aktualisierungen für diverse Komponenten - CMC, Server, iKVM und modulare E/A-Infrastrukturgeräte.
- Dell OpenManage™ Software-Integration - Ermöglicht Ihnen, die CMC-Webschnittstelle vom Dell OpenManage Server Administrator oder IT Assistent zu starten.
- CMC-Warnungen - Warnt Sie anhand einer E-Mail-Benachrichtigung oder eines SNMP-Traps vor potenziellen Problemen mit verwalteten Knoten.
- Remote-Stromverwaltung - Bietet Remote-Stromverwaltungsfunktionen wie z. B. Herunterfahren und Reset einer beliebigen Gehäusekomponente von einer Verwaltungskonsole aus.
- Berichterstattung Stromverbrauch.
- SSL-Verschlüsselung (Secure Sockets Layer) - Bietet sichere Remote-Systemverwaltung über die Webschnittstelle.
- Sicherheitsverwaltung auf Kennwortebene - Verhindert den unbefugten Zugriff auf ein Remote-System.
- Rollenbasierte Autorität - Bietet zuweisbare Berechtigungen für verschiedene Systemverwaltungsaufgaben.
- Start-URL für die Webschnittstelle des Integrated Dell Remote Access Controller (iDRAC).
- Unterstützung für WS-Management.
- FlexAddress™-Funktion - Ersetzt die werkseitig zugewiesenen World Wide Name / Media Access Control (WWN/MAC)-Kennungen durch gehäusebezogene WWN/MAC-Kennungen für einen bestimmten Steckplatz; ein optionales Upgrade (weitere Informationen erhalten Sie unter "FlexAddress verwenden").
- Grafische Anzeige des Gehäusekomponentenstatus und Funktionszustand.
- Unterstützung für einfach- und multi-Slot-Server.
- Sofortige Aktualisierung der Firmware mehrerer iDRAC-Verwaltungskonsolen.
- LCD iDRAC-Konfigurationsassistent unterstützt iDRAC-Netzwerkkonfiguration.
- iDRAC-Einzelanmeldung.
- Network Time Protocol (NTP)-Unterstützung.
- Verbesserte Serverübersichts-, Stromberichterstattungs- und Stromsteuerungsseiten.
- Erzwungenes CMC-Failover und virtuelles "Neueinsetzen" von Servern.

Sicherheitsfunktionen

Der CMC gibt die folgenden Sicherheitsfunktionen an:

- Benutzerauthentifizierung durch Active Directory (optional) oder durch hardwaregespeicherte Benutzer-IDs und Kennwörter
- Rollenbasierte Berechtigung, die einem Administrator ermöglicht, spezifische Berechtigungen für jeden Benutzer zu konfigurieren
- Benutzer-ID- und Kennwort-Konfiguration über die Webschnittstelle
- Die Webschnittstelle unterstützt eine 128-Bit-SSL 3.0-Verschlüsselung und 40-Bit-SSL 3.0-Verschlüsselung (für Länder, in denen 128-Bit nicht akzeptiert werden)

  ANMERKUNG: Telnet unterstützt SSL-Verschlüsselung nicht.

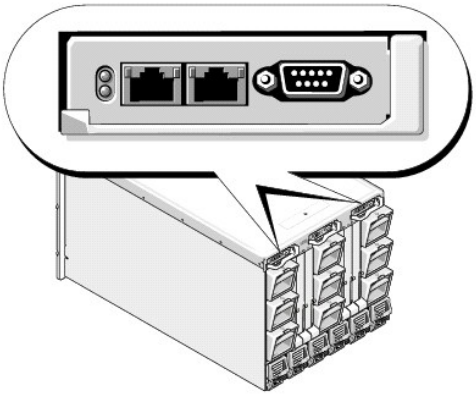
- Konfigurierbare IP-Schnittstellen (wo anwendbar)
- Beschränkung der Anmeldefehlschläge pro IP-Adresse, mit Anmeldeblockierung der IP-Adresse bei Überschreitung der Grenze
- Einstellbare automatische Sitzungszeitlimit, und Anzahl der gleichzeitigen Sitzungen
- Beschränkter IP-Adressenbereich für Clients, die an den CMC angeschlossen werden
- Secure Shell (SSH), die eine verschlüsselte Transportschicht für höhere Sicherheit verwendet.
- Einfache Anmeldung, Zweifaktor-Authentifizierung und Authentifizierung mit öffentlichem Schlüssel

---

Gehäuseübersicht

Abbildung 1-1 Abbildung 1-1 zeigt die Vorderkante des CMC (Einsatz) und die CMC-Steckplätze im Gehäuse.

Abbildung 1-1. Dell M1000e-Gehäuse und CMC



Hardwarespezifikationen

TCP/IP-Schnittstellen

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

Tabelle 1-1 gibt die vom CMC verwendeten Schnittstellen zum Abhören von Serververbindungen an. Tabelle 1-2 gibt die Schnittstellen an, die der CMC als Clients nutzt.

Tabelle 1-1. Abhörschnittstellen des CMC-Servers

Anschlussnummer	Funktion
22*	SSH
23*	Telnet
80*	http
161	SNMP-Agent
443*	HTTPS
* Konfigurierbarer Anschluss	

Tabelle 1-2. CMC-Client-Schnittstelle

Anschlussnummer	Funktion
25	SMTP
53	DNS
68	DHCP-zugewiesene IP-Adresse
69	TFTP
162	SNMP-Trap
514*	Remote-Syslog

636	LDAPS
3269	LDAPS für globalen Katalog (GC)
* Konfigurierbarer Anschluss	

Unterstützte Remote-Zugriffsverbindungen

Tabelle 1-3 führt die Verbindungsfunktionen auf.

Tabelle 1-3. Unterstützte Remote-Zugriffsverbindungen

Verbindung	Funktionen
CMC-NIC	• 10 MBit/s/100 MBit/s/1 GBit/s Ethernet über CMC-GbE-Schnittstelle • DHCP-Unterstützung • SNMP-Traps und E-Mail-Ereignis-Benachrichtigung • Dedizierte Netzwerkschnittstelle für die CMC-Webschnittstelle • Netzwerkschnittstelle für den iDRAC und E/A-Module (IOMs) • Unterstützung für die Telnet/SSH-Befehlskonsole und RACADM CLI-Befehle einschließlich Systemstart-, Reset-, Hochfahren-, und Herunterfahren- Befehle
Serielle Schnittstelle	• Unterstützung für die serielle Konsolen- und RACADM CLI-Befehle einschließlich Systemstart-, Reset-, Hochfahren-, und Herunterfahren-Befehle • Unterstützung für den binären Austausch für Anwendungen, die speziell dafür vorgesehen sind, ein Binärprotokoll zur Kommunikation mit einem bestimmten E/A-Modultyp zu nutzen • Serielle Schnittstelle kann mit dem Befehl connect (oder racadm connect) an die serielle Konsole eines Servers oder E/A-Moduls angeschlossen werden.
Weitere Verbindungen	• Zugriff auf die Dell-CMC-Konsole über das Avocent® Integrated KVM Switch-Modul (iKVM)

Unterstützte Plattformen

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

Informationen zu den neuesten unterstützten Plattformen finden Sie im Dell PowerEdge-Kompatibilitätshandbuch auf Dells Support-Website unter **support.dell.com**.

Unterstützte Web-Browser

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

Lokalisierte Versionen der CMC-Webschnittstelle können folgendermaßen angezeigt werden:

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

Unterstützte Verwaltungskonsolenanwendungen

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

Unterstützung für das WS-Management

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

Der Zugriff auf WS-Management erfordert Anmeldung mit lokalen Benutzerberechtigungen und Standardauthentifizierung über das SSL-Protokoll (Secured Socket Layer) auf Port 443. Informationen zum Einrichten von Benutzerkonten finden Sie im Abschnitt „cfgSessionManagement-Datenbankeigenschaften" im *Dell Chassis Management Controller Administrator-Referenzhandbuch*.

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

- Profil zu Zuordnungsfähigkeiten
- Profil zur Basismetrik
- Profil zum Basisserver
- Profil zum Computersystem
- Profil zum modularen System
- Profil zum physischen Bestand
- Profil zur Dell-Stromzuweisung
- Profil zur Dell-Stromversorgung
- Profil zur Dell-Stromtopologie
- Profil zur Stromzustandsverwaltung
- Profil zur Profilregistrierung
- Profil zum Datensatzprotokoll
- Profil zur Ressourcenbelegung
- Profil zur rollenbasierten Autorisierung
- Profil zu Sensoren
- Profil zum Serviceprozessor
- Profil zur einfachen Identitätsverwaltung
- Dell Active Directory-Clientprofil
- Boot-Steuerungsprofil
- Dell Einfaches NIC-Profil

Die CMC WS-MAN-Implementierung verwendet SSL auf Port 443 für Transportsicherheit und unterstützt Standardauthentifizierung. Informationen zum Einrichten von Benutzerkonten finden Sie im Abschnitt „cfgSessionManagement-Datenbankeigenschaften" im *Dell Chassis Management Controller Administrator-Referenzhandbuch*. Web Services-Schnittstellen können durch wirksames Einsetzen der Client-Infrastruktur genutzt werden, wie Windows® WinRM und Powershell CLI, Open Source-Dienstprogramm wie WSMANCLI und Anwendungsprogrammierumgebungen wie Microsoft® .NET®.

Zusätzliche Implementierungsrichtlinien, Weißbücher, Profil- und Code-Beispiele finden Sie im Dell Tech Center unter **www.delltechcenter.com**. Für weitere Informationen, siehe auch:

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

Weitere nützliche Dokumente

Zusätzlich zu diesem *Benutzerhandbuch* bieten die folgenden Dokumente weiterführende Informationen zum Setup und den Betrieb des CMC: All diese Dokumente können unter support.dell.com eingesehen werden:

- Die *CMC-Online-Hilfe* enthält Informationen zur Verwendung der Webschnittstelle.
- Die Chassis Management Controll (CMC) Secure Digital (SD) Card Technical Spezifikation bietet ein minimal-BIOS und Firmware-Version, Installation und Benutzerinformationen.
- Das Benutzerhandbuch zu Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise für Blade-Server gibt Informationen zur Installation sowie Konfiguration und Wartung des iDRAC auf verwalteten Systemen an.
- Das *Dell OpenManage™ IT Assistant-Benutzerhandbuch* gibt Informationen über die Anwendung des IT Assistant an.
- Die Dokumentation zu Ihrer Verwaltungskonsolenanwendung von Drittanbietern.
- Das *Dell OpenManage Server Administrator-Benutzerhandbuch* enthält Informationen über die Installation und Verwendung von Server Administrator.
- *Das* Benutzerhandbuch zu den Dell Update Packages enthält Informationen über das Abrufen und Verwenden von Dell Update Packages als Teil Ihrer Systemaktualisierungsstrategie.

Die folgenden Systemdokumente stehen außerdem zur Verfügung für weitere Informationen über das System, auf dem Ihr CMC installiert ist:

- In den mit dem System gelieferten Sicherheitshinweisen finden Sie wichtige Informationen zur Sicherheit und zu den Betriebsbestimmungen. Weitere Betriebsbestimmungen finden Sie auf der Website zur ?Einhaltung gesetzlicher Vorschriften unter www.dell.com/regulatory_compliance. Garantiebestimmungen können als separates Dokument beigelegt sein.
- Im zusammen mit der Rack-Lösung gelieferten *Rack-Installationshandbuch* bzw. in der *Rack-Installationsanleitung* wird beschrieben, wie das System in einem Rack installiert wird.
- Im *Hardware-Benutzerhandbuch* finden Sie Informationen über Systemfunktionen, sowie darüber, wie Fehler im System behoben und Systemkomponenten installiert oder ausgetauscht werden.
- 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.
- Möglicherweise sind auch Aktualisierungen beigelegt, in denen Änderungen am System, an der Software und/oder an der Dokumentation beschrieben sind.

  ANMERKUNG: Lesen Sie diese Aktualisierungen immer zuerst, da sie frühere Informationen gegebenenfalls außer Kraft setzen.

- Gegebenenfalls sind Versionsinformationen oder Infodateien vorhanden. Diese geben den letzten Stand der Änderungen am System oder an der Dokumentation wieder und enthalten erweitertes technisches Referenzmaterial für erfahrene Benutzer oder Techniker.
- Weitere Informationen zu IOM-Netzwerkeinstellungen finden Sie in den Dokumenten Dell PowerConnect™ M6220 Switch - Wichtige Informationen und Dell PowerConnect 6220 Series Port Aggregator - Weißbuch.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Stromverwaltung

Dell Chassis Management Controller Firmware Version 2.10, Benutzerhandbuch

---

Übersicht

Das Dell PowerEdge M1000e-Servergehäuse ist der energieeffizienteste modulare Server auf dem Markt. Er beinhaltet hocheffiziente Netzteile und Lüfter, verfügt über ein optimiertes Layout, sodass die Luft leichter durch das System strömen kann, und enthält im gesamten Gehäuse energieoptimierte Komponenten. Das verbesserte Hardware-Design ist mit fortschrittlichen Stromverwaltungsfunktionen gekoppelt, die im CMC (Chassis Management Controller), in Netzteilen und im iDRAC integriert sind. Sie können damit die Stromeffizienz weiter verbessern und die Stromumgebung umfassend kontrollieren.

Das modulare PowerEdge M1000e-Gehäuse nimmt Wechselstrom auf und verteilt die Last auf alle aktive interne Netzteileinheiten (PSUs). Das System kann bis zu 7928 Watt Wechselstrom verwalten, der Servermodulen und der damit verbundenen Gehäuseinfrastruktur zugeteilt wird.

ANMERKUNG: Die tatsächliche Stromzuteilung hängt von der Konfiguration und der Auslastung ab.

Die Stromverwaltungsfunktionen des M1000e helfen Administratoren, das Gehäuse zu konfigurieren, um den Stromverbrauch zu reduzieren und die Stromverwaltung auf die individuellen Bedürfnisse und Umgebungen zuzuschneiden.

Das M1000e-Gehäuse kann für eine von drei Redundanzregeln konfiguriert werden, die das Netzteilverhalten beeinflussen und bestimmen, wie der Gehäuse-Redundanzstatus Administratoren gemeldet wird.

Wechselstrom-Redundanzmodus

Die Wechselstrom-Redundanzregel macht es möglich, dass ein modulares Gehäusesystem in einem Modus betrieben wird, in dem es Netzstromausfälle überbrücken kann. Diese Ausfälle können ihren Ursprung im Wechselstromnetz, in der Verkabelung oder in einer Netzteileinheit selbst haben.

Bei der Konfiguration eines Systems für Wechselstromredundanz werden die Netzteileinheiten (PSUs) in abgestimmte Sätze (oder Stromkreise) aufgeteilt: Netzteileinheiten-Steckplätze 1, 2 und 3 im ersten Stromkreis (Stromkreis A) und Netzteileinheiten-Steckplätze 4, 5 und 6 im zweiten Stromkreis (Stromkreis B). Jede Netzteileinheit in einem abgestimmten Satz gehört zu einem anderen Wechselstromkreis und muss für ordentlichen Betrieb in einem Wechselstromredundanzmodus dementsprechend verkabelt sein. Die Last wird über alle aktiven Netzteileinheiten verteilt. Die Last auf einer einzelnen Netzteileinheit überschreitet niemals 50 Prozent ihrer Kapazität. Mit Wechselstromredundanz kann das System den Verlust eines gesamten Wechselstromkreises oder bis zu 50 Prozent seiner Kapazität (mit Versagen einzelner Netzteileinheiten) überbrücken. Das System versorgt das modulare Gehäusesystem weiter ausreichend mit Strom.

Der Wechselstromredundanzmodus ist die Standardwerkseinstellung für eine Konfiguration mit 6 Netzteileinheiten (PSUs). Das Gehäuse ist für Wechselstromredundanz konfiguriert.

ANMERKUNG: Ein System funktioniert nur in einem Wechselstromredundanzmodus, wenn die erforderlichen Bedingungen erfüllt sind. Im Besonderen muss jeder Wechselstromkreis mit abgestimmten Netzteileinheiten bestückt sein, und die Gesamtlast darf die Kapazität eines einzelnen Stromkreises nicht übersteigen.

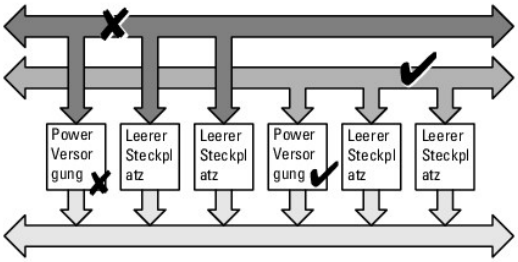
Wechselstromredundanzstufen

Der CMC unterstützt drei Stufen von *N+N* Wechselstromredundanz: 1+1, 2+2 und 3+3.

In Wechselstromredundanz meldet der CMC alle aktiven Netzteile als eingeschaltet (online). Dadurch wird gewährleistet, dass das System zu keinem Zeitpunkt ausfällt, wenn ein Stromkreis von einem Stromausfall betroffen ist. Wenn eine der *N* Netzteileinheiten in einem Stromkreis ausfällt, meldet der CMC den Gehäuseredundanzstatus als Keine Redundanz. E-Mail und/oder SNMP-Alarme werden an Administratoren gesendet, falls das Ereignis Redundanzverlust für Alarmierung konfiguriert wurde.

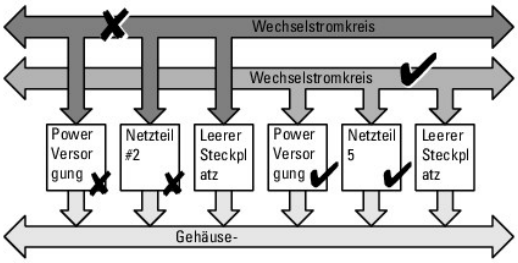
- 1+1 Wechselstromredundanzstufe – an jedem Wechselstromkreis ist mindestens eine Netzteileinheit angeschlossen.

Abbildung 8-1. 1+1 Redundanzstufe



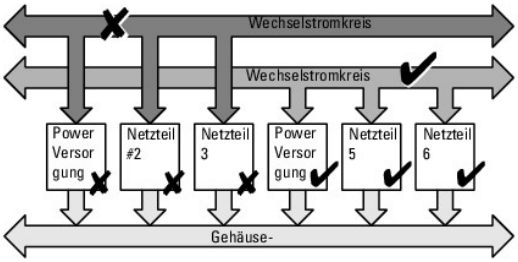
- 2+2 Wechselstromredundanzstufe – an jedem Wechselstromkreis sind mindestens zwei Netzteileinheiten angeschlossen.

Abbildung 8-2. 2+2 Redundanzstufe



- 3+3 Wechselstromredundanzstufe – an jedem Wechselstromkreis sind drei Netzteileinheiten angeschlossen. Da drei Netzteileinheiten das gesamte Gehäuse versorgen können, wird diese Konfiguration nicht von einem völligen Ausfall eines der Wechselstromnetze beeinflusst, die Stromversorgung des Gehäuses wird nicht unterbrochen.

Abbildung 8-3. 3+3 Redundanzstufe



ANMERKUNG: Wenn eine einzelne Netzteileinheit in dieser Konfiguration ausfällt, werden die beiden anderen Netzteileinheiten des befallenen Stromkreises als **Online** markiert. In diesem Zustand kann jede der verbleibenden Netzteileinheiten ausfallen, ohne dass der Betrieb des Systems unterbrochen wird. Wenn eine Netzteileinheit ausfällt, wird der Gehäusezustand als "Nicht-kritisch" markiert. Wenn der kleinere Stromkreis die Summe der Gehäusestromzuteilungen nicht unterstützen kann, wird der Wechselstromredundanzstatus als **Keine Redundanz** gemeldet und der Gehäusezustand als **Kritisch** angezeigt.

ANMERKUNG: Das Gehäuse benötigt lediglich 3 Netzteileinheiten (PSUs), um alle Blades zu betreiben. Zur Unterstützung von Wechselstromredundanz muss jedoch ein ausgeglichener Satz von Netzteileinheiten vorhanden sein. Die Hälfte der Einheiten wird bei der Berechnung der Stromkapazitäten berücksichtigt. Die andere Hälfte wird für Wechselstromredundanz markiert. Wenn weniger Netzteileinheiten installiert werden, als für den Betrieb der Server erforderlich sind, wird Redundanz möglicherweise als **Keine Redundanz** gemeldet, oder Server können u. U. nicht gestartet werden.

Netzteilredundanz-Modus

Der Netzteilredundanz-Modus ist nützlich, wenn keine redundanten Stromkreise zur Verfügung stehen und sich Benutzer gegen den Ausfall eines einzelnen Netzteils und demzufolge der Server in einem modularen Gehäuse schützen möchten. Zu diesem Zweck wird die Kapazität einer Netzteileinheit über den Zuteilungsanforderungen als Online-Reserve zurückbehalten. Das bildet einen Netzteilredundanzpool.

Alle außerhalb dieses Pools installierten Netzteileinheiten werden nicht verwendet. Diese Netzteileinheiten stoßen zum Redundanzpool, falls Einheiten innerhalb des Pools ausfallen.

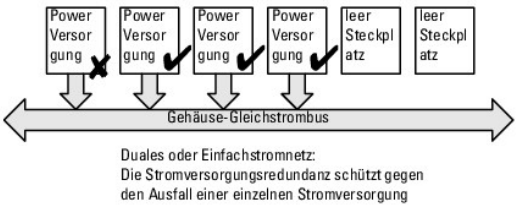
Netzteilredundanzstufen

Der CMC unterstützt drei Stufen von Netzteilredundanz: 1+1, 2+1 und 3+1. Bei dieser Option läuft die zusätzliche Netzteileinheit immer mit, um zu gewährleisten, dass der Ausfall einer einzelnen Netzteileinheit jederzeit überbrückt werden kann. Abbildung 8-4 zeigt eine Konfiguration mit vier Netzteileinheiten in den ersten vier Netzteileinheiten-Steckplätzen. Der CMC erfordert jedoch nicht, dass die vier Netzteileinheiten in einer bestimmten Steckplatzposition vorhanden sind.

Dynamische Netzteilzuschaltung (DPSE) ermöglicht, dass Netzteileinheiten als Standby eingesetzt werden.

Der Zustand *Standby* zeigt einen Aus-Zustand (OFF) an. Bei Aktivierung von DPSE werden zusätzliche Netzteileinheiten in den Standby-Modus versetzt, um die Effizienz zu erhöhen und Energie zu sparen.

Abbildung 8-4. Netzteilredundanz: 3+1 Netzteilredundanz



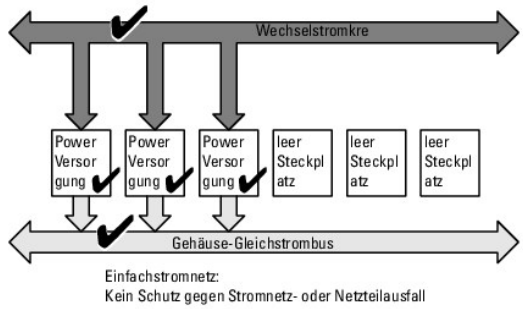
Keine-Redundanz-Modus

Der Modus *Keine Redundanz* ist die Standardwerkseinstellung für eine Konfiguration mit drei Netzteileinheiten (PSUs). Für das Gehäuse ist keine Stromredundanz konfiguriert. Bei dieser Konfiguration ist der Gesamt-Redundanzstatus des Gehäuses immer Keine Redundanz.

Abbildung 8-5 zeigt die drei Netzteileinheiten in den ersten drei Netzteileinheit-Steckplätzen. Der CMC erfordert jedoch nicht, dass die drei Netzteileinheiten in einer bestimmten Steckplatzposition vorhanden sind.

ANMERKUNG: Alle aktiven Netzteileinheiten im Gehäuse werden als **Online** aufgeführt. Alle zusätzlichen Netzteileinheiten können für erhöhte Energieeffizienz ausgeschaltet werden; diese werden als **Standby** markiert, falls DPSE aktiviert ist. Alle Netzteileinheiten im Gehäuse werden als **Online** aufgeführt, falls DPSE im Modus **Keine Redundanz** deaktiviert wird.

Abbildung 8-5. Keine Redundanz



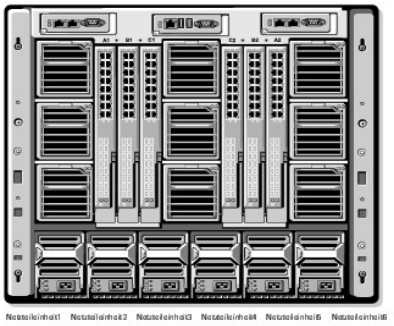
Ein Ausfall einer Netzteileinheit bewirkt, dass die anderen Netzteileinheiten nach Bedarf aus dem Standby-Modus geschaltet werden, um die Gehäusestromzuteilungen zu versorgen. Wenn bei 4 Netzteileinheiten eine ausfällt, wird die vierte Netzteileinheit online geschaltet. Ein Gehäuse kann maximal 6 Netzteileinheiten online geschaltet haben.

Bei Aktivierung von DPSE werden zusätzliche Netzteileinheiten in den Standby-Modus versetzt, um die Effizienz zu erhöhen und Energie zu sparen.

Strombudget für Hardwaremodule

Abbildung 8-6 zeigt ein Gehäuse mit einer Konfiguration für 6 Netzteileinheiten. Die Netzteileinheiten im Gehäuse sind von links nach rechts von 1 bis 6 nummeriert.

Abbildung 8-6. Gehäuse mit einer Konfiguration von sechs Netzteileinheiten



Der CMC hält ein Strombudget für das Gehäuse ein, das die für alle installierten Server und Komponenten notwendige Wattleistung reserviert.

Der CMC teilt der CMC-Infrastruktur und den Bladeservern im Gehäuse Strom zu. Die CMC-Infrastruktur besteht aus Komponenten im Gehäuse, z. B. Lüfter, E/A-Module und iKVM (falls vorhanden). Das Gehäuse kann bis zu 16 Bladeserver aufweisen, die über den iDRAC mit dem Gehäuse kommunizieren. Weitere Informationen finden Sie im *iDRAC-Benutzerhandbuch* unter **support.dell.com / manuals**.

Der iDRAC stellt dem CMC seine Strombereichsanforderungen vor Einschaltung des Bladeservers bereit. Der Strombereich besteht aus den maximalen und minimalen Stromanforderungen, die für den Betrieb des Servers erforderlich sind. Die anfängliche Schätzung von iDRAC basiert auf einem Modell für den ungünstigsten Fall, bei dem alle Komponenten im Bladeserver Maximalstrom beziehen. Diese Schätzung ist oft höher als die tatsächlichen Anforderungen des Bladeservers.

Wenn ein Server in einem Gehäuse eingeschaltet wird, schätzt die iDRAC-Software die Stromanforderungen neu ein und fordert eine nachfolgende Änderung des Strombereichs (normalerweise wird der Strombereich reduziert).

Der CMC gewährt dem Bladeserver den angeforderten Strom und die zugeteilte Wattleistung wird vom verfügbaren Budget subtrahiert. Sobald dem Server eine Stromanforderung gewährt wurde, kontrolliert die iDRAC-Software des Servers den tatsächlichen Stromverbrauch. Der iDRAC-Strombereich kann, abhängig von den tatsächlichen Stromanforderungen, sich im Lauf der Zeit ändern. Der iDRAC verlangt nur eine Stromerhöhung, wenn die Server den zugeteilten Strom vollständig verbrauchen.

Unter schwerer Last kann jedoch die Prozessorleistung des Servers herabgesetzt werden, um zu gewährleisten, dass der Stromverbrauch unterhalb der benutzerdefinierten **Systemeingangstromobergrenze** bleibt.

Das PowerEdge M1000e-Gehäuse kann ausreichend Strom für die Spitzenleistung der meisten Serverkonfigurationen bereitstellen, aber viele verfügbare Serverkonfigurationen verbrauchen nicht die maximale Strommenge, die das Gehäuse liefern kann. Um Rechenzentren bei der Strombereitstellung für ihre Gehäuse zu unterstützen, erlaubt das M1000e dem Benutzer, eine Systemeingangstromobergrenze anzugeben. Damit kann sichergestellt werden, dass der Gesamt-Wechselstromverbrauch des Gehäuses unter einem festgelegten Schwellenwert bleibt. Zunächst stellt der CMC sicher, dass ausreichend Strom für die Lüfter, E/A-Module, iKVM (falls vorhanden) und dem CMC selbst verfügbar ist. Diese Stromzuteilung wird als Der Gehäuseinfrastruktur zugewiesener Eingangsstrom bezeichnet. Sobald die Server in einem Gehäuse eingeschaltet sind, kann die **Systemeingangstromobergrenze** nicht auf einen niedrigeren Wert gesetzt werden, der voraussetzen würde, dass sich ein Server ausschaltet, um die Anforderung zu erfüllen.

Wenn es für das Gesamtstrombudget erforderlich ist, unter dem Wert der Systemeingangstromobergrenze zu bleiben, teilt der CMC den Servern einen Wert

zu, der unter ihrer maximal angeforderten Strommenge liegt. Strom wird den Servern basierend auf ihrer **Server**-Priorität zugeteilt: Server der Priorität 1 erhalten maximale Strommenge vor Servern der Priorität 2 usw. Server mit niedrigerer Priorität erhalten basierend auf der Einstellung **Maximale Systemeingangskapazität** und der benutzerdefinierten Einstellung **Systemeingangstromobergrenze** möglicherweise weniger Strom als Server der Priorität 1.

Konfigurationsänderungen, z. B. ein zusätzlicher Server im Gehäuse, erfordern u. U., dass die Systemeingangstromobergrenze erhöht wird. Der Strombedarf in einem modularen Gehäuse steigt ebenfalls, wenn sich die Temperatur ändert und die Lüfter mit höherer Geschwindigkeit laufen müssen, wodurch sie mehr Strom verbrauchen. Der Einbau von E/A-Modulen und iKVM erhöht den Strombedarf des modularen Gehäuses ebenfalls. Eine geringe Menge Strom wird selbst von ausgeschalteten Servern verbraucht, um die Funktion des Management-Controllers aufrechtzuerhalten. Zusätzliche Server können nur dann in einem modularen Gehäuse eingesetzt werden, wenn ausreichend Strom verfügbar ist. Die Systemeingangstromobergrenze kann jederzeit bis zu einem Maximalwert von 7928 Watt erhöht werden, um das Hochfahren von zusätzlichen Servern zu ermöglichen.

Änderungen im modularen Gehäuse, die die Stromzuteilung verringern, sind das Ausschalten von Servern, die Entfernung von Servern, E/A-Modulen oder des iKVM sowie der Wechsel des Gehäuses in einen ausgeschalteten Zustand. Die **Systemeingangstromobergrenze** kann neu konfiguriert werden, wenn das Gehäuse eingeschaltet (ON) oder ausgeschaltet (OFF) ist.

Serversteckplatz-Stromprioritätseinstellungen

Der CMC ermöglicht es Ihnen, eine Strompriorität für jeden der 16 Serversteckplätze eines Gehäuses festzulegen. Die Prioritätseinstellungen gehen von 1 (höchste) bis 9 (niedrigste). Diese Einstellungen werden Steckplätzen des Gehäuses zugewiesen. Die Priorität des Steckplatzes trifft auf jeden Server zu, der diesen Steckplatz später belegt. Der CMC verwendet die Steckplatz-Priorität, um vorzugsweise den Servern mit der höchsten Priorität Strom zuzuweisen.

Der Strom wird gemäß der Standard-Serversteckplatzpriorität gleichmäßig verteilt. Durch die Änderung der Steckplatz-Priorität können Administratoren festlegen, welche Server bei der Stromzuteilung bevorzugt werden sollen. Wenn für die kritischeren Servermodule die Standard-Steckplatzpriorität von 1 beibehalten wird und die Priorität der weniger kritischen Servermodule auf den Prioritätswert 2 oder niedriger gesetzt werden, werden die Servermodule mit der Priorität 1 zuerst hochgefahren. Diese Server mit höherer Priorität erhalten dann ihre maximale Stromzuteilung, während die Server mit niedrigerer Priorität eventuell nicht genug Strom erhalten, um ihre maximale Leistung zu bringen. Sie könnten sogar ausgeschaltet bleiben, je nachdem, wie niedrig der Grenzwert gesetzt ist und wie sich die Stromanforderung des Servers gestaltet.

Wenn ein Administrator den Servern niedriger Priorität manuell Strom zuteilt, bevor die Server mit hoher Priorität versorgt werden, sind die Servermodule niedriger Priorität die ersten, deren Stromzuteilung auf den minimalen Wert gesenkt wird. Sobald die verfügbare Stromzuteilung aufgebraucht ist, fordert der CMC Strom von Servern mit gleicher oder niedrigerer Priorität bis zu deren Mindeststrompegel zurück.

ANMERKUNG: E/A-Module, Lüfter und iKVM (falls vorhanden) erhalten die höchste Priorität. Der CMC fordert Strom nur zurück, um den Strombedarf eines Moduls oder Servers mit höherer Priorität zu erfüllen.

Dynamische Netzteilzuschaltung

Der Modus "Dynamische Zuschaltung von Netzteileinheiten" (DPSE) ist standardmäßig deaktiviert. Die dynamische Zuschaltung von Netzteileinheiten (DPSE) spart Strom, da nur die minimale Anzahl von Netzteileinheiten eingesetzt wird, die für die Versorgung des Gehäuses notwendig ist. Dies führt zu einer besseren Auslastung der Online-Netzteileinheiten und verbessert demzufolge deren Effizienz. Die Lebensdauer der Netzteileinheiten wird erhöht, es wird weniger Wärme erzeugt und Strom wird eingespart, da die Netzteileinheiten auf effizienteren Leistungsstufen eingesetzt werden.

Der CMC überwacht die Gesamtstromzuteilung des Gehäuses und versetzt nicht erforderliche Netzteileinheiten in den Zustand Standby. So wird die Gesamtstromzuteilung des Gehäuses über weniger Netzteileinheiten erbracht. Da die Online-Netzteileinheiten effizienter sind, wenn sie mit höherer Ausnutzung laufen, verbessert dies ihre Effizienz. Außerdem erhöht sich die Lebensdauer der Standby-Netzteileinheiten.

Das System läuft mit so wenig aktiven Netzteileinheiten wie möglich am effizientesten. Bedenken Sie also:

- Der Modus Keine Redundanz mit dynamischer Zuschaltung von Netzteileinheiten (DPSE) ist sehr energieeffizient – nur die minimale Anzahl von Netzteileinheiten ist online. Nicht erforderliche Netzteileinheiten werden in den Standby-Modus versetzt.
- Auch der Netzteilredundanzmodus mit dynamischer Zuschaltung von Netzteileinheiten (DPSE) bietet Energieeffizienz. Mindestens zwei Netzteileinheiten sind aktiv, wobei eine Netzteileinheit die Konfiguration versorgt und eine andere für Redundanz sorgt, falls eine Netzteileinheit ausfällt. Der Netzteileinheitredundanzmodus schützt vor dem Ausfall beliebiger Netzteileinheiten, bietet aber keinen Schutz bei einem Ausfall des Wechselstromnetzes.
- Beim Wechselstromredundanzmodus mit dynamischer Zuschaltung von Netzteileinheiten (DPSE) sind mindestens zwei von sechs Netzteileinheiten aktiv, eine in jedem Stromkreis. Es besteht ein guter Ausgleich zwischen Effizienz und maximaler Verfügbarkeit für eine teilbelastete modulare Gehäusekonfiguration.
- Das Deaktivieren der dynamischen Zuschaltung von Netzteileinheiten bietet die geringste Effizienz, da alle sechs Netzteileinheiten aktiv sind und die Last teilen. Dies führt zu einer schlechteren Ausnutzung der einzelnen Netzteile.

Die dynamische Zuschaltung von Netzteileinheiten (DPSE) kann für alle drei oben erläuterten Redundanzkonfigurationen aktiviert werden: Keine Redundanz, Netzteilredundanz und Wechselstromredundanz.

- Bei der Konfiguration Keine Redundanz mit dynamischer Zuschaltung von Netzteileinheiten (DPSE) kann das M1000e bis zu fünf Netzteileinheiten in den Zustand Standby versetzen. In einer Konfiguration mit 6 Netzteileinheiten werden einige Netzteileinheiten in Standby versetzt und bleiben unbenutzt,

um die Energieeffizienz zu verbessern. Die Entfernung oder der Ausfall einer Online-Netzteileinheit in dieser Konfiguration setzt eine Netzteileinheit vom Zustand Standby in den Zustand Online; es kann allerdings 2 Sekunden dauern, bis Standby-Netzteileinheiten aktiv werden, sodass es bei einigen Servern während dieser Umschaltung in der Konfiguration Keine Redundanz zu einem Stromverlust kommen kann.

ANMERKUNG: In einer Konfiguration mit drei Netzteileinheiten kann die Serverlast verhindern, dass Netzteileinheiten in den Zustand Standby gesetzt werden.

- In einer Netzteilredundanz-Konfiguration lässt das Gehäuse, neben den für die Versorgung des Gehäuses erforderlichen Netzteileinheiten, immer eine zusätzliche Netzteileinheit eingeschaltet und als Online markiert. Der Stromverbrauch wird überwacht. Es können je nach Gesamtsystemlast bis zu vier Netzteileinheiten in den Zustand Standby gesetzt werden. In einer Konfiguration mit sechs Netzteileinheiten sind immer mindestens zwei Netzteileinheiten eingeschaltet.

  Da ein Gehäuse mit der Konfiguration Netzteilredundanz immer über eine zusätzliche Netzteileinheit verfügt, kann das Gehäuse den Ausfall einer Online-Netzteileinheit überbrücken und trotzdem noch genug Strom für die installierten Servermodule zur Verfügung stellen. Der Ausfall der Online-Netzteileinheit führt dazu, dass eine Standby-Netzteileinheit online geschaltet wird. Der gleichzeitige Ausfall mehrerer Netzteileinheiten kann zum Stromverlust bei einigen Servermodulen führen, während die Standby-Netzteileinheiten hochfahren.

- Bei der Konfiguration Wechselstromredundanz werden beim Einschalten des Gehäuses alle Netzteileinheiten in Betrieb genommen. Der Stromverbrauch wird überwacht. Wenn die Systemkonfiguration und der Stromverbrauch es ermöglichen, werden Netzteileinheiten paarweise in den Standby-Zustand versetzt - je eine von jedem Wechselstromnetz (ausgenommen auf der 1+1 Redundanzstufe). Da der Online-Status von Netzteileinheiten in einem Netz den des anderen Netzes wiederspiegelt, kann das Gehäuse den Stromverlust eines gesamten Netzes ausgleichen, ohne die Stromversorgung des Gehäuses zu unterbrechen.

  Ein erhöhter Strombedarf führt bei der Wechselstromredundanz-Konfiguration zum paarweisen Einsatz von Netzteileinheiten aus dem Standby-Zustand - eine von jedem Wechselstromnetz (ausgenommen auf der 1+1 Redundanzstufe). So wird die gespiegelte Konfiguration beibehalten, die für die Doppelnetz-Redundanz notwendig ist.

ANMERKUNG: Wenn dynamische Zuschaltung von Netzteileinheiten (DPSE) aktiviert ist, werden die Standby-Netzteileinheiten **Online** genommen, um bei erhöhtem Bedarf in allen drei Wechselstromredundanzmodi Strom anzufordern.

Redundanzregeln

Eine Redundanzregel ist ein konfigurierbarer Satz von Eigenschaften, die festlegen, wie der CMC den Strom im Gehäuse verwaltet. Die folgenden Redundanzregeln sind mit oder ohne dynamische Zuschaltung von Netzteileinheiten konfigurierbar:

- Wechselstromredundanz
- Netzteilredundanz
- Keine Redundanz

Die Standard-Redundanzkonfiguration eines Gehäuses hängt von der Zahl der enthaltenen Netzteileinheiten ab, wie in Tabelle 8-1 dargestellt.

Tabelle 8-1. Standard-Redundanzkonfiguration

Konfiguration der Netzteileinheiten	Standard-Redundanzregel	Standardeinstellung für die dynamische Zuschaltung von Netzteileinheiten
Sechs Netzteileinheiten	Wechselstromredundanz	Deaktiviert
Drei Netzteileinheiten	Keine Redundanz	Deaktiviert

Wechselstromredundanz

Im Wechselstromredundanzmodus mit 6 Netzteileinheiten sind alle Netzteileinheiten aktiv. Die drei Netzteile zur Linken müssen mit einen AC-Stromnetz verbunden sein, während die drei Netzteile zur Rechten mit einem anderen AC-Stromnetz verbunden sein müssen.

VORSICHTSHINWEIS: Um einen Systemfehler zu vermeiden und effizient funktionierende Wechselstromredundanz zu gewährleisten, muss sichergestellt werden, dass es einen ausgeglichenen Satz von Netzteileinheiten gibt, der mit separaten Wechselstromkreisen verkabelt ist.

Falls ein Wechselstromkreis ausfällt, übernehmen die drei Netzteileinheiten des funktionierenden Wechselstromkreises die Funktion, ohne dass Unterbrechungen für Server oder Infrastruktur auftreten.

VORSICHTSHINWEIS: Im Wechselstromredundanzmodus muss ein ausgeglichener Satz von Netzteileinheiten (mindestens eine Netzteileinheit pro Stromkreis) vorhanden sein. Wenn diese Bedingung nicht erfüllt ist, besteht die Gefahr von Redundanzverlust.

Netzteilredundanz

Wenn Netzteilredundanz aktiviert ist, befindet sich eine Ersatz-Netzteileinheit im Gehäuse. Diese stellt sicher, dass der Ausfall einer anderen Netzteileinheit nicht dazu führt, dass die Stromversorgung der Server oder des Gehäuses unterbrochen wird. Der Netzteilredundanzmodus erfordert bis zu vier Netzteileinheiten. Weitere Netzteileinheiten, falls vorhanden, werden zur Verbesserung der Energieeffizienz des Systems eingesetzt, falls dynamische Zuschaltung von Netzteileinheiten (DPSE) aktiviert ist. Der Ausfall von Netzteilen nach Redundanzverlust kann ein Herunterfahren der Server im Gehäuse bewirken.

Keine Redundanz

Der Strom von bis zu drei Netzteilen wird verwendet, um das gesamte Gehäuse zu versorgen. Ein Gehäuse mit 6 Netzteileinheiten kann mit voller Leistung funktionieren, solange nicht mehr als 3 Netzteileinheiten ausfallen.

VORSICHTSHINWEIS: Im Modus "Keine Redundanz" werden nur drei Netzteile ohne Sicherung verwendet. Der Ausfall einer der drei verwendeten Netzteileinheiten kann dazu führen, dass die Stromversorgung der Server unterbrochen wird und Daten verloren gehen.

Stromeinsparung und Strombudgetänderungen

Der CMC kann Strom einsparen, wenn die vom Benutzer konfigurierte maximale Stromgrenze erreicht ist. Wenn der Strombedarf die benutzerdefinierte **Systemeingangstromobergrenze** überschreitet, verringert der CMC die Stromzufuhr zu den Servern mit niedriger Priorität, um Strom für Server und andere Module mit höherer Priorität im Gehäuse freizugeben.

Wenn alle oder mehrere Steckplätze im Gehäuse mit derselben Prioritätsstufe konfiguriert sind, verringert der CMC die Stromzufuhr zu den Servern in aufsteigender Steckplatznummernfolge. Beispiel: Wenn die Server in Steckplatz 1 und 2 dieselbe Prioritätsstufe haben, wird die Stromzufuhr für den Server in Steckplatz 1 verringert, bevor die Stromzufuhr für den Server in Steckplatz 2 verringert wird.

ANMERKUNG: Sie können jedem der Server im Gehäuse eine Prioritätsstufe zuweisen, indem Sie ihm eine Nummer von 1 bis einschließlich 9 geben. Die Standardprioritätsstufe für alle Server ist 1. Je niedriger die Zahl, desto höher die Prioritätsstufe.

Anleitungen zum Zuweisen von Serverprioritätsstufen finden Sie unter "RACADM verwenden".

Sie können Serverpriorität über die GUI zuweisen:

1. Klicken Sie in der Systemstruktur auf **Server**.
2. Wählen Sie auf der Registerkarte **Stromverwaltung** die Unterregisterkarte → **Priorität** aus.

Ausfall einer Netzteileinheit unter der Regeloption "Herabgesetzt" oder "Keine Redundanz"

Im Stromeinsparungsmodus verringert der CMC die Stromzufuhr zu Servern, wenn ein Ereignis mit der Folge unzureichender Stromversorgung auftritt, wie z. B. der Ausfall einer Netzteileinheit. Nachdem der Strom in Servern verringert wurde, berechnet der CMC den Strombedarf des Gehäuses neu. Falls die Stromanforderungen nach wie vor nicht erfüllt werden, schaltet der CMC u. U. auch Bladeserver mit niedriger Priorität aus.

Der Strom für Server mit höherer Priorität wird stufenweise wiederhergestellt, wobei der Strombedarf innerhalb des Strombudgets verbleibt.

ANMERKUNG: Informationen zum Festlegen der Redundanzregel finden Sie unter "Konfiguration von Strom-Budget und Redundanz".

Regel zur Zuschaltung neuer Server

Wenn ein neuer Server eingeschaltet wird, muss der CMC die Stromzufuhr zu Servern mit niedriger Priorität möglicherweise verringern, um den neuen Server mit mehr Strom zu versorgen, wenn das Hinzufügen des neuen Servers den verfügbaren Strom für das System überschreitet. Dies kann eintreten, wenn der Administrator ein Stromlimit für das Gehäuse konfiguriert hat, das unter dem liegt, was für eine vollständige Stromzuweisung für die Server nötig wäre, oder wenn unzureichend Strom für den Minimalstromverbrauch aller Server im Gehäuse verfügbar ist. Wenn durch die Reduktion des zugewiesenen Stroms der

Server mit niedriger Priorität nicht genügend Strom freigesetzt werden kann, kann es sein, dass der neue Server nicht hochfährt.

Der höchste erforderliche Strombedarf im Dauerbetrieb von Gehäuse und allen Servern, einschließlich des neuen Servers, entspricht bei Volllast dem Strombedarf im ungünstigsten Fall. Ist diese Strommenge vorhanden, wird keinem Server mehr Strom zugewiesen, als im schlechtesten Falle notwendig und somit kann der neue Server hochfahren.

Kann der Strombedarf für den schlechtesten Fall nicht geliefert werden, wird der Strom der niedriger priorisierten Server soweit reduziert, bis genügend Strom für den Bootvorgang des neuen Server freigesetzt wurde.

Tabelle 8-2 beschreibt die vom CMC ergriffenen Maßnahmen, wenn ein neuer Server im oben beschriebenen Szenario eingeschaltet wird.

Tabelle 8-2. CMC-Reaktion, beim Einschaltversuch eines Servers

Strom für den ungünstigsten Fall ist verfügbar	CMC-Reaktion	Server einschalten
Ja	Keine Stromeinsparung erforderlich	Zugelassen
Nein	Stromeinsparung ausführen: • Für neuen Server benötigter Strom ist verfügbar • Für neuen Server benötigter Strom ist nicht verfügbar	Zugelassen Nicht zugelassen

Wenn eine Netzteileinheit ausfällt, ergibt sich ein nicht-kritischer Funktionszustand und es wird ein Netzteileinheit-Ausfallereignis erzeugt. Die Entfernung einer Netzteileinheit führt zu einem Netzteileinheiten-Entfernungsereignis.

Wenn eines der beiden Ereignisse aufgrund von Stromzuteilungen zu Redundanzverlust führt, wird ein *Redundanzverlust*-Ereignis erzeugt.

Wenn nachfolgend die Stromkapazität oder die Benutzer-Stromkapazität größer ist als die Serverzuteilungen, werden Server geringere Leistung erbringen oder im schlechteren Fall herunterfahren. Beide Bedingungen wirken sich zuerst auf Server mit niedriger Priorität aus.

Tabelle 8-3 beschreibt die Firmware-Reaktion, wenn eine Netzteileinheit heruntergefahren oder entfernt wird, in Bezug auf verschiedene Redundanzkonfigurationen von Netzteileinheiten.

Tabelle 8-3. Auswirkung auf das Gehäuse bei Ausfall oder Entfernung einer Netzteileinheit

Konfiguration der Netzteileinheiten	Dynamische Netzteileinheit Zuschaltung	Firmware-Reaktion
Wechselstromredundanz	Deaktiviert	Der CMC alarmiert bei Verlust der Wechselstromredundanz.
Netzteilredundanz	Deaktiviert	Der CMC alarmiert bei Verlust der Netzteilredundanz.
Keine Redundanz	Deaktiviert	Verringerung der Stromversorgung für Server mit niedriger Priorität, falls nötig.
Wechselstromredundanz	Aktiviert	Der CMC alarmiert bei Verlust der Wechselstromredundanz. Netzteile im Stand-by-Modus (wenn vorhanden) werden eingeschaltet, um den Stromverlust in Folge eines Netzteilfehlers oder -ausfalls zu kompensieren.
Netzteilredundanz	Aktiviert	Der CMC alarmiert bei Verlust der Netzteilredundanz. Netzteile im Stand-by-Modus (wenn vorhanden) werden eingeschaltet, um den Stromverlust in Folge eines Netzteilfehlers oder -ausfalls zu kompensieren.
Keine Redundanz	Aktiviert	Verringerung der Stromversorgung für Server mit niedriger Priorität, falls nötig.

Entfernung von Netzteileinheiten unter der Regeloption "Herabgesetzt" oder "Keine Redundanz"

Der CMC kann beginnen, Strom zu sparen, wenn Sie eine Netzteileinheit entfernen oder ein Netzteileinheit-Stromkabel abziehen. Der CMC verringert die Stromzufuhr zu den Servern mit niedriger Priorität, bis der Stromverbrauch von den verbleibenden Netzteileinheiten im Gehäuse unterstützt wird. Wenn Sie mehr als eine Netzteileinheit entfernen, berechnet der CMC den Strombedarf neu, wenn die zweite Netzteileinheit entfernt wird, um die Reaktion der Firmware

zu bestimmen. Falls die Stromanforderungen nach wie vor nicht erfüllt werden, schaltet der CMC u. U. auch Bladeserver mit niedriger Priorität aus.

Grenzen

- Der CMC unterstützt ein automatisches Herunterfahren von Servern mit niedriger Priorität nicht, um einen Server mit höherer Priorität einzuschalten; ein Herunterfahren kann jedoch vom Benutzer initiiert und ausgeführt werden.
- Änderungen der Redundanzregel der Netzteileinheiten sind durch die Anzahl an Netzteileinheiten im Gehäuse begrenzt. Das M1000e-Gehäuse wird mit einer von zwei Konfigurationen geliefert: drei Netzteileinheiten oder sechs Netzteileinheiten. Sie können eine beliebige der drei in der Liste "Redundanzregeln" aufgeführten Redundanzkonfigurationseinstellungen von Netzteileinheiten auswählen.

Netzteil- und Redundanzregeländerungen im Systemereignisprotokoll.

Änderungen des Netzteilzustands und der Stromredundanzregeln werden als Ereignisse protokolliert. Ereignisse, die mit den Netzteilen zusammenhängen und Einträge im Systemereignisprotokoll (SEL) verursachen, sind das Hinzufügen und Entfernen von Netzteilen, Hinzufügen und Entfernen der Netzteileingangsleistung sowie Aussagen zur Netzteilausgangsleistung sowie deren Rücknahme. Tabelle 8-4 listet die SEL-Einträge auf, die mit Netzteiländerungen zusammenhängen.

Tabelle 8-4. SEL-Ereignisse für Netzteiländerungen

Netzteilereignis	Systemereignisprotokoll (SEL)-Eintrag
Einfügen	Vorhandenes Netzteil festgestellt
Entfernen	Vorhandenes Netzteil nicht mehr feststellbar
Wechselstromeingang	Netzteileingangsverlust nicht mehr feststellbar
Wechselstrom-Eingangsverlust	Netzteileingangsverlust festgestellt
Gleichstromausgabe hergestellt	Netzteilausfall nicht mehr feststellbar
Gleichstromausgabeverlust	Netzteilausfall festgestellt

Ereignisse, die mit Änderungen der Stromredundanzregeln zusammenhängen, die Einträge im SEL verursachen, sind Redundanzverlust und Redundanzwiederherstellung für das modulare Gehäuse, das entweder für eine Wechselstromredundanzregel oder eine Netzteilredundanzregel konfiguriert ist. Ein modulares Gehäuse mit der Stromregel Keine Redundanz erstellt einen SEL-Eintrag bei unzureichenden Ressourcen. Die Keine Redundanz-Stromregel wird protokolliert, wenn die Zahl der funktionierenden Netzteileinheiten im Gehäuse unter die minimale Anzahl von drei fällt. Ebenso wird ein SEL-Eintrag für ausreichende Ressourcen erstellt, wenn die Zahl der funktionierenden Netzteile für die Keine Redundanz-Stromregel wieder ausreichend ist. Tabelle 8-5 listet die SEL-Einträge auf, die mit Änderungen der Stromredundanzregeln zusammenhängen.

Tabelle 8-5. SEL-Ereignisse für Änderungen des Stromredundanzstatus

Stromregelereignis	Systemereignisprotokoll (SEL)-Eintrag
Redundanzverlust	ein Redundanzverlust wurde festgestellt
Redundanz wiederhergestellt	Redundanzwiederherstellung wurde festgestellt

Redundanzstatus und allgemeiner Stromzustand

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

ANMERKUNG: Der CMC führt keine Vorabprüfung dieser Bedingungen durch, wenn Sie die Redundanzregel auf oder von "Wechselstromredundanz" ändern. Das Konfigurieren der Redundanzregel kann demzufolge unverzüglich zu Redundanzverlust oder zu einer wiedererlangten Bedingung führen.

Konfiguration und Verwaltung der Energieeinstellungen

Sie können die webbasierten und RACADM-Benutzeroberflächen zum Verwalten und Konfigurieren der Stromsteuerung im CMC verwenden. Genauer gesagt können Sie:

- Anzeigen der Stromzuteilungen, des Verbrauchs und des Status des Gehäuses, der Server und der Netzteile

- Konfigurieren der Systemeingangstromobergrenze und der Redundanzregel für das Gehäuse
- Ausführen der Stromsteuerungsvorgänge (Einschalten, Ausschalten, System-Reset, Aus- und Einschalten) für das Gehäuse

Funktionszustand der Netzteileinheiten anzeigen

Die Seite Stromversorgung-Status zeigt den Status und die Messwerte der Netzteile an, die dem Gehäuse zugeordnet sind.

Webschnittstelle verwenden

Der Funktionszustand der Netzteile kann auf zwei Arten eingesehen werden: im Abschnitt Gehäuse-Grafiken auf der Seite Gehäusestatus oder auf der Seite Netzteilstatus. Die Seite Gehäuse-Grafiken bietet einen grafischen Überblick über alle Netzteileinheiten, die im Gehäuse installiert sind.

Um den Funktionszustand aller Netzteile mittels Gehäuse-Grafiken einzusehen:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Die Seite Gehäusezustand wird angezeigt. Die rechte Sektion der Gehäuse-Grafiken stellt die Rückansicht des Gehäuses dar und enthält den Funktionszustand aller Netzteile. Der Netzteile-Funktionszustand wird durch die Farbe des Netzteil-Symbols angegeben:
   - Grün – Netzteil wird erkannt, mit Strom versorgt und kommuniziert mit dem CMC; es gibt keine Anzeichen eines ungünstigen Zustands.
   - Gelb – Zeigt den Ausfall einer Netzteileinheit an. Einzelheiten zur Fehlerbedingung finden Sie im CMC-Protokoll.
   - Grau – Tritt während der Initialisierung von Netzteileinheiten auf und gewöhnlich auch beim Einschalten des Gehäuses und beim Einsetzen von Netzteileinheiten. Netzteil ist vorhanden und nicht eingeschaltet. Es kommuniziert nicht mit dem CMC und es gibt keine Anzeichen eines ungünstigen Zustands.
3. Bewegen Sie den Cursor über eine einzelne Netzteil-Grafik und ein entsprechender Texthinweis oder Bildschirmtipp wird angezeigt. Der Texthinweis liefert zusätzliche Informationen zu diesem Netzteil.
4. Die Netzteilgrafik ist mit der entsprechenden Seite der CMC-GUI verknüpft, um sofortige Navigation zur Seite Stromversorgung-Status für alle Netzteile zu ermöglichen.

Um den Funktionszustand der Netzteileinheiten einzusehen, verwenden Sie die Seite Netzteilstatus:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur Netzteile aus. Die Seite Stromversorgung-Status wird angezeigt.

Tabelle 8-6 und Tabelle 8-7 enthalten Erläuterungen zu den Informationen auf der Seite Stromversorgung-Status.

Tabelle 8-6. Informationen zum Funktionszustand von Netzteilen

Bauteil	Beschreibung		
Name	Zeigt den Namen des Netzteils an: PS-[n], wobei [n] die Nummer des Netzteils ist.		
Vorhanden	Gibt an, ob die Netzteileinheit Vorhanden oder Nicht vorhanden ist.		
Funktionszustand		OK	Zeigt an, dass die Netzteileinheit vorhanden ist und mit dem CMC kommuniziert. Im Falle eines Fehlers bei der Kommunikation zwischen dem CMC und dem Netzteil kann der CMC den Funktionsstatus der Netzteileinheit weder abrufen noch anzeigen.
		Warnung	Zeigt an, dass Warnungen ausgegeben wurden und Korrekturmaßnahmen ergriffen werden müssen. Wenn innerhalb des vom Administrator festgelegten Zeitraums keine Korrekturmaßnahmen vorgenommen werden, kann dies zu kritischen oder schwerwiegenden Stromausfällen führen, die sich wiederum auf die Integrität des Gehäuses auswirken können.
		Schwerwiegend	Gibt an, dass mindestens eine Fehlermeldung für das Netzteil erstellt wurde. Der Status "Schwerwiegend" zeigt einen Stromausfall im Gehäuse an, es müssen umgehend Korrekturmaßnahmen durchgeführt werden.
Stromstatus	Zeigt den Betriebszustand der Netzteile an (einer der Folgenden): Initialisierung, Online, Standby, Diagnosemodus, Fehler, Offline, **Unbekannt** oder Abwesend.		
Kapazität	Zeigt die Stromkapazität des Netzteils in Watt.		

Tabelle 8-7. Informationen zum Systemstrom-Funktionszustand

Bauteil	Beschreibung
Gesamter Stromfunktionszustand	Zeigt den Funktionszustand (**OK, Nicht-kritisch, Kritisch, Nicht behebbar, Andere, Unbekannt**) für die Stromverwaltung des gesamten Gehäuses an.
Systemstromstatus	Zeigt den Stromstatus (**Ein, Aus, Einschalten, Ausschalten**) des Gehäuses an.
Redundanz	Zeigt den Netzteilredundanzstatus an. Zu den Werten gehören: **Nein**: Netzteile sind nicht redundant. **Ja** - Volle Redundanz wirksam.

RACADM verwenden

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

```
racadm getpminfo
```

Weitere Information über getpminfo, einschließlich Ausgabedetails, finden Sie im *Chassis Management Controller Administrator-Referenzhandbuch* auf der Dell Support-Website unter **support.dell.com**.

Anzeige des Stromverbrauchsstatus

Der CMC zeigt den tatsächlichen Eingangsstromverbrauch für das gesamte System auf der Seite **Stromverbrauchsstatus** an.

Webschnittstelle verwenden

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, benötigen Sie Administratorrechte für die Gehäusesteuerung (**Chassis Control Administrator**).

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf Chassis (Gehäuse).
3. Klicken Sie auf die Registerkarte Stromverwaltung und dann die Unterregisterkarte Stromverbrauch. Die Seite Stromverbrauch wird angezeigt.

Tabelle 8-8 bis Tabelle 8-11 beschreiben die auf der Seite **Stromverbrauch** angezeigten Informationen.

ANMERKUNG: Der Stromredundanzstatus wird auch unter **Netzteile** in der Systemstruktur **System** auf der Registerkarte → **Status** angezeigt.

RACADM verwenden

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

```
racadm getpminfo
```

Tabelle 8-8. Stromstatistik in Echtzeit

Bauteil	Beschreibung
Systemeingangsleistung	Zeigt den aktuellen gesamten Netzstromverbrauch aller Module im Gehäuse an, gemessen von der Netzstromeingangsseite der Netzteileinheiten. Der Wert für die Systemeingangsleistung wird sowohl in Watt, als auch in BTU/h (British Thermal Unit per hour) angegeben.

Systemspitzenleistung	Zeigt den Maximalstromverbrauch auf Systemeingangsebene an, da dieser Wert als letzter gelöscht wurde. Über diese Eigenschaft können Sie den maximalen Stromverbrauch des Systems (Gehäuse und Module) verfolgen, der über einen bestimmten Zeitraum hinweg verzeichnet wurde. Klicken Sie auf die Unterregisterkarte Konfiguration auf der Seite Strombudgetstatus, um diesen Wert zu löschen. Der Wert für die Systemspitzenleistung wird sowohl in Watt, als auch in BTU/h (British Thermal Unit per hour) angegeben.
Startzeit der Systemspitzenleistung	Zeigt das Datum und die gespeicherte Zeit an, zu der der Wert des Stromverbrauchs bei Systemspitzen zuletzt gelöscht worden ist. Der Zeitstempel wird im Format hh:mm:ss MM/TT/JJJJ angezeigt, wobei hh die Stunden (0 - 24), mm die Minuten (00 - 60), ss die Sekunden (00 - 60), MM den Monat (1 - 12), TT die Tage (1 - 31) und JJJJ das Jahr angeben. Dieser Wert wird mittels Reset Spitzen-/Minimalstromwertstatistik und bei CMC-Reset oder -Ausfall zurückgesetzt.
Spitzenstromverbrauch des Systems, Zeitstempel	Zeigt Datum und Uhrzeit des in dem festgelegten Aufzeichnungszeitraum gemessenen Spitzenstromverbrauchs des Systems an. Der Zeitstempel wird im Format **hh:mm:ss MM/TT/JJJJ** angegeben, wobei **hh** die Stunden (0 - 24), **mm** die Minuten (00 - 60), **ss** die Sekunden (00 - 60), **MM** den Monat (1 - 12), **TT** den Tag (1 - 31) und **JJJJ** das Jahr bezeichnen.
Minimalsystemstrom	Zeigt den niedrigsten Wert des Netzstromverbrauchs des Systems (in Watt) über den Zeitraum an, seitdem der Benutzer diesen Wert das letzte Mal zurückgesetzt hat. Über diese Eigenschaft können Sie den minimalen Stromverbrauch des Systems (Gehäuse und Module) verfolgen, der über einen bestimmten Zeitraum hinweg aufgezeichnet wurde. Klicken Sie auf die Unterregisterkarte **Konfiguration** auf der Seite **Strombudgetstatus**, um diesen Wert zu löschen. Der Wert für die Systemminimalleistung wird sowohl in Watt, als auch in BTU/h (British Thermal Unit per hour) angegeben. Dieser Wert wird mittels Reset Spitzen-/Minimalstromwertstatistik und, bei CMC-Reset oder -Ausfall, zurückgesetzt.
Startzeit der Systemminimalleistung	Zeigt das Datum und die gespeicherte Zeit an, zu der der Wert des minimalen Systemstromverbrauchs zuletzt gelöscht worden ist. Der Zeitstempel wird im Format hh:mm:ss MM/TT/JJJJ angezeigt, wobei hh die Stunden (0 - 24), mm die Minuten (00 - 60), ss die Sekunden (00 - 60), MM den Monat (1 - 12), TT die Tage (1 - 31) und JJJJ das Jahr angeben. Dieser Wert wird mittels Reset Spitzen-/Minimalstromwertstatistik und, bei CMC-Reset oder -Ausfall, zurückgesetzt.
Minimaler Stromverbrauch des Systems, Zeitstempel	Zeigt Datum und Uhrzeit des in dem festgelegten Aufzeichnungszeitraum gemessenen minimalen Stromverbrauchs des Systems an. Das Format des Zeitstempels entspricht dem unter **Spitzenstromverbrauch des Systems, Zeitstempel** beschriebenen Format.
Systemleerlaufleistung	Zeigt den geschätzten Stromverbrauch des Gehäuses im Leerlauf an. Der Leerlaufzustand wird definiert als Zustand bei dem das Gehäuse eingeschaltet ist und alle Module Strom verbrauchen, während Sie sich im Leerlauf befinden. Dies ist ein geschätzter, kein gemessener Wert. Er errechnet sich aus der kumulativen, den Gehäuseinfrastrukturkomponenten zugewiesenen Strommenge (E/A-Module, Lüfter, iKVM, iDRAC-Controller und Frontblenden-LCDs) und dem Minimalbedarf aller Server, denen Strom zugewiesen ist und die sich im eingeschalteten Zustand befinden. Der Wert für die Systemleerlaufleistung wird sowohl in Watt, als auch in BTU/h (British Thermal Unit per hour) angegeben.
Systempotentialleistung	Zeigt den geschätzten Stromverbrauch des Gehäuses, wenn es mit maximalem Stromverbrauch betrieben wird. Der maximale Stromverbrauch wird als der Zustand definiert, bei dem das Gehäuse eingeschaltet ist und alle Module den größtmöglichen Stromverbrauch haben. Dies ist ein geschätzter Wert, abgeleitet vom historischen Gesamtstromverbrauch der Systemkonfiguration und nicht ein gemessener Wert. Er errechnet sich aus der kumulativen Strommenge, die den Gehäuseinfrastrukturkomponenten (E/A-Module, Lüfter, iKVM, iDRAC-Controller und Frontblenden-LCDs) zugeteilt ist, und dem Maximalbedarf aller eingeschalteten Server, denen Strom zugeteilt ist. Der Wert für die Systempotentialleistung wird sowohl in Watt, als auch in BTU/h (British Thermal Unit per hour) angegeben.
Auslesen des Systemeingangsstroms	Zeigt die gesamte Eingangsstromaufnahme des Gehäuses an, basierend auf der Summe der Eingangsstromaufnahme jedes einzelnen Netzteilmoduls im Gehäuse. Der Wert für die Systemeingangsstromaufnahme wird in Ampere angezeigt.

Tabelle 8-9. Status der Echtzeit-Energiestatistik

Bauteil	Beschreibung
Systemenergieverbrauch	Zeigt den aktuellen gesamten Netzstromverbrauch aller Module im Gehäuse an, gemessen von der Netzstromeingangsseite der Netzteileinheiten. Der kumulative Wert wird in kWh angegeben.
Startzeit der Systemenergiedaten	Zeigt das Datum und die gespeicherte Zeit an, zu der der Wert für den Systemenergieverbrauch zuletzt gelöscht wurde und der neue Messzyklus begann. Der Zeitstempel wird im Format hh:mm:ss MM/TT/JJJJ angezeigt, wobei hh für die Stunden (0-24) steht, mm für die Minuten (00-60), ss die Sekunden bezeichnet (00-60), MM den Monat angibt (1-12), DD für die Tage steht (1-31) und JJJJ das Jahr angibt. Dieser Wert wird mittels Reset Energiestatistik zurückgesetzt und bleibt bei CMC-Reset oder -Ausfall erhalten.
Systemenergieverbrauch, Zeitstempel	Zeigt das Datum und die Zeit an, zu der der Systemenergieverbrauch für die Anzeige berechnet worden ist. Der Zeitstempel wird im Format hh:mm:ss MM/TT/JJJJ angezeigt, wobei hh für die Stunden (0-24) steht, mm für die Minuten (00-60), ss die Sekunden bezeichnet (00-60), MM den Monat angibt (1-12), DD für die Tage steht (1-31) und JJJJ das Jahr angibt.

Tabelle 8-10. Systemstromstatus

Bauteil	Beschreibung
Gesamter Stromfunktionszustand	Zeigt den Funktionszustand (**OK**, **Nicht-kritisch**, **Kritisch**, **Nicht behebbar**, **Andere**, **Unbekannt**) für das Stromsubsystem des Gehäuses an.
Systemstromstatus	Zeigt den Stromstatus (**Ein**, **Aus**, **Netzstrom ein**, **Ausschalten**) des Gehäuses an.
Redundanz	Zeigt den Redundanzstatus an. Gültige Werte sind: **Nein** - Netzteileinheiten sind nicht redundant **Ja** - Volle Redundanz wirksam.

Tabelle 8-11. Servermodule

Bauteil	Beschreibung
Steckplatz	Zeigt die Position des Servermoduls an. Die **Steckplatznummer** ist eine sequenzielle Nummer (1-16), die das Servermodul nach seiner Position im Gehäuse identifiziert.
Name	Zeigt den Servernamen an. Der Servername kann vom Benutzer neu definiert werden.
Vorhanden	Zeigt an, ob der Server im Steckplatz vorhanden ist (Ja oder Nein). Wenn dieses Feld die Erweiterung von # (wobei das Zeichen # für 1 - 8 steht) anzeigt, dann bezeichnet die darauf folgende Nummer den Hauptsteckplatz eines Multi-Steckplatz-Servers.
Tatsächlich (Wechselstrom)	Echtzeit-Messung des tatsächlichen Stromverbrauchs des Servers. Die Messung ist in Watt angegeben.
Gesamtstrom-Startzeit	Echtzeitmessung des Gesamtstroms, den der Server seit der letzten Zeitanzeige im Feld Zeit starten verbraucht hat. Die Messung wird in Kilowattstunden (kWh) angegeben.
Spitzenverbrauch-Zeitstempel	Zeigt den Spitzenstromverbrauch des Servers an, der zu einem bestimmten Zeitpunkt aufgetreten ist. Die Zeit, zu der der Spitzenstromverbrauch aufgetreten ist, wird im Zeitstempel-Feld angegeben. Die Messung wird in Watt angezeigt.

Strombudgetstatus anzeigen

Der CMC enthält auf der Seite **Strombudgetstatus** Übersichten zum Stromstatus der Stromsubsysteme.

Webschnittstelle verwenden

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, benötigen Sie Administratorrechte für die Gehäusesteuerung (**Chassis Control Administrator**).

1. Melden Sie sich bei der CMC-Webschnittstelle an**.**
2. Klicken Sie in der Systemstruktur auf Chassis (Gehäuse).
3. Klicken Sie auf die Registerkarte Power Management (Stromverwaltung). Die Seite Strombudgetstatus wird angezeigt.

Tabelle 8-12 bis Tabelle 8-15 beschreiben die auf der Seite **Strombudgetstatus** angezeigten Informationen.

Unter "Konfiguration von Strom-Budget und Redundanz" finden Sie Informationen zur Konfiguration der Einstellungen für diese Daten.

RACADM verwenden

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

```
racadm getpbinfo
```

Weitere Informationen über getpbinfo einschließlich Ausgabedetails finden Sie im Abschnitt getpbinfo des Chassis Management Controller Administrator-Referenzhandbuchs.

Tabelle 8-12. Regelkonfiguration des Systemstroms

Bauteil	Beschreibung
Systemeingangstromobergrenze	Zeigt die benutzerdefinierte Grenze für den maximalen Stromverbrauch des gesamten Systems an (Gehäuse, CMC, Server, E/A-Module, Netzteileinheiten, iKVM und Lüfter). Der CMC wird diese Grenze über reduzierte Serverstromzuweisungen oder durch Abschalten niedrig priorisierter Servermodule, einhalten. Der Wert für die Systemeingangstromobergrenze wird in Watt, BTU/h und Prozent angezeigt. Übersteigt der Stromverbrauch des Gehäuses die Systemeingangstromobergrenze, wird die Leistung der niedrig priorisierten Server soweit reduziert, dass der Gesamtstromverbrauch unter die Grenze fällt. In Fällen, in denen die Server auf die gleiche Priorität gesetzt sind, basiert die Auswahl der Server zur Stromreduktion oder Abschaltung auf der Reihenfolge der Steckplatznummern. So wird beispielsweise der Server in Steckplatz 1 als Erster, der Server in Slot 16 als Letzter, ausgewählt.

Redundanzregel	Zeigt die aktuelle Redundanzkonfiguration an: Wechselstromredundanz, Netzteilredundanz oder Keine Redundanz. **Wechselstromredundanz** – die Leistungsaufnahme wird entsprechend der Last über alle Netzteileinheiten verteilt. Die Hälfte der Netzteileinheiten sollte mit einem Wechselstromkreis verkabelt sein und die andere Hälfte mit einem anderen Stromkreis. Wenn das System im Modus Wechselstromredundanz optimal läuft, wird die Leistung auf alle aktiven Netzteile verteilt. In dem Fall, dass ein Stromkreis ausfällt, laufen die Netzteileinheiten des funktionierenden Wechselstromkreises mit 100%iger Kapazität. **Netzteilredundanz** - Die Netzteileinheit mit der höchsten Kapazität im Gehäuse verbleibt als Reserve, sodass ein Ausfall einer der Netzteileinheiten nicht dazu führt, dass die Servermodule oder das Gehäuse herunterfahren. **Netzteilredundanz** verwendet nicht alle 6 Netzteileinheiten. Es werden maximal 4 Netzteileinheiten verwendet, und die übrigen Netzteileinheiten können in den Standby-Modus versetzt werden, falls dynamische Zuschaltung von Netzteileinheiten (DPSE) aktiviert ist. **Keine Redundanz** - Der Strom von allen drei Netzteilen an einem Wechselstromkreis (Netz) wird zur Stromversorgung des gesamten Gehäuses, einschließlich Gehäuse, Server, E/A-Modulen, iKVM und CMC verwendet. **VORSICHTSHINWEIS: Der Modus Keine Redundanz verwendet nur drei Netzteile gleichzeitig, ohne ein Backup. Der Ausfall eines der drei verwendeten Netzteile kann dazu führen, dass die Servermodule nicht mit Strom versorgt werden und Daten verloren gehen.**
Dynamische Netzteilzuschaltung	Zeigt an, ob die **Dynamische Zuschaltung von Netzteilen** aktiviert oder deaktiviert ist. Wenn diese Funktion aktiviert ist, kann der CMC ungenügend genutzte Netzteileinheiten anhand der festgelegten Redundanzregel und der Stromanforderungen des Systems in den Standby-Modus setzen. Werden ungenügend genutzte Netzteileinheiten in den Standby-Modus gesetzt, erhöht sich die Nutzung und der Wirkungsgrad der angeschlossenen Netzteileinheiten, wodurch Strom eingespart wird.

Tabelle 8-13. Strombudgetierung

Bauteil	Beschreibung
Maximale Eingangsstromkapazität des Systems	Der maximale Eingangsstrom den die verfügbaren Netzteile dem System zur Verfügung stellen können (in Watt).
Eingangsleistungsredundanzreserve	Zeigt die redundante Strommenge (in Watt) in Reserve an, die im Falle eines Ausfalls des Wechselstromkreises oder der Netzteileinheit zur Verfügung steht. Wenn das Gehäuse so konfiguriert ist, dass es im Modus Wechselstromredundanz ausgeführt wird, entspricht die Eingangsleistungsredundanzreserve der Reservestrommenge, die bei einem Ausfall eines Wechselstromkreises zur Verfügung steht. Wenn das Gehäuse so konfiguriert ist, dass es im Modus Netzteilredundanz betrieben wird, entspricht die Angabe unter Eingangsleistungsredundanzreserve der Reservestrommenge, die im Falle eines Ausfalls einer bestimmten Netzteileinheit zur Verfügung steht.
Server-zugewiesene Eingangsleistung	Zeigt (in Watt) die kumulative Eingangsleistung, die der CMC auf der Basis der Konfiguration den Servern zuweist.
Gehäuseinfrastruktur-zugewiesene Eingangsleistung	Zeigt (in Watt) die kumulative Eingangsleistung, die der CMC der Gehäuseinfrastruktur (Lüfter, E/A-Module, iKVM, CMC, Stand-by-CMC und iDRAC auf den Servern) zuweist.
Gesamter, für die Zuteilung verfügbarer, Eingangsstrom	Zeigt das gesamte Strombudget des Gehäuses in Watt an, das für den Gehäusebetrieb zur Verfügung steht.
Stand-by-Eingangsstromkapazität	Zeigt die Menge des Stand-by-Eingangsstroms (in Watt), der im Falle eines Netzteilfehlers oder der Entfernung eines Netzteils aus dem System, zur Verfügung steht. Dieses Feld zeigt Werte, wenn das System vier oder mehr Netzteile besitzt und die dynamische Netzteilzuschaltung aktiviert ist. **ANMERKUNG:** Es ist möglich eine Netzteileinheit im Standby-Modus zu sehen, ohne, dass sie zum Wert der Stand-by- Eingangsstromkapazität beiträgt. In diesem Fall trägt die Stromleistung dieser Netzteileinheit zum Gesamten, für die Zuteilung verfügbaren, Eingangsstrom bei.

Tabelle 8-14. Servermodule

Bauteil	Beschreibung
Steckplatz	Zeigt die Position des Servermoduls an. Die **Steckplatznummer** ist eine sequenzielle Nummer (1-16), die das Servermodul nach seiner Position im Gehäuse identifiziert.
Name	Zeigt den Servernamen an. Der Servername kann vom Benutzer neu definiert werden.
Typ	Zeigt den Typ des Servers an.
Priorität	Zeigt die dem Serversteckplatz im Gehäuse zur Strombudgetierung zugewiesene Prioritätsstufe an. Der CMC verwendet diesen Wert in seinen Berechnungen, wenn Strom basierend auf benutzerdefinierten Stromgrenzen oder auf Netzteil- oder Stromnetzausfällen reduziert oder neu zugeteilt werden muss. **Prioritätsstufen**: 1 (höchste) bis 9 (niedrigste) Standardeinstellung: **1**

	ANMERKUNG: Die Prioritätsstufe des Serversteckplatzes wird dem Serversteckplatz zugewiesen, nicht dem im Steckplatz eingesetzten Server. Wenn Sie einen Server in einen anderen Steckplatz im Gehäuse oder in ein anderes Gehäuse einsetzen, bestimmt die zuvor dem neuen Steckplatz zugewiesene Priorität die Priorität des neu eingesetzten Servers.
Stromzustand	Zeigt den Stromzustand des Servers: • k.A.: Der CMC hat den Stromzustand des Servers nicht bestimmt. • AUS: Sowohl Gehäuse, als auch Server sind ausgeschaltet. • EIN: Sowohl Gehäuse, als auch Server sind eingeschaltet. • Einschalten: Vorrübergehender Zustand zwischen AUS und EIN. Ist der Einschaltvorgang abgeschlossen ändert sich der Stromzustand zu EIN. • Abschalten: Vorrübergehender Zustand zwischen EIN und AUS. Ist der Abschaltvorgang abgeschlossen ändert sich der Stromzustand zu AUS.
Budgetzuweisung - Tatsächlich	Zeigt die Strombudget-Zuweisung für die Servermodule an. • Tatsächlich: aktuelle Strombudgetzuweisung für jeden Server.

Tabelle 8-15. Systemnetzteile

Bauteil	Beschreibung
Name	Zeigt den Namen der Netzteileinheit im Format NT-*n* an, wobei *n* die Nummer der Netzteileinheit ist.
Stromzustand	Zeigt den Stromzustand des Netzteils an **- Initialisieren, Online**, **Standby**, **Diagnose**, **Fehlerhaft**, **Unbekannt** oder **Nicht vorhanden** (fehlend).
Eingangsspannung	Zeigt die derzeitige Eingangsspannung des Netzteils an.
Eingangsstrom	Zeigt den derzeitigen Eingangsstrom des Netzteils an.
Ausgangsnennleistung	Zeigt die maximale Ausgangsnennleistung des Netzteils an.

Konfiguration von Strom-Budget und Redundanz

Der Stromverwaltungsdienst des CMC optimiert den Stromverbrauch für das gesamte Gehäuse (Gehäuse, Server, E/A-Module, iKVM, CMC und Netzteileinheiten) und teilt den unterschiedlichen Modulen je nach Bedarf Strom neu zu.

Webschnittstelle verwenden

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, benötigen Sie Administratorrechte für die Gehäusesteuerung (**Chassis Control Administrator**).

1. **Melden Sie sich bei der CMC-Webschnittstelle an.**
2. Klicken Sie in der Systemstruktur auf Chassis (Gehäuse).
3. Klicken Sie auf der Registerkarte Stromverwaltung auf die Unterregisterkarte → Konfiguration. Die Seite Budget/Redundancy Configuration (Budget/Redundanz-Konfiguration) wird angezeigt.
4. Legen Sie einige oder alle in Tabelle 8-16 beschriebenen Eigenschaften entsprechend Ihrer Bedürfnisse fest.
5. Klicken Sie auf Apply (Übernehmen), um die Änderungen zu speichern.

Um den Inhalt der Seite Budget-/Redundanzkonfiguration zu aktualisieren, klicken Sie auf Aktualisieren. Um den Inhalt auszudrucken, klicken Sie auf Drucken.

Tabelle 8-16. Konfigurierbare Strombudget- / Redundanzeigenschaften

Bauteil	Beschreibung
Systemeingangstromobergrenze	Die Systemeingangstromobergrenze ist der maximale Wechselstrom, den das System den Servern und der Gehäuseinfrastruktur zuweisen darf. Sie kann vom Benutzer auf jeden Wert gesetzt werden, der den Minimalstrombedarf der eingeschalteten Server und Gehäuseinfrastruktur übersteigt; der Versuch einen Wert zu konfigurieren, der unter dem Minimalstrombedarf der Server und der Gehäuseinfrastruktur liegt, wird scheitern. Den Wert für den der Server- und Gehäuseinfrastruktur zugewiesenen Strom finden Sie über die Benutzerschnittstelle auf der Statusseite Gehäuse → Stromverwaltung → Strombudget im Abschnitt Strombudgetierung oder über den CLI RACADM Hilfsbefehl (`racadm getpbinfo`).

	Benutzer können einen oder mehrere Server ausschalten, um die aktuelle Stromzuweisung zu reduzieren und erneut versuchen, einen niedrigeren Wert für die Systemeingangstromobergrenze (wenn gewünscht) zu setzen, oder die Obergrenze einfach vor dem Einschalten der Server festlegen. Um diese Einstellung zu ändern, kann ein Wert in jeder Einheit eingegeben werden. Die Schnittstelle sorgt dafür, dass das Einheitenfeld, das als letztes geändert wurde, der übermittelte Wert sein wird, wenn diese Änderungen angewandt werden. **ANMERKUNG:** Das Hilfsprogramm Datacenter Capacity Planner (DCCP) unter www.dell.com/calc enthält Informationen zur Kapazitätsplanung. **ANMERKUNG:** Werden Werte, die in Watt angegeben sind, geändert, wird der übermittelte Wert exakt das widerspiegeln, was angewandt wird. Werden die Änderungen jedoch entweder in BTU/h oder in Prozent übermittelt, kann der übermittelte Wert nicht exakt widerspiegeln, was wirklich angewandt wird. Das liegt daran, dass diese Werte in Watt umgerechnet und dann angewandt werden; bei einer solchen Konvertierung können Rundungsfehler auftreten.
Redundanzregel	Diese Option ermöglicht das Auswählen folgender Varianten: • Keine Redundanz - Der Strom von allen drei Netzteilen an einem Wechselstromkreis (Netz) wird zur Stromversorgung des gesamten Gehäuses, einschließlich Gehäuse, Server, E/A-Modulen, iKVM und CMC, verwendet. **ANMERKUNG:** Der Modus Keine Redundanz verwendet nur drei Netzteileinheiten gleichzeitig. Wenn 3 Netzteileinheiten installiert sind, steht kein Backup zur Verfügung. Der Ausfall eines der drei verwendeten Netzteile kann dazu führen, dass den Servern Strom fehlt und/oder sie Daten verlieren. Wenn mehr als drei Netzteileinheiten vorhanden sind, dann können die zusätzlichen Netzteileinheiten zur Verbesserung der Energieeffizienz in den Standby-Modus versetzt werden, falls dynamische Zuschaltung von Netzteileinheiten (DPSE) aktiviert ist. • Netzteilredundanz: Die Kapazität des nennwerthöchsten Netzteils im Gehäuse wird als Reserve bewahrt, um so sicherzustellen, dass ein Ausfall irgendeines Netzteils nicht zum Herunterfahren der Servermodule oder des Gehäuses führt (aktive Reserve). Der Modus Netzteilredundanz unterstützt nicht alle sechs Netzteile, sondern nur eine Maximalzahl von vier und ein Minimum von zwei Netzteilen. Zusätzliche Netzteileinheiten können zur Verbesserung der Energieeffizienz in Standby-Modus versetzt werden, falls dynamische Zuschaltung von Netzteileinheiten (DPSE) aktiviert ist. Der Modus Netzteilredundanz verhindert, dass Servermodule hochgefahren werden, wenn der Stromverbrauch des Gehäuses die Nennleistung übersteigt. Ein Ausfall von zwei Netzteilen in diesem Modus kann dazu führen, dass einige oder alle Servermodule im Gehäuse herunterfahren. Die Servermodulleistung wird in diesem Modus nicht herabgesetzt. • Wechselstromredundanz: Dieser Modus teilt die 6 Netzteileinheiten in zwei Stromkreise auf (die Netzteileinheiten 1 - 3 bilden Stromkreis 1 und die Netzteileinheiten 4 - 6 bilden Stromkreis 2). In dieser Konfiguration sind alle 6 Netzteileinheiten online. Ausfall einer Netzteileinheit oder Verlust von Wechselstrom zu einem Stromkreis führt zum Status von "Redundanzverlust".
Aktivieren der Dynamische Netzteilzuschaltung	Aktiviert (wenn markiert) die Dynamische Stromverwaltung Im Modus Dynamische Netzteilzuschaltung werden die Netzteile auf Basis des Stromverbrauch eingeschaltet (online) oder ausgeschaltet (Standby), um den Energieverbrauch des gesamten Gehäuses zu optimieren. Sie haben, als Beispiel, ein Strombudget von 5000 Watt, Ihre Redundanzregeln sind auf Wechselstromredundanz konfiguriert und Sie haben sechs Netzteileinheiten im Einsatz. Der CMC legt fest, dass vier Netzteileinheiten die Wechselstromredundanz leisten und die anderen beiden im Stand-by-Modus bleiben. Wenn beispielsweise zusätzliche 2000 W Strom für neu installierte Server benötigt wird, oder wenn die Energieeffizienz der bestehenden Systemkonfiguration verbessert werden muss, dann werden die zwei Standby-Netzteileinheiten in Betrieb genommen.
Netzschalter des Gehäuses deaktivieren	Deaktiviert (wenn markiert) den Gehäusenetzschalter. Wenn das Kontrollkästchen ausgewählt ist und Sie versuchen, den Stromstatus des Gehäuses über den Gehäusenetzschalter zu ändern, wird die Maßnahme ignoriert.

RACADM verwenden

So aktivieren Sie die Redundanz und legen die Redundanzregel fest:

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, benötigen Sie Administratorrechte für die Gehäusesteuerung (**Chassis Control Administrator**).

1. Öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC und melden Sie sich an.
2. Legen Sie die Eigenschaften wie erforderlich fest:
   - Um eine Redundanzregel auszuwählen, geben Sie Folgendes ein:

     ```
     racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy <Wert>
     ```

     wobei der <*Wert*> 0 (Keine Redundanz), 1 (Wechselstromredundanz) oder 2 (Netzteilredundanz) sein kann. Die Standardeinstellung ist 0.

     Zum Beispiel legt der folgende Befehl:

```
racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy 1
```

die Redundanzregel auf 1 fest.

- Um die dynamische Zuschaltung von Netzteileinheiten zu aktivieren oder deaktivieren, geben Sie Folgendes ein:

```
racadm config -g cfgChassisPower -o cfgChassisDynamicPSUEngagementEnable <Wert>
```

wobei der <*Wert*> 0 (deaktivieren) oder 1 (aktivieren) sein kann. Die Standardeinstellung ist 1.

Zum Beispiel legt der folgende Befehl:

```
racadm config -g cfgChassisPower -o cfgChassisDynamicPSUEngagementEnable 0
```

die dynamische Zuschaltung von Netzteileinheiten.

Weitere Informationen über RACADM-Befehle für Gehäusestrom finden Sie in den Abschnitten config, getconfig, getpbinfo und cfgChassisPower im *CMC Administrator-Referenzhandbuch*.

Vergabe von Prioritätsstufen an Server

Über Server-Prioritätsstufen wird festgelegt, von welchen Servern das CMC-Modul bei zusätzlichem Strombedarf Strom bezieht.

ANMERKUNG: Die Priorität, die Sie einem Server zuweisen, ist nicht an den Server selbst sondern an den Serversteckplatz gekoppelt. Wenn der Server an einen anderen Steckplatz verlegt wird, müssen Sie die Priorität für den neuen Steckplatz erneut konfigurieren.

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, müssen Sie die Berechtigung als **Gehäusekonfigurations-Administrator** besitzen.

Webschnittstelle verwenden

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf Servers (Server). Die Seite Servers Status (Serverstatus) wird angezeigt.
3. Klicken Sie auf die Registerkarte Power Management (Stromverwaltung). Die Seite Server Priority (Serverpriorität) wird angezeigt. Hier sind alle Server in Ihrem Gehäuse aufgeführt.
4. Wählen Sie für einen, mehrere oder alle Server eine Prioritätsstufe von 1 bis 9 aus, wobei 1 die höchste Prioritätsstufe ist. Der Standardwert ist 1. Sie können mehreren Servern dieselbe Prioritätsstufe zuweisen.
5. Klicken Sie auf Apply (Übernehmen), um die Änderungen zu speichern.

RACADM verwenden

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

```
racadm config -g cfgServerInfo -o cfgServer Priority - i <Steckplatznummer> <Prioritätsstufe>
```

wobei sich <*Steckplatznummer*> (1-16) auf die Position des Servers bezieht und der Wert für die <*Prioritätsstufe*> zwischen 1 und 9 liegt.

Zum Beispiel legt der folgende Befehl:

```
racadm config -g cfgServerInfo -o cfgServerPriority - i 5 1
```

legt die Prioritätsstufe 1 für den Server in Steckplatz 5 fest.

Strombudget einrichten

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, benötigen Sie Administratorrechte für die Gehäusesteuerung (**Chassis Control Administrator**).

Webschnittstelle verwenden

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf Chassis (Gehäuse). Die Seite Komponenten-Funktionszustand wird angezeigt.
3. Klicken Sie auf die Registerkarte Power Management (Stromverwaltung). Die Seite Power Budget Status (Strombudgetstatus) wird angezeigt.
4. Klicken Sie auf die Unterregisterkarte Configuration. Die Seite Budget/Redundancy Configuration (Budget/ Redundanz-Konfiguration) wird angezeigt.
5. Geben Sie einen Budgetwert von bis zu 7928 Watt in das Textfeld Systemeingangstromobergrenze ein.

   ANMERKUNG: Das Strombudget ist auf maximal drei von insgesamt sechs Netzteilen beschränkt. Wen versucht wird, einen Strombudgetwert festzulegen, der die Stromleistungskapazität des Gehäuses überschreitet, zeigt das CMC-Modul eine Fehlermeldung an.

   ANMERKUNG: Werden Werte, die in Watt angegeben sind, geändert, wird der übermittelte Wert exakt das widerspiegeln, was angewandt wird. Werden die Änderungen jedoch entweder in BTU/h oder in Prozent übermittelt, kann der übermittelte Wert nicht exakt widerspiegeln, was wirklich angewandt wird. Das liegt daran, dass diese Werte in Watt umgerechnet und dann angewandt werden; bei einer solchen Konvertierung können Rundungsfehler auftreten.

6. Klicken Sie auf Apply (Übernehmen), um die Änderungen zu speichern.

RACADM verwenden

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

```
racadm config -g cfgChassisPower -o cfgChassisPowerCap <Wert>
```

wobei <Wert> eine Zahl zwischen 2715 und 7928 ist und die maximale Stromgrenze in Watt angibt. Die Standardeinstellung ist 7928.

Zum Beispiel legt der folgende Befehl:

```
racadm config -g cfgChassisPower -o cfgChassisPowerCap 5400
```

das maximale Strombudget mit 5400 Watt fest.

ANMERKUNG: Das Strombudget ist auf maximal drei von insgesamt sechs Netzteilen beschränkt. Wenn versucht wird, einen Strombudgetwert festzulegen, der die Stromleistungskapazität des Gehäuses überschreitet, zeigt das CMC-Modul eine Fehlermeldung an.

Herabsetzen des Serverstroms zur Einhaltung des Strombudgets

Der CMC reduziert Stromzuteilungen von Servern mit niedriger Priorität, wenn zusätzlicher Strom benötigt wird, um den Systemstromverbrauch unterhalb der benutzerdefinierten **Systemeingangstromobergrenze** zu halten. Wenn beispielsweise ein neuer Server zugeschaltet wird, kann der CMC die Stromzufuhr zu Servern mit niedriger Priorität verringern, um den neuen Server mit mehr Strom zu versorgen. Wenn die Strommenge nach der Verringerung der Stromzuteilung zu Servern mit niedriger Priorität nach wie vor nicht ausreicht, drosselt der CMC die Server mit höherer Priorität bis ausreichend Strom freigegeben ist, um den neuen Server mit Strom zu versorgen.

Der CMC reduziert Server-Stromzuteilung in zwei Fällen:

- Der Gesamtstromverbrauch übersteigt konfigurierbare **Systemeingangstromobergrenze** (siehe "Strombudget einrichten").
- Ein Stromausfall tritt in einer nicht-redundanten Konfiguration auf

Informationen zum Zuweisen von Prioritäten zu Servern finden Sie unter "Durchführen von Energieverwaltungsmaßnahmen am Gehäuse".

Durchführen von Energieverwaltungsmaßnahmen am Gehäuse

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, benötigen Sie Administratorrechte für die Gehäusesteuerung (**Chassis Control Administrator**).

ANMERKUNG: Stromsteuerungsvorgänge wirken sich auf das gesamte Gehäuse aus. Informationen über Stromsteuerungsmaßnahmen an einem E/A-Modul finden Sie unter "Stromsteuerungsvorgänge für ein E/A-Modul ausführen". Informationen über Stromsteuerungsmaßnahmen an einem Server finden Sie unter "Durchführen von Energieverwaltungsmaßnahmen an einem Server".

Mit dem CMC können Sie im Remote-Zugriff verschiedene Stromverwaltungsmaßnahmen auf dem gesamten Gehäuse (Gehäuse, Server, E/A-Module, iKVM und Netzteileinheiten) ausführen, wie z. B. ordnungsgemäßes Herunterfahren.

Webschnittstelle verwenden

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf Chassis (Gehäuse).
3. Klicken Sie auf die Registerkarte Power Management (Stromverwaltung). Die Seite Power Budget Status (Strombudgetstatus) wird angezeigt.
4. Klicken Sie auf die Unterregisterkarte Control (Steuerung) Die Seite Power Management (Stromverwaltung) wird angezeigt.
5. Wählen Sie einen der folgenden **Stromsteuerungsvorgänge** aus, indem Sie auf die Optionsschaltfläche klicken:

   - **System einschalten** – Schaltet den Systemstrom ein (entspricht dem Drücken des Netzschalters, wenn der Systemstrom ausgeschaltet ist). Diese Option ist deaktiviert, wenn das Gehäuse bereits eingeschaltet ist.

   ANMERKUNG: Der Vorgang schaltet das Gehäuse und andere Untersysteme ein (iDRAC auf den Servern, EAMs und iKVM). Die Server werden nicht eingeschaltet.

   - **System ausschalten** - Schaltet den Systemstrom aus. Diese Option ist deaktiviert, wenn das Gehäuse bereits AUSgeschaltet ist.

   ANMERKUNG: Der Vorgang schaltet den Systemstrom ab (Gehäuse, Server, EAMs, iKVM und Netzteile). Der CMC bleibt eingeschaltet, befindet sich aber im Standby-Modus; ein Netzteil und Lüfter liefern Kühlung für den CMC in diesem Zustand. Das Netzteil wird auch den Lüfter, der auf niedriger Drehzahl läuft, mit Strom versorgen.

   - System aus- und einschalten (Hardwareneustart) - Schaltet den Server aus und startet ihn daraufhin neu. Diese Option ist deaktiviert, wenn das Gehäuse bereits AUSgeschaltet ist.

   ANMERKUNG: Dieser Vorgang schaltet des gesamte System ab und bootet dann neu (Gehäuse, dauerhaft eingeschaltete Server, EAMs, iKVM und Netzteile).

   - **CMC zurücksetzen** - Setzt den CMC zurück, ohne diesen auszuschalten (Softwareneustart). (Diese Option ist deaktiviert, wenn der CMC bereits ausgeschaltet ist.)

   ANMERKUNG: Diese Maßnahme setzt nur den CMC zurück. Es sind keine anderen Komponenten betroffen.

   - **Nicht-ordnungsgemäßes Herunterfahren** - Diese Handlung erzwingt ein nicht-ordnungsgemäßes Herunterfahren des gesamten Systems (Gehäuse, EAMs, iKVM und Netzteile). Es wird nicht versucht, das Betriebssystem ordnungsgemäß herunterzufahren, bevor die Server stromlos geschaltet werden.

- Klicken Sie auf **Anwenden**. Daraufhin werden Sie über ein Dialogfeld zur Bestätigung des Vorgangs aufgefordert.
- Klicken Sie auf OK, um die Stromverwaltungsmaßnahme auszuführen (z. B. das System zurücksetzen).

RACADM verwenden

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

```
racadm chassisaction -m chassis <Maßnahme>
```

wobei *<Maßnahme>* powerup, powerdown, powercycle, nongraceshutdown oder reset ist.

Stromsteuerungsvorgänge für ein E/A-Modul ausführen

Sie können im Remote-Zugriff ein einzelnes E/A-Modul zurücksetzen oder ein- und ausschalten.

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, benötigen Sie Administratorrechte für die Gehäusesteuerung (**Chassis Control Administrator**).

Webschnittstelle verwenden

1. **Melden Sie sich bei der CMC-Webschnittstelle an.**
2. Wählen Sie die Option I/O Modules (E/A-Module). Die Seite I/O Modules Status (E/A-Modulstatus) wird angezeigt.
3. Klicken Sie auf die Registerkarte Power Management (Stromverwaltung). Die Seite Energiesteuerung wird angezeigt.
4. Wählen Sie den Vorgang, den Sie ausführen möchten (Zurücksetzen oder Aus- und einschalten), aus dem Drop-Down-Menü neben dem E/A- Modul in der Liste aus.
5. Klicken Sie auf **Anwenden**. Daraufhin werden Sie über ein Dialogfeld zur Bestätigung des Vorgangs aufgefordert.
6. Klicken Sie auf OK, um die Stromverwaltungsmaßnahme auszuführen (z. B. um zu veranlassen, dass das E/A-Modul aus- und eingeschaltet wird).

RACADM verwenden

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

```
racadm chassisaction -m switch-<n> <Maßnahme>
```

wobei *<n>* als Ziffern 1 - 6 das EAM angeben (A1, A2, B1, B2, C1, V2) und *<Maßnahme>* den Vorgang anzeigt, den Sie ausführen möchten: powercycle oder reset.

Durchführen von Energieverwaltungsmaßnahmen an einem Server

ANMERKUNG: Um Stromverwaltungsmaßnahmen durchführen zu können, benötigen Sie Administratorrechte für die Gehäusesteuerung (**Chassis Control Administrator**).

Mit dem CMC können Sie im Remote-Zugriff verschiedene Stromverwaltungsmaßnahmen ausführen, z. B. das ordnungsgemäße Herunterfahren eines individuellen Servers im Gehäuse.

Webschnittstelle verwenden

1. **Melden Sie sich bei der CMC-Webschnittstelle an.**
2. Erweitern Sie den Eintrag Server in der Systemstruktur, und wählen Sie den Server, an dem Sie eine Energieverwaltungsmaßnahme ausführen möchten. Die Seite Serverstatus wird angezeigt.
3. Klicken Sie auf die Registerkarte Power Management (Stromverwaltung). Die Seite Server-Stromverwaltung wird angezeigt.
4. Stromstatus zeigt den Stromzustand des Servers (einer der Folgenden Zustände):
   - k.A. - Der CMC hat die Stromversorgung des Servers noch nicht bestimmt.
   - Aus - Entweder der Server oder das Gehäuse sind ausgeschaltet.
   - Ein - Sowohl Gehäuse, als auch Server sind eingeschaltet.
   - Einschalten - vorrübergehender Zustand zwischen Aus und Ein. Ist der Vorgang erfolgreich abgeschlossen, wird der Stromzustand dann auf Ein stehen.
   - Ausschalten - vorrübergehender Zustand zwischen Ein und Aus. Ist der Vorgang erfolgreich abgeschlossen, wird der Stromzustand dann auf Aus

stehen.

5. Wählen Sie eine der folgenden **Stromsteuerungsvorgänge** aus, indem Sie auf die Optionsschaltfläche klicken:
   - **Server einschalten**- Schaltet den Serverstrom ein (entspricht dem Drücken des Netzschalters, wenn der Serverstrom ausgeschaltet ist). Diese Option ist deaktiviert, wenn der Server bereits eingeschaltet ist.
   - **Server ausschalten**- Schaltet den Serverstrom aus (entspricht dem Drücken des Netzschalters, wenn der Serverstrom eingeschaltet ist).
   - Ordentliches Herunterfahren - Schaltet den Server aus und startet ihn daraufhin neu.
   - **System zurücksetzen (Softwareneustart)** - Startet den Server neu, ohne ihn auszuschalten. Diese Option ist deaktiviert, wenn der Server ausgeschaltet ist.
   - **System aus- und einschalten (Hardwareneustart)** - Schaltet den Server aus und startet ihn daraufhin neu. Diese Option ist deaktiviert, wenn der Server ausgeschaltet ist.
6. Klicken Sie auf **Anwenden**. Daraufhin werden Sie über ein Dialogfeld zur Bestätigung des Vorgangs aufgefordert.
7. Klicken Sie auf OK ", um die Stromverwaltungsmaßnahme auszuführen (z. B. den Server zurückzusetzen).

ANMERKUNG: Alle Stromsteuerungsvorgänge können über die Seite Server→Stromverwaltung→Steuerung auf mehreren Servern durchgeführt werden.

RACADM verwenden

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

```
racadm serveraction -m <Modul> <Maßnahme>
```

wobei *<Modul>* den Server nach Steckplatznummer (1-16) im Gehäuse angibt und *<Maßnahme>* den Vorgang, den Sie ausführen möchten: `powerup`, `powerdown`, `powercycle`, `nongradeshutdown` oder `hardreset`.

Fehlerbehebung

Informationen zur Fehlerbehebung bei Netzteilen und bei der Stromversorgung finden Sie unter "Fehlerbehebung und Wiederherstellung".

Wechselstromkreis 1

Wechselstromkreis 2

Gehäuse-Gleichstrombus

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

RACADM-Befehlszeilenschnittstelle verwenden

Dell Chassis Management Controller Firmware Version 2.10, Benutzerhandbuch

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

Die RACADM-Schnittstelle ist je nach Speicherort des von Ihnen verwendeten ausführbaren Programms **racadm** in "Lokal" oder "Remote" aufgeteilt:

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

- Remote-RACADM - RACADM-Befehle werden auf einer Management Station mit der Option **-r** und dem DNS-Namen oder der IP-Adresse des CMC ausgeführt.
- RACADM lokal - melden Sie sich über Telnet, SSH, einer seriellen Verbindung oder der iKVM am CMC an. Mit RACADM lokal wird die RACADM-Implementierung ausgeführt, die Teil der CMC-Firmware ist.

Sie können RACADM-Befehle in Skripts im Remote-Zugriff zum Konfigurieren mehrerer CMCs verwenden. Der CMC unterstützt kein Scripting, was bedeutet, dass Sie keine Skripts direkt vom CMC ausführen können. Für weitere Informationen zur Konfiguration mehrerer CMCs, siehe "Mehrere CMCs in mehreren Gehäusen konfigurieren".

Verwendung einer seriellen, Telnet- oder SSH-Konsole

Sie können sich am CMC entweder mit einer seriellen oder einer Telnet-/SSH-Verbindung anmelden oder über die Dell-CMC-Konsole mit iKVM. Informationen zum Konfigurieren des CMC für seriellen oder Remote-Zugriff finden Sie unter "CMC zur Verwendung von Befehlszeilenkonsolen konfigurieren". Die gemeinsam verwendeten Unterbefehlsoptionen sind unter Tabelle 4-2 aufgelistet. Eine vollständige Liste der RACADM-Unterbefehle finden Sie im Kapitel RACADM-Unterbefehle des *Dell Chassis Management Controller Administrator-Referenzhandbuch*.

Am CMC anmelden

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

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

Sie sind am CMC angemeldet.

Textkonsole starten

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

Für weitere Informationen über das Verbinden zum CMC über iKVM, siehe "iKVM-Modul verwenden".

RACADM verwenden

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

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

```
racadm help (racadm-Hilfe)
```

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

```
racadm help <Unterbefehl>
```

RACADM-Unterbefehle

Tabelle 4-1 enthält eine kurze Liste mit gemeinsamen in RACADM verwendeten Unterbefehlen. Eine vollständige Liste der RACADM-Unterbefehle, einschließlich Syntax und gültigen Einträgen, finden Sie im Kapitel RACADM-Unterbefehle des *Dell Chassis Management Controller Administrator-Referenzhandbuch*.

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

Bei der Eingabe eines RACADM-Unterbefehls muss dem Befehl das Präfix `racadm` vorausgestellt werden. Zum Beispiel:

```
racadm help (racadm-Hilfe)
```

Tabelle 4-1. RACADM-Unterbefehle

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

getchassisname	Zeigt den Namen des Gehäuses an.
getconfig	Zeigt die aktuellen CMC-Konfigurationseigenschaften an.
getdcinfo	Zeigt allgemeine Fehlkonfigurationsinformationen von E/A-Modulen und Tochterkarten an.
getflexaddr	Zeigt den Status aktiviert/deaktiviert der FlexAddress auf Basis der einzelnen Steckplätze/Architekturen an. Wenn mit der -i-Option verwendet, zeigt der Befehl die WWN und die MAC-Adresse für einen bestimmten Steckplatz an.
getioinfo	Zeigt allgemeine E/A-Modulinformationen an.
getkvminfo	Zeigt Informationen über die iKVM an.
getled	Zeigt die LED-Einstellungen auf einem Modul an.
getmacaddress	Zeigt die MAC-Adresse eines Servers an.
getmodinfo	Zeigt die Konfigurations- und Statusinformationen zu einem Modul an.
getniccfg	Zeigt die derzeitige IP-Konfiguration für den Controller an.
getpbinfo	Zeigt Strombudget-Statusinformationen an.
getpminfo	Zeigt Strombudget-Statusinformationen an.
getraclog	Zeigt das CMC-Protokoll an.
getractime	Zeigt die CMC-Uhrzeit an.
getredundancymode	Zeigt den Redundanzmodus des CMC an.
getsel	Zeigt das Systemereignisprotokoll (Hardwareprotokoll) an.
getsensorinfo	Zeigt Informationen zu Systemsensoren an.
getslotname	Zeigt den Namen eines Steckplatzes im Gehäuse an.
getssninfo	Zeigt Informationen über aktive Sitzungen an.
getsvctag	Zeigt Service-Tag-Nummern an.
getsysinfo	Zeigt allgemeine Informationen zum CMC und zum System an.
gettracelog	Zeigt das CMC-Ablaufprotokoll an. Bei Verwendung mit dem Schalter -i zeigt der Befehl die Anzahl von Einträgen im CMC-Ablaufprotokoll an.
getversion	Zeigt die aktuelle Software-Version und Modellinformationen an und gibt Auskunft darüber, ob das Gerät aktualisiert werden kann.
ifconfig	Zeigt die aktuelle CMC-IP-Konfiguration an.
netstat	Zeigt die Routingtabelle und die aktuellen Verbindungen an.
ping	Überprüft, ob die Ziel-IPv4-Adresse vom CMC aus erreichbar ist mit den Inhalten der aktuellen Routing-Tabelle.
ping6	Überprüft, ob die Ziel-IPv4-Adresse vom CMC aus erreichbar ist mit den Inhalten der aktuellen Routing-Tabelle.
racdump	Zeigt die gesamten Gehäuse- und Konfigurationsstatusinformationen sowie alle historischen Verlaufsprotokolle an Wird zur Überprüfung der Konfiguration nach der Zuweisung und währen der Debugging-Sitzungen verwendet.
racreset	Setzt den CMC zurück.
racresetcfg	Setzt den CMC auf die Standardkonfiguration zurück.
remoteimage	Verbinden, Trennen oder Bereitstellen einer Datenträgerdatei auf einem Remote-Server
serveraction	Führt Stromverwaltungsvorgänge auf dem verwalteten System aus.
setassettag	Legt die Systemkennnummer für das Gehäuse fest.
setchassisname	Legt den Namen des Gehäuses fest.
setflexaddr	Aktiviert/deaktiviert FlexAddress auf einem bestimmten Steckplatz/Architektur wenn die Funktion FlexAddress für das Gehäuse aktiviert ist.
setled	Legt die LED-Einstellungen zu einem Modul fest.
setniccfg	Stellt die IP-Konfiguration für den Controller ein.
setractime	Legt die CMC-Uhrzeit fest.
setslotname	Legt den Namen eines Steckplatzes im Gehäuse fest.
setsysinfo	Legt den Namen und die Position des Gehäuses fest.
sshpkauth	Ermöglicht Ihnen das Hochladen von maximal 6 unterschiedlichen, öffentlichen SSH-Schlüsseln, das Löschen existierender Schlüssel und das Anzeigen der im CMC?bereits vorhandenen Schlüssel.
sslcertdownload	Lädt ein von einer Zertifizierungsstelle unterzeichnetes Zertifikat herunter.
sslcertupload	Lädt ein von einer Zertifizierungsstelle unterzeichnetes Zertifikat oder Serverzertifikat auf den CMC hoch.
sslcertview	Zeigt ein von Zertifizierungsstelle unterzeichnetes Zertifikat oder Serverzertifikat auf dem CMC an.
sslcsrgen	Erstellt die SSL-CSR und lädt sie herunter.
sslresetcfg	Regeneriert das selbst-signierte Zertifikat, das vom der grafischen CMC-Web-Benutzerschnittstelle verwendet wird.
testemail	Zwingt den CMC, eine E-Mail über den CMC NIC zu senden.
testfeature	Erlaubt Ihnen die Konfigurationsparameter einer bestimmten Funktion zu prüfen. Zum Beispiel, unterstützt sie das Testen der Active Directory-Konfiguration unter Verwendung einfacher Authentifizierung (Benutzername und Kennwort) oder unter Verwendung von Kerberos-Authentifizierung (einfache Anmeldung oder Smart Card-Anmeldung).
testtrap	Zwingt den CMC, ein SNMP über den CMC-NIC zu senden.
traceroute	Druckt die Route der IPv4-Pakete zu einem Netzwerkknoten.
traceroute6	Druckt die Route der IPv6-Pakete zu einem Netzwerkknoten.

RACADM im Remote-Zugriff aufrufen

Tabelle 4-2 Listet die Optionen für die Fernzugriff-RACADM-Unterbefehle auf.

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

Option	Beschreibung

`-r <RAC-Ip-Adresse>`
 	
`-r <RAC-Ip-Adresse>:<Port>`
	Bestimmt die Remote-IP-Adresse des Controllers.
	
	Verwenden Sie <Port Nummer>, wenn die CMC-Schnittstellennummer nicht der Standardschnittstelle (443) entspricht

`-i`	Weist RACADM an, den Benutzer interaktiv nach dem Benutzernamen und dem Kennwort zu fragen.
`-u <Benutzername>`	Gibt den Benutzernamen an, der verwendet wird, um die Befehlstransaktion zu authentifizieren. Wenn die Option -u verwendet wird, muss die Option -p auch verwendet werden und die Option -i (interaktiv) ist nicht zulässig.
`-p <Kennwort>`	Gibt das Kennwort an, das zur Authentifizierung der Befehlstransaktion verwendet wird. Wenn die Option -p verwendet wird, ist die Option -i nicht zulässig.

Um RACADM im Fernzugriff aufzurufen, geben Sie die folgenden Befehle ein:

```
racadm -r <CMC-IP-Adresse> -u <Benutzername> -p <Kennwort> <Unterbefehl> <Unterbefehlsoptionen>
```

```
racadm -i -r <CMC-IP-Adresse> <Unterbefehl> <Unterbefehlsoptionen>
```

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

Zum Beispiel:

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

```
racadm -i -r 192.168.0.120 getsysinfo
```

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

```
racadm -r <CMC-IP-Adresse>:<Schnittstelle> -u <Benutzername> -p <Kennwort> <Unterbefehl> <Unterbefehlsoptionen>
```

```
racadm -i -r <CMC-IP-Adresse>:<Schnittstelle> <Unterbefehl> <Unterbefehlsoptionen>
```

RACADM-Remote-Fähigkeit aktivieren und deaktivieren

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

Die RACADM-Remote-Fähigkeit ist standardmäßig im CMC aktiviert. In den folgenden Befehlen gibt -g die Konfigurationsgruppe an, zu der das Objekt gehört, und -o das Konfigurationsobjekt, das konfiguriert werden soll.

Zum Deaktivieren der RACADM-Remote-Fähigkeit geben Sie Folgendes ein:

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

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

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

RACADM im Remote-Zugriff verwenden

ANMERKUNG: ANMERKUNG: Konfigurieren Sie die IP-Adresse auf dem CMC, bevor Sie die RACADM-Remote-Fähigkeit verwenden. Für weitere Informationen zum Einstellen Ihres CMC, siehe "Installation und Setup des CMC".

Mit der Remote-Option (-r) der RACADM-Konsole können Sie eine Verbindung zum Managed System herstellen und RACADM-Unterbefehle von einer Remote-Konsole oder einer Management Station ausführen. Um die Remote-Fähigkeit verwenden zu können, sind ein gültiger Benutzername (Option -u) und Kennwort (Option -p) sowie die CMC-IP-Adresse erforderlich.

Bestätigen Sie, dass Sie über die entsprechenden Berechtigungen verfügen, bevor Sie versuchen, RACADM im Remote-Zugriff aufzurufen. Um Ihre Benutzerberechtigungen anzuzeigen, geben Sie Folgendes ein:

```
racadm getconfig -g cfguseradmin -i n
```

wobei *n* Ihre Benutzer-ID (1-16) ist.

Wenn Sie Ihre Benutzer-ID nicht kennen, versuchen Sie verschiedene Werte für *n*.

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

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

```
racadm getconfig -f <Dateiname> -r <IP-Adresse>

oder

racadm sslcertupload -t 1 -f c:\cert\cert.txt
```

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

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

cfgUserAdmin - cfgUserAdminUserName

cfgEmailAlert - cfgEmailAlertAddress

cfgTraps - cfgTrapsAlertDestIPAddr

cfgStandardSchema - cfgSSADRoleGroupName

cfgServerInfo - cfgServerBmcMacAddress

RACADM-Fehlermeldungen

Informationen zu RACADM-CLI-Fehlermeldungen finden Sie unter "Fehlerbehebung".

RACADM zum Konfigurieren des CMC verwenden

ANMERKUNG: Um den CMC das erste Mal konfigurieren zu können, müssen Sie zum Ausführen von RACADM-Befehlen auf einem Remote-System als Benutzer **root** angemeldet sein. Es kann ein anderer Benutzer erstellt werden, der Ihnen die Berechtigung zum Konfigurieren des CMC erteilt.

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

CMC-IPv4-Netzwerkeigenschaften konfigurieren

Ursprünglichen Zugriff auf den CMC einrichten

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

Dieser Abschnitt erklärt, wie die ursprüngliche CMC-Netzwerkkonfiguration mit RACADM-Befehlen ausgeführt wird. Alle in diesem Abschnitt beschriebenen Konfigurationsschritte können über das Frontblenden-LCD ausgeführt werden. Siehe Netzwerkbetrieb mit dem LCD-Konfigurationsassistent konfigurieren".

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

Weitere Informationen über Netzwerk-Unterbefehle finden Sie in den Kapiteln zu den RACADM-Unterbefehlen und Gruppen- und Objektdefinitionen der iDRAC-Eigenschaftendatenbank des *Dell Chassis Management Controller Administrator-Referenzhandbuch*.

ANMERKUNG: Um CMC-Netzwerkeinstellungen einrichten zu können, müssen Sie die Berechtigung als Gehäusekonfigurations-Administrator besitzen.

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

Aktuelle IPv4-Netzwerkeinstellungen anzeigen

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

```
racadm getniccfg
```

oder

```
racadm getconfig -g cfgCurrentLanNetworking
```

Aktuelle IPv6-Netzwerkeinstellungen anzeigen

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

```
racadm getconfig -g cfgIpv6LanNetworking
```

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

```
racadm getsysinfo
```

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

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

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

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

racadm config -g cfgLanNetworking -o cfgNicIpAddress <Statische IP-Adresse>

racadm config -g cfgLanNetworking -o cfgNicGateway <Statisches Gateway>

racadm config -g cfgLanNetworking -o cfgNicNetmask <Statische Subnetzmaske>
```

Aktuelle Netzwerkeinstellungen anzeigen

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

```
racadm getniccfg
```

```
oder
```

```
racadm getconfig -g cfgCurrentLanNetworking
```

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

```
racadm getsysinfo
```

Lokale Netzwerkeinstellungen (LAN) konfigurieren

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

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

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

CMC-NIC aktivieren

Um den CMC-IPv4-NIC zu aktivieren/deaktivieren, geben Sie Folgendes ein:

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

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

ANMERKUNG: Der CMC-IPv4-NIC ist standardmäßig aktiviert.

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

```
racadm config -g cfgIpv6LanNetworking -o cfgNicEnable 1
```

```
racadm config -g cfgIpv6LanNetworking -o cfgNicEnable 0
```

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

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

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

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

```
racadm config -g cfgLanNetworking -o cfgNicIpAddress <statische IP-Adresse>
```

```
racadm config -g cfgLanNetworking -o cfgNicGateway <Statisches Gateway>
```

```
racadm config -g cfgLanNetworking -o cfgNicNetmask <statische Subnetzmaske>
```

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

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

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6AutoConfig 0
```

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6Address <IPv6-Adresse>
```

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6PrefixLength 64
```

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

DCHP für die NIC-Adresse aktivieren oder deaktivieren

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

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

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

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

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

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

Um die Funktion 'DHCP für DNS-Server-Adressen für IPv6' zu deaktivieren und bevorzugte statische und alternative DNS-Server-Adressen festzulegen, geben Sie Folgendes ein:

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

Statische DNS-Server-IP-Adressen einrichten

ANMERKUNG: Diese Einstellungen sind nur gültig, wenn die Funktion 'DCHP für DNS-Server-Adresse' deaktiviert ist.

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

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

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

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

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

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

DNS-Einstellungen (nur IPv4) konfigurieren

- CMC-Registrierung. Um den CMC am DNS-Server zu registrieren, geben Sie Folgendes ein:

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

ANMERKUNG: Einige DNS-Server registrieren nur Namen mit 31 Zeichen oder weniger. Stellen Sie sicher, dass sich der bestimmte Name im DNS-erforderlichen Limit befindet.

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

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

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

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

- DNS-Domänenname. Der Standard-DNS-Domänenname ist ein einzelnes, leeres Zeichen. 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.

Automatische Verhandlung, Duplexmodus und Netzwerkgeschwindigkeit konfigurieren

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

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

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

```
racadm config -g cfgNetTuning -o cfgNetTuningNicFullDuplex <Duplexmodus>
```

wobei

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

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

wobei

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

Maximale Paketgröße (MTU) festlegen

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

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

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

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

SMTP-Server-IP-Adresse festlegen

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

```
racadm config -g cfgRemoteHosts -o cfgRhostsFwUpdateIpAddr <SMTP-IP-Adresse>
```

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

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

Netzwerksicherheitseinstellungen konfigurieren

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

IP-Bereichsüberprüfung aktivieren

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

- cfgRacTuneIpRangeAddr
- cfgRacTuneIpRangeMask

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

a. **cfgRacTuneIpRangeMask** Bit-weise mit einer eingehenden IP-Adresse

b. **cfgRacTuneIpRangeMask** Bit-weise mit **cfgRacTuneIpRangeAddr**

RACADM zum Konfigurieren von Benutzern verwenden

Bevor Sie beginnen

Sie können bis zu 16 Benutzer in der CMC-Eigenschaftsdatenbank konfigurieren. Bevor Sie einen CMC-Benutzer manuell aktivieren, prüfen Sie, ob aktuelle Benutzer vorhanden sind. Wenn Sie einen neuen CMC konfigurieren oder den RACADM-Befehl racresetcfg ausgeführt haben, ist der einzige aktuelle Benutzer root mit dem Kennwort calvin. Der Unterbefehl racresetcfg setzt den CMC auf die ursprünglichen Standardeinstellungen zurück.

VORSICHTSHINWEIS: Verwenden Sie den Befehl racresetcfg mit Vorsicht, da *alle* Konfigurationsparameter auf die ursprünglichen Standardeinstellungen zurückgesetzt werden. Alle vorherigen Änderungen gehen verloren.

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

Um zu überprüfen, ob ein Benutzer vorhanden ist, öffnen Sie eine Telnet-/SSH-Textkonsole für den CMC, melden sich an und geben Folgendes ein:

```
racadm getconfig -u <Benutzername>
```

```
oder
```

geben Sie den folgenden Befehl einmal für jeden Index von 1 - 16 ein:

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

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

```
# cfgUserAdminIndex=XX
```

```
cfgUserAdminUserName=
```

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

ANMERKUNG: Wenn Sie einen Benutzer mit dem Unterbefehl racadm config manuell aktivieren oder deaktivieren, *muss* der Index mit der Option -i angegeben werden. Beobachten Sie, ob das im vorausgehenden Beispiel angezeigte Objekt cfgUserAdminIndex das Zeichen # enthält. Ebenso: Wenn der Befehl **racadm** config -f racadm.cfg zur Angabe einer beliebigen Anzahl von zu schreibenden Gruppen/Objekten verwendet wird, kann der Index nicht angegeben werden. Ein neuer Benutzer wird dem ersten verfügbaren Index hinzugefügt. Dieses Verhalten gibt mehr Flexibilität beim Konfigurieren eines zweiten CMC mit denselben Einstellungen wie die des Haupt-CMC.

CMC-Benutzer hinzufügen

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

1. Legen Sie den Benutzernamen fest.
2. Legen Sie das Kennwort fest.
3. Legen Sie die Benutzerberechtigungen fest. Weitere Informationen über Benutzerberechtigungen finden Sie unter Tabelle 5-18, Tabelle 5-19 und in der Tabelle 3-1 des Kapitels über Datenbankeigenschaften im Dell Chassis Management Controller Administrator-Referenzhandbuch.
4. Aktivieren Sie den Benutzer.

Beispiel

Das folgende Beispiel beschreibt, wie man einen neuen Benutzer genannt "John" mit dem Kennwort "123456" und mit ANMELDUNGS-Berechtigung am CMC hinzufügt.

ANMERKUNG: In Tabelle 3-1 des Kapitels Datenbankeigenschaften im Dell Chassis Management Controller Firmware Administrator-Referenzhandbuch finden Sie eine Liste der gültigen Bitmaskenwerte für bestimmte Benutzerberechtigungen. Der Standardberechtigungswert ist 0, was darauf hinweist, dass der Benutzer über keine aktivierten Berechtigungen verfügt.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 john
```

```
racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456
```

```
racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminPrivilege 0x00000001
```

```
racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminEnable 1
```

Um zu überprüfen, ob der Benutzer mit den richtigen Berechtigungen erfolgreich hinzugefügt wurde, verwenden Sie einen der folgenden Befehle:

```
racadm getconfig -u john
```

```
oder
```

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

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

Bevor Sie beginnen

Sie können bis zu 6 öffentliche Schlüssel konfigurieren, die mit dem Dienst-Benutzernamen über die SSH-Schnittstelle verwendet werden können. Verwenden Sie vor dem Hinzufügen oder Löschen öffentlicher Schlüssel unbedingt den Anzeigebefehl, um zu sehen, welche Schlüssel bereits eingerichtet sind, sodass kein Schlüssel versehentlich überschrieben oder gelöscht wird. Der Dienst-Benutzername ist ein spezielles Benutzerkonto, das für den Zugriff auf den CMC über SSH verwendet werden kann. Wenn PKA über SSH eingerichtet ist und korrekt verwendet wird, müssen Sie bei der Anmeldung beim CMC keinen Benutzernamen und kein Kennwort eingeben. Das kann sehr nützlich sein für automatisierte Skripts zur Durchführung verschiedener Funktionen.

Beachten Sie vor dem Einrichten dieser Funktionen Folgendes:

- Es gibt keine GUI-Unterstützung zur Verwaltung dieser Funktionen; Sie können nur RACADM verwenden.
- Beim Hinzufügen neuer öffentlicher Schlüssel müssen Sie sicherstellen, dass bestehende Schlüssel nicht bereits den Index belegen, zu dem der neue Schlüssel hinzugefügt werden soll. Der CMC führt vor dem Hinzufügen eines Schlüssels keine Prüfungen durch, um sicherzustellen, dass keine vorherigen Schlüssel gelöscht werden. Sobald ein neuer Schlüssel hinzugefügt wurde, tritt er automatisch in Kraft, solange die SSH-Schnittstelle aktiviert ist.
- Beachten Sie bei Verwendung des Anmerkungsabschnitts des öffentlichen Schlüssels, dass nur die ersten 16 Zeichen vom CMC verwendet werden. Die Anmerkung des öffentlichen Schlüssels wird vom CMC verwendet, um SSH-Benutzer bei Verwendung des RACADM-Befehls `getssninfo` zu unterscheiden, da alle PKA-Benutzer den Dienst-Benutzernamen zur Anmeldung verwenden.

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

  ```
  racadm getssninfo

  Typ Benutzer IP -Adresse Anmeldung Datum/Zeit

  SSH PC1 x.x.x.x 16.06.09 09:00:00

  SSH PC2 x.x.x.x 16.06.09 09:00:00
  ```

  Weitere Informationen über sshpkauth finden Sie im *Dell Chassis Management Controller Administrator-Referenzhandbuch.*

Generieren öffentlicher Schlüssel für Windows

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

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

So verwenden Sie den PuTTY-Schlüsselgenerator für Windows-Clients zum Erstellen des Grundschlüssels:

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

   ANMERKUNG: Der CMC blendet möglicherweise keine Meldung ein, wenn Sie Schlüssel mit einem Wert kleiner als 768 oder größer als 4096 hinzufügen, doch wenn Sie versuchen, sich anzumelden, werden diese Schlüssel fehlschlagen.

3. Klicken Sie auf **Generieren** und bewegen Sie die Maus gemäß der Anleitung in das Fenster.

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

   Sie können auch einen Kennsatz eingeben, um den Schüssel sicher zu machen. Speichern Sie den privaten Schüssel auf jeden Fall.

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...**, wenn das Konto mit der Textoption hinzugefügt wird.

Generieren öffentlicher Schlüssel für Linux

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

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

ANMERKUNG: Bei den Optionen wird Groß-/Kleinschreibung unterschieden.

Hierbei

kann die Option -t entweder dsa oder rsa sein.

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

–C Option ermöglicht das Ändern der Anmerkung des öffentlichen Schlüssel und ist optional.

Der Kennsatz ist optional.

Befolgen Sie die Anweisungen. Wenn der Befehl beendet ist, verwenden Sie die öffentliche Datei zur Übergabe an den RACADM zum Hochladen der Datei.

Öffentliche Schlüssel anzeigen

Um öffentliche Schlüssel anzuzeigen, die Sie zum CMC hinzugefügt haben, geben Sie Folgendes ein:

```
racadm sshpkauth –I svcacct –k all –v
```

Um jeweils nur einen Schlüssel anzuzeigen, ersetzen Sie `all` durch eine Zahl zwischen 1 und 6. Um zum Beispiel Schlüssel 2 anzuzeigen, geben Sie Folgendes ein:

```
racadm sshpkauth –I svcacct –k 2 –v
```

Öffentliche Schlüssel hinzufügen

Um einen öffentlichen Schlüssel mit den Datei-Upload-Optionen zum CMC hinzuzufügen, geben Sie Folgendes ein:

```
racadm sshpkauth –I svcacct –k 1 –p 0xfff –f <Dateiname des öffentlichen Schlüssels>
```

ANMERKUNG: Sie können die Datei-Upload-Option nur mit Remote-RACADM verwenden.

Berechtigungen öffentlicher Schlüssel sind in Tabelle 3-1 im Kapitel "Datenbankeigenschaften" im *Dell Chassis Management Controller Administrator-Referenzhandbuch* zu finden.

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

```
racadm sshpkauth –I svcacct –k 1 –p 0xfff –t "<Text des öffentlichen Schlüssels>"
```

Öffentliche Schlüssel löschen

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

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

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

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

Anmeldung mit Authentifizierung mit öffentlichem Schlüssel

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

Anmeldung:

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

Oder

```
ssh service@<IP-Adresse>
```

wobei 'IP-Adresse' die IP-Adresse des CMC ist.

Senden von racadm-Befehlen:

```
ssh service@<Domäne> racadm getversion
```

```
ssh service@<Domäne> racadm getsel
```

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

CMC-Benutzer mit Berechtigungen aktivieren

Um einen Benutzer mit bestimmten Administratorrechten (rollenbasierte Autorität) zu aktivieren, müssen Sie zuerst einen verfügbaren Benutzerindex ausfindig machen, indem Sie die unter "Bevor Sie beginnen" beschriebenen Schritte ausführen. Geben Sie im Anschluss daran die folgenden Befehlszeilen mit dem neuen Benutzernamen und neuen Kennwort ein.

ANMERKUNG: In Tabelle 3-1 des Kapitels "Datenbankeigenschaften" im *Dell Chassis Management Controller Administrator-Referenzhandbuch* finden Sie eine Liste der gültigen Bitmaskenwerte für bestimmte Benutzerberechtigungen. Der Standardberechtigungswert ist 0, was darauf hinweist, dass der Benutzer über keine aktivierten Berechtigungen verfügt.

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <Index> <Benutzerberechtigungs-Bitmaskenwert>
```

Einen CMC-Benutzer deaktivieren

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

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

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

Konfiguration von SNMP- und E-Mail-Warnmeldungen

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

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

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

Mehrere CMCs in mehreren Gehäusen konfigurieren

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

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

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

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

   ANMERKUNG: Die erstellte Konfigurationsdatei ist myfile.cfg. Sie können die Datei umbenennen.

   ANMERKUNG: Die erstellte .cfg-Datei enthält keine Benutzerkennwörter. Wenn die .cfg-Datei auf den neuen CMC hochgeladen wurde, müssen Sie alle Kennwörter erneut hinzufügen.

   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.

2. Modifizieren Sie die Konfigurationsdatei mit einem Nur-Text-Editor (optional). Formatierungen in der Konfigurationsdatei können die RACADM-Datenbank beschädigen.
3. Verwenden Sie die neu erstellte Konfigurationsdatei, um einen Ziel-CMC zu modifizieren.

   Geben Sie Folgendes in die Befehlszeile ein:

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

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

   ```
   racadm reset
   ```

Der Unterbefehl **getconfig -f myfile.cfg** (Schritt 1) fordert die CMC-Konfiguration für den primären CMC an und erstellt die Datei **myfile.cfg**. Falls erforderlich, können Sie die Datei umbenennen oder an einem anderen Ort speichern.

Sie können den Befehl **getconfig** dazu verwenden, die folgenden Maßnahmen auszuführen:

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

Der Unterbefehl **config** lädt die Informationen auf andere CMCs. Der Server Administrator verwendet den Befehl **config** zum Synchronisieren der Benutzer- und Kennwort-Datenbank.

CMC-Konfigurationsdatei erstellen

Die CMC-Konfigurationsdatei, <*Dateiname*>**.cfg**, wird mit dem Befehl `racadm config -f <Dateiname>.cfg` verwendet, um eine einfache Textdatei zu erstellen. Mit dem Befehl können Sie eine Konfigurationsdatei erstellen (ähnlich einer **.ini**-Datei) und den CMC von dieser Datei aus konfigurieren.

Es kann ein beliebiger Dateiname verwendet werden und die Datei erfordert keine **.cfg**-Erweiterung (obwohl sich dieser Unterabschnitt auf diese Endung bezieht).

ANMERKUNG: Weitere Informationen über den **getconfig**-Unterbefehl finden Sie im *Dell Chassis Management Controller Administrator-Referenzhandbuch*.

RACADM parst die Datei **.cfg**, wenn Sie zum ersten Mal auf den CMC geladen wird, um zu überprüfen, dass gültige Gruppen- und Objektnamen vorhanden sind und dass einige einfache Syntaxregeln eingehalten werden. Fehler werden mit der Zeilennummer markiert, in der der Fehler ermittelt wurde, und eine Meldung

beschreibt das Problem. Die gesamte Datei wird auf Richtigkeit geparst und alle Fehler angezeigt. Schreibbefehle werden nicht zum CMC übertragen, wenn ein Fehler in der **.cfg**-Datei festgestellt wird. Sie müssen *alle* Fehler korrigieren, bevor eine Konfiguration erfolgen kann.

Um auf Fehler zu überprüfen, bevor Sie die Konfigurationsdatei erstellen, verwenden Sie die Option -**c** mit dem Unterbefehl **config**. Mit der Option -**c** überprüft `config` nur die Syntax und schreibt nicht auf den CMC.

Verwenden Sie die folgenden Richtlinien zum Erstellen einer **.cfg**-Datei:

- Wenn der Parser auf eine indizierte Gruppe trifft, ist der Wert des verankerten Objekts für die Unterscheidung der einzelnen Indizes ausschlaggebend.

  Die Parser liest alle Indizes aus dem CMC für diese Gruppe aus. Alle Objekte innerhalb dieser Gruppe sind Modifizierungen, wenn der CMC konfiguriert wird. Wenn ein modifiziertes Objekt einen neuen Index darstellt, wird der Index während der Konfiguration auf dem CMC erstellt.

- Sie können in einer **.cfg**-Datei keinen gewünschten Index angeben.

  Indizes können erstellt und gelöscht werden. Mit der Zeit kann die Gruppe durch genutzte und ungenutzte Indizes fragmentiert werden. Wenn ein Index vorhanden ist, wird er modifiziert. Wenn kein Index vorhanden ist, wird der erste verfügbare Index verwendet. Diese Methode ermöglicht Flexibilität beim Hinzufügen indizierter Einträge, wobei der Benutzer keine genauen Index-Übereinstimmungen zwischen allen verwalteten CMCs erstellen muss. Neue Benutzer werden dem ersten verfügbaren Index hinzugefügt. Dadurch kann eine **.cfg**-Datei, die auf einem CMC richtig geparst und ausgeführt wird, auf einem anderen möglicherweise nicht richtig ausgeführt werden, falls alle Indizes belegt sind und ein neuer Benutzer hinzugefügt werden muss.

- Verwenden Sie den Unterbefehl `racresetcfg`, um beide CMCs mit identischen Eigenschaften zu konfigurieren.

  Verwenden Sie den Unterbefehl `racresetcfg`, um den CMC auf die ursprünglichen Standardeinstellungen zurückzusetzen, und führen Sie dann den Befehl `racadm config -f <Dateiname>.cfg` aus. Stellen Sie sicher, dass die **.cfg**-Datei alle gewünschten Objekte, Benutzer, Indizes und andere Parameter enthält. Im Kapitel über Datenbankeigenschaften des *Dell Chassis Management Controller Administrator-Referenzhandbuch* finden Sie eine vollständige Liste von Objekten und Gruppen.

VORSICHTSHINWEIS: Verwenden Sie den Unterbefehl racresetcfg, um die Datenbank und die iDRAC-NIC-Einstellungen auf die ursprünglichen Standardeinstellungen zurückzusetzen und alle Benutzer und Benutzerkonfigurationen zu entfernen. Während der Stammbenutzer verfügbar ist, werden die Einstellungen anderer Benutzer ebenfalls auf die Standardeinstellungen zurückgesetzt.

Parsen-Regeln

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

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

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

  Beispiel:

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

(#
# Dies ist eine Anmerkung
[cfgUserAdmin]
cfgUserAdminPageModemInitString=<Modem init # Dies ist kein Kommentar>)
```

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

  Das Anfangszeichen [, das einen Gruppennamen anzeigt, *muss* in Spalte Eins sein. Der Gruppenname *muss* vor allen anderen Objekten in dieser Gruppe angegeben werden. Objekte, die keinen zugewiesenen Gruppennamen enthalten, erzeugen Fehler. Die Konfigurationsdaten sind in Gruppen organisiert, wie es im Kapitel Datenbankeigenschaften des *Dell Chassis Management Controller Administrator-Referenzhandbuch* beschrieben ist.

  Das folgende Beispiel zeigt einen Gruppennamen, ein Objekt und den Eigenschaftswert des Objekts an.

```
[cfgLanNetworking] -{Gruppenname}
```

```
cfgNicIpAddress=143.154.133.121 {Objektname} {Objektwert}
```

- Alle Parameter werden als "Objekt=Wert"-Paaren ohne Leerzeichen zwischen "Objekt", "=" und "Wert" angegeben.

Leerstellen nach dem Wert werden ignoriert. Eine Leerstelle innerhalb einer Wertezeichenkette bleibt unverändert. Jedes Zeichen rechts neben dem = (z. B. ein zweites =, ein #, [,] usw.) wird wie eingegeben übernommen. Bei diesen Zeichen handelt es sich um gültige Modemchat-Skriptzeichen.

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

- Der **.cfg**-Parser ignoriert einen Index-Objekteintrag.

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

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

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

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

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

Benutzer müssen ein indiziertes Objekt manuell mit folgendem Befehl entfernen:

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

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

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

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

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

```
[cfgUserAdmin]
```

```
cfgUserAdminUserName=<BENUTZERNAME>
```

Wenn Sie `racadm getconfig -f <MeinBeispiel>.cfg` eingeben, erstellt der Befehl eine .**cfg**-Datei für die aktuelle CMC-Konfiguration. Diese Konfigurationsdatei kann als Beispiel und Ausgangspunkt für Ihre eindeutige **.cfg**-Datei verwendet werden.

CMC-IP-Adresse modifizieren

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

Beispiel:

```
#

# Object Group (Objektgruppe) "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1
```

Die Datei wird wie folgt aktualisiert:

```
#

# Object Group (Objektgruppe) "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.9.143

# comment, the rest of this line is ignored (Kommentar, der Rest dieser Zeile wird ignoriert)

cfgNicGateway=10.35.9.1
```

Mit dem Befehl `racadm config -f <meineDatei>.cfg` wird die Datei geparst, und Fehler werden nach Zeilennummer identifiziert. Eine korrekte Datei aktualisiert die entsprechenden Einträge. Derselbe, im vorherigen Beispiel verwendete Befehl `getconfig` kann außerdem zur Bestätigung der Aktualisierung verwendet werden.

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

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

RACADM zum Konfigurieren von Eigenschaften auf iDRAC verwenden

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

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

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

Wenn die Firmware auf dem Blade-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 von Funktionen, die auf dem Blade-Server nicht unterstützt werden, als *N/A (k.A.)* angezeigt.

Beispiel:

```
$ racadm getconfig -g cfgSessionManagement -m server-1

# cfgSsnMgtWebServerMaxSessions=N/A

# cfgSsnMgtWebServerActiveSessions=N/A

# cfgSsnMgtWebServerTimeout=N/A

# cfgSsnMgtSSHMaxSessions=N/A

# cfgSsnMgtSSHActiveSessions=N/A

# cfgSsnMgtSSHTimeout=N/A

# cfgSsnMgtTelnetMaxSessions=N/A

# cfgSsnMgtTelnetActiveSessions=N/A

# cfgSsnMgtTelnetTimeout=N/A
```

Fehlerbehebung

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

Tabelle 4-3. Serielle und RACADM-Befehle verwenden: Häufig gestellte Fragen
Fragen

Frage	Antwort
Nach Durchführung eines CMC-Reset (mit Hilfe des RACADM-Unterbefehls racreset) gebe ich einen Befehl ein, woraufhin folgende Meldung angezeigt wird: racadm <*Unterbefehl*> Transport: ERROR: (RC=-1) Was bedeutet diese Meldung?	Sie müssen warten, bis der CMC-Reset abgeschlossen ist, bevor Sie einen anderen Befehl ausstellen.
Wenn ich die RACADM-Unterbefehle verwende, erhalte ich Fehler, die ich nicht verstehe.	Es können ein oder mehrere der folgenden Fehler bei der Verwendung von RACADM auftreten: • Lokale Fehlermeldungen – Probleme, wie z B. Syntax, typografische Fehler und falsche Namen. Beispiel: ERROR: <Meldung> Verwenden Sie den RACADM-Unterbefehl **help**, um richtige Syntax- und Anwendungsinformationen anzuzeigen. • Fehlermeldungen, die sich auf den CMC beziehen - Probleme, bei denen der CMC keine Maßnahme ausführen kann. Dies kann auch "racadm-Befehl fehlerhaft" lauten. Geben Sie für Informationen zum Debuggen **racadm gettracelog** ein.
Während ich Remote-RACADM verwendet habe, ist die Eingabeaufforderung zu ">" gewechselt, und ich kann nicht zur Eingabeaufforderung "$" zurückkehren.	Wenn Sie in den Befehl doppelte Anführungszeichen (") eingeben, wechselt die Befehlszeilenschnittstelle zur Eingabeaufforderung ">" und stellt alle Befehle in die Warteschlange. Um zur Eingabeaufforderung "$" zurückzukehren, geben Sie <Strg>–d ein.

Ich habe versucht, die folgenden Befehle zu verwenden und erhielt eine Fehlermeldung "Nicht gefunden":
 	
`$ logout`
 	
`$ quit`
	Die Abmelde- und Verlassen-Befehle sind in der CMC-Befehlszeilenschnittstelle nicht unterstützt.

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

Fehlerbehebung und Wiederherstellung

Dell Chassis Management Controller Firmware Version 2.10, Benutzerhandbuch

---

Übersicht

Dieser Abschnitt erklärt, wie Tasks unter Verwendung der CMC-Webschnittstelle ausgeführt werden, die sich auf die Wiederherstellung und Behebung eines Problems auf dem Remote-Zugriffsystem beziehen.

- Netzstrom auf einem Remote-System verwalten
- Gehäuseinformationen anzeigen
- Ereignisprotokolle anzeigen
- Diagnosekonsole verwenden
- Komponenten zurücksetzen
- Fehlerbehebung bei Network Time Protocol (NTP)-Problemen
- Fehlerbehebung bei Netzwerkproblemen
- Fehlerbehebung bei Warnmeldungsproblemen
- Deaktivieren vergessener Passworte
- Fehlercodes und -protokolle

Hilfsprogramme zur Gehäuseüberwachung

LEDs zum Identifizieren von Komponenten im Gehäuse konfigurieren

Sie können die LEDs von Komponenten für alle oder einzelne Komponenten so einrichten (Gehäuse, Server und E/A-Module), dass sie zum Identifizieren der Komponente im Gehäuse blinken.

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

Webschnittstelle verwenden

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

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf Chassis (Gehäuse).
3. Klicken Sie auf das Register Fehlerbehebung.
4. Klicken Sie auf das Unterregister Identifizieren. Die Seite Identifizieren wird mit einer Liste aller Komponenten im Gehäuse angezeigt.
5. Zur Aktivierung des Blinkens einer Komponenten-LED, markieren Sie das Kontrollkästchen neben dem Gerätenamen und klicken Sie dann auf Blinken.
6. Zur Deaktivierung des Blinkens einer Komponenten-LED, markieren Sie das Kontrollkästchen neben dem Gerätenamen und klicken Sie dann auf Nicht-blinken.

RACADM verwenden

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

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

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

- `server-n`, wobei *n* = 1-16
- `switch-n`, wobei *n* = 1–6
- `cmc-activ`

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

- 0 - kein Blinken (Standardeinstellung)
- 1 - Blinken

Konfiguration von SNMP-Alarmen

SNMP (Einfaches Netzwerkverwaltungsprotokoll)-Traps, oder Ereignis-Traps, sind E-Mail-Ereigniswarnungen ähnlich. Sie werden von einer Management Station verwendet, um unangeforderte Daten vom CMC zu empfangen.

Sie können den CMC so konfigurieren, dass Ereignis-Traps erstellt werden. Tabelle 11-1 gibt einen Überblick zu Ereignissen an, die SNMP- und E-Mail-Alarme auslösen. Für Informationen zu E-Mail-Warnungen, siehe "Konfiguration von E-Mail-Alarmen".

ANMERKUNG: Beginnend mit CMC Version 2.10 ist SNMP jetzt IPv6-aktiviert. Sie können eine IPv6-Adresse oder einen vollqualifizierten Domänennamen (FQDN) im Ziel für eine Ereigniswarnung einschließen.

Tabelle 11-1. Gehäuseereignisse, die zu SNMP

Ereignis	Beschreibung
Lüftersondenfehler	Ein Lüfter läuft zu langsam oder überhaupt nicht.
Batteriesondenwarnung	Eine Batterie funktioniert nicht mehr.
Temperatursondenwarnung	Die Temperatur geht auf den oberen bzw. unteren Grenzwert zu.
Temperatursondenfehler	Die Temperatur ist für einen ordnungsgemäßen Betrieb zu hoch oder zu niedrig.
Redundanz herabgesetzt	Redundanz der Lüfter bzw. Netzteile wurde herabgesetzt.
Redundanz verloren	Es besteht keine Redundanz mehr für die Lüfter und/oder Netzteile.
Netzteilwarnung	Das Netzteil nähert sich einem Fehlerzustand.
Netzteilfehler	Das Netzteil ist fehlerhaft.
Netzteil nicht vorhanden	Ein erwartetes Netzteil ist nicht vorhanden.
Hardwareprotokollfehler	Das Hardwareprotokoll ist nicht funktionsfähig.
Hardwareprotokollwarnung	Das Hardwareprotokoll ist fast voll.
Server nicht vorhanden	Ein erwarteter Server ist nicht vorhanden.
Serverfehler	Der Server funktioniert nicht.
KVM nicht vorhanden	Erwartetes KVM-Modul ist nicht vorhanden.
KVM-Fehler	KVM-Modul funktioniert nicht.
E/A-Modul nicht vorhanden	Ein erwartetes E/A-Modul ist nicht vorhanden.
E/A-Modul-Fehler	Das E/A-Modul funktioniert nicht.
Unverträgliche Firmware-Version	Die Firmware passt nicht zu der des Gehäuses oder der Server.

Gehäusestrom-Schwellenfehler	Die Leistungsaufnahme innerhalb des Gehäuses hat die Eingangsleistungsgrenze des Systems erreicht.

Sie können SNMP-Warnungen über die Webschnittstelle oder RACADM hinzufügen und konfigurieren.

Webschnittstelle verwenden

ANMERKUNG: Zum Hinzufügen oder konfigurieren von SNMP-Warnungen, müssen Sie Administratorrechte zur Konfiguration des Gehäuses besitzen.

ANMERKUNG: Um die Sicherheit zu erhöhen, empfiehlt Dell nachdrücklich, das vorgegebene Kennwort für das Benutzerkonto root (User 1) bei der Ersteinrichtung zu ändern. Das Konto root ist das werkseitig voreingestellte Verwaltungskonto des CMC-Moduls. Sie können das Standardkennwort für das Stammkonto ändern, indem Sie auf Benutzer-ID 1 klicken, um die Seite Benutzerkonfiguration zu öffnen. Hilfe zu dieser Seite finden Sie über den Link Hilfe, der sich auf dieser Seite ganz oben rechts in der Ecke befindet.

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur Gehäuse aus.
3. Klicken Sie auf das Register Warnungsverwaltung. Die Seite Gehäuseereignisse wird angezeigt.
4. Aktivieren Sie Warnmeldungen:
   a. Aktivieren Sie die Kontrollkästchen der Ereignisse, für die Sie Warnmeldungen aktivieren möchten. Um alle Ereignisse für Warnmeldungen zu aktivieren, wählen Sie das Kontrollkästchen Alle auswählen aus.
   b. Klicken Sie auf Anwenden, um die Einstellungen zu speichern.
5. Klicken Sie auf das Unterregister Traps-Einstellungen. Die Seite Warnungsziele bei Gehäuseereignissen wird angezeigt.
6. Geben Sie eine gültige Adresse in ein leeres Ziel-Feld ein.

   ANMERKUNG: Eine gültige Adresse ist eine Adresse, die die Trap- Warnungen empfängt. Verwenden Sie das 4-Punkt-IPv4-Format, Standard-IPv6-Adressnotation oder FQDN. Zum Beispiel: 123.123.123.123 oder 2001:db8:85a3::8a2e:370:7334 oder dell.com

7. Geben Sie die SNMP-Community-Zeichenkette ein, zu der die Ziel- Management Station gehört.

   ANMERKUNG: Die Community-Zeichenkette auf der Seite **Warnungsziele bei Gehäuseereignissen** unterscheidet sich von der Community-Zeichenkette auf der Seite **Gehäuse→Netzwerk / Sicherheit→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 / Sicherheit→Dienste** ist die Community-Zeichenkette, die von Management Stationen zur Abfrage des SNMP-Dämon-Programms auf dem CMC verwendet wird.

8. Klicken Sie auf Apply (Übernehmen), um die Änderungen zu speichern.

So testen Sie einen Ereignis-Trap für ein Warnungsziel:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur Gehäuse aus.
3. Klicken Sie auf das Register Warnungsverwaltung. Die Seite Gehäuseereignisse wird angezeigt.
4. Klicken Sie auf das Unterregister Traps-Einstellungen. Die Seite Warnungsziele bei Gehäuseereignissen wird angezeigt.
5. Klicken Sie in der Spalte Test-Trap neben dem Ziel auf Senden.

ANMERKUNG: Geben Sie Trap-Ziele als entsprechend formatierte numerische Adressen (IPv6 oder IPv4) oder vollqualifizierte Domänennamen (FQDNs) an. Wählen Sie ein Format, das mit Ihrer Netzwerk-Technologie/Infrastruktur übereinstimmt. Die **testtrap**-Funktionalität kann keine inkorrekten Einstellungen aufgrund der aktuellen Netzwerkkonfiguration erkennen (z. B. die Verwendung eines IPv6-Ziels in einer reinen IPv4-Umgebung).

RACADM verwenden

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

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

2. Aktivieren Sie Warnmeldungen, indem Sie Folgendes eingeben:

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

3. Geben Sie die Ereignisse an, für die der CMC Warnmeldungen erstellen soll, indem Sie Folgendes eingeben:

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

wobei <*Maskenwert*> ein Hexadezimalwert zwischen 0x0 und 0x017fffdf ist.

Um den Maskenwert zu ermitteln, verwenden Sie einen wissenschaftlichen Rechner im Hexadezimalmodus und fügen die zweiten Werte der einzelnen Masken (1, 2, 4 usw.) mit der Taste <ODER> hinzu.

Um z. B. Trap-Warnungen bei Batteriesondenwarnungen (0x2), Netzteilausfällen (0x1000) und KVM-Fehlern (0x80000) zu aktivieren, geben Sie 2 <ODER> 1000 <ODER> 200000 ein, und drücken Sie die Taste <=>.

Der daraus hervorgehende Hexadezimalwert ist 208002, und der Maskenwert für den RACADM-Befehl ist 0x208002.

Tabelle 11-2. Filtermasken für Ereignis-Traps

Ereignis	Filtermaskenwert
Lüftersondenfehler	0x1
Batteriesondenwarnung	0x2
Temperatursondenwarnung	0x8
Temperatursondenfehler	0x10
Redundanz herabgesetzt	0x40
Redundanz verloren	0x80
Netzteilwarnung	0x800
Netzteilfehler	0x1000
Netzteil nicht vorhanden	0x2000
Hardwareprotokollfehler	0x4000
Hardwareprotokollwarnung	0x8000
Server nicht vorhanden	0x10000
Serverfehler	0x20000
KVM nicht vorhanden	0x40000
KVM-Fehler	0x80000
E/A-Modul nicht vorhanden	0x100000
E/A-Modul-Fehler	0x200000
Unverträgliche Firmware-Version	0x00400000
Gehäusestrom-Schwellenfehler	0x01000000

4. Aktivieren Sie Trap-Warnmeldungen, indem Sie Folgendes eingeben:

```
racadm config -g cfgTraps -o cfgTrapsEnable 1 -i <Index>
```

wobei <*Index*> ein Wert von 1 - 4 ist. Die Indexnummer wird vom CMC verwendet, um bis zu vier konfigurierbare Ziele für Trap-Warnungen zu unterscheiden. Geben Sie Trap-Ziele als entsprechend formatierte numerische Adressen (IPv6 oder IPv4) oder vollqualifizierte Domänennamen (FQDNs) an.

5. Bestimmen Sie eine Ziel-IP-Adresse, um Trap-Warnungen zu erhalten, indem Sie Folgendes eingeben:

```
racadm config -g cfgTraps -o cfgTrapsAlertDestIPAddr <IP-Adresse> -i <Index>
```

wobei <*IP-Adresse*> ein gültiges Ziel ist und <*Index*> der Indexwert, den Sie in Schritt 4 angegeben haben.

6. Geben Sie den Community-Namen an, indem Sie Folgendes eingeben:

```
racadm config -g cfgTraps -o cfgTrapsCommunityName <Community-Name> -i <Index>
```

wobei <*Community-Name*> die SNMP-Community ist, zu der das Gehäuse gehört, und <*Index*> der Indexwert, den Sie in Schritt 4 und 5 angegeben haben.

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

ANMERKUNG: Die Befehle in den Schritten 2-6 überschreiben alle vorhandenen Einstellungen, die Sie für den angegebenen Index konfiguriert haben (1-4). Um festzustellen, ob ein Index über zuvor konfigurierte Werte verfügt, geben Sie Folgendes ein: racadm get config -g cfgTraps -i <Index>. Wenn der Index konfiguriert ist, werden für die Objekte cfgTrapsAlertDestIPAddr und cfgTrapsCommunityName Werte angezeigt.

So testen Sie einen Ereignis-Trap für ein Warnungsziel:

```
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>
```

Konfiguration von E-Mail-Alarmen

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

Tabelle 11-1 liefert einen Überblick über die Ereignisse, die einen SNMP- und E-Mail-Alarm auslösen. Informationen zu SNMP-Warnungen finden Sie unter "Konfiguration von SNMP-Alarmen".

Sie können E-Mail-Warnungen über die Webschnittstelle oder RACADM hinzufügen und konfigurieren.

Webschnittstelle verwenden

ANMERKUNG: Zum Hinzufügen oder Konfigurieren von E-Mail-Warnungen müssen Sie die Berechtigung als Gehäusekonfigurations-Administrator besitzen.

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur Gehäuse aus.
3. Klicken Sie auf das Register Warnungsverwaltung. Die Seite Gehäuseereignisse wird angezeigt.
4. Aktivieren Sie Warnmeldungen:
   a. Aktivieren Sie die Kontrollkästchen der Ereignisse, für die Sie Warnmeldungen aktivieren möchten. Um alle Ereignisse für Warnmeldungen zu aktivieren, wählen Sie das Kontrollkästchen Alle auswählen aus.
   b. Klicken Sie auf Anwenden, um die Einstellungen zu speichern.
5. Klicken Sie auf das Unterregister E-Mail-Warnungseinstellungen. Die Seite E-Mail-Warnungsziele wird angezeigt.
6. Geben Sie die IP-Adresse des SMTP-Servers an:
   a. Machen Sie das Feld SMTP- (E-Mail-)Server ausfindig, und geben Sie dann die SMTP-Hostnamen oder die IP-Adresse ein.

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

   b. Geben Sie den gewünschten E-Mail-Absender für die Warnung ein oder lassen Sie das Feld frei, um den standardmäßigen E-Mail- Absender zu verwenden. Die Voreinstellung ist: cmc@[IP_Adresse], wobei [IP_Adresse] der IP-Adresse des CMC entspricht. Wenn Sie einen Wert eingeben möchten, ist der Syntax für den E-Mail-Namen EMailName[@Domäne] und eine E-Mail-Domäne kann optional angegeben werden. Falls @Domäne nicht spezifiziert ist, und es gibt eine aktive CMC-Netzwerkdomäne, dann wird EMailName@cmc.Domäne als Quell-E-Mail-Adresse verwendet. Ist @Domäne nicht näher spezifiziert und der CMC hat keine aktive Netzwerkdomäne, dann wird die IP-Adresse des CMC verwendet (z. B.: EMailName@[IP_Adresse]).

c. Klicken Sie auf Anwenden, um die Änderungen zu speichern.

7. Geben Sie die E-Mail-Adresse(n) an, die die Warnungen empfangen soll(en):

   a. Geben Sie eine gültige E-Mail-Adresse in ein leeres Feld Ziel-E-Mail- Adresse ein.

   b. Geben Sie optional einen Namen ein. Dies ist der Name der Organisation, die die E-Mail erhält. Wird ein Name für eine ungültige E-Mail-Adresse eingegeben, wird er ignoriert.

   c. Klicken Sie auf Anwenden, um die Einstellungen zu speichern.

Um eine Test-E-Mail an ein E-Mail-Warnungs-Ziel zu senden, gehen Sie wie folgt vor:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur Gehäuse aus.
3. Klicken Sie auf das Register Warnungsverwaltung. Die Seite Gehäuseereignisse wird angezeigt.
4. Klicken Sie auf das Unterregister E-Mail-Warnungseinstellungen. Die Seite E-Mail-Warnungsziele wird angezeigt.
5. Klicken Sie in der Spalte Ziel-E-Mail-Adresse neben dem Ziel auf Senden.

RACADM verwenden

1. Öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC und melden Sie sich an.
2. Aktivieren Sie Warnmeldungen, indem Sie Folgendes eingeben:

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

   ANMERKUNG: Es kann nur eine Filtermaske für SNMP- und E-Mail- Warnungen festgelegt werden. Sie können Schritt 3 überspringen, wenn Sie bereits eine Filtermaske festgelegt haben.

3. Geben Sie die Ereignisse an, für die der CMC Warnmeldungen erstellen soll, indem Sie Folgendes eingeben:

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

   wobei *<Maskenwert>* ein hexadezimaler Wert zwischen 0x0 und 0x017fffdf ist und mit den vorangestellten Zeichen 0x ausgedrückt werden muss. Tabelle 11-2 liefert die Filtermasken für jeden Ereignistyp. Eine Anleitung zum Berechnen des Hexadezimalwerts für die Filtermaske, die Sie aktivieren möchten, finden Sie in Schritt 3 in "RACADM verwenden".

4. Aktivieren Sie E-Mail-Warnungen, indem Sie Folgendes eingeben:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable 1 -i <Index>
   ```

   wobei *<Index>* ein Wert von 1 - 4 ist. Die Indexnummer wird vom CMC verwendet, um bis zu vier konfigurierbare Ziel-E-Mail-Adressen zu unterscheiden.

5. So geben Sie eine Ziel-E-Mail-Adresse an, um E-Mail-Warnungen zu erhalten:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertAddress <E-Mail-Adresse> -i <Index>
   ```

   wobei *<E-Mail-Adresse>* eine gültige E-Mail-Adresse und *<Index>* der Indexwert ist, den Sie in Schritt 4 angegeben haben.

6. Geben Sie den Namen des Teilnehmers an, der E-Mail-Warnungen empfangen soll, indem Sie Folgendes eingeben:

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertAddress <E-Mail-Name> -i <Index>
   ```

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

7. Richten Sie den SMTP-Host ein, indem Sie die Datenbankeigenschaft `cfgRhostsSmtpServerIpAddr` durch folgende Eingabe konfigurieren:

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

wobei `host.domain` ein vollständig qualifizierter Domänenname ist.

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

ANMERKUNG: Die Befehle in den Schritten 2-6 überschreiben alle vorhandenen Einstellungen, die Sie für den angegebenen Index konfiguriert haben (1-4). Um festzustellen, ob ein Index über zuvor konfigurierte Werte verfügt, geben Sie Folgendes ein: racadm get config -g cfgEmailAlert -i <Index>. Wenn der Index konfiguriert ist, werden für die Objekte cfgEmailAlertAddress und cfgEmailAlertEmailName Werte angezeigt.

Erste Schritte, um Fehler eines Remote-System zu beheben

Die folgenden Fragen werden im Allgemeinen für die Fehlerbehebung bei vorrangigen Problemen des verwalteten Systems gestellt:

1. Ist das System ein- oder ausgeschaltet?
2. Wenn eingeschaltet, funktioniert das Betriebssystem, ist es abgestürzt oder nur blockiert?
3. Wenn ausgeschaltet, wurde der Strom unerwartet ausgeschaltet?

Strom überwachen und Stromsteuerungsbefehle am Gehäuse ausführen

Sie können die Webschnittstelle oder RACADM für Folgendes verwenden:

- Aktuellen Stromstatus des Systems anzeigen.
- Durchführen eines ordentlichen Herunterfahrens durch das Betriebssystem beim Neustart; Ein- oder Ausschalten des Systems.

Informationen zur Stromverwaltung auf dem CMC und zum Konfigurieren des Strombudgets, der Redundanz und der Stromsteuerung finden Sie unter "Stromverwaltung".

Strombudgetstatus anzeigen

Wie Sie über die Webschnittstelle oder RACADM den Strombudgetstatus für das Gehäuse, die Server und die Netzteileinheiten anzeigen, erfahren Sie unter "Anzeige des Stromverbrauchsstatus".

Einen Stromsteuerungsvorgang ausführen

Für Anleitungen zum Hochfahren, Herunterfahren, Zurücksetzen oder Ein- und Ausschalten des Systems verwenden Sie die CMC-Webschnittstelle oder RACADM und beachten Sie "Durchführen von Energieverwaltungsmaßnahmen am Gehäuse", "Stromsteuerungsvorgänge für ein E/A-Modul ausführen" und "Durchführen von Energieverwaltungsmaßnahmen an einem Server".

Fehlerbehebung beim Netzteil

Verwenden Sie die nachfolgenden Elemente zur Unterstützung bei der Fehlerbehebung von Netzteil- und anderen strombezogenen Problemen:

- Problem: Es wurde versucht, die Stromredundanzrichtlinie auf Wechselstromredundanz zu konfigurieren, doch der Vorgang schlug fehl.
  - Lösung A: Diese Art von Betrieb erfordert, dass 2, 4 oder 6 Netzteile (1, 2 bzw. 3 in jedem Stromkreis) Eingangsleistung erhalten, die im modularen Gehäuse verfügbar und nutzbar sein soll. Stellen Sie für jeglichen Wechselstromredundanz-Betrieb sicher, dass eine vollständige

Netzteilkonfiguration mit sechs Netzteilen verfügbar ist, bevor versucht wird, die Stromredundanzrichtlinie auf Wechselstromredundanz zu ändern.

- Lösung B: Prüfen Sie, ob alle Netzteile ordnungsgemäß an die zwei Wechselstromkreise angeschlossen sind; die drei Netzteile auf der linken Seite müssen an einen Wechselstromkreis angeschlossen werden und die drei Netzteile auf der rechten Seite müssen an einen anderen Wechselstromkreis angeschlossen werden, wobei beide Wechselstromkreise ordnungsgemäß funktionieren müssen. Sie können Stromredundanz nicht auf Wechselstromredundanz konfigurieren, wenn einer der Wechselstromkreise nicht funktioniert.

- Problem: Der Netzteilzustand wird als Fehlgeschlagen (Kein Wechselstrom) angezeigt, selbst wenn ein Netzkabel angeschlossen ist und der Stromverteiler ausreichenden Wechselstromausgang erzeugt.
  - Lösung: Das Netzkabel prüfen und wieder einsetzen. 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 ersetzen zu lassen.
- Problem: Dynamische Netzteilzuschaltung ist aktiviert, doch keines der Netzteile wird im Standby-Modus angezeigt.
  - Lösung: Dies tritt auf, wenn eine Konfiguration mit sechs Netzteilen für Wechselstromredundanz konfiguriert ist und der Gehäusebetrieb die Stromkapazität von mindestens drei Netzteilen erfordert. Nur wenn der im Gehäuse verfügbare Überschussstrom die Kapazität von mindestens einem Netzteil eines Netzteilpaars überschreitet, wird ein Netzteil jedes Satzes von Online- und Redundanz-Netzteilen in den Standby-Modus geschaltet.
- Problem: Es wurde ein neuer Server in das Gehäuse mit sechs Netzteilen eingesetzt, doch der Server schaltet nicht ein.
  - Lösung A: Prüfen Sie die Eingangsleistungsgrenze des Systems - die Einstellung ist u. U. zu niedrig konfiguriert, um ein Einschalten weiterer Server zu ermöglichen.
  - Lösung B: Prüfen Sie die Strompriorität des Serversteckplatzes, die dem neu eingesetzten Server zugewiesen ist, und stellen Sie sicher, dass die Priorität nicht niedriger ist als die Strompriorität aller übrigen Serversteckplätze.
- Problem: Verfügbare Leistung schwankt, selbst wenn die modulare Gehäusekonfiguration nicht verändert wurde.
  - Lösung: CMC 1.2 und höhere Versionen verfügen über dynamisches Lüfter-Leistungsmanagement, das Serverstromzuweisungen kurzzeitig verringert, wenn das Gehäuse im Bereich der benutzerseitig konfigurierten maximalen Leistungsgrenze (Spitze) betrieben wird; es bewirkt, dass den Lüftern Strom durch Verringerung von Serverleistung zugewiesen wird, sodass die Eingangsleistungsaufnahme unterhalb der Eingangsleistungsgrenze des Systems gehalten werden kann. Dieses Verhalten ist normal.
- Problem: 2000 W wird als Überschuss für Systemspitzen gemeldet.
  - Lösung: Das Gehäuse hat in der derzeitigen Konfiguration 2000 W Überschussstrom verfügbar, und die Eingangsleistungsgrenze des Systems kann sicher um diesen gemeldeten Wert verringert werden, ohne dass die Serverleistung beeinträchtigt wird.
- Problem: Eine Teilmenge der Server hat nach einem Ausfall eines Wechselstromkreises einen Stromausfall erfahren, obwohl das Gehäuse in der Wechselstromredundanz-Konfiguration mit sechs Netzteilen betrieben wurde.
  - Lösung: Dies kann auftreten, wenn die Netzteile zum Zeitpunkt, an den der Wechselstromkreis ausfällt, nicht korrekt an die redundanten Wechselstromkreise angeschlossen sind. Die Wechselstromredundanz-Richtlinie schreibt vor, dass die drei Netzteile auf der linken Seite an einen Wechselstromkreis angeschlossen werden und die drei Netzteile auf der rechten Seite an einen anderen Wechselstromkreis angeschlossen werden. Wenn zwei Netzteileinheiten nicht korrekt angeschlossen sind (z. B. Netzteileinheit 3 und Netzteileinheit 4 an die falschen Wechselstromkreise) bewirkt ein Ausfall des Wechselstromkreises einen Ausfall der Stromversorgung zu den Servern niedrigster Priorität.
- Problem: Die Server niedrigster Priorität haben nach einem Ausfall der Netzteileinheit einen Stromausfall erfahren.
  - Lösung: Dieses Verhalten wird erwartet, wenn die Gehäusestromrichtlinie auf Keine Redundanz konfiguriert wurde. Um weitere Netzteilfehler und ein nachfolgendes Abschalten der Server zu vermeiden, Stellen Sie sicher, dass das Gehäuse mindestens vier Netzteile aufweist und für die Netzteilredundanz-Richtlinie konfiguriert ist, sodass ein Ausfall der Netzteileinheit den Serverbetrieb nicht beeinträchtigt.
- Problem: Die Gesamtserverleistung verringert sich, wenn 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.

Gehäusezusammenfassungen anzeigen

Der CMC enthält Rollup-Übersichten zu Gehäuse, primären und Standby-CMCs, iKVM, Lüftern, Temperatursensoren und E/A-Modulen (IOMs).

Webschnittstelle verwenden

So zeigen Sie Zusammenfassungen zu Gehäuse, CMCs, iKVM und E/A-Modulen an:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf Chassis (Gehäuse).
3. Klicken Sie auf das Register Zusammenfassung. Die Seite Gehäusezusammenfassung wird angezeigt.

Tabelle 11-3, Tabelle 11-4, Tabelle 11-5 und Tabelle 11-6 beschreiben die dargestellten Informationen.

Bauteil	Beschreibung
Name	Zeigt den Namen des Gehäuses an. Der Name identifiziert das Gehäuse auf dem Netzwerk. Für Informationen zur Konfiguration des Gehäusenamens, siehe "Steckplatznamen bearbeiten".
Model	Zeigt das Gehäusemodell oder den Hersteller an. Z. B. PowerEdge 2900.
Service-Tag-Nummer	Zeigt die Service-Tag-Nummer des Gehäuses an. Die Service-Tag-Nummer ist eine vom Hersteller eindeutig identifizierbare Nummer für Support und Wartung.
Systemkennnummer	Zeigt die Systemkennnummer des Gehäuses an.
Standort	Zeigt die Position des Gehäuses an.
CMC Failover-bereit	Zeigt an (Ja, Nein), ob der Standby-CMC (falls vorhanden) im Falle eines Failovers die Funktion übernehmen kann.
Systemstromstatus	Zeigt den Systemstromstatus an.

Bauteil	Beschreibung
Informationen zum primären CMC	
Name	Zeigt den Namen des CMC an. Z. B. primärer CMC oder Standby-CMC.
Beschreibung	Enthält eine kurze Beschreibung zum Zweck des CMC.
Uhrzeit/Datum	Zeigt das Datum und die Uhrzeit an, die auf dem aktiven oder primären CMC festgelegt wurden.
Aktive CMC-Position	Zeigt die Steckplatzposition des aktiven oder primären CMC an.
Redundanz-Modus	Wird angezeigt, wenn der Standby-CMC im Gehäuse vorhanden ist.
Primäre Firmware-Version	Zeigt die Firmware-Version des aktiven oder primären CMC an.
Letzte Aktualisierung der Firmware	Zeigt an, wann die Firmware das letzte Mal aktualisiert wurde. Wenn noch keine Aktualisierungen ausgeführt wurden, wird für diese Eigenschaft - angezeigt.
Hardwareversion	Zeigt die Hardware-Version des aktiven oder primären CMC an.
MAC-Adresse	Zeigt die MAC-Adresse für den CMC-NIC. Die MAC-Adresse ist eine eindeutig identifizierte Adresse für das Netzwerk des CMC.
IP-Adresse	Zeigt die IP-Adresse des CMC-NIC an.
Gateway	Zeigt das Gateway des CMC-NIC an.
Subnetzmaske	Zeigt die Subnetzmaske des CMC-NIC an.
DHCP (für NIC-IP-Adresse) verwenden	Zeigt an, ob der CMC aktiviert ist, um automatisch eine IP-Adresse vom DHCP-Server (Dynamisches Host-Konfigurationsprotokoll) anzufordern und abzurufen (Ja oder Nein). Die Standardeinstellung für diese Eigenschaft ist Nein.
Primärer DNS-Server	Gibt den Namen des primären?DNS-Servers an.
Alternativer DNS-Server	Gibt den Namen des Ersatz-DNS-Servers an.
DHCP für den DNS-Domänennamen verwenden	Signalisiert die Verwendung des DHCP an, um den DND-Domainnamen zu erhalten (Ja, Nein).
DNS-Domänenname	Enthält den DNS-Domänennamen.
Informationen zum Standby-CMC	
Vorhanden	Zeigt an (Ja, Nein), ob ein zweiter CMC (Standby-CMC) installiert ist.
Standby-Firmware-Version	Zeigt die auf dem Standby-CMC installierte CMC-Firmware-Version an.

Bauteil	Beschreibung
Vorhanden	Zeigt an, ob das iKVM-Modul vorhanden ist (Ja oder Nein).
Name	Zeigt den Namen des iKVM-Moduls an. Der Name identifiziert das iKVM-Modul im Netzwerk.
Hersteller	Zeigt das iKVM-Modell oder den Hersteller an.
Teilenummer	Zeigt die Teilenummer des iKVM an. Die Teilenummer ist eine vom Hersteller eindeutig identifizierbare Nummer. Die Namenskonventionen von Teilenummern sind von Hersteller zu Hersteller unterschiedlich.
Firmware-Version	Zeigt die iKVM-Firmware-Version an.
Hardwareversion	Zeigt die iKVM-Hardware-Version an.

Stromstatus	Zeigt den iKVM-Stromstatus an: Ein, Aus, - (Nicht vorhanden).
Frontblenden-USB/Video aktiviert	Gibt an, ob der Fronblendenbildschirm und die USB-Anschlüsse aktiviert sind (Ja oder Nein).
Wählen Sie die Option 'Allow access to CMC CLI from iKVM' (Zugriff auf CMC-Befehlszeilenschnittstelle über iKVM zulassen).	Gibt an, dass CLI-Zugriff auf dem iKVM aktiviert ist (Ja oder Nein).

Bauteil	Beschreibung
Standort	Zeigt den von den E/A-Modulen belegten Steckplatz an. Es gibt sechs Steckplätze, die nach Gruppennamen (A, B oder C) und Steckplatznummer (1 oder 2) benannt sind. Steckplatznamen: A-1, A-2, B-1, B-2, C-1 oder C-2.
Vorhanden	Zeigt an, ob das EAM vorhanden ist (Ja oder Nein).
Name	Zeigt den Namen des EAM an.
Architektur	Zeigt die Architektur an.
Stromstatus	Zeigt den Stromstatus des EAMs an: Ein, Aus oder - (Nicht vorhanden).
Service-Tag-Nummer	Zeigt die Service-Tag-Nummer des EAMs an. Die Service-Tag-Nummer ist eine vom Hersteller eindeutig identifizierbare Nummer für Support und Wartung.

RACADM verwenden

1. Öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC und melden Sie sich an.
2. Um Gehäuse- und CMC-Zusammenfassungen anzuzeigen, geben Sie Folgendes ein:

```
racadm getsysinfo
```

Um die iKVM-Zusammenfassung anzuzeigen, geben Sie Folgendes ein:

```
racadm getkvminfo
```

Um die EAM-Zusammenfassung anzuzeigen, geben Sie Folgendes ein:

```
racadm getioinfo
```

Gehäuse- und Komponenten-Funktionszustand anzeigen

Webschnittstelle verwenden

So zeigen Sie Zusammenfassungen zum Gehäuse und zum Komponenten-Funktionszustand an:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf Chassis (Gehäuse). Die Seite Gehäusestatus wird angezeigt.

Der Abschnitt Gehäuse-Grafiken bietet eine grafische Darstellung der Gehäusevorder- und -rückseite. Die grafische Darstellung bietet einen visuellen Überblick über die im Gehäuse installierten Komponenten und deren Funktionszustand.

Jede Grafik zeigt eine Echtzeit-Darstellung der installierten Komponente. Der Komponentenzustand wird durch die Farbe in der Komponentengrafik angezeigt.

- Grün - Das Bauteil wird erkannt, mit Strom versorgt und kommuniziert mit dem CMC; es gibt keine Anzeichen eines ungünstigen Zustands.
- Bernstein - Das Bauteil wird erkannt, wird oder wird nicht mit Strom versorgt oder kommuniziert oder kommuniziert nicht mit dem CMC; ein

ungünstiger Zustand könnte vorhanden sein.

- Grau - Das Bauteil wird erkannt und nicht mit Strom versorgt. Es kommuniziert nicht mit dem CMC und es gibt keine Anzeichen eines ungünstigen Zustands.

Alle Bauteile zeigen einen entsprechenden Texthinweis oder Bildschirmtipp, wenn die Maus über die Komponentengrafik bewegt wird. Der Komponentenstatus wird dynamisch aktualisiert und die Farben der Komponentengrafiken und die Texthinweise werden automatisch zu Darstellung des aktuellen Status geändert.

Die Komponentenuntergrafik ist auch mit der entsprechenden Seite der CMC-GUI verknüpft, um sofort die Navigation zur Statusseite für die jeweilige Komponente zu ermöglichen.

Der Abschnitt Komponenten-Funktionszustand zeigt den Status für jede Komponente mit einem Symbol an. Tabelle 11-7 liefert Beschreibungen für jedes Symbol.

Tabelle 11-8. Hardwareprotokollinformationen

Bauteil	Beschreibung	
	OK	Zeigt an, dass die Komponente vorhanden ist und mit der CMC kommuniziert.
	Zur Information	Zeigt Informationen über die Komponente an, wenn keine Änderung des Funktionszustands vorliegt.
	Warnung	Zeigt an, dass Warnungen ausgegeben wurden und Korrekturmaßnahmen ergriffen werden müssen. Wenn keine Korrekturmaßnahmen innerhalb der vom Administrator festgelegten Zeit ergriffen werden, kann dies zum Ausfall der Komponente, zu Kommunikationsfehlern zwischen der Komponente und dem CMC und zu kritischen oder schwerwiegenden Fehlern führen, die Auswirkungen auf die Integrität des Gehäuses haben können.
	Schwerwiegend	Zeigt an, dass mindestens eine Fehlerwarnung ausgegeben wurde. Dies bedeutet, dass der CMC weiterhin mit der Komponente kommunizieren kann und der angegebene Funktionszustand kritisch ist. Es müssen sofort Korrekturmaßnahmen ergriffen werden. Geschieht dies nicht, kann dies dazu führen, dass die Komponente ausfällt oder die Kommunikation mit dem CMC abgebrochen wird.
	Unknown (Unbekannt)	Zeigt den Zeitpunkt an, zu dem das Gehäuse erstmalig eingeschaltet wurde. Die Komponenten des Gehäuseswerden zunächst immer als "unbekannt" angezeigt, bis sie vollständig hochgefahren sind.
	Kein Wert	Zeigt an, dass die Komponente am Steckplatz nicht vorhanden ist oder der CMC nicht mit der Komponente kommunizieren kann. **ANMERKUNG:** Es ist nicht möglich, dass das Gehäuse nicht vorhanden ist.

RACADM verwenden

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

```
racadm getmodinfo
```

Ereignisprotokolle anzeigen

Die Seiten **Hardwareprotokoll und CMC-Protokoll** zeigen systemkritische Ereignisse auf dem verwalteten System an.

Hardwareprotokoll anzeigen

Der CMC erstellt ein Hardwareprotokoll von Ereignissen, die im Gehäuse auftreten. Sie können das Hardwareprotokoll über die Webschnittstelle und Remote-RACADM anzeigen.

ANMERKUNG: Um das Hardwareprotokoll zu löschen, müssen Sie die Berechtigung als Administrator zum Löschen von Protokollen besitzen.

ANMERKUNG: Sie können den CMC so konfigurieren, dass E-Mail- oder SNMP- Traps gesendet werden, wenn bestimmte Ereignisse auftreten. Informationen zur Konfiguration des CMC zum Aussenden von Warnungen finden Sie unter "Konfiguration von SNMP-Alarmen" und "Konfiguration von E-Mail-Alarmen".

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

(Kritisches Systemsoftwareereignis: Redundanz verloren

Mittwoch, 09. Mai15:26:28 2007 normales Systemsoftwareereignis: Löschen des Protokolls wurde bestätigt

Mittwoch, 09. Mai16:06:00 2007 Systemsoftwareereignis Warnmeldung: vorhergesagter Fehler wurde bestätigt

Mittwoch, 09. Mai15:26:31 2007 kritisches Systemsoftwareereignis: Protokoll voll wurde bestätigt

Mittwoch, 09. Mai15:47:23 2007 unbekanntes Systemsoftwareereignis: unbekanntes Ereignis)
```

Webschnittstelle verwenden

Sie können das Hardwareprotokoll in der CMC-Webschnittstelle anzeigen oder löschen oder davon eine Textdateiversion speichern.

Tabelle 11-8 enthält Beschreibungen der Informationen, die auf der Seite Hardwareprotokoll in der CMC-Webschnittstelle angezeigt werden.

So zeigen Sie das Hardwareprotokoll an:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf Chassis (Gehäuse).
3. Klicken Sie auf das Register Protokolle.
4. Klicken Sie auf das Unterregister Hardwareprotokoll. Die Seite Hardwareprotokoll wird angezeigt.

So speichern Sie eine Kopie des Hardwareprotokolls auf der verwalteten Station oder im Netzwerk:

Klicken Sie Protokoll speichern. Ein Dialogfeld öffnet sich; wählen Sie einen Speicherort für eine Textdatei des Protokolls aus.

ANMERKUNG: Weil das Protokoll als Textdatei gespeichert wurde, werden die Grafiken, die zur Kennzeichnung des Schweregrads in der Benutzeroberfläche verwendet werden, nicht angezeigt. In der Textdatei wird der Schweregrad mit den Worten OK, Zur Information, Unbekannt, Warnung und Schwerwiegend angezeigt.
Die Einträge von Datum und Uhrzeit werden in aufsteigender Reihenfolge angezeigt. Wenn <SYSTEMSTART> in der Spalte Datum/Uhrzeit erscheint, bedeutet dies, dass das Ereignis während des Herunterfahrens oder Starts eines Moduls aufgetreten ist, wenn weder Datum noch Uhrzeit verfügbar sind.

So löschen Sie das Hardwareprotokoll:

Klicken Sie auf Protokoll löschen.

ANMERKUNG: Der CMC erstellt einen neuen Protokolleintrag, der darauf hinweist, dass das Protokoll gelöscht wurde.

Bauteil	Beschreibung		
Schweregrad		OK	Zeigt ein normales Ereignis an, das keine Korrekturmaßnahmen erfordert.
		Zur Information	Zeigt einen Eintrag über ein Ereignis zur Information an, in dem der Schweregradstatus nicht verändert wurde.
		Unknown (Unbekannt)	Zeigt ein nicht-kritisches Ereignis an, bei dem demnächst Korrekturmaßnahmen vorgenommen werden sollten, um Systemfehler zu vermeiden.
		Warnung	Zeigt ein kritisches Ereignis an, das umgehend Korrekturmaßnahmen erfordert, um Systemfehler zu vermeiden.
		Schwerwiegend	Zeigt ein kritisches Ereignis an, das umgehend Korrekturmaßnahmen erfordert, um Systemfehler zu vermeiden.
Uhrzeit/Datum	Gibt das genaue Datum und die genaue Uhrzeit an, als das Ereignis eingetreten ist (z. B. Wed May 02 16:26:55 2007). Wenn Datum/Uhrzeit nicht angezeigt wird, ist das Ereignis zum Zeitpunkt des Systemstarts aufgetreten.		
Beschreibung	Liefert eine kurze Ereignisbeschreibung, erstellt vom CMC (zum Beispiel, Redundanz verloren, Server eingesetzt).		

RACADM verwenden

1. Öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC und melden Sie sich an.
2. Um das Hardwareprotokoll anzuzeigen, geben Sie Folgendes ein:

```
racadm getsel
```

Um das Hardwareprotokoll zu löschen, geben Sie Folgendes ein:

```
racadm clrsel
```

CMC-Protokoll anzeigen

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

ANMERKUNG: Um das Hardwareprotokoll zu löschen, müssen Sie die Berechtigung als Administrator zum Löschen von Protokollen besitzen.

Webschnittstelle verwenden

Sie können eine Textdateiversion des CMC-Protokolls anzeigen, speichern und über die CMC-Webschnittstelle löschen.

Sie können die Protokolleinträge nach Quelle, Datum/Uhrzeit oder Beschreibung neu sortieren, indem Sie auf die Spaltenüberschrift klicken. Wenn Sie erneut auf eine Spaltenüberschrift klicken, wird die Sortierung rückgängig gemacht.

Tabelle 11-9 enthält Beschreibungen der Informationen, die auf der Seite CMC-Protokoll in der CMC-Webschnittstelle angezeigt werden.

So zeigen Sie das CMC-Protokoll an:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf Chassis (Gehäuse).
3. Klicken Sie auf das Register Protokolle.
4. Klicken Sie auf das Unterregister CMC-Protokoll. Die Seite CMC- Protokoll wird angezeigt.

Um eine Kopie des CMC-Protokolls auf der verwalteten Station oder im Netzwerk zu speichern, klicken Sie auf Protokoll speichern. Ein Dialogfeld öffnet sich; wählen Sie einen Speicherort für eine Textdatei des Protokolls aus.

Tabelle 11-9. CMC-Protokollinformationen

Befehl	Ergebnis
Quelle	Zeigt die Benutzeroberfläche (wie z. B. den CMC), die zu dem Ereignis geführt hat.
Uhrzeit/Datum	Gibt das genaue Datum und die genaue Uhrzeit an, als das Ereignis eingetreten ist (z. B. Wed May 02 16:26:55 2007).
Beschreibung	Umfasst eine kurze Beschreibung der Maßnahme, wie Anmeldung oder Abmeldung, Fehler bei der Anmeldung oder Löschen der Protokolle. Beschreibungen werden vom CMC erstellt.

RACADM verwenden

1. Öffnen Sie eine serielle, Telnet- oder SSH-Textkonsole für den CMC und melden Sie sich an.
2. Um das Hardwareprotokoll anzuzeigen, geben Sie Folgendes ein:

```
racadm getraclog
```

Um das Hardwareprotokoll zu löschen, geben Sie Folgendes ein:

```
racadm clrraclog
```

Firmware-Update Fehlermeldungen

Das CMC-Protokoll kann auch Fehlercodes als Teil der Protokollinformationen anzeigen. Die untenstehende Tabelle enthält die CMC-Protokoll-Fehlercodes des Firmware-Aktualisierungen.

Tabelle 11-10. Firmware-Update Fehlermeldungen

Fehlerklasse	Fehlerwert (Hex)	Fehlerwert (Dezimal)
ERR_NO_PRIVILEGE	0x1400	5120
ERR_LOC_CMC_STATE	0x1401	5121
ERR_INV_TARG_LINK	0x1402	5122
ERR_ILLEGAL_CMC_STATE	0x1403	5123
ERR_MX_NULL_PARAM	0x1404	5124
ERR_CLASS_UNSUPPORTED	0x1405	5125
ERR_INAPPROPRIATE_REQUEST	0x1406	5126

ERR_MX_BAD_PARAM	0x1407	5127
ERR_INVALID_TARGET	0x1408	5128
ERR_URL_NOT_FOUND	0x1409	5129
ERR_CANCEL_PID_KILL	0x140A	5130
ERR_REROUTE_PEER	0x140B	5131
ERR_BAD_URL	0x140C	5132
ERR_PAYLOAD_TOO_BIG	0x140D	5133
ERR_BAD_IP_CONV	0X140E	5134
ERR_BAD_HDR_PARAM	0x140F	5135
ERR_BAD_FILENAME	0x1410	5136
ERR_TARGET_NOT_READY	0x1411	5137
ERR_TFTP_GET_FAIL	0x1412	5138
ERR_WAITPID_FAIL	0x1413	5139
ERR_REBOOT_FAIL	0x1414	5140
ERR_UNSUPPORTED_PROTOCOL	0x1415	5141
BAD_FTP_PASSWORD	0x1416	5142
ERR_FORK_FAILED	0x1417	5143
ERR_MALLOC_ERROR	0x1418	5144
ERR_PEER_ABSENT	0x1419	5145
ERR_UPDATE_FAIL	0x141A	5146
ERR_OPEN_FILE_FAIL	0x141B	5147
ERR_IMAGE_FILE_NOT_ACCESSIBLE	0x141C	5148
ERR_FCNTL_GET_FAIL	0x141D	5149
ERR_FCNTL_SET_FAIL	0x141E	5150
ERR_POLL_FAIL	0x141F	5151
ERR_SEND_FAIL	0x1420	5152
ERR_CONNECT_FAIL	0x1421	5153
ERR_SOCKET_FAIL	0x1422	5154
ERR_RESOLVE_REMOTE_IP_ADDR_FAIL	0x1423	5155
ERR_TIMEOUT	0x1424	5156
ERR_RECV_FAIL	0x1425	5157
ERR_INVENTORY_COUNT	0x1426	5158
ERR_FWUPD_INIT_CALL	0x1427	5159
ERR_FWUPD_START_UPDATE_CALL	0x1428	5160
ERR_OP_NOT_CANCELABLE	0x1429	5161
BAD_FTP_USERNAME	0x142A	5162
DEVICE_NOT_AVAILABLE	0x142B	5163

Diagnosekonsole verwenden

Über die Seite Diagnosekonsole kann ein fortgeschrittener Benutzer oder ein Benutzer unter der Leitung des technischen Supports mithilfe von CLI-Befehlen Probleme diagnostizieren, die mit der Gehäusehardware in Beziehung stehen.

ANMERKUNG: Zum Modifizieren dieser Einstellungen müssen Sie die Berechtigung als Administrator zum Ausführen von Debug-Befehlen besitzen.

So greifen Sie auf die Seite Diagnosekonsole zu:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf Chassis (Gehäuse).
3. Klicken Sie auf das Register Fehlerbehebung.
4. Klicken Sie auf das Unterregister Diagnose. Die Seite Diagnosekonsole wird angezeigt.

Sie führen einen Diagnose-CLI-Befehl aus, indem Sie den Befehl in das Feld RACADM-Befehl eingeben tippen und dann auf Senden klicken, um den Diagnosebefehl auszuführen. Es wird eine Seite mit Diagnoseergebnissen
eingeblendet.

Klicken Sie zum Zurückkehren auf die Seite Diagnosekonsole auf Zurück zur Seite Diagnosekonsole oder Aktualisieren.

Die Diagnosekonsole unterstützt die Befehle, die in Tabelle 11-11 aufgelistet sind sowie die RACADM-Befehle.

Tabelle 11-11. Unterstützte Diagnosebefehle

Befehl	Ergebnis
arp	Zeigt den Inhalt der Tabelle des Adressauflösungsprotokolls (ARP) an. ARP-Einträge dürfen nicht hinzugefügt oder gelöscht werden.
ifconfig	Zeigt den Inhalt der Netzwerkschnittstellentabelle an.
netstat	Druckt den Inhalt der Routing-Tabelle aus.
ping *<IP-Adresse>*	Überprüft, ob die Ziel-*<IP-Adresse>* unter Verwendung des Inhalts der aktuellen Routingtabelle vom CMC aus erreichbar ist. In das Feld rechts neben dieser Option muss eine Ziel-IP-Adresse eingegeben werden. Ein ICMP-Echo-Paket (Internet-Steuerungsmeldungsprotokoll) wird basierend auf dem aktuellen Inhalt der Routingtabelle zur Ziel-IP-Adresse gesendet.
gettracelog	Zeigt das Ablaufverfolgungsprotokoll an (Anzeige des Protokolls kann einige Sekunden in Anspruch nehmen). Der Befehl gettracelog -i gibt die Anzahl der Einträge im Ablaufverfolgungsprotokoll zurück. **ANMERKUNG:** Weitere Informationen über den gettracelog- Befehl finden Sie im Abschnitt "gettracelog" im Dell Chassis Management Controller Administrator-Referenzhandbuch.

Komponenten zurücksetzen

Auf der Seite Komponenten zurücksetzen können Benutzer den aktiven CMC zurücksetzen oder Server virtuell neu einsetzen, wodurch ein Entfernen und Wiedereinsetzen der entsprechenden Server simuliert wird. Falls das Gehäuse einen Standby-CMC aufweist, bewirkt das Zurücksetzen des aktiven CMC einen Failover und der Standby-CMC wird aktiviert.

ANMERKUNG: Zum Zurücksetzen von Komponenten müssen Sie die Berechtigung als Debug-Befehl-Administrator besitzen.

So greifen Sie auf die Seite Diagnosekonsole zu:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf Chassis (Gehäuse).
3. Klicken Sie auf das Register Fehlerbehebung.
4. Klicken Sie auf die Unterregisterkarte Komponenten zurücksetzen. Die Seite Komponenten zurücksetzen wird angezeigt. Der Abschnitt CMC-Zusammenfassung auf der Seite Komponenten zurücksetzen zeigt die folgenden Informationen an:

Attribut	Beschreibung		
Funktionszustand		OK	Der CMC ist vorhanden und kommuniziert mit seinen Komponenten.
		Zur Information	Zeigt Informationen über den CMC an, wenn beim Funktionsstatus (OK, Warnung, Schwerwiegend) keine Änderung eingetreten ist.
		Warnung	Warnungsereignisse wurden ausgestellt und Korrekturmaßnahmen müssen ergriffen werden. Wenn innerhalb des vom Administrator festgelegten Zeitraums keine Korrekturmaßnahmen vorgenommen werden, könnten kritische oder schwerwiegende Fehler auftreten, die sich wiederum auf die Integrität des CMC auswirken können.
		Schwerwiegend	Mindestens eine Fehlerwarnung wurde ausgegeben. Ein schwerwiegender Status repräsentiert einen CMC-Systemfehler. Es müssen umgehend Korrekturmaßnahmen getroffen werden.
Uhrzeit/Datum	Zeigt das Datum und die Uhrzeit für den CMC unter Verwendung des Formats MM/TT/JJJJ, wobei MM der Monat, DD der Tag und JJJJ das Jahr ist.		
Aktive CMC-Position	Zeigt die Position des primären CMCs an.		
Redundanz-Modus	Zeigt Redundant an, wenn ein Standby-CMC im Gehäuse vorhanden ist und zeigt Keine Redundanz an, wenn kein Standby-CMC im Gehäuse vorhanden ist.		

5. Der Abschnitt Virtuelles Neueinsetzen von Servern auf der Seite Komponenten zurücksetzen zeigt die folgenden Informationen an:

Attribut	Beschreibung		
Steckplatz	Zeigt den vom Server im Gehäuse besetzten Steckplatz an. Steckplatznummern sind sequenzielle IDs, von 1 bis 16, die bei der Identifizierung der Position des Servers im Gehäuse hilfreich sind.		
Name	Zeigt den Namen des Servers in jedem Steckplatz an.		
Vorhanden	Zeigt an, ob der Server im Steckplatz vorhanden ist (Ja oder Nein).		
Funktionszustand		OK	Der Server ist vorhanden und kommuniziert mit dem CMC. Im Falle eines Fehlers bei der Datenübertragung zwischen dem CMC und dem Server kann der CMC den Funktionszustand des Servers weder abrufen noch anzeigen.
		Zur Information	Zeigt Informationen über den Server an, wenn beim Funktionsstatus (OK, Warnung, Schwerwiegend) keine Änderung eingetreten ist.
		Warnung	Warnungsereignisse wurden ausgestellt und Korrekturmaßnahmen müssen ergriffen werden. Wenn innerhalb des vom Administrator festgelegten Zeitraums keine Korrekturmaßnahmen vorgenommen werden, könnten kritische oder schwerwiegende Fehler auftreten, die sich wiederum auf die Integrität des Servers auswirken können.
		Schwerwiegend	Mindestens eine Fehlerwarnung wurde ausgegeben. Ein schwerwiegender Status repräsentiert einen CMC-Systemfehler. Es müssen umgehend Korrekturmaßnahmen getroffen werden.
iDRAC-Status	Zeigt den Status des durch den Server-iDRAC eingebetteten Verwaltungscontrollers an: • K. A - Server ist nicht vorhanden oder das Gehäuse ist nicht eingeschaltet. • Bereit - iDRAC ist bereit und funktioniert normal. • Beschädigt - iDRAC-Firmware ist beschädigt. Verwenden Sie das iDRAC-Firmware-Aktualisierungsdienstprogramm, um die Firmware zu reparieren. • Fehlgeschlagen - Kann nicht mit iDRAC kommunizieren. Verwenden Sie das Kontrollkästchen Virtuelles Neueinsetzen, um den Fehler zu beseitigen. Falls dies fehlschlägt, entfernen Sie den Server manuell und setzen Sie ihn wieder ein, um den Fehler zu beseitigen. • FW-Aktualisierung - iDRAC-Firmware-Aktualisierung läuft; warten Sie, bis die Aktualisierung beendet ist, bevor Sie eine weitere Aktion starten. • Initialisierung - iDRAC-Rücksetzung läuft; warten Sie, bis der Controller den Einschaltvorgang abgeschlossen hat, bevor Sie eine weitere Aktion starten.		
Stromzustand	Zeigt den Serverstromstatus an: • - - Der CMC hat die Stromversorgung des Servers nicht bestimmt. • Aus - Der Server oder das Gehäuse ist ausgeschaltet. • Ein - Das Gehäuse und der Server sind eingeschaltet. • Einschalten - vorübergehender Zustand zwischen Aus und Ein. Wenn der Einschaltvorgang abgeschlossen ist, ändert sich der Stromzustand zu EIN. • Ausschalten - vorübergehender Zustand zwischen Ein und Aus. Wenn der Abschaltvorgang abgeschlossen ist, ändert sich der Stromzustand zu AUS.		
Virtuelles Neueinsetzen	Wählen Sie das Kontrollkästchen aus, um diesen Server virtuell neu einzusetzen.		

6. Um einen Server virtuell neu einzusetzen, klicken Sie auf das Kontrollkästchen des neu einzusetzenden Servers und wählen Sie dann Auswahl anwenden. Dieser Vorgang simuliert das Entfernen und Wiedereinsetzen eines Servers.

7. Wählen Sie CMC zurücksetzen/Failover aus, um zu bewirken, dass der aktive CMC zurückgesetzt wird. Wenn ein Standby-CMC vorhanden und ein Gehäuse vollständig redundant ist, tritt ein Failover auf und bewirkt, dass der Standby-CMC aktiv wird.

Fehlerbehebung bei Network Time Protocol (NTP)-Fehlern

Nach der Konfiguration des CMC zur Synchronisierung der Uhr mit einem Remote-Zeitserver über das Netzwerk, kann es 2-3 Minuten dauern, bevor eine Änderung des Datums und der Uhrzeit in Kraft tritt. Falls nach dieser Zeit nach wie vor keine Änderung auftritt, handelt es sich möglicherweise um ein Problem, das untersucht werden muss. Der CMC kann seine Uhr möglicherweise aus verschiedenen Gründen nicht synchronisieren:

- Es könnte ein Problem mit den NTP-Server 1-, NTP-Server 2- und NTP-Server 3-Einstellungen vorliegen.
- Es wurden versehentlich ein ungültiger Hostname oder eine ungültige IP-Adresse eingegeben.
- Es könnte ein Netzwerkverbindungsproblem geben, das verhindert, dass der CMC mit den konfigurierten NTP-Servern kommunizieren kann.
- Es könnte ein DNS-Problem geben, das verhindert, dass NTP-Server-Hostnamen aufgelöst werden können.

Der CMC bietet Hilfsprogramme zur Behebung dieser Fehler, wobei das CMC-Ablaufverfolgungsprotokoll die primäre Quelle für Fehlerbehebungsinformationen ist. Dieses Protokoll enthält eine Fehlermeldung für NTP-bezogene Ausfälle. Wenn der CMC sich nicht mit einem konfigurierten Remote-NTP-Server synchronisieren kann, basiert der CMC sein Timing auf der lokalen Systemuhr.

Wenn der CMC anstatt mit einen Remote-Zeitserver mit der lokalen Systemuhr synchronisiert ist, enthält das Ablaufverfolgungsprotokoll einen Eintrag der folgenden Art:

```
Jan 8 20:02:40 cmc ntpd[1423]: synchronized to LOCAL(0), stratum 10
```

Sie können den ntpd-Status auch prüfen, indem Sie den folgenden racadm-Befehl eingeben:

```
racadm getractime –n
```

Wenn kein '*' bei einem der konfigurierten Server angezeigt wird, ist möglicherweise etwas nicht richtig konfiguriert. Die Ausgabe des obigen Befehls enthält auch detaillierte NTP-Statistikdaten, die bei der Analyse, warum der Server nicht synchronisiert, nützlich sein können. Wenn Sie versuchen, einen NTP-Server zu konfigurieren, der Windows-basiert ist, wird empfohlen, dass Sie den MaxDist-Parameter für ntpd erhöhen. Bevor Sie diesen Parameter ändern, sollten Sie alle möglichen Auswirkungen einer solchen Änderung verstehen, insbesondere weil die Standardeinstellung ausreichend groß sein sollte, um mit den meisten NTP-Servern zu funktionieren. Um den Parameter zu ändern, geben Sie folgenden Befehl ein:

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpMaxDist 32
```

Nach Durchführung der Änderung starten Sie den ntpd neu, indem Sie NTP deaktivieren, 5-10 Sekunden warten und dann NTP wieder aktivieren.

ANMERKUNG: NTP benötigt 3 zusätzliche Minuten, um neu zu synchronisieren.

Um NPT zu deaktivieren, geben Sie Folgendes ein:

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpEnable 0
```

Um NPT zu aktivieren, geben Sie Folgendes ein:

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpEnable 1
```

Wenn Sie der Meinung sind, dass die NTP-Server korrekt konfiguriert sind, und dieser Eintrag ist im Ablaufverfolgungsprotokoll vorhanden, dann ist dies eine Bestätigung, dass der CMC sich nicht mit einem konfigurierten NTP-Server synchronisieren kann.

Es könnte andere NTP-bezogene Ablaufverfolgungsprotokolleinträge geben, die bei der Fehlerbehebung nützlich sein können. Falls es sich eine fehlerhafte Konfiguration einer NTP-Server-IP-Adresse handelt, könnte ein Eintrag der folgenden Art vorhanden sein:

```
Jan 8 19:59:24 cmc ntpd[1423]: Cannot find existing interface for address 1.2.3.4 Jan 8 19:59:24 cmc ntpd[1423]: configuration of 1.2.3.4 failed
```

Fall 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
```

Informationen zur Eingabe des Befehls gettracelog zur Prüfung des Ablaufverfolgungsprotokolls unter Verwendung der CMC-GUI finden Sie unter "Diagnosekonsole verwenden".

LED-Farben und Blinkmuster interpretieren

Die LEDs am Gehäuse liefern Informationen anhand der Farbe und durch Blinken bzw. nicht Blinken:

- Beständig grün leuchtende LEDs zeigen an, dass die Komponente eingeschaltet ist. Wenn die grüne LED blinkt, weist dies auf ein kritisches, jedoch routinemäßiges Ereignis hin, wie z. B. das Hochladen von Firmware, währenddessen die Einheit nicht betriebsbereit ist. Dies zeigt keinen Fehler an.
- Eine blinkende gelbe LED an einem Modul weist auf einen Fehler an diesem Modul hin.
- Blaue, blinkende LEDs können vom Benutzer konfiguriert und zur Identifikation genutzt werden (siehe "LEDs zum Identifizieren von Komponenten im Gehäuse konfigurieren").

Tabelle 11-14 listet die üblichen LED-Muster auf dem Gehäuse auf.

Tabelle 11-14. LED-Farbe und Blinkmuster

Komponente	LED-Farbe, Blinkmuster	Bedeutung
CMC	Grün, beständig leuchtend	Netzstrom eingeschaltet
	Grün, blinkend	Firmware wird hochgeladen
	Grün, dunkel	Ausgeschaltet
	Blau, beständig leuchtend	Übergeordnet/primär
	Blau, blinkend	Vom Benutzer aktivierter Modulidentifikator
	Gelb, beständig leuchtend	Nicht verwendet
	Gelb, blinkend	Fehler
	Blau, dunkel	Untergeordnet/Standby
iKVM	Grün, beständig leuchtend	Netzstrom eingeschaltet
	Grün, blinkend	Firmware wird hochgeladen
	Grün, dunkel	Ausgeschaltet
	Gelb, beständig leuchtend	Nicht verwendet
	Gelb, blinkend	Fehler
	Gelb, dunkel	Kein Fehler
Server	Grün, beständig leuchtend	Netzstrom eingeschaltet
	Grün, blinkend	Firmware wird hochgeladen
	Grün, dunkel	Ausgeschaltet
	Blau, beständig leuchtend	Normal
	Blau, blinkend	Vom Benutzer aktivierter Modulidentifikator
	Gelb, beständig leuchtend	Nicht verwendet
	Gelb, blinkend	Fehler
	Blau, dunkel	Kein Fehler
E/A-Modul (Herkömmlich)	Grün, beständig leuchtend	Netzstrom eingeschaltet
	Grün, blinkend	Firmware wird hochgeladen
	Grün, dunkel	Ausgeschaltet
	Blau, beständig leuchtend	Normal/übergeordneter Stapel
	Blau, blinkend	Vom Benutzer aktivierter Modulidentifikator
	Gelb, beständig leuchtend	Nicht verwendet
	Gelb, blinkend	Fehler
	Blau, dunkel	Kein Fehler/untergeordneter Stapel
E/A-Modul (Passthrough)	Grün, beständig leuchtend	Netzstrom eingeschaltet
	Grün, blinkend	Nicht verwendet
	Grün, dunkel	Ausgeschaltet
	Blau, beständig leuchtend	Normal
	Blau, blinkend	Vom Benutzer aktivierter Modulidentifikator
	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
Netzteileinheit	(Oval) Grün, beständig leuchtend	Wechselstrom OK
	(Oval) Grün, blinkend	Nicht verwendet
	(Oval) Grün, dunkel	Wechselstrom nicht OK
	Gelb, beständig leuchtend	Nicht verwendet
	Gelb, blinkend	Fehler
	Gelb, dunkel	Kein Fehler
	(Kreis) Grün, beständig leuchtend	Gleichstrom OK
	(Kreis) Grün, dunkel	Gleichstrom nicht OK

Fehlerbehebung an einem CMC, der nicht mehr reagiert

ANMERKUNG: Es ist nicht möglich, sich über eine serielle Konsole am Standby- CMC anzumelden.

Wenn Sie sich nicht über eine der Schnittstellen am CMC anmelden können (Webschnittstelle, Telnet, SSH, Remote-RACADM oder seriell), können Sie die Funktionsfähigkeit des CMC durch Beobachtung der LEDs auf dem CMC überprüfen, Wiederherstellungsinformationen über die serielle DB-9-Schnittstelle abrufen oder das CMC-Firmware-Abbild wiederherstellen.

Problem durch Beobachtung der LEDs erkennen

Wenn Sie den CMC von vorne betrachten, so wie er im Gehäuse installiert ist, sehen Sie auf der linken Seite der Karte zwei LEDs.

Obere LED - Die obere grüne LED zeigt die Stromversorgung an. Wenn Sie NICHT an ist:

1. Überprüfen Sie, dass mindestens ein Netzteil mit Netzstrom versorgt wird.
2. Überprüfen Sie, dass die CMC-Karte korrekt sitzt. Sie können die Entriegelung betätigen, den CMC entfernen, den CMC neu installieren und darauf achten, dass die Platine vollständig eingeschoben ist und der Riegel richtig einrastet.

Untere LED - Die untere LED ist mehrfarbig. Wenn der CMC aktiv ist und ausgeführt wird und keine Probleme vorliegen, leuchtet die untere LED blau. Wenn die LED gelb leuchtet, wurde ein Fehler erkannt. Der Fehler kann durch jedes der drei folgenden Ereignisse verursacht worden sein:

- Kernfehler. In diesem Fall muss die CMC-Platine ausgetauscht werden.
- Selbsttestfehler. In diesem Fall muss die CMC-Platine ausgetauscht werden.
- Beschädigung des Image. In diesem Fall können Sie den CMC durch Hochladen des CMC-Firmware-Image wiederherstellen.

ANMERKUNG: Ein normaler CMC-Start/Reset dauert länger als eine Minute, um das Betriebssystem vollständig hochzufahren und zur Anmeldung verfügbar zu sein. Die blaue LED ist auf dem aktiven CMC aktiviert. In einer redundanten Konfiguration mit zwei CMCs ist nur die obere grüne LED auf dem Standby-CMC aktiviert.

Wiederherstellungsinformationen über die serielle DB-9-Schnittstelle abrufen

Wenn die untere LED gelb leuchtet, sollten über die serielle DB-9-Schnittstelle, die sich an der Vorderseite des CMC befindet, Wiederherstellungsinformationen verfügbar sein.

So rufen Sie Wiederherstellungsinformationen ab:

1. Installieren Sie ein NULL-Modemkabel zwischen dem CMC und dem Client-Computer.
2. Öffnen Sie einen Terminalemulator Ihrer Wahl (wie z. B. HyperTerminal oder Minicom). Stellen Sie Folgendes ein: 8 Bit, keine Parität, keine Ablaufsteuerung, Baudrate 115200.

   Bei einem Kernspeicherfehler wird alle 5 Sekunden eine Fehlermeldung angezeigt.
3. Drücken Sie die Eingabetaste. Wenn die Eingabeaufforderung Wiederherstellung angezeigt wird, stehen zusätzliche Informationen zur Verfügung. Die Eingabeaufforderung zeigt die CMC-Steckplatznummer und den Fehlertyp an.

Um die Ursache des Fehlers und die Syntax für einige Befehle anzuzeigen, geben Sie Folgendes ein:

```
recover
```

Drücken Sie dann auf <Eingabe>. Beispiele von Eingabeaufforderungen:

```
recover1[self test] CMC 1 Selbsttestfehler
```

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

- Wenn die Eingabeaufforderung auf einen Selbsttestfehler hinweist, befinden sich keine betriebsfähigen Komponenten auf dem CMC. Der CMC ist unbrauchbar und muss zu Dell zurückgeschickt werden.
- Wenn die Eingabeaufforderung Beschädigte Firmware-Images anzeigt, folgen Sie den Schritten unter "Firmware-Image wiederherstellen", um das Problem zu beheben.

Firmware-Image wiederherstellen

Der CMC geht in den Wiederherstellungsmodus über, wenn ein normaler Start des CMC-Betriebssystems nicht möglich ist. Im Wiederherstellungsmodus steht ein kleiner Teilsatz an Befehlen zur Verfügung, mit denen Sie Flash-Geräte durch Hochladen der Firmware-Aktualisierungsdatei **firmimg.cmc** neu programmieren können. Dies ist dieselbe Firmware-Image-Datei, die auch für normale Firmware-Aktualisierungen verwendet wird. Während des Wiederherstellungsvorgangs wird die laufende Aktivität angezeigt. Nachdem der Wiederherstellungsvorgang abgeschlossen wurde, wird das CMC-Betriebssystem gestartet.

Wenn Sie recover eingeben und dann bei der Eingabeaufforderung zur Wiederherstellung auf <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 RJ45 ganz links an.

ANMERKUNG: Im Wiederherstellungsmodus können Sie den CMC normalerweise nicht pingen, da kein aktiver Netzwerkstapel vorhanden ist. Mit dem Befehl recover ping <TFTP-Server-IP> können Sie den TFTP-Server pingen, um die LAN- Verbindung zu überprüfen. Möglicherweise müssen Sie auf einigen Systemen den Befehl recover reset nach setniccfg verwenden.

Fehlerbehebung bei Netzwerkproblemen

Mit dem internen CMC-Ablaufverfolgungsprotokoll können Sie CMC-Warnmeldungen und den CMC-Netzwerkbetrieb debuggen. Sie können über die CMC-Webschnittstelle (siehe "Diagnosekonsole verwenden") oder RACADM (siehe "RACADM-Befehlszeilenschnittstelle verwenden" und Abschnitt gettracelog-Befehl im *Dell Chassis Management Controller Firmware Version 2.0 Administrator-Referenzhandbuch*) auf das Ablaufverfolgungsprotokoll zugreifen.

Das Ablaufverfolgungsprotokoll verfolgt die folgenden Informationen:

- DHCP - Verfolgt Pakete, die an einen DHCP-Server gesendet und von ihm empfangen werden.
- DDNS - Verfolgt dynamische Aktualisierungsanfragen und Antworten des DNS-Servers.
- Konfigurationsänderungen an den Netzwerkschnittstellen.

Das Verlaufsprotokoll kann auch spezifische Fehlercodes der CMC-Firmware enthalten, die sich auf die interne CMC-Firmware beziehen und nicht auf das Betriebssystem des verwalteten Systems.

Deaktivieren eines verlorenen Kennworts

VORSICHTSHINWEIS: Viele Reparaturarbeiten dürfen nur von qualifizierten Servicetechnikern durchgeführt werden. Fehlerbehebungsmaßnahmen oder einfache Reparaturen sollten Sie nur dann selbst übernehmen, wenn dies mit der Produktdokumentation im Einklang steht oder Sie vom Team des Online- oder Telefonsupports dazu aufgefordert werden. Schäden durch nicht von Dell genehmigte Wartungsversuche werden nicht durch die Garantie abgedeckt. Lesen und befolgen Sie die zusammen mit dem Produkt gelieferten Sicherheitshinweise.

Um Verwaltungsvorgänge auszuführen, benötigt der Benutzer Administrator-Rechte. Die CMC-Software hat eine Benutzerkonten-Passwortschutzfunktion, die deaktiviert werden kann, wenn das Administratorkennwort vergessen wurde,. Wenn das Administratorkennwort vergessen wurde, kann es mit Hilfe des PASSWORD_RSET-Jumpers auf dem der CMC-Platine wiederhergestellt werden.

Die CMC-Platine hat einen zwei-Pin-Reset-Jumper, wie unter Abbildung 11-1 gezeigt. Wird ein Jumper auf den Reset-Kontakt gesteckt, werden das Standardadministratorkonto und -passwort aktiviert und auf die voreingestellten Werte Benutzername: root und Passwort:calvin gesetzt. Das Administratorkonto wird ungeachtet dessen, ob das Konto entfernt wurde oder nicht oder ob das Passwort geändert wurde, zurückgesetzt.

ANMERKUNG: Stellen Sie sicher, dass sich das CMC-Modul in einem passiven Modus befindet, bevor Sie beginnen.

1. Drücken Sie die CMC-Freigaberiegel auf dem Handgriff und drehen Sie den Handgriff von der Modulvorderseite weg. Schieben Sie das CMC- Modul aus dem Gehäuse.

ANMERKUNG: Elektrostatische Entladungen (ESD) können elektronische Komponenten im Computer beschädigen. Unter bestimmten Bedingungen baut sich im Körper oder in einem Gegenstand wie einem Peripheriegerät elektrostatische Elektrizität auf; diese entlädt sich dann auf einen anderen Gegenstand, etwa den Computer. Um Beschädigungen durch elektrostatische Entladungen zu vermeiden, sollten Sie die statische Elektrizität Ihres Körpers ableiten, bevor Sie elektronische Komponenten im Innern des Computers berühren.

2. Entfernen Sie den Jumper-Stecker von Passwort-Reset-Kontakt und setzen Sie einen 2-Pin-Jumper zur Aktivierung des Standard-Administrator- Kontos ein. Abbildung 11-1 zeigt die Position des Kennwort-Jumpers auf der CMC-Systemplatine.

Abbildung 11-1. Kennwort-Reset-Jumperposition

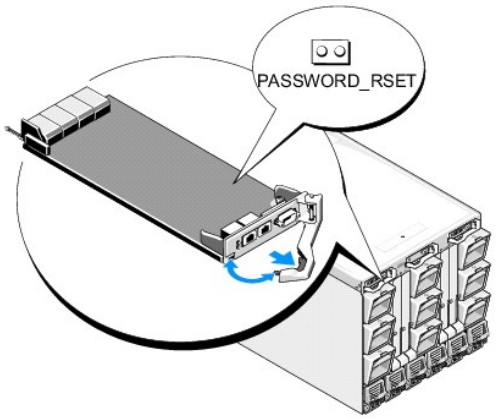


Tabelle 11-15. CMC Kennwort-Jumpereinstellungen

PASSWORD_RSET	(Standardeinstellung)	Die Kennwort-Resetfunktion ist deaktiviert.
		Die Kennwort-Resetfunktion ist deaktiviert.

3. Schieben Sie das CMC-Modul in das Gehäuse. Schließen Sie alle Kabel erneut an, die eventuell abgezogen wurden.
4. Leiten Sie eine Umschaltung ein, um das Modul zu aktivieren, das die grafische Benutzeroberfläche verwendet, um folgende Schritte einzuleiten:
   a. Sie navigieren zur Seite Gehäuse, und klicken auf die Registerkarte Energieverwaltung und dann auf die Unterregisterkarte Steuerung.
   b. Wählen Sie die Schaltfläche Reset CMC (warmer Start).

c. Klicken Sie auf Anwenden.

5. Die CMC wird automatisch auf redundantes Modul umgeschaltet und das Modul wird jetzt aktiv. Melden Sie sich am aktiven CMC mit dem Standard-Administrator-Benutzernamen, root,und dem Kennwort calvin an und stellen Sie sämtliche notwendigen Benutzerkonteneinstellungen wieder her. Die vorhandenen Konten und Kennwörter werden nicht deaktiviert und sind noch immer aktiv.

Nachdem Sie sämtliche Kontenaktualisierungen abgeschlossen haben, entfernen Sie den 2-Pin-Jumper und setzen Sie den Jumper-Stecker wieder auf.

ANMERKUNG: Stellen Sie sicher, dass sich das CMC-Modul in einem passiven Modus befindet, bevor Sie beginnen.

1. Drücken Sie die CMC-Freigaberiegel auf dem Handgriff und drehen Sie den Handgriff von der Modulvorderseite weg. Schieben Sie das CMC- Modul aus dem Gehäuse.
2. Entfernen Sie den 2-Pin-Jumper und setzen Sie den Jumper-Stecker wieder auf.
3. Schieben Sie das CMC-Modul in das Gehäuse. Schließen Sie alle Kabel wieder an, die eventuell getrennt wurden.

Warnmeldungen zur Fehlerbehebung

Verwenden Sie das CMC- und das Verlaufsprotokoll, um CMC-Fehlermeldungen zu behandeln. Der Erfolg oder das Fehlschlagen jedes einzelnen E-Mail- und/oder SNMP-Trap-Sendeversuches wird im CMC-Protokoll gespeichert. Zusätzliche Informationen, die die speziellen Fehler beschreiben, werden im Verlaufsprotokoll mitgespeichert. Da SNMP jedoch die Übergabe von Traps nicht bestätigt, ist es am besten, die Pakete auf dem verwalteten System mit Hilfe eines Netzwerkanalysators oder eines Hilfsprogramms wie **snmputil** von Microsoft zu verfolgen.

Sie können SNMP-Warnungen über die Webschnittstelle konfigurieren. Für weitere Informationen, siehe "Konfiguration von SNMP-Alarmen".

Zurück zum Inhaltsverzeichnis

Zurück zum Inhaltsverzeichnis

CMC-Webschnittstelle verwenden

Dell Chassis Management Controller Firmware Version 2.10, Benutzerhandbuch

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

Sie können auch alle Konfigurations-Aufgaben für die Webschnittstelle mit lokalen RACADM-Befehlen oder Befehlszeilenkonsolen (serielle Konsole, Telnet oder SSH) ausführen. Weitere Informationen zur Verwendung des lokalen RACADM finden Sie unter "RACADM-Befehlszeilenschnittstelle verwenden". Informationen zur Verwendung der Befehlszeilenkonsolen finden Sie unter "CMC zur Verwendung von Befehlszeilenkonsolen konfigurieren".

ANMERKUNG: Wenn Sie den Microsoft® Internet Explorer® verwenden, die Verbindung über einen Proxy herstellen und der Fehler "Die XML-Seite kann nicht angezeigt werden" auftritt, müssen Sie den Proxy deaktivieren, um fortfahren zu können.

Auf die CMC-Webschnittstelle zugreifen

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

1. Öffnen Sie einen unterstützten Webbrowser.

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

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

   `https://<CMC-IP-Adresse>`

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

   `https://<CMC-IP-Adresse>:<Anschlussnummer>`

   wobei <CMC-IP-Adresse> die IP-Adresse des CMC-Moduls und <Anschlussnummer> die Nummer des HTTPS-Ports ist.

   Die CMC-**Anmeldeseite** wird angezeigt.

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

1. Öffnen Sie einen unterstützten Webbrowser.

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

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

   `https://[<CMC-IP-Adresse>]`

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

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

   `https://[<CMC-IP-Adresse]:<Anschlussnummer>`

   wobei *<CMC-IP-Adresse>* die IP-Adresse des CMC-Moduls und *<Anschlussnummer>* die Nummer des HTTPS-Ports ist.

   Die **CMC-Anmeldeseite** wird angezeigt.

Anmeldung

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

ANMERKUNG: Der Standardbenutzername für das CMC-Modul ist **root** und das Standardkennwort ist **calvin**. Das Konto root ist das werkseitig voreingestellte Verwaltungskonto des CMC-Moduls. Um die Sicherheit zu erhöhen, empfiehlt Dell nachdrücklich, das vorgegebene root-Kennwort bei der Ersteinrichtung zu ändern.

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

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

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

So melden Sie sich an:

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

   ANMERKUNG: Dieses Feld unterscheidet Groß- und Kleinschreibung.

2. Geben Sie im Feld Password Ihr CMC-Benutzerkennwort oder Active Directory-Benutzerkennwort ein.

   ANMERKUNG: Dieses Feld unterscheidet Groß- und Kleinschreibung.

3. Klicken Sie auf OK oder drücken Sie die Eingabetaste.

Abmeldung

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

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

CMC-Basiseinstellungen konfigurieren

Einstellung des Gehäusenamens

Sie können den Namen festlegen, der zur Identifizierung des Gehäuses im Netzwerk verwendet wird. (Der Standardname ist "Dell Rack System".) So wird beispielsweise eine SNMP-Abfrage des Gehäusenamens den Namen zurückgeben, den Sie konfiguriert haben.

So legen Sie den Gehäusenamen fest:

1. Melden Sie sich bei der CMC-Webschnittstelle an. Die Seite Komponenten-Funktionszustand wird angezeigt.
2. Klicken Sie auf die Registerkarte Setup. Die Seite Allgemeine Gehäuseeinstellungen wird angezeigt.
3. Geben Sie den neuen Namen in das Feld Gehäusename ein, und klicken Sie dann auf Anwenden.

Datum und Uhrzeit auf dem CMC einstellen

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

1. Melden Sie sich bei der CMC-Webschnittstelle an. Die Seite Komponenten-Funktionszustand wird angezeigt.
2. Klicken Sie auf die Registerkarte Setup. Die Seite Allgemeine Gehäuseeinstellungen wird angezeigt.
3. Klicken Sie auf die Unterregisterkarte Datum/Uhrzeit. Die Seite Datum/Uhrzeit wird angezeigt.
4. Um Datum und Uhrzeit mit einem Network Time Protocol (NTP)-Server zu synchronisieren, markieren Sie NTP aktivieren und geben Sie bis zu drei NTP-Server an.
5. Um Datum und Uhrzeit manuell einzustellen, heben Sie die Markierung von NTP aktivieren auf und editieren Sie die Felder Datum und Uhrzeit, wählen Sie die Zeitzone aus dem Drop-Down-Menü und klicken Sie auf Anwenden.

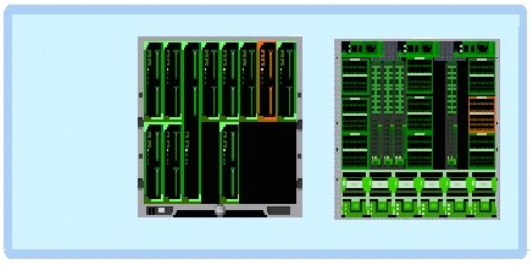
Anleitungen zum Einstellen von Datum und Uhrzeit mit der Befehlszeilenschnittstelle finden Sie in den Abschnitten `config`-Befehl und `cfgRemoteHosts`-Datenbankeigenschaftengruppen im *Dell Chassis Management Controller Administrator-Referenzhandbuch*.

Systemzustand überwachen

Gehäuse- und Komponenten-Zusammenfassungen anzeigen

Der CMC zeigt eine grafische Darstellung des Gehäuses auf der Seite Gehäuse-Grafiken, die Ihnen einen visuellen Überblick über die Status der installierten Komponenten liefert. Die Seite Gehäuse-Grafiken wird dynamisch aktualisiert und die Farben der Komponenten-Untergrafiken und Texthinweise werden automatisch geändert, um den derzeitigen Zustand anzuzeigen.

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



Die Seite Komponentenfunktionszustand enthält den Gesamtfunktionszustand für das Gehäuse, primäre und Standby-CMCs, Servermodule, E/A-Module (EAMs), Lüfter, iKVM, Netzteile und Temperatursensoren. Die Seite Zusammenfassung Gehäuse bietet einen textbasierten Überblick über Gehäuse, Primär- und Stand-by-CMCs, iKVM und EAMs. Für Anleitungen zum Betrachten der Gehäuse- und der Komponentenzusammenfassung, siehe Gehäusezusammenfassungen anzeigen.

Gehäuse- und Komponenten-Funktionszustand anzeigen

Die Seite Gehäuse-Grafiken bietet einen grafischen Überblick der Gehäusevorder- und -rückseite. Die grafische Darstellung bietet einen visuellen Überblick über die im Gehäuse installierten Komponenten und deren Funktionszustand.

Die Seite Komponenten-Funktionszustand bietet einen allgemeinen Überblick zum Funktionszustand aller Gehäusekomponenten. Anleitungen zum Anzeigen der Gehäuse- und Komponenten-Funktionszustände finden Sie unter "Gehäuse- und Komponenten-Funktionszustand anzeigen".

Strombudgetstatus anzeigen

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

Anleitungen zum Anzeigen des Strombudgetstatus finden Sie unter "Anzeige des Stromverbrauchsstatus". Weitere Informationen über die Stromverwaltung des CMC erhalten Sie unter "Stromverwaltung".

Servermodellnamen und Service-Tag-Nummer anzeigen

Man erhält den Modellnamen und die Service-Tag-Nummer der einzelnen Server sofort, indem man die folgenden Schritte ausführt:

- Erweitern Sie die Server in der Systemstruktur. Es werden alle Server (1 - 16) in der erweiterten Liste der Server angezeigt. Namen von Steckplätzen ohne Server sind grau unterlegt.
- Bewegen Sie den Cursor über den Steckplatznamen oder die Steckplatznummer eines Servers; falls verfügbar, wird ein Tooltip mit dem Modellnamen und der Service-Tag-Nummer des Servers angezeigt

Funktionszustand von allen Servern anzeigen

Der Funktionszustand aller Server kann auf zwei Arten eingesehen werden: im Abschnitt Gehäuse-Grafiken auf der Seite Gehäusezustand oder auf der Seite Serverzustand. Gehäuse-Grafiken bietet einen grafischen Überblick über alle im Gehäuse installierten Server.

Um den Funktionszustand aller Server mittels Gehäuse-Grafiken einzusehen:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Die Seite Gehäusezustand wird angezeigt. Die mittlere Sektion der Gehäuse-Grafiken stellt die Vorderansicht des Gehäuses dar und enthält den Funktionszustand aller Server. Der Serverfunktionszustand wird durch die Farbe des Serversymbols angegeben:
   - Grün - Server wird erkannt, mit Strom versorgt und kommuniziert mit dem CMC; es gibt keine Anzeichen eines ungünstigen Zustands.
   - Bernstein - Server wird erkannt, kann jedoch mit Strom versorgt sein, oder nicht, kann mit dem CMC kommunizieren oder nicht; ein ungünstiger Zustand könnte vorhanden sein.
   - Grau - Server wird erkannt und nicht mit Strom versorgt. Es kommuniziert nicht mit dem CMC und es gibt keine Anzeichen eines ungünstigen Zustands.

Die Seite Status der Server enthält Übersichten zu den Servern im Gehäuse.

So zeigen Sie den Funktionszustand von allen Servern an:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur Server aus. Die Seite Servers Status (Serverstatus) wird angezeigt.

Tabelle 5-1 enthält Beschreibungen zu den Informationen auf der Seite Status der Server.

Tabelle 5-1. Informationen zum Status aller Server (fortgesetzt)

Bauteil	Beschreibung		
Steckplatz	Zeigt die Position des Servers an. Die Steckplatznummer ist eine sequenzielle Nummer, die das Servermodul anhand seiner Position im Gehäuse identifiziert.		
Name	Zeigt den Namen des Servers an, der standardmäßig mit dem Steckplatznamen (STECKPLATZ-01 bis STECKPLATZ-16) identifiziert wird. **ANMERKUNG:** Sie können den standardmäßigen Servernamen ändern. Anleitungen hierzu finden Sie unter "Steckplatznamen bearbeiten".		
Model	Zeigt den Namen des Servermodells an. Wenn dieses Feld leer ist, ist der Server nicht vorhanden. Wenn dieses Feld die Erweiterung von # (wobei das Zeichen # für 1 - 8 steht) anzeigt, dann bezeichnet die Nummer (#) den Hauptsteckplatz eines Multi-Steckplatz-Servers.		
Funktionszustand		OK	Zeigt an, dass der Server vorhanden ist und mit dem CMC kommuniziert.
		Zur Information	Zeigt Informationen zum Server an, wenn keine Änderung des Funktionszustands vorliegt.
		Warnung	Zeigt an, dass nur Warnungen ausgegeben wurden und *Korrekturmaßnahmen ergriffen werden müssen.* Wenn innerhalb des vom Administrator festgelegten Zeitraums keine Korrekturmaßnahmen vorgenommen werden, könnten kritische oder schwerwiegende Fehler auftreten, die sich wiederum auf die Integrität des Geräts auswirken können.
		Schwerwiegend	Zeigt an, dass mindestens eine Fehlerwarnung ausgegeben wurde. Ein schwerwiegender Status repräsentiert einen Systemfehler auf dem Server. Es müssen umgehend Korrekturmaßnahmen getroffen werden.
		Kein Wert	Wenn sich kein Server im Steckplatz befindet, werden keine Informationen zum Funktionszustand angezeigt.
iDRAC GUI starten		Klicken Sie mit der linken Maustaste auf das Symbol, um die iDRAC-Verwaltungskonsole für einen Server in einem neuen Fenster oder einer neuen Registerkarte des Browsers zu starten. Dieses Symbol wird nur für einen Server angezeigt, auf den die folgenden Bedingungen zutreffen: 1. Der Server ist vorhanden 2. Das Gehäuse ist eingeschaltet 3. Die LAN-Schnittstelle auf dem Server ist aktiviert **ANMERKUNG:** Wenn der Server vom Gehäuse entfernt wird, die IP-Adresse des iDRAC geändert wird oder die Netzwerkverbindung beim iDRAC Probleme aufweist, wird durch Klicken auf das Symbol iDRAC GUI starten eventuell eine Fehlerseite auf der iDRAC LAN- Schnittstelle angezeigt.		
Stromzustand	Zeigt den Stromstatus des Gehäuses an. - k.A. - Der CMC hat die Stromversorgung des Servers noch nicht bestimmt. - Aus - Entweder der Server oder das Gehäuse sind ausgeschaltet. - Ein - Sowohl Gehäuse, als auch Server sind eingeschaltet. - Einschalten - vorübergehender Zustand zwischen Aus und Ein. Ist der Vorgang erfolgreich abgeschlossen, wird der Stromzustand dann auf Ein stehen. - Ausschalten - vorübergehender Zustand zwischen Ein und Aus. Ist der Vorgang erfolgreich abgeschlossen, wird der Stromzustand dann auf Aus stehen.		
Service-Tag-Nummer	Zeigt die Service-Tag-Nummer des Servers an. Die Service-Tag-Nummer ist eine vom Hersteller eindeutig identifizierbare Nummer im Falle von Fragen und Wartungsdiensten. Wenn kein Server vorhanden ist, ist dieses Feld leer.		

Informationen zum Starten der iDRAC-Verwaltungskonsole und Richtlinien über Einzelanmeldeverfahren finden Sie unter "iDRAC mit Einzelanmeldung starten".

Steckplatznamen bearbeiten

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

- Namen dürfen maximal 15 druckbare ASCII-Zeichen (ASCII-Codes 32 bis 126) enthalten, mit Ausnahme des doppelten Anführungszeichens (", ASCII 34). Wenn Sie einen RACADM-Befehl zum Ändern der Steckplatzbezeichnung mit Spezialzeichen (~!@#$%^&*) verwenden, muss der Stringname in doppelte Anführungszeichen gesetzt werden, damit die Umgebung den Befehl korrekt an den CMC übergeben kann.
- Steckplatznamen müssen innerhalb des Gehäuses eindeutig sein. Derselbe Name darf nicht für einen zweiten Steckplatz verwendet werden.
- Für Zeichenketten wird nicht zwischen Groß- und Kleinschreibung unterschieden. `Server-1`, `server-1` und `SERVER-1` gelten als gleiche Namen.
- Steckplatznamen dürfen nicht mit einer der folgenden Zeichenketten beginnen:
  - `Switch-`
  - `Fan-`

- PS-
- KVM
- DRAC-
- MC-
- Chassis
- Housing-Left
- Housing-Right
- Housing-Center

- Die Zeichenketten Server-1 bis Server-16 können verwendet werden, allerdings nur für den entsprechenden Steckplatz. Z. B. ist Server-3 ein gültiger Name für Steckplatz 3, aber nicht für Steckplatz 4. Beachten Sie, dass Server-03 ein gültiger Namen für einen *beliebigen* Steckplatz ist.

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

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

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

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

So bearbeiten Sie einen Steckplatznamen:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur Server im Menü Gehäuse.
3. Klicken Sie auf die Registerkarte Setup und die Unterregisterkarte Steckplatznamen. Die Seite Steckplatznamen wird angezeigt.
4. Geben Sie den aktualisierten oder neuen Namen eines Steckplatzes in das Feld Steckplatzname ein. Wiederholen Sie diese Maßnahme für jeden Steckplatz, den Sie umbenennen möchten.
5. Klicken Sie auf Anwenden.
6. Um den Standardsteckplatznamen (STECKPLATZ-01 bis STECKPLATZ-16, basierend auf der Position des Serversteckplatzes) zum Server wiederherzustellen, drücken Sie auf Standardwert wiederherstellen.

Festlegen des ersten Startlaufwerks für Server

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

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

Das von Ihnen angegebene Startlaufwerk muss vorhanden sein und einen startfähigen Datenträger enthalten. Tabelle 5-2 listet die Startlaufwerke auf, die sie angeben können.

Tabelle 5-2. Startlaufwerke

Startlaufwerke	Beschreibung
PXE	Start von einem PXE (Preboot Execution Environment)-Protokoll über die Netzwerkschnittstellenkarte.
Festplatte	Start von der Festplatte auf dem Server.
Lokale CD/DVD	Start von einem CD-/DVD-Laufwerk auf dem Server.
Virtuelle Floppy	Start vom virtuellen Diskettenlaufwerk. Das Diskettenlaufwerk (oder ein Disketten-Image) befindet sich auf einem anderen Computer im Verwaltungsnetzwerk und ist mit dem Konsolen-Viewer der iDRAC-GUI verbunden.
Virtuelle CD/DVD	Start von einem virtuellen CD-/DVD-Laufwerk oder CD/-DVD-ISO-Image. Das optische Laufwerk oder die ISO-Image-Datei befindet sich auf einem anderen Computer oder einer anderen Festplatte im Verwaltungsnetzwerk und ist mit dem Konsolen-Viewer der iDRAC-GUI verbunden.
iSCSI	Start von einem iSCSI-Gerät (Internetschnittstelle für kleine Computer).

lokale SD-Karte	Bootvorgang über die lokale SD-Karte (Secure Digital) - nur bei M610/M710/805/M905-Systemen.
Diskette	Start von einer Diskette im lokalen Diskettenlaufwerk.

ANMERKUNG: Um das erste Startlaufwerk für Server festzulegen, müssen Sie die Berechtigung als **Server Administrator** oder Gehäusekonfigurations-Administrator besitzen und auf dem iDRAC angemeldet sein.

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

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf **Servers** (Server), und klicken Sie dann auf **Setup→ Deploy First Boot Device** (Erstes Startgerät einrichten und bereitstellen). Daraufhin wird eine Liste mit Servern (ein Server pro Zeile) angezeigt.
3. Wählen Sie für jeden Server das zu verwendende Startlaufwerk aus der Liste aus.
4. Wenn Sie möchten, dass der Server jedes Mal vom ausgewählten Gerät startet, deaktivieren Sie für den Server das Kontrollkästchen **Einmaliger Start**.

   Wenn der Server beim nächsten Hochfahren einmalig von dem ausgewählten Gerät starten soll, aktivieren Sie das Kontrollkästchen **Einmaliger Start** für den betreffenden Server.
5. Klicken Sie auf **Anwenden**.

Funktionszustand eines einzelnen Servers anzeigen

Der Funktionszustand aller Server kann auf zwei Arten eingesehen werden: im Abschnitt Gehäuse-Grafiken auf der Seite Gehäusezustand oder auf der Seite Serverzustand.

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

Um den Funktionszustand aller Server mittels Gehäuse-Grafiken einzusehen:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Die Seite Gehäusezustand wird angezeigt. Die mittlere Sektion der Gehäuse-Grafiken stellt die Vorderansicht des Gehäuses dar und enthält den Funktionszustand aller Server. Der Serverfunktionszustand wird durch die Farbe des Serversymbols angegeben:
   - Grün - Server wird erkannt, mit Strom versorgt und kommuniziert mit dem CMC; es gibt keine Anzeichen eines ungünstigen Zustands.
   - Bernstein - Server wird erkannt, kann jedoch mit Strom versorgt sein, oder nicht, kann mit dem CMC kommunizieren oder nicht; ein ungünstiger Zustand könnte vorhanden sein.
   - Grau - Server wird erkannt und nicht mit Strom versorgt. Es kommuniziert nicht mit dem CMC und es gibt keine Anzeichen eines ungünstigen Zustands.
3. Bewegen Sie den Cursor über eine einzelne Servergrafik und ein entsprechender Texthinweis oder Bildschirmtipp wird angezeigt. Der Texthinweis liefert zusätzliche Informationen zu dem Server.
4. Die Servergrafik ist mit der entsprechenden Seite im CMC GUI verknüpft, um sofort die Navigation zur Seite Serverstatus für diesen Server zu ermöglichen.

Die Seite Serverstatus (nicht zu verwechseln mit der Seite Status der Server) enthält eine Übersicht des Servers und eine Start-URL der Webschnittstelle für den Integrated Dell Remote Access Controller (iDRAC), also die zum Verwalten des Servers verwendete Firmware.

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

So zeigen Sie den Funktionszustand eines einzelnen Servers an:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Erweitern Sie in der Systemstruktur Server. Es werden alle Server (1–16) in der erweiterten Liste der Server angezeigt.
3. Klicken Sie auf den Server (Steckplatz), den Sie anzeigen möchten. Die Seite Serverstatus wird angezeigt.

Tabelle 5-3 bis Tabelle 5-8 enthalten Erläuterungen zu den Informationen auf der Seite Status der Server.

Tabelle 5-3. Individueller Serverstatus - Eigenschaften

Bauteil	Beschreibung		
Steckplatz	Zeigt den vom Server auf dem Gehäuse besetzten Steckplatz an. Steckplatznummern sind sequenzielle IDs von 1 bis 16 (im Gehäuse befinden sich 16 verfügbare Steckplätze), die hilfreich bei der Identifizierung der Position des Servers im Gehäuse sind.		
Steckplatzname	Zeigt den Namen des Steckplatzes an, in dem sich der Server befindet.		
Vorhanden	Zeigt an, ob der Server im Steckplatz vorhanden ist (Ja oder Nein). Wenn der Server nicht vorhanden ist, sind die Serverinformationen zu Funktionszustand, Stromzustand und Service-Tag-Nummer unbekannt (werden nicht angezeigt).		
Funktionszustand		OK	Zeigt an, dass der Server vorhanden ist und mit dem CMC kommuniziert. Im Falle eines Fehlers bei der Datenübertragung zwischen dem CMC und dem Server kann der CMC den Funktionszustand des Servers weder abrufen noch anzeigen.
		Zur Information	Zeigt Informationen über den Server an, wenn beim Funktionsstatus (OK, Warnung, Schwerwiegend) keine Änderung eingetreten ist.
		Warnung	Zeigt an, dass nur Warnungen ausgegeben wurden und *Korrekturmaßnahmen ergriffen werden müssen.* Wenn innerhalb des vom Administrator festgelegten Zeitraums keine Korrekturmaßnahmen vorgenommen werden, könnten kritische oder schwerwiegende Fehler auftreten, die sich wiederum auf die Integrität des Servers auswirken können.
		Schwerwiegend	Zeigt an, dass mindestens eine Fehlerwarnung ausgegeben wurde. Ein schwerwiegender Status repräsentiert einen Systemfehler auf dem Server. *Es müssen umgehend Korrekturmaßnahmen getroffen werden.*
		Kein Wert	Wenn sich kein Server im Steckplatz befindet, werden keine Informationen zum Funktionszustand angezeigt.
Servermodell	Zeigt das Modell des Servers im Gehäuse an. Beispiele: PowerEdge M600, PowerEdge M605.		
Service-Tag-Nummer	Zeigt die Service-Tag-Nummer des Servers an. Die Service-Tag-Nummer ist eine vom Hersteller eindeutig identifizierbare Nummer im Falle von Fragen und Wartungsdiensten. Wenn kein Server vorhanden ist, ist dieses Feld leer.		
iDRAC Firmware	Zeigt die derzeit auf dem Server installierte iDRAC-Version an.		
CPLD-Version	Zeigt die CPLD-Versionsnummer (Complex Programmable Logic Device) des Servers an.		
BIOS-Version	Zeigt die BIOS-Version auf dem Server an.		
Betriebssystem	Zeigt das Betriebssystem auf dem Server an.		

Tabelle 5-4. Individueller Serverstatus - iDRAC-Systemereignisprotokoll

Bauteil	Beschreibung		
Schweregrad		OK	Zeigt ein normales Ereignis an, das keine Korrekturmaßnahmen erfordert.
		Zur Information	Zeigt einen Informationseintrag über ein Ereignis an, in dem der Schweregradstatus nicht verändert wurde.
		Unknown (Unbekannt)	Zeigt ein unbekanntes/nicht-kategorisiertes Ereignis an.
		Warnung	Zeigt ein nicht-kritisches Ereignis an, bei dem demnächst Korrekturmaßnahmen vorgenommen werden müssen, um Systemfehler zu vermeiden.
		Schwerwiegend	Zeigt ein kritisches Ereignis an, das umgehend Korrekturmaßnahmen erfordert, um Systemfehler zu vermeiden.
Uhrzeit/Datum	Gibt das genaue Datum und die genaue Uhrzeit an, als das Ereignis eingetreten ist (z. B. Wed May 02 16:26:55 2007).		
Beschreibung	Enthält eine kurze Beschreibung des Ereignisses.		

Tabelle 5-5. Individueller Serverstatus - iDRAC-Netzwerkeinstellungen

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

Tabelle 5-6. Individueller Serverstatus - IPv4 iDRAC-Netzwerkeinstellungen

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

Tabelle 5-7. Individueller Serverstatus - IPv6 iDRAC-Netzwerkeinstellungen

Bauteil	Beschreibung
Aktiviert	Zeigt an, ob das IPv6-Protokoll beim LAN verwendet wird (Ja).
AutoConfiguration aktiviert	Zeigt an, ob AutoConfiguration für IPv6 aktiviert ist (Ja). Wenn AutoConfiguration aktiviert ist, ruft der Server die IPv6-Konfiguration (**IPv6-Adresse, Präfixlänge** und **IPv6-Gateway**) automatisch von einem IPv6-Router in Ihrem Netzwerk ab. Der Server verfügt immer über eine eindeutige IPv6-Adresse über Ihr Netzwerk und kann bis zu 16 IPv6-Adressen erhalten.
Lokale Adresse verbinden	Dem CMC zugewiesene IPv6-Adresse, basierend auf der MAC-Adresse des CMC.
Gateway	Zeigt das IPv6-Gateway für die iDRAC-Netzwerkschnittstelle an.
IPv6-Adresse	Zeigt eine IPv6-Adresse für die iDRAC-Netzwerkschnittstelle an. Es können bis zu 16 dieser Adressen bestehen. Die Präfixlänge, falls nicht Null, wird nach dem Schrägstrich ("/") angegeben.

Tabelle 5-8. Individueller Serverstatus - WWN/MAC-Adresse

Bauteil	Beschreibung
Steckplatz	Zeigt den vom Server auf dem Gehäuse besetzten Steckplatz an.
Standort	Zeigt den von den E/A-Modulen besetzen Standort an. Die sechs Standorte werden mit einer Kombination von Gruppenname (A, B oder C) und Steckplatznummer (1 oder 2) identifiziert. Steckplatznamen: A1, A2, B1, B2, C1 oder C2.
Architektur	Zeigt den Typ der E/A-Architektur an.
Server-zugewiesen	Zeigt die dem Server zugewiesenen WWN/MAC-Adressen an, die in die Hardware der Steuerung eingebettet sind. WWN/MAC-Adressen, die - anzeigen, weisen darauf hin, dass keine Schnittstelle für die angegebene Architektur installiert ist.
Gehäuse-zugewiesen	Zeigt die dem Gehäuse zugewiesenen WWN/MAC-Adressen an, die für einen bestimmten Steckplatz verwendet werden. WWN/MAC-Adressen, die - anzeigen, weisen darauf hin, dass die FlexAddress-Funktion nicht installiert ist. **ANMERKUNG:** Ein grünes Häkchen in der Spalte Server-zugewiesen oder Gehäuse-zugewiesen zeigt den Typ der aktiven Adressen an. **ANMERKUNG:** Wenn FlexAddress aktiviert ist, zeigen Steckplätze ohne installierte Server die Gehäuse-zugewiesene MAC/WWN- Zuweisung für die eingebetteten Ethernet-Controller (Architektur A) an. Die Gehäuse-zugewiesenen Adressen für Architekturen B und C zeigen - an, außer wenn diese Architekturen auf Servern mit besetzen Steckplätzen in Verwendung sind; es wird angenommen dass dieselben Architekturtypen in den nicht besetzen Steckplätzen angewendet werden.

Informationen zum Starten der iDRAC-Verwaltungskonsole und Richtlinien über Einzelanmeldeverfahren finden Sie unter "iDRAC mit Einzelanmeldung starten".

Funktionszustand der E/A-Module anzeigen

Der Funktionszustand aller Server kann auf zwei Arten eingesehen werden: im Abschnitt Gehäuse-Grafiken auf der Seite Gehäusezustand oder auf der Seite Serverzustand. Die Seite Gehäuse-Grafiken bietet einen grafischen Überblick über die im Gehäuse installierten EAMs.

Um den Funktionszustand der EAMs mittel Gehäuse-Grafiken anzuzeigen:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Die Seite Gehäusezustand wird angezeigt. Die rechte Sektion der Gehäuse-Grafiken stellt die Rückansicht des Gehäuses dar und enthält den Funktionszustand aller EAMs. Der EAM-Funktionszustand wird durch die Farbe des EAM-Symbols angegeben:
   - Grün - EAM wird erkannt, mit Strom versorgt und kommuniziert mit dem CMC; es gibt keine Anzeichen eines ungünstigen Zustands.
   - Bernstein - EAM wird erkannt, kann jedoch mit Strom versorgt sein, oder nicht, kann mit dem CMC kommunizieren oder nicht; ein ungünstiger Zustand könnte vorhanden sein.
   - Grau - EAM wird erkannt und nicht mit Strom versorgt. Es kommuniziert nicht mit dem CMC und es gibt keine Anzeichen eines ungünstigen Zustands.
3. Bewegen Sie den Cursor über eine einzelne EAM-Grafik und ein entsprechender Texthinweis oder Bildschirmtipp wird angezeigt. Der Texthinweis liefert zusätzliche Informationen zu diesem EAM.
4. Die EAM-Grafik ist mit der entsprechenden Seite im CMC GUI verknüpft, um sofort die Navigation zur Seite Status der E/A-Module für dieses EAM zu ermöglichen.

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

Funktionszustand der Lüfter anzeigen

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

Der Funktionszustand der Lüfter kann auf zwei Arten eingesehen werden: im Abschnitt Gehäuse-Grafiken auf der Seite Gehäusezustand oder auf der Seite Lüfterzustand. Die Seite Gehäuse-Grafiken bietet einen grafischen Überblick über einen einzelnen Server, der im Gehäuse installiert ist. Um den Funktionszustand aller Lüfter mittels Gehäuse-Grafiken einzusehen:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Die Seite Gehäusezustand wird angezeigt. Die rechte Sektion der Gehäuse-Grafiken stellt die Rückansicht des Gehäuses dar und enthält den Funktionszustand aller Lüfter. Der Lüfter-Funktionszustand wird durch die Farbe des Lüfter-Symbols angegeben:
   - Grün - Lüfter wird erkannt, mit Strom versorgt und kommuniziert mit dem CMC; es gibt keine Anzeichen eines ungünstigen Zustands.
   - Bernstein - Lüfter wird erkannt, kann jedoch mit Strom versorgt sein, oder nicht, kann mit dem CMC kommunizieren oder nicht; ein ungünstiger Zustand könnte vorhanden sein.
   - Grau - Lüfter wird erkannt und nicht mit Strom versorgt. Es kommuniziert nicht mit dem CMC und es gibt keine Anzeichen eines ungünstigen Zustands.
3. Bewegen Sie den Cursor über eine einzelne Lüfter-Grafik und ein entsprechender Texthinweis oder Bildschirmtipp wird angezeigt. Der Texthinweis liefert zusätzliche Informationen zu diesem Lüfter.
4. Die Lüftergrafik ist mit der entsprechenden Seite im CMC GUI verknüpft, um sofort die Navigation zur Seite Lüfterstatus zu ermöglichen.

Die Seite Lüfterstatus zeigt die Messwerte für den Status und die Geschwindigkeit (in Umdrehungen pro Minute oder 1/Min.) der Lüfter im Gehäuse an. Es können ein oder mehrere Lüfter vorhanden sein.

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

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

So zeigen Sie den Funktionszustand der Lüftereinheiten an:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur Lüfter aus. Die Seite Status der Lüfter wird angezeigt.

Tabelle 5-9 enthält Beschreibungen zu den Informationen auf der Seite Status der Lüfter.

Tabelle 5-9. Informationen zum Funktionsstatus der Lüfter (fortgesetzt)

Bauteil	Beschreibung		
Name	Zeigt den Lüfternamen im folgenden Format an: FAN-n, wobei n die Nummer des Lüfters darstellt.		
Vorhanden	Zeigt an, ob der Lüfter vorhanden ist (**Ja** oder **Nein**).		
Funktionszustand		OK	Zeigt an, dass die Lüftereinheit vorhanden ist und mit dem CMC kommuniziert. Im Falle eines Fehlers bei der Datenübertragung zwischen dem CMC und der Lüftereinheit kann der CMC den Funktionsstatus der Lüftereinheit weder abrufen noch anzeigen.
		Schwerwiegend	Zeigt an, dass mindestens eine Fehlerwarnung ausgegeben wurde. Ein schwerwiegender Status weist auf einen Systemfehler im Lüftermodul hin, und es müssen sofort Korrekturmaßnahmen ergriffen werden, um ein Überhitzen und Herunterfahren des Systems zu verhindern.
		Unknown (Unbekannt)	Wird angezeigt, wenn das Gehäuse zuerst eingeschaltet wird. Im Falle eines Fehlers bei der Datenübertragung zwischen dem CMC und der Lüftereinheit kann der CMC den Funktionsstatus der Lüftereinheit weder abrufen noch anzeigen.
Taktrate	Zeigt die Geschwindigkeit des Lüfters in 1/Min. an.		

iKVM-Status anzeigen

Das Lokalzugriffs-KVM-Modul für das Dell M1000e-Servergehäuse heißt Avocent® Integrated KVM Switch Modul oder iKVM. Der Funktionszustand des mit dem Gehäuse verbundenen iKVM kann auf der Seite Gehäuse-Grafiken eingesehen werden.

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

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Die Seite Gehäusezustand wird angezeigt. Der rechte Abschnitt von Gehäuse-Grafiken zeigt die Rückansicht des Gehäuses und enthält den Funktionszustand des iKVM. Der iKVM-Funktionszustand wird durch die Farbe der iKVM-Grafik angezeigt:
   - Grün - iKVM wird erkannt, mit Strom versorgt und kommuniziert mit dem CMC; es gibt keine Anzeichen eines ungünstigen Zustands
   - Bernstein - iKVM wird erkannt, wird oder wird nicht mit Strom versorgt oder kommuniziert oder kommuniziert nicht mit dem CMC; ein ungünstiger Zustand könnte vorhanden sein.
   - Grau - iKVM wird erkannt und nicht mit Strom versorgt. Es kommuniziert nicht mit dem CMC und es gibt keine Anzeichen eines ungünstigen Zustands.
3. Bewegen Sie den Cursor über die iKVM-Grafik und ein entsprechender Texthinweis oder Bildschirmtipp wird angezeigt. Der Texthinweis liefert zusätzliche Informationen zu diesem iKVM.
4. Die iKVM-Grafik ist mit der entsprechenden GUI-Seite des CMC verknüpft, um sofort die Navigation zur Seite iKVM-Status zu ermöglichen.

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

- "iKVM-Status und -Eigenschaften anzeigen"
- "Frontblende aktivieren oder deaktivieren"
- "Dell CMC-Konsole über iKVM aktivieren."
- "Aktualisieren der iKVM-Firmware"

Weitere Informationen zum iKVM finden Sie unter "iKVM-Modul verwenden".

Funktionszustand der Netzteileinheiten anzeigen

Der Funktionszustand der Netzteileinheiten innerhalb des Gehäuses kann auf zwei Arten eingesehen werden: im Abschnitt Gehäuse-Grafiken auf der Seite Gehäusezustand oder auf der Seite Stromversorgung-Zustand. Die Seite Gehäuse-Grafiken bietet einen grafischen Überblick über alle Netzteile, der im Gehäuse installiert ist.

Um den Funktionszustand aller Netzteile mittels Gehäuse-Grafiken einzusehen:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Die Seite Gehäusezustand wird angezeigt. Die rechte Sektion der Gehäuse-Grafiken stellt die Rückansicht des Gehäuses dar und enthält den Funktionszustand aller Netzteile. Der Netzteile-Funktionszustand wird durch die Farbe des Netzteil-Symbols angegeben:
   - Grün - Netzteil wird erkannt, mit Strom versorgt und kommuniziert mit dem CMC; es gibt keine Anzeichen eines ungünstigen Zustands.
   - Bernstein - Netzteil wird erkannt, kann jedoch mit Strom versorgt sein, oder nicht, kann mit dem CMC kommunizieren oder nicht; ein ungünstiger Zustand könnte vorhanden sein.
   - Grau - Netzteil wird erkannt und nicht mit Strom versorgt. Es kommuniziert nicht mit dem CMC und es gibt keine Anzeichen eines ungünstigen Zustands.
3. Bewegen Sie den Cursor über eine einzelne Netzteil-Grafik und ein entsprechender Texthinweis oder Bildschirmtipp wird angezeigt. Der Texthinweis liefert zusätzliche Informationen zu diesem Netzteil.
4. Die Netzteilgrafik ist mit der entsprechenden Seite der CMC-GUI verknüpft, um sofortige Navigation zur Seite Stromversorgung-Status für alle Netzteile zu ermöglichen.

Die Seite Stromversorgung-Status zeigt den Status und die Messwerte der Netzteile an, die dem Gehäuse zugeordnet sind. Weitere Informationen über die Stromverwaltung des CMC finden Sie unter "Stromverwaltung".

So zeigen Sie den Funktionszustand der Netzteileinheiten an:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur Netzteile aus. Die Seite Stromversorgung-Status wird angezeigt.

Tabelle 5-10 und Tabelle 5-11 enthalten Erläuterungen zu den Informationen auf der Seite Stromversorgung-Status.

Tabelle 5-10. Informationen zum Funktionszustand von Netzteilen

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

Tabelle 5-11. Systemstromstatus

Bauteil	Beschreibung
Gesamter Stromfunktionszustand	Zeigt den Funktionszustand (**OK, Nicht-kritisch, Kritisch, Nicht behebbar, Andere, Unbekannt**) für die Stromverwaltung des gesamten Gehäuses an.
Systemstromstatus	Zeigt den Stromstatus (Ein, Aus, Netzstrom ein, Ausschalten) des Gehäuses an.
Redundanz	Zeigt den Netzteilredundanzstatus an. Zu den Werten gehören: **Nein**: Netzteile sind nicht redundant. **Ja** - Volle Redundanz wirksam.

Status der Temperatursensoren anzeigen

Auf der Seite Temperatursensorinformationen werden der Status und die Messwerte der Temperatursonden auf dem gesamten Gehäuse (Gehäuse, Server, E/A-Module und iKVM) angezeigt.

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

So zeigen Sie den Funktionszustand der Temperatursonden an.

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur Temperatursensoren aus. Die Seite Temperatursensorinformationen wird angezeigt.

Tabelle 5-12 enthält Beschreibungen zu den Informationen auf der Seite Temperatursensorinformationen.

Tabelle 5-12.

Bauteil	Beschreibung		
ID	Zeigt die Zahlencode-ID der Temperatursonde an.		
Name	Zeigt den Namen jeder Temperatursonde an Gehäuse, Servern, E/A-Modulen sowie iKVM an. Beispiele: Umgebungstemperatur, Server 1 Temperatur, E/A-Modul 1, iKVM Temperatur.		
Vorhanden	Zeigt an, ob der Sensor im Gehäuse vorhanden (Ja) oder nicht vorhanden (Nein) ist.		
Funktionszustand		OK	Zeigt an, dass die Lüftereinheit vorhanden ist und mit dem CMC kommuniziert. Zeigt an, dass der Funktionszustand der Temperatursonde OK ist.
		Schwerwiegend	Zeigt an, dass der Temperatursensor einen Fehler aufweist und der Funktionszustand kritisch ist. **Es müssen sofort Korrekturmaßnahmen ergriffen werden.**
		Unknown (Unbekannt)	Wird angezeigt, wenn das Gehäuse zuerst eingeschaltet wird. Im Falle eines Kommunikationsfehlers zwischen dem CMC und der Temperatursonde kann der CMC den Funktionsstatus der Temperatursonde weder abrufen noch anzeigen.
Messwert	Zeigt die aktuelle Temperatur in Grad Celsius und Grad Fahrenheit an.		
Maximaler Schwellenwert	Zeigt die höchste Temperatur in Grad Celsius und Grad Fahrenheit an, wobei eine Fehlerwarnung ausgegeben wird.		
Minimaler Schwellenwert	Zeigt die niedrigste Temperatur in Grad Celsius und Grad Fahrenheit an, wobei eine Fehlerwarnung ausgegeben wird.		

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

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

Architekturkonfiguration

Der Abschnitt Architekturkonfiguration zeigt den Typ der Eingabe/Ausgabe-Architektur an, der für Architektur A, Architektur B und Architektur C installiert ist. Ein grünes Häkchen zeigt an, dass die Architektur für FlexAddress aktiviert ist. Die Funktion FlexAddress wird verwendet, um dem Gehäuse zugewiesene und Steckplatz-beständige WWN/MAC-Adressen verschiedenen Architekturen und Steckplätzen innerhalb des Gehäuses zuzuweisen. Diese Funktion ist je Architektur und je Steckplatz aktiviert.

ANMERKUNG: Weitere Informationen zur Funktion FlexAddress finden Sie unter "FlexAddress verwenden".

WWN/MAC-Adressen

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

CMC-Netzwerkeigenschaften konfigurieren

ANMERKUNG: Netzwerkkonfigurationsänderungen können zu Verbindungsverlust der aktuellen Netzwerkanmeldung führen.

Ursprünglichen Zugriff auf den CMC einrichten

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

ANMERKUNG: Um CMC-Netzwerkeinstellungen einrichten zu können, müssen Sie die Berechtigung als Gehäusekonfigurations-Administrator besitzen.

1. Melden Sie sich bei der Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf **Chassis** (Gehäuse).
3. Klicken Sie auf die Registerkarte Netzwerk/Sicherheit. Die Seite Netzwerkkonfiguration wird eingeblendet.
4. Aktivieren oder deaktivieren Sie DHCP für den CMC, indem Sie das Kontrollkästchen DHCP verwenden (für CMC-NIC-IP-Adresse) auswählen oder abwählen.
5. Wenn Sie DHCP deaktiviert haben, geben Sie die IP-Adresse, das Gateway und die Subnetzmaske ein.
6. Klicken Sie unten auf der Seite auf **Änderungen anwenden**.

Lokale Netzwerkeinstellungen (LAN) konfigurieren

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

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

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

1. Melden Sie sich bei der Webschnittstelle an.
2. Klicken Sie auf die Registerkarte **Netzwerk/Sicherheit**.Die Konfiguration der CMC-Netzwerkeinstellungen wird unter Tabelle 5-13 bis Tabelle 5-15 beschrieben.
3. Klicken Sie auf **Änderungen übernehmen**.

Um den IP-Bereich und die Einstellungen für das Blocken von IPs zu konfigurieren, klicken Sie auf Erweiterte Einstellungen (siehe "CMC-Netzwerksicherheitseinstellungen konfigurieren").

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

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

Tabelle 5-13. Netzwerkeinstellungen

Einstellung	Beschreibung

CMC MAC-Adresse	Zeigt die MAC-Adresse des Gehäuses an, die eine eindeutig identifizierbare Adresse für das Gehäuse im Netzwerk ist.
CMC NIC aktivieren	Aktiviert den NIC des CMC. Standardeinstellung: Aktiviert. Wenn diese Option ausgewählt ist: • Kommuniziert der CMC mit dem Netzwerk des Computers und ist über dieses zugänglich. • Webschnittstelle, CLI (Remote-RACADM), WSMAN, Telnet und SSH, die mit dem CMC verbunden sind, stehen zur Verfügung. Wenn diese Option nicht ausgewählt ist: • Kann der CMC NIC nicht über das Netzwerk kommunizieren. • Die Kommunikation durch den CMC zum Gehäuse steht nicht zur Verfügung. • Webschnittstelle, CLI (Remote-RACADM), WSMAN, Telnet und SSH, die mit dem CMC verbunden sind, stehen nicht zur Verfügung. • Auf die iDRAC-Webschnittstelle des Servers, CLI lokal, E/A-Module und iKVM kann noch zugegriffen werden. • Netzwerkadressen für den iDRAC und CMC können in diesem Fall von der Gehäuse-LCD abgelesen werden. **ANMERKUNG:** Der Zugriff auf die anderen Gehäusekomponenten im Netzwerk ist nicht betroffen, wenn das Netzwerk im Gehäuse deaktiviert (oder verloren gegangen) ist.
CMC auf DNS registrieren	Diese Eigenschaft registriert den CMC-Namen auf dem DNS-Server. Standard: standardmäßig nicht markiert (deaktiviert) **ANMERKUNG:** Einige DNS-Server registrieren nur Namen mit 31 Zeichen oder weniger. Stellen Sie sicher, dass sich der bestimmte Name im DNS-erforderlichen Limit befindet.
DNS-CMC-Name	Zeigt den CMC-Namen nur an, wenn CMC auf DNS registrieren ausgewählt ist. Der Standard-CMC-Name ist CMC_service_tag, wobei service tag die Service-Kennnummer des Gehäuses darstellt. Die maximale Zeichenzahl beträgt 63. Das erste Zeichen muss ein Buchstabe (a-z, A-Z) sein, gefolgt von einem alphanumerischen Zeichen (a-z, A-Z, 0-9) oder einem Bindestrich (-).
DHCP für den DNS-Domänennamen verwenden	Verwendet den Standard-DNS-Domänennamen. Dieses Kontrollkästchen ist nur dann aktiv, wenn **DHCP verwenden (für NIC-IP-Adresse)** ausgewählt ist. Standardeinstellung: Aktiviert.
DNS-Domänenname	Der Standard-DNS-Domänenname ist ein leeres Zeichen. Dieses Feld kann nur bearbeitet werden, wenn das Kontrollkästchen DHCP für den DNS-Domänennamen verwenden ausgewählt ist.
Automatische Verhandlung (1 Gb)	Legt fest, ob der CMC automatisch den Duplex-Modus und die Netzwerkgeschwindigkeit festlegt, indem er mit dem nächstgelegenen Router oder Switch kommuniziert (Ein), oder ob Sie den Duplex-Modus und die Netzwerkgeschwindigkeit manuell festlegen können (Aus). Standardeinstellung: Ein Wenn Automatische Verhandlung eingeschaltet ist, kommuniziert CMC automatisch mit dem nächsten Router oder Switch und arbeitet mit einer Geschwindigkeit von 1 Gb. Wenn Automatische Verhandlung ausgeschaltet ist, müssen Sie den Duplexmodus und die Netzwerkgeschwindigkeit manuell festlegen.
Netzwerkgeschwindigkeit	Legen Sie die Netzwerkgeschwindigkeit in Übereinstimmung mit der Netzwerkumgebung auf 1 GBit/s, 100 MBit/s oder 10 MBit/s fest. **ANMERKUNG:** Die Einstellung der Netzwerkgeschwindigkeit muss mit Ihrer Netzwerkkonfiguration übereinstimmen, um einen effektiven Netzwerkdurchsatz zu gewährleisten. Wenn die Netzwerkgeschwindigkeit geringer eingestellt wird als die Geschwindigkeit Ihrer Netzwerkkonfiguration, steigt der Verbrauch der Bandbreite und die Netzwerkkommunikation wird verlangsamt. Stellen Sie fest, ob Ihr Netzwerk höhere Netzwerkgeschwindigkeiten unterstützt, und stellen Sie sie entsprechend ein. Wenn Ihre Netzwerkkonfiguration mit keinem dieser Werte übereinstimmt, empfiehlt Dell, die Automatische Verhandlung zu verwenden oder sich mit dem Hersteller Ihrer Netzwerkausstattung in Verbindung zu setzen. **ANMERKUNG:** Um eine Geschwindigkeit von 1000 Mb oder 1 Gb zu verwenden, wählen Sie Automatische Verhandlung.
Duplexmodus	Legen Sie den Duplex-Modus in Übereinstimmung mit der Netzwerkumgebung auf "Voll" oder "Halb" fest. Auswirkungen: Wenn Automatische Verhandlung für ein Gerät eingeschaltet ist, für ein anderes jedoch nicht, kann das Gerät mit automatischer Verhandlung die Netzwerkgeschwindigkeit des anderen Geräts festlegen, den Duplexmodus jedoch nicht. In diesem Fall setzt sich der Duplex-Modus während der Verhandlung automatisch auf Standard (Halb-Duplex). Ein derartiger Duplex-Übereinstimmungsfehler resultiert in einer langsamen Netzwerkverbindung. **ANMERKUNG:** Die Einstellungen der Netzwerkgeschwindigkeit und des Duplex-Modus sind nicht verfügbar, wenn die automatische Verhandlung auf "Ein" gestellt ist.
MTU	Legt den Wert für die maximale Größe der Übertragungseinheit (MTU) fest bzw. das größte Paket, das über die Schnittstelle übertragen werden kann. Konfigurationsbereich: 576 - 1500. Standardeinstellung: 1500. **ANMERKUNG:** IPv6 erfordert einen MTU-Wert von mindestens 1280. Wenn IPv6 aktiviert und **cfgNetTuningMtu** auf einen niedrigeren Wert gesetzt ist, verwendet der CMC einen MTU-Wert von 1280.

Tabelle 5-14. IPv4-Einstellungen

Einstellung	Beschreibung

IPv4 aktivieren	Der CMC kann das IPv4-Protokoll verwenden, um im Netzwerk zu kommunizieren. Wenn dieses Feld deaktiviert wird, wird dadurch IPv6-Netzwerkverkehr nicht verhindert. Standardeinstellung: Markiert (aktiviert).
DHCP aktivieren	Hierdurch kann der CMC automatisch vom Server des IPv4-DHCP (dynamisches Host-Konfigurationsprotokoll) eine IP-Adresse anfordern und abrufen. Standardeinstellung: Markiert (aktiviert). Wenn diese Option ausgewählt ist, ruft der CMC die IPv4-Konfiguration (IP-Adresse, Subnetzmaske und Gateway) automatisch von einem DHCP-Server in Ihrem Netzwerk ab. Dem CMC in Ihrem Netzwerk ist immer eine eindeutige IP-Adresse zugewiesen. **ANMERKUNG:** Wenn diese Funktion aktiviert ist, werden die Eigenschaftsfelder **Statische IP-Adresse**, **Statische Subnetzmaske** und **Statisches Gateway** (die sich auf der Seite **Netzwerkkonfiguration** unmittelbar neben dieser Option befinden) deaktiviert. Hierbei werden alle zu einem früheren Zeitpunkt eingegebenen Werte für diese Eigenschaften ignoriert. Falls diese Option nicht aktiviert ist, müssen die **statische IP-Adresse**, die **statische Subnetzmaske** und das **statische Gateway** unmittelbar im Anschluss an diese Option auf der Seite **Netzwerkkonfiguration** manuell eingegeben werden.
Statische IP-Adresse	Gibt die IPv4-Adresse für die CMC-NIC an.
Statische Subnetzmaske	Gibt die statische IPv4-Subnetzmaske für die CMC-NIC.
Statischer Gateway	Gibt das IPv4-Gateway für die CMC-NIC an. **ANMERKUNG:** Die Felder **Statische IP-Adresse**, **Statische Subnetzmaske** und **Statisches Gateway** sind nur aktiviert, wenn **DHCP aktivieren** (das Eigenschaftsfeld, das diesen Feldern vorangeht) deaktiviert (nicht markiert) ist. In diesem Fall müssen die **statische IP-Adresse**, die **statische Subnetzmaske** und das **statische Gateway** für den Gebrauch durch den CMC über das Netzwerk manuell eingegeben werden. **ANMERKUNG:** Die Felder **Statische IP-Adresse**, **Statische Subnetzmaske** und **Statisches Gateway** gelten nur für das Gehäusegerät. Sie haben keine Auswirkung auf die anderen über das Netzwerk zugänglichen Komponenten der Gehäuselösung, zum Beispiel Servernetzwerk, lokaler Zugriff, E/A-Module und iKVM.
DHCP zum Abrufen von DNS-Serveradressen verwenden	Ruft die primären und sekundären DNS-Serveradressen vom DHCP-Server statt von den statischen Einstellungen ab. Standardeinstellung: Standardmäßig markiert (aktiviert) **ANMERKUNG:** Wenn DHCP verwenden (für NIC-IP- Adresse) aktiviert ist, aktivieren Sie die Eigenschaft DHCP zum Abrufen von DNS-Serveradressen verwenden. Wenn diese Option aktiviert ist, ruft der CMC seine DNS-IP-Adresse automatisch von einem DHCP-Server im Netzwerk ab. **ANMERKUNG:** Wenn diese Eigenschaft aktiviert ist, sind die Eigenschaftsfelder des statischen bevorzugten DNS- Servers und des Statisch Alternierenden DNS -Servers (die sich unmittelbar nach dieser Option auf der Seite Netzwerkkonfiguration befinden) deaktiviert, und alle zu einem früheren Zeitpunkt eingegebenen Werte für diese Eigenschaften werden ignoriert. Wenn diese Option nicht ausgewählt ist, ruft der CMC die DNS-Server-IP-Adresse vom statisch bevorzugten DNS-Server und statisch alternierenden DNS-Server ab. Die Adressen dieser Server werden in den Textfeldern festgelegt, die dieser Option auf der Seite Netzwerkkonfiguration unmittelbar folgen.
Statischer bevorzugter DNS-Server	Legt die statische IP-Adresse für den bevorzugten DNS-Server fest. Der statische bevorzugte DNS -Server wird nur implementiert, wenn DHCP zum Abrufen von DNS-Serveradressen verwenden deaktiviert ist.
Statischer bevorzugter DNS-Server	Legt die statische IP -Adresse für den alternierenden DNS -Server fest. Der statisch alternierende DNS-Server wird nur implementiert, wenn DHCP zum Abrufen von DNS-Serveradressen verwenden deaktiviert ist. Wenn Sie über keinen alternierenden DNS-Server verfügen, geben Sie eine IP-Adresse mit 0.0.0.0 ein.

Tabelle 5-15. IPv6-Einstellungen

Einstellung	Beschreibung
IPv6 aktivieren	Der CMC kann das IPv6-Protokoll verwenden, um im Netzwerk zu kommunizieren. Wenn dieses Feld deaktiviert wird, wird dadurch IPv4-Netzwerkverkehr nicht verhindert. Standardeinstellung: Markiert (aktiviert).
AutoConfiguration aktivieren	Der CMC kann das IPv6-Protokoll verwenden, um IPv6-bezogene Adress- und Gateway-Einstellungen von einem IPv6-Router zu erhalten, der zur Bereitstellung dieser Informationen konfiguriert ist. Der CMC hat dann eine eindeutige IP-Adresse in Ihrem Netzwerk. Standardeinstellung: Markiert (aktiviert). **ANMERKUNG:** Wenn diese Funktion aktiviert ist, werden die Eigenschaftsfelder **Statische IPv6-Adresse, Statische Präfixlänge** und **Statisches Gateway** (die sich auf der Seite **Netzwerkkonfiguration** unmittelbar neben dieser Option befinden) deaktiviert. Hierbei werden alle zu einem früheren Zeitpunkt eingegebenen Werte für diese Eigenschaften ignoriert. Falls diese Option nicht aktiviert ist, müssen die statische IPv6-Adresse, die statische Präfixlänge und das statische Gateway unmittelbar im Anschluss an diese Option auf der Seite **Netzwerkkonfiguration** manuell eingegeben werden.
Statische IPv6-Adresse	Gibt die IPv6-Adresse für die CMC-NIC an, wenn AutoConfiguration nicht aktiviert ist.
Statische Präfixlänge	Gibt die IPv6-Präfixlänge für die CMC-NIC an, wenn AutoConfiguration nicht aktiviert ist.
Statischer Gateway	Gibt das statische IPv6-Gateway für die CMC-NIC an, wenn AutoConfiguration nicht aktiviert ist. **ANMERKUNG:** Die Felder **Statische IPv6-Adresse**, **Statische Präfixlänge** und **Statisches Gateway** sind nur aktiviert, wenn **AutoConfiguration aktivieren** (das Eigenschaftsfeld, das diesen Feldern vorangeht) deaktiviert (nicht markiert) ist. In diesem Fall müssen die **statische IPv6-Adresse**, die **statische Präfixlänge** und das **statische Gateway** für Gebrauch durch den CMC über das IPv6-Netzwerk manuell eingegeben werden. **ANMERKUNG:** Die Felder **Statische IPv6-Adresse**, **Statische Präfixlänge** und **Statisches Gateway** gelten nur für das Gehäusegerät. Sie haben keine Auswirkung auf die anderen über das Netzwerk zugänglichen Komponenten der Gehäuselösung, zum Beispiel Servernetzwerk, lokaler Zugriff, E/A-Module und iKVM.
Statischer	Legt die statische IPv6-Adresse für den bevorzugten DNS-Server fest. Der Eintrag für den statisch bevorzugten DNS-Server wird

bevorzugter DNS-Server	nur berücksichtigt, wenn **DHCP zum Abrufen von DNS-Serveradressen verwenden** deaktiviert/nicht markiert ist. Es gibt in beiden Konfigurationsbereichen, IPv4 und IPv6, einen Eintrag für diesen Server.
Statischer bevorzugter DNS-Server	Legt die statische IPv6-Adresse für den alternierenden DNS-Server fest. Wenn Sie über keinen alternierenden DNS-Server verfügen, geben Sie eine IPv6-Adresse von "::" ein. Der Eintrag für den statisch alternierenden DNS-Server wird nur berücksichtigt, wenn **DHCP zum Abrufen von DNS-Serveradressen verwenden** deaktiviert/nicht markiert ist. Es gibt in beiden Konfigurationsbereichen, IPv4 und IPv6, einen Eintrag für diesen Server.

CMC-Netzwerksicherheitseinstellungen konfigurieren

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

1. Melden Sie sich bei der Webschnittstelle an.
2. Klicken Sie auf die Registerkarte **Netzwerk/Sicherheit**. Die Seite Netzwerkkonfiguration wird angezeigt.
3. Klicken Sie auf die Schaltfläche Erweiterte Einstellungen. Die Seite Netzwerksicherheit wird angezeigt.
4. Konfigurieren Sie die CMC-Netzwerksicherheitseinstellungen.

Tabelle 5-16 beschreibt die **Einstellungen** auf der Seite **Netzwerksicherheit**.

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

Tabelle 5-16. Einstellungen der Seite "Netzwerksicherheit"

Einstellungen	Beschreibung
IP-Bereich aktiviert	Aktiviert die Funktion zum Prüfen des IP-Bereichs, mit der ein bestimmter Bereich an IP-Adressen definiert wird, die auf den CMC zugreifen können.
IP-Bereichs-Adresse	Bestimmt die Haupt-IP-Adresse für die Bereichsüberprüfung.
IP-Bereichsmaske	Definiert einen bestimmten Bereich von IP-Adressen, die auf den CMC zugreifen können; ein Vorgang, der sich IP-Bereichsüberprüfung nennt. IP-Bereichsüberprüfung lässt den Zugriff auf den CMC nur von Clients oder Management Stations zu, deren IP-Adressen innerhalb des vom Benutzer angegebenen Bereichs liegen. Alle anderen Anmeldungsversuche werden abgelehnt. Zum Beispiel: IP-Bereichsmaske: 255.255.255.0 (11111111.11111111.11111111.00000000) IP-Bereichsadresse: 192.168.0.255 (11000000.10101000.00000000.11111111) Der sich ergebende IP-Adressenbereich beinhaltet alle Adressen mit 192.168.0, d. h., eine beliebige Adresse von 192.168.0.0 bis 192.168.0.255.
IP-Blockierung aktiviert	Aktiviert die Funktion des Blockierens der IP-Adresse, wodurch die Anzahl fehlgeschlagener Anmeldeversuche von einer bestimmten IP-Adresse für einen zuvor ausgewählten Zeitraum eingeschränkt wird.
• **IP-Blockierung, Zählung von Fehlversuchen**	Legt die Anzahl von Anmeldungsfehlversuchen einer IP-Adresse fest, bevor die Anmeldungsversuche von dieser Adresse zurückgewiesen werden.
• **IP-Blockierung, Fenster der Fehlversuche**	Legt die Zeitspanne in Sekunden fest, in der Fehler bei der Zählung im IP-Blockierungsausfall auftreten müssen, um die Strafzeit für die IP-Blockade auszulösen.
• **IP-Blockierungs-Penalty-Zeit**	Die Zeitspanne in Sekunden, während der Anmeldungsversuche von einer IP-Adresse aufgrund übermäßiger Fehlversuche zurückgewiesen werden. **ANMERKUNG:** Die Felder Zählung IP-Blockierungsausfall, Fenster IP-Blockierungsausfall und Strafzeit IP-Blockierung sind nur dann aktiv, wenn das Kontrollkästchen "IP-Blockierung aktiviert" (das Eigenschaftsfeld, das diesen Feldern vorausgeht) markiert (aktiviert) ist. In diesem Falle müssen Sie manuell die Eigenschaften Zählung IP-Blockierungsausfall, Fenster IP-Blockierungsausfall und Strafzeit IP-Blockierung eingeben.

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

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

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

VLAN konfigurieren

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

1. Melden Sie sich bei der Webschnittstelle an.
2. Klicken Sie auf der Registerkarte **Netzwerk/Sicherheit** auf die Unterregisterkarte → **VLAN**. Die Seite VLAN-Tag-Einstellungen wird angezeigt.

   VLAN-Tags sind Gehäuseeigenschaften. Sie bleiben mit dem Gehäuse verbunden, selbst wenn eine Komponente entfernt wird.

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

   Tabelle 5-17 beschreibt die **Einstellungen** auf der Seite **Netzwerksicherheit**.

Tabelle 5-17. VLAN-Tag-Einstellungen

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

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

Sie können auch über die Registerkarten **Gehäuse**→ **Server**→ **Setup** und die Unterregisterkarte → **VLAN** auf diese Seite zugreifen.

CMC-Benutzer hinzufügen und konfigurieren

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

Benutzertypen

Es gibt zwei Typen von Benutzern: CMC-Benutzer und iDRAC-Benutzer. CMC-Benutzer werden auch als "Gehäusenutzer" bezeichnet. Da iDRAC auf dem Server resident ist, werden iDRAC-Nutzer auch als "Servernutzer" bezeichnet.

CMC-Benutzer können lokale Benutzer oder Nutzer des Active Directory sein. iDRAC-Benutzer können auch lokale Benutzer oder Nutzer des Active Directory 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 Benutzerkonfigurations-Administrator direkt am Server anmelden. Der Benutzerkonfigurations-Administrator kann keinen Serverbenutzer vom CMC erstellen, oder umgekehrt. Diese Regel schützt die Sicherheit und Integrität der Server.

Tabelle 5-18, Tabelle 5-19 und Tabelle 5-20 beschreiben CMC-Benutzerprivilegien (lokal oder Active Directory) und welche Operationen ein CMC-Benutzer auf dem Gehäuse und auf den Servern, für die seine Rechte gewährt wurden, ausführen kann. Die Bezeichnung Benutzer sollte daher als CMC-Benutzer verstanden werden. Serverbenutzer werden eindeutig angegeben.

Tabelle 5-18. Benutzertypen

Berechtigung	Beschreibung
Benutzer: CMC-Anmeldung	Benutzer mit der Berechtigung als **Benutzer: CMC-Anmeldung** können sich am CMC anmelden. Ein Benutzer, der nur über die Anmeldeberechtigung verfügt, kann die CMC-Daten anzeigen, jedoch keine Daten hinzufügen oder modifizieren oder Befehle ausführen. Es ist möglich, dass Benutzer andere Berechtigungen ohne Anmeldeberechtigung besitzen. Diese Funktion ist sinnvoll, wenn einem Benutzer vorübergehend kein Zugang gewährt werden soll. Wenn die Anmeldeberechtigung dieses Benutzers wiederhergestellt wird, erhält der Benutzer alle zuvor gewährten Berechtigungen zurück.
Gehäusekonfigurations-Administrator	Benutzer mit der Berechtigung als Gehäusekonfigurations-Administrator können Daten hinzufügen oder ändern, die: • das Gehäuse identifizieren, wie z. B. den Gehäusenamen und die Gehäuseposition • speziell dem Gehäuse zugewiesen sind, wie z. B. IP-Modus (statisch oder DHCP), statische IP-Adresse, statischer Gateway und statische Subnetzmaske • dem Gehäuse Dienste zur Verfügung stellen, wie z. B. Datum und Uhrzeit, Firmware-Aktualisierung und CMC-Reset • dem Gehäuse zugeordnet sind, wie z. B. der Name des Steckplatzes und die Steckplatzpriorität. Obwohl sich diese Eigenschaften auf die Server beziehen, handelt es sich bei ihnen ausschließlich um Gehäuseeigenschaften, die sich auf die Steckplätze und nicht auf die Server selbst beziehen. Aus diesem Grund können Steckplatznamen und Steckplatzprioritäten hinzugefügt oder geändert werden, ungeachtet, ob sich Server in den Steckplätzen befinden oder nicht. Wenn ein Server auf ein anderes Gehäuse verschoben wird, werden der Steckplatzname und die Priorität, die dem im neuen Gehäuse belegten Steckplatz zugewiesen werden, übertragen. Der vorherige Steckplatzname und die vorherige Priorität verbleiben beim vorherigen Gehäuse.
Benutzerkonfigurations-Administrator	Benutzer mit Berechtigung als Benutzerkonfigurations-Administrator können: • Einen neuen Benutzer hinzufügen • Einen vorhandenen Benutzer löschen • Das Kennwort eines Benutzers ändern • Die Berechtigungen eines Benutzers ändern • Die Anmeldungsberechtigung eines Benutzers aktivieren oder deaktivieren, aber den Namen des Benutzers und andere Berechtigungen in der Datenbank beibehalten.
Administrator zum Löschen von Protokollen	CMC-Benutzer mit der Berechtigung Löschen durch Administrator können das Hardwareprotokoll und CMC-Protokoll löschen.
Gehäusesteuerungs-Administrator (Strombefehle)	CMC-Benutzer mit der Berechtigung als Administrator für die Gehäuse-Energieversorgung können alle Vorgänge im Zusammenhang mit der Energieversorgung ausführen: • Steuerung von Gehäusestromvorgängen, einschließlich Strom einschalten, Strom ausschalten und Strom aus- und einschalten.
Server Administrator	Die Server Administrator-Berechtigung ist eine Pauschalberechtigung, die einem CMC-Benutzer alle Rechte zum Ausführen beliebiger Vorgänge auf beliebigen, im Gehäuse vorhandenen Servern gewährt. Wenn ein Benutzer mit Berechtigung als CMC-Server-Administrator eine Maßnahmen zum Ausführen auf einem Server anweist, sendet die CMC-Firmware den Befehl zum Zielserver, ohne die Berechtigungen des Benutzers auf dem Server zu überprüfen. Mit anderen Worten: die CMC-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 über die Berechtigung zum Ausführen des Befehls verfügen Wenn ein CMC-Benutzer ohne Berechtigung als Server-Administrator eine Maßnahme anweist, die auf einem Server ausgeführt werden soll, sendet der CMC mit dem Benutzernamen und dem Anmeldenamen und 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.
Server Administrator (Fortsetzung)	Serverkonfigurations-Administrator: • IP-Adresse einstellen • Gateway einstellen • Subnetzmaske einstellen • Erstes Startlaufwerk einstellen Benutzerkonfigurations-Administrator: • iDRAC-Stammkennwort einstellen • iDRAC-Reset Serversteuerungs-Administrator:

	• Netzstrom ein • Stromversorgung aus • Aus- und einschalten • Ordentliches Herunterfahren • Serverneustart
Warnungstests für Benutzer	CMC-Benutzer mit der Berechtigung für Warnungstests für Benutzer können Test-Warnungsmeldungen versenden.
Debug-Befehl-Administrator	CMC-Benutzer mit der Berechtigung als Debug-Administrator können Systemdiagnosebefehle ausführen.
Architektur A-Administrator	CMC-Benutzer mit der Berechtigung als Architektur-A-Administrator können das E/A-Modul für Architektur A einrichten und konfigurieren, welches sich entweder in Steckplatz A1 oder Steckplatz A2 der E/A-Steckplätze befindet.
Architektur B-Administrator	CMC-Benutzer mit der Berechtigung als Architektur-B-Administrator können das E/A-Modul für Architektur B einrichten und konfigurieren, welches sich entweder in Steckplatz B1 oder Steckplatz B2 der E/A-Steckplätze befindet.
Architektur C-Administrator	CMC-Benutzer mit der Berechtigung als Architektur-C-Administrator können das E/A-Modul für Architektur C einrichten und konfigurieren, welches sich entweder in Steckplatz C1 oder Steckplatz C2 der E/A-Steckplätze befindet.

Die CMC-Benutzergruppen bieten eine Reihe von Benutzergruppen, die voreingestellte Benutzerrechte haben. Die Berechtigungen sind unter Tabelle 5-18 aufgelistet und beschrieben. In der folgenden Tabelle werden die Benutzergruppen und die vordefinierten Benutzerrechte aufgelistet.

Tabelle 5-19. CMC-Gruppenberechtigungen

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

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

Tabelle 5-20. Vergleich der Berechtigungen zwischen CMC-Administrator, Hauptbenutzer und Gastbenutzer

Berechtigungssatz	Administratorrechte	Hauptbenutzer Berechtigungen	Gastbenutzer Berechtigungen
Benutzer: CMC-Anmeldung	✔	✔	✔
Gehäusekonfigurations-Administrator	✔	✖	✖
Benutzerkonfigurations-Administrator			

	✔	✖	✖
Administrator zum Löschen von Protokollen	✔	✔	✖
Gehäusesteuerungs-Administrator (Strombefehle)	✔	✔	✖
Superbenutzer	✔	✖	✖
Server Administrator	✔	✔	✖
Warnungstests für Benutzer	✔	✔	✖
Debug-Befehl-Administrator	✔	✖	✖
Architektur A-Administrator	✔	✔	✖
Architektur B-Administrator	✔	✔	✖
Architektur C-Administrator	✔	✔	✖

Benutzer hinzufügen und verwalten

Von den Seiten Benutzer und Benutzerkonfiguration in der Webschnittstelle können Sie Informationen zu CMC-Benutzern anzeigen, einen neuen Benutzer hinzufügen und Einstellungen für einen vorhandenen Benutzer ändern.

Sie können bis zu 16 lokale Benutzer konfigurieren. Wenn zusätzliche Benutzer erforderlich sind und Ihre Firma die Microsoft® Active Directory®-Dienstsoftware verwendet, können Sie Active Directory für den Zugriff auf den CMC konfigurieren. Über die Active Directory-Konfiguration wären Sie in der Lage, zusätzlich zu den 16 lokalen Benutzern für existierende Benutzer in der Active Directory-Software CMC-Benutzerberechtigungen hinzuzufügen und zu steuern. Weitere Informationen finden Sie unter CMC mit Microsoft Active Directory verwenden.

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

ANMERKUNG: Um die Sicherheit zu erhöhen, empfiehlt Dell nachdrücklich, das vorgegebene Kennwort für das Benutzerkonto root (User 1) bei der Ersteinrichtung zu ändern. Das Konto root ist das werkseitig voreingestellte Verwaltungskonto des CMC-Moduls. Um das vorgegebene Kennwort für das Konto root zu ändern, klicken Sie auf User ID 1 (Benutzer-ID 1), um die Seite User Configuration (Benutzerkonfiguration) zu öffnen. Hilfe zu dieser Seite finden Sie über den Link Hilfe, der sich auf dieser Seite ganz oben rechts in der Ecke befindet.

So fügen Sie CMC-Benutzer hinzu und konfigurieren diese:

ANMERKUNG: Zur Ausführung der folgenden Schritte müssen Sie die Berechtigung Benutzerkonfigurations-Administrator haben.

1. Melden Sie sich bei der Webschnittstelle an.
2. Klicken Sie auf die Registerkarte **Network/Security** (Netzwerk/Sicherheit) und anschließend auf die Unterregisterkarte **Users** (Benutzer). Die Seite Benutzer wird angezeigt und führt die **Benutzer-ID**, den Benutzernamen, die CMC-Berechtigung sowie den **Anmeldestatus** zu **jedem Benutzer** auf, einschließlich derer des Stammbenutzers. Benutzerkennungen, zu denen keine Benutzerinformationen angezeigt werden, stehen für die Konfiguration zur Verfügung.
3. Klicken Sie auf eine verfügbare Benutzerkennung. Die Seite User Configuration (Benutzerkonfiguration) wird angezeigt.

   Klicken Sie auf Refresh (Aktualisieren), um den Inhalt der Seite Users (Benutzer) zu aktualisieren. Um den Inhalt der Seite Users zu drucken, klicken Sie auf Print (Drucken).
4. Wählen Sie die allgemeinen Einstellungen für den Benutzer aus.

Tabelle 5-21 beschreibt die **allgemeinen** Einstellungen zur Konfiguration eines neuen oder vorhandenen CMC-Benutzernamens und -Kennworts.

Tabelle 5-21. Allgemeine Benutzereinstellungen

Eigenschaft	Beschreibung
Benutzer-ID	(Nur-Lesen) kennzeichnet einen Benutzer anhand einer der 16 voreingestellten, sequenziellen Nummern, die für CLI-Scriptingzwecke verwendet werden. Die Benutzer-ID kennzeichnet einen bestimmten Benutzer, wenn der Benutzer mit dem CLI-Hilfsprogramm (RACADM) konfiguriert wird. Die Benutzer-ID kann nicht bearbeitet werden. Wenn Sie Informationen für den Benutzer 'root' bearbeiten, ist dieses Feld statisch. Sie können den Benutzernamen für 'root' nicht bearbeiten.
Benutzer aktivieren	Aktiviert oder deaktiviert den Zugriff des Benutzer auf den CMC.
Benutzername	Bestimmt oder zeigt den eindeutigen CMC-Benutzernamen, der dem Benutzer zugeordnet ist. Der Benutzername kann aus bis zu 16 Zeichen bestehen. CMC-Benutzernamen dürfen keine Schrägstriche (/) oder Punkte (.) enthalten. **ANMERKUNG:** Wenn Sie den Benutzernamen ändern, wird der neue Name erst dann auf der Benutzeroberfläche angezeigt, wenn Sie sich das nächste Mal anmelden. Jeder Benutzer, der sich anmeldet, nachdem der neue Benutzername übernommen wurde, kann die Änderung sofort sehen.
Kennwort ändern	Lässt das Ändern des Kennworts eines vorhandenen Benutzers zu. Geben Sie das neue Kennwort im Feld Neues Kennwort ein. Das Kontrollkästchen Kennwort ändern kann nicht ausgewählt werden, wenn gerade ein neuer Benutzer konfiguriert wird. Es kann nur dann ausgewählt werden, wenn die Einstellung für einen bestehenden Benutzer geändert wird.
Kennwort	Legt ein neues Kennwort für einen vorhandenen Benutzer fest. Um ein Kennwort zu ändern, müssen Sie auch das Kontrollkästchen Kennwort ändern auswählen. Das Kennwort darf bis zu 20 Zeichen enthalten, die während der Eingabe als Punkte dargestellt werden.
Kennwort bestätigen	Bestätigt das Kennwort, das Sie im Feld Neues Kennwort eingegeben haben. **ANMERKUNG:** ANMERKUNG: Die Felder Neues Kennwort und Neues Kennwort bestätigen können nur bearbeitet werden, wenn Sie (1) gerade einen neuen Benutzer konfigurieren; oder (2) gerade die Einstellungen eines vorhandenen Benutzers bearbeiten und das Kontrollkästchen Kennwort ändern ausgewählt ist.

5. Ordnen Sie den Benutzer einer CMC-Benutzergruppe zu. Tabelle 5-18 beschreibt die CMC-Benutzerrechte. Tabelle 5-19 beschreibt die **Benutzergruppenberechtigungen** für die Einstellungen der **CMC- Benutzerberechtigungen**. Tabelle 5-20 zeigt einen Vergleich der Berechtigungen zwischen Administratoren, Hauptbenutzern und Gastbenutzern.

   Wenn Sie eine Benutzerberechtigungs-Einstellung aus dem Drop-Down-Menü CMC Group" (CMC-Gruppe) wählen, werden die aktiven Zugriffsrechte (erkennbar an den markierten Kontrollkästchen in der Liste) entsprechend den vordefinierten Einstellungen für die betreffende Gruppe angezeigt.

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

6. Klicken Sie auf **Änderungen übernehmen**.

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

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

Microsoft Active Directory-Zertifikate konfigurieren und verwalten

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

ANMERKUNG: Weitere Informationen zur Active Directory-Konfiguration und dazu, wie Active Directory mit dem Standardschema oder einem erweiterten Schema konfiguriert wird, finden Sie unter CMC mit Microsoft Active Directory verwenden.

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

So greifen Sie auf das Active Directory-Hauptmenü zu:

1. Melden Sie sich bei der Webschnittstelle an.
2. Klicken Sie auf die Registerkarte **Netzwerksicherheit** und dann auf das **Active Directory**-Unterregister. Die Seite Active Directory-Hauptmenü wird angezeigt.

Tabelle 5-22 führt die Optionen der Seite Active Directory-Hauptmenü auf.

Tabelle 5-22. Optionen der Hauptmenüseite des Active Directory

Feld	Beschreibung
Konfigurieren	Konfigurieren und verwalten Sie die folgenden Active Directory-Einstellungen für den CMC: CMC-Name, Root-Domänenname, CMC-Domänenname, Active Directory-Authentifizierungszeitüberschreitung, Auswahl des Active Directory-Schemas (Erweitert oder Standard) und Rollengruppen-Einstellungen.
AD-Zertifikat hochladen	Laden Sie ein von einer Zertifizierungsstelle signiertes Zertifikat für Active Directory auf den CMC hoch. Dieses Zertifikat, das Sie vom Active Directory erhalten, gewährt Ihnen Zugang zum CMC.
Zertifikat herunterladen	Lädt mit dem Windows Download Manager ein CMC-Serverzertifikat auf Ihre Management Station oder Ihr freigegebenes Netzwerk herunter. Wenn Sie diese Option wählen und auf Weiter klicken, wird das Dialogfeld Datei herunterladen eingeblendet. Verwenden Sie dieses Dialogfeld, um auf Ihrer Management Station oder Ihrem freigegebenen Netzwerk einen Speicherort für das Serverzertifikat zu bestimmen.
Zertifikat anzeigen	Zeigt das von der Zertifizierungsstelle signierte Zertifikat für Active Directory an, das auf den CMC hochgeladen wurde. **ANMERKUNG:** Standardmäßig beinhaltet der CMC kein von einer Zertifizierungsstelle signiertes Zertifikat für Active Directory. Sie müssen ein aktuelles, von einer Zertifizierungsstelle signiertes Serverzertifikat, hochladen.
Kerberos-Keytab hochladen	Lädt eine Kerberos-Keytab-Datei für Active Directory auf den CMC hoch. Sie können die Kerberos-Keytab-Datei vom Active Directory Server aus erzeugen, indem Sie das Dienstprogramm **ktpass.exe** ausführen. Diese Keytab-Datei stellt eine Vertrauensstellung zwischen dem Active Directory Server und dem CMC her. **ANMERKUNG:** Der CMC verfügt nicht über eine Kerberos- Keytab-Datei für Active Directory. Sie müssen eine neu erzeugte Kerberos-Keytab-Datei hochladen. Genauere Informationen finden Sie unter "Einfache Anmeldung konfigurieren".

Active Directory konfigurieren (Standardschema und erweitertes Schema)

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

ANMERKUNG: Bevor Sie die Active Directory-Funktion konfigurieren oder verwenden, muss sichergestellt sein, dass der Active Directory-Server für die Kommunikation mit dem CMC konfiguriert ist.

1. Stellen Sie sicher, dass alle SSL-Zertifikate (Secure Socket Layer) für die Active Directory-Server von derselben Zertifizierungsstelle signiert und auf den CMC hochgeladen wurden.
2. Melden Sie sich an der Webschnittstelle an, und wechseln Sie zum Active Directory-Hauptmenü.
3. Wählen Sie **Konfigurieren** aus, und klicken Sie dann auf **Weiter**. Die Seite **Active Directory-Konfiguration und Verwaltung** wird angezeigt.
4. Wählen Sie das Kontrollkästchen Active Directory aktivieren unter der Überschrift Allgemeine Einstellungen aus.
5. Geben Sie die erforderlichen Informationen in die übrigen Felder ein. Siehe Tabelle 5-23.

Tabelle 5-23. Eigenschaften der allgemeinen Active Directory-Einstellungen

Einstellung	Beschreibung
Root-Domänenname	Bestimmt den vom Active Directory verwendeten Domänennamen. Der Root-Domänenname ist der voll qualifizierte Root-Domänenname für die Gesamtstruktur. **ANMERKUNG:** Der Root-Domänenname muss ein gültiger Domänenname sein, für den die Namenskonvention x.y verwendet wird, wobei x eine ASCII-Zeichenkette aus 1-256 Zeichen ohne Leerstellen zwischen den Zeichen und *y* ein gültiger Domänentyp wie com, edu, gov, int, mil, net oder org ist. Standardeinstellung: Null (leer)
AD-Zeitüberschreitung	Die Wartezeit in Sekunden, bis die Active Directory-Abfragen beendet sind. Der Mindestwert ist größer oder gleich 15 Sekunden. Standardeinstellung: 120 Sekunden

AD-Server zur Suche bestimmen (optional)	Aktiviert (wenn markiert) den weitergeleiteten Aufruf des Domänen-Controllers und globalen Katalogs. Wenn Sie diese Option aktivieren, müssen Sie in den folgenden Einstellungen auch den Domänen-Controller und die globalen Katalogspeicherorte bestimmen. **ANMERKUNG:** Der Name auf dem Active Directory- Zertifizierungsstellenzertifikat wird nicht auf den festgelegten Active Directory-Server oder den globalen Katalogserver abgestimmt sein.
Domänen-Controller	Legt den Server fest, auf dem der Active Directory-Dienst installiert wird. Diese Option ist nur gültig, wenn **AD-Server zur Suche bestimmen (optional)** aktiviert ist.
Globaler Katalog	Legt den Speicherort des globalen Katalogs auf dem Active Directory-Domänen-Controller fest. Der globale Katalog ist eine Ressource zum Durchsuchen einer Active Directory-Gesamtstruktur. Diese Option ist nur gültig, wenn **AD-Server zur Suche bestimmen (optional)** aktiviert ist.

6. Wählen Sie ein Active Directory-Schema unter der Überschrift Auswahl des Active Directory-Schemas aus. Siehe Tabelle 5-24.
7. Wenn Sie Erweitertes Schema ausgewählt haben, geben Sie die folgenden erforderlichen Informationen im Abschnitt Erweiterte Schemaeinstellungen ein, und gehen Sie dann direkt zu Schritt 9. Wenn Sie das Standard-Schema ausgewählt haben, gehen Sie zu Schritt 8.
   - CMC-Gerätename - Der Name, der die CMC-Karte im Active Directory eindeutig kennzeichnet. Der CMC-Gerätename muss dem allgemeinen Namen des neuen CMC-Objekts entsprechen, das Sie im Domänen-Controller erstellt haben. Der Name muss eine ASCII Zeichenkette mit 1 bis 256 Zeichen ohne Leerstellen sein. Standardeinstellung: Null (leer)
   - CMC-Domänenname - Der DNS-Name (Zeichenkette) der Domäne, in der sich das CMC-Objekt des Active Directory befindet (Beispiel: cmc.com). Der Name muss ein gültiger Domänenname sein und aus *x.y* bestehen, wobei *x* eine ASCII-Zeichenkette mit 1 bis 256 Zeichen ohne Leerstellen und *y* ein gültiger Domänentyp, wie z. B. com, edu, gov, int, mil, net, org ist. Standardeinstellung: Null (leer)

ANMERKUNG: Verwenden Sie den NetBIOS-Namen nicht. Der CMC- Domänenname ist der vollständig qualifizierte Domänenname der Subdomäne, auf der sich das CMC-Geräteobjekt befindet.

Tabelle 5-24. Optionen für das Active Directory-Schema

Einstellung	Beschreibung
Standardschema verwenden	Verwenden Sie das Standardschema mit Active Directory, das nur Active Directory-Gruppenobjekte verwendet. Bevor Sie den CMC konfigurieren, um die Option für das Active Directory-Standardschema zu verwenden, müssen Sie zuerst die Active Directory-Software konfigurieren: 1. Öffnen Sie auf einem Active Directory-Server (Domänen-Controller) das Active Directory-Benutzer- und -Computer-Snap-In. 2. Erstellen Sie eine Gruppe oder wählen Sie eine bestehende Gruppe aus. Der Name der Gruppe und der Name dieser Domäne müssen auf dem CMC entweder mit der Webschnittstelle oder mit RACADM konfiguriert werden.
Erweitertes Schema verwenden	Verwendet das Erweiterte Schema mit Active Directory, das nur Dell-definierte Active Directory-Objekte verwendet. Bevor Sie den CMC konfigurieren, um die Optionen für das erweiterte Active Directory-Schema zu konfigurieren, müssen Sie zuerst die Active Directory-Software konfigurieren: 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. SSL auf allen Domänen-Controllern aktivieren. 5. Active Directory-Eigenschaften für den CMC entweder mit der CMC-Webschnittstelle oder mit RACADM konfigurieren.

8. Wenn Sie das Standardschema ausgewählt haben, geben Sie die folgenden Informationen im Abschnitt Standardschemaeinstellungen ein. Wenn Sie das erweiterte Schema ausgewählt haben, gehen Sie zu Schritt 9.
   - Rollengruppen - Die dem CMC zugeordneten Rollengruppen. Um die Einstellungen für eine Rollengruppe zu ändern, klicken Sie auf die Rollengruppennummer in der Rollengruppenliste. Die Seite **Rollengruppe konfigurieren** wird angezeigt.

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

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

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

Um den Inhalt der Seite **Active Directory-Konfiguration und Verwaltung** zu aktualisieren, klicken Sie auf Aktualisieren.

Um den Inhalt der Seite **Active Directory-Konfiguration und Verwaltung** zu drucken, klicken Sie auf Drucken.

Um die Rollengruppen für Active Directory zu konfigurieren, klicken Sie auf die einzelne Rollengruppe (1-5). Siehe Tabelle 5-19 und Tabelle 5-18.

ANMERKUNG: Um die Einstellungen der Seite Active Directory-Konfiguration und -Verwaltung speichern zu können, müssen Sie auf Anwenden klicken, bevor Sie mit der Seite Benutzerdefinierte Rollengruppe fortfahren.

Ein von einer Zertifizierungsstelle signiertes Active Directory-Zertifikat hochladen

Auf der Seite **Active Directory-Hauptmenü**:

1. Wählen Sie **AD-Zertifikat hochladen** aus, und klicken Sie dann auf **Weiter**. Die Seite **Zertifikat hochladen** wird angezeigt.
2. Geben Sie den Dateipfad im Textfeld ein und klicken Sie auf Durchsuchen, um die Datei auszuwählen.

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

3. Klicken Sie auf **Anwenden**. Wenn das Zertifikat ungültig ist, wird eine Fehlermeldung angezeigt.

Um den Inhalt der Seite **Active Directory-Zertifizierungsstellenzertifikat hochladen** zu aktualisieren, klicken Sie auf Aktualisieren.

Um den Inhalt der Seite **Active Directory-Zertifizierungsstellenzertifikat hochladen** zu drucken, klicken Sie auf Drucken.

Von einer Zertifizierungsstelle signiertes Active Directory-Zertifikat anzeigen

ANMERKUNG: Wenn Sie ein Active Directory-Serverzertifikat auf den CMC hochgeladen haben, stellen Sie sicher, dass das Zertifikat noch gültig und nicht abgelaufen ist.

Auf der Seite **Active Directory-Hauptmenü**:

1. Wählen Sie **Zertifikat anzeigen** aus, und klicken Sie dann auf **Weiter**.
2. Klicken Sie auf die entsprechende Schaltfläche der Seite **Active Directory- CA-Zertifikat**, um fortzufahren.

Tabelle 5-25. Informationen zum Active Directory-CA-Zertifikat

Feld	Beschreibung
Seriennummer	Seriennummer des Zertifikats
Informationen des Antragstellers	Vom Bewerber eingegebene Zertifikatsattribute
Ausstellerinformationen	Vom Aussteller zurückgegebene Zertifikatsattribute.
Gültig von	Datum der Zertifikatsausstellung.
Gültig bis	Verfalldatum des Zertifikats.

3. Um den Inhalt der Seite **Active Directory-Zertifizierungsstellenzertifikat anzeigen** zu aktualisieren, klicken Sie auf Aktualisieren.

Um den Inhalt der Seite **Active Directory-Zertifizierungsstellenzertifikat anzeigen** zu drucken, klicken Sie auf **Drucken**.

Sichere CMC-Datenübertragung mit SSL und digitalen Zertifikaten

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

- Secure Sockets Layer (SSL)
- Zertifikatsignierungsanforderung (CSR)

- Zugriff auf das SSL-Hauptmenü
- Ein neues CSR erstellen
- Serverzertifikat hochladen
- Serverzertifikat anzeigen

Secure Sockets Layer (SSL)

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

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

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

Dieses Verschlüsselungsverfahren gewährt eine hohe Stufe von Datenschutz. Der CMC verwendet den SSL 128-Bit-Verschlüsselungsstandard, die sicherste Form der Verschlüsselung, die für Webbrowser in Nordamerika allgemein verfügbar ist.

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

Zertifikatsignierungsanforderung (CSR)

Eine CSR ist eine digitale Aufforderung an eine Zertifizierungsstelle (in der Webschnittstelle CA genannt) zum Erhalt eines sicheren Serverzertifikats. Sichere Server-Zertifikate sind erforderlich zur Sicherstellung der Identität eines entfernten Systems und zur Vergewisserung, dass mit dem entfernten System ausgetauschte Informationen von anderen weder gesehen noch geändert. Um Sicherheit für den CMC zu gewährleisten, wird dringend empfohlen, eine CSR zu erstellen, die CSR an eine Zertifizierungsstelle zu senden und das von der Zertifizierungsstelle zurückgesandte Zertifikat hochzuladen.

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

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

Zugriff auf das SSL-Hauptmenü

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

ANMERKUNG: Jedes von Ihnen hochgeladene Serverzertifikat muss aktuell (nicht abgelaufen) und von einer Zertifizierungsstelle signiert sein.

1. Melden Sie sich bei der Webschnittstelle an.
2. Klicken Sie auf die Registerkarte **Netzwerk/Sicherheit** und dann auf das **SSL-Unterregister**. Die Seite SSL-Hauptmenü wird angezeigt.

Verwenden Sie die Optionen auf der Seite **SSL-Hauptmenü**, um eine CSR zu erstellen und diese an eine Zertifizierungsstelle zu senden. Die CSR-Informationen werden in der CMC-Firmware gespeichert.

Neue Zertifikatsignierungsanforderung erstellen

Um Sicherheit zu gewährleisten, empfiehlt Dell eindringlich, ein sicheres Serverzertifikat zu erwerben und auf den CMC hochzuladen. Sichere Serverzertifikate garantieren die Identität eines Remote-Systems und stellen sicher, dass Daten, die mit dem Remote-System ausgetauscht werden, nicht von anderen angezeigt oder geändert werden können. Ohne ein sicheres Serverzertifikat ist der CMC durch Zugriff von unberechtigten Benutzern gefährdet.

Tabelle 5-26. SSL-Hauptmenüoptionen

Feld	Beschreibung
Eine neue Zertifikatsignierungsanforderung erstellen (CSR)	Wählen Sie diese Option aus und klicken Sie auf **Weiter**, um die Seite Zertifikatsignierungsanforderung (CSR) erstellen zu öffnen, auf der Sie eine CSR-Anforderung für ein sicheres Web-Zertifikat erstellen können, das an eine Zertifizierungsstelle gesendet wird. **ANMERKUNG:** Jede neue CSR überschreibt die vorherige CSR der Firmware. Damit eine Zertifizierungsstelle Ihre CSR anerkennt, muss die CSR im CMC mit dem von der Zertifizierungsstelle zurückgesendeten Zertifikat übereinstimmen.
Serverzertifikat basierend auf erstellter CSR hochladen	Wählen Sie diese Option aus und klicken Sie auf **Weiter**, um die Seite **Zertifikat hochladen** anzuzeigen, auf der Sie ein vorhandenes Zertifikat hochladen können, über das Ihr Unternehmen verfügt und das zur Zugriffssteuerung für den CMC verwendet wird. **ANMERKUNG:** iDRAC akzeptiert lediglich X509-Base-64- kodierte Zertifikate. DER-kodierte Zertifikate werden nicht angenommen. Durch das Hochladen eines neuen Zertifikats wird das mit dem CMC gelieferte Standardzertifikat ersetzt.
Webserver-Schlüssel und Zertifikat hochladen	Wählen Sie diese Option aus und klicken Sie auf **Weiter**, um die Seite **Webserver-Schlüssel und Zertifikat hochladen** zu öffnen, auf der Sie einen vorhandenen Webserver-Schlüssel und ein vorhandenes Zertifikat hochladen können, über das Ihr Unternehmen verfügt und das zur Zugriffssteuerung für den CMC verwendet wird. **ANMERKUNG:** Nur X.509-Base-64-kodierte Zertifikate werden vom CMC akzeptiert. Binäre DER-kodierte Zertifikate werden nicht akzeptiert. Durch das Hochladen eines neuen Zertifikats wird das mit dem CMC gelieferte Standardzertifikat ersetzt.
Serverzertifikat anzeigen	Wählen Sie die Option aus und klicken Sie auf die Schaltfläche **Weiter**, um die Seite Serverzertifikat zu öffnen, auf der Sie das aktuelle Serverzertifikat anzeigen können.

Um ein sicheres Serverzertifikat für den CMC zu erwerben, müssen Sie eine Zertifikatsignierungsanforderung (CSR) an eine Zertifizierungsstelle Ihrer Wahl senden. Unter einer CSR versteht man eine digitale Anforderung für ein signiertes, sicheres Serverzertifikat, das Informationen über Ihre Organisation und einen eindeutigen Identifizierungsschlüssel enthält.

Wenn auf der Seite Zertifikatsignierungsanforderung erstellen eine CSR erstellt wird, erhalten Sie die Aufforderung, eine Kopie in der Management Station oder im freigegebenen Netzwerk zu speichern, und eindeutige Informationen zur Erstellung der CSR werden im CMC abgelegt. Diese Informationen werden später verwendet, um das Serverzertifikat, das Sie von der Zertifizierungsstelle erhalten, zu beglaubigen. Nachdem Sie das Serverzertifikat von der Zertifizierungsstelle erhalten, müssen Sie es auf den CMC hochladen.

ANMERKUNG: Damit der CMC das von der Zertifizierungsstelle zurückgesandte Serverzertifikat akzeptiert, müssen die Authentifizierungsinformationen, die im neuen Zertifikat enthalten sind, mit den Informationen übereinstimmen, die bei der Erstellung der CSR auf dem CMC gespeichert wurden.

VORSICHTSHINWEIS: Bei der Erstellung einer neuen CSR, wird jede vorherige CSR auf dem CMC überschrieben. Wenn eine wartende CSR überschrieben wird, bevor das Serverzertifikats von der Zertifizierungsstelle bewilligt wird, wird das Serverzertifikat vom CMC nicht angenommen, weil die zur Authentifizierung des Zertifikats verwendeten Informationen verloren gegangen sind. Geben Sie acht, dass sie bei der Erstellung einer CSR keine wartende CSR überschreiben.

Um eine CSR zu erstellen:

1. Wählen Sie auf der Seite **SSL-Hauptmenü** die Option **Neue Zertifikatsignierungsanforderung (CSR) erstellen**, und klicken Sie dann auf **Weiter**. Die Seite **Zertifikatsignierungsanforderung (CSR) erstellen** wird angezeigt.
2. Geben Sie für jeden CSR-Attributwert einen Wert ein.

   Tabelle 5-27 beschreibt die Optionen der Seite **Zertifikatsignierungsanforderung (CSR) erstellen**.
3. Klicken Sie auf Erstellen. Ein Dialogfeld Dateidownload erscheint.
4. Speichern Sie die Datei csr.txt auf der Management Station oder im freigegebenen Netzwerk. (Sie können die Datei auch jetzt öffnen und später speichern.) Diese Datei werden Sie später an die Zertifizierungsstellen senden.

Tabelle 5-27. Optionen der Seite "Zertifikatsignierungsanforderung (CSR) erstellen"

Feld	Beschreibung

Allgemeiner Name	Der genaue Name, der zertifiziert werden soll (normalerweise der Domänenname des Web Servers, z. B. www.xyzFirma.com/). Gültig: Alphanumerische Zeichen (A-Z, a-z, 09); Bindestriche, Unterstriche und Punkte. Nicht gültig: Nicht-alphanumerische Zeichen, die nicht oben angegeben sind (wie z. B., aber nicht beschränkt auf, @ # $ % & *); Zeichen, die hauptsächlich in nicht-englischen Sprachen verwendet werden, wie z. B. ß, å, é, ü.
Name der Organisation	Der Name, der sich auf Ihre Organisation bezieht (z. B. Unternehmen XYZ). Gültig: Alphanumerische Zeichen (A-Z, a-z, 09); Bindestriche, Unterstriche Punkte und Leerzeichen. Nicht gültig: Nicht-alphanumerische Zeichen, die nicht oben angegeben sind (wie z. B., aber nicht begrenzt auf, @ # $ % & *).
Organisationseinheit	Der Name, der mit einer organisatorischen Einheit in Verbindung gebracht wird, wie z.B. eine Abteilung (zum Beispiel Unternehmensgruppe). Gültig: Alphanumerische Zeichen (A-Z, a-z, 09); Bindestriche, Unterstriche Punkte und Leerzeichen. Nicht gültig: Nicht-alphanumerische Zeichen, die nicht oben angegeben sind (wie z. B., aber nicht begrenzt auf, @ # $ % & *).
Ort	Die Stadt oder ein anderer Standort Ihrer Organisation (zum Beispiel: Atlanta, Hongkong). Gültig: Alphanumerische Zeichen (A-Z, a-z, 09) und Leerzeichen. Nicht gültig: Nicht-alphanumerische Zeichen, die nicht oben angegeben sind (wie z. B., aber nicht beschränkt auf, @ # $ % & *).
Zustand	Der Staat, das Land oder Territorium, in denen sich die Einheit befindet, die sich für eine Zertifizierung bewirbt (zum Beispiel: Texas, New South Wales, Andhra Pradesh). **ANMERKUNG:** Verwenden Sie keine Abkürzungen. Gültig: Alphanumerische Zeichen (Groß- und Kleinbuchstaben; 0-9) und Leerzeichen. Nicht gültig: Nicht-alphanumerische Zeichen, die nicht oben angegeben sind (wie z. B., aber nicht beschränkt auf, @ # $ % & *).
Land	Das Land, in dem sich die Organisation, die sich für die Zertifizierung bewirbt, befindet.
E-Mail	Die E-Mail-Adresse Ihrer Firma. Sie können eine beliebige E-Mail-Adresse eingeben, die der CSR zugeordnet sein soll. Die E-Mail-Adresse muss gültig sein und das @-Zeichen enthalten (z. B. Name@UnternehmenXYZ.com). **ANMERKUNG:** Diese E-Mail-Adresse ist ein optionales Feld.

Serverzertifikat hochladen

1. Auf der Seite **SSL-Hauptmenü** wählen Sie **Server-Zertifikat hochladen** und klicken Sie auf **Weiter**. Die Seite **Zertifikat hochladen** wird angezeigt.
2. Geben Sie den Dateipfad im Textfeld ein und klicken Sie auf Durchsuchen, um die Datei auszuwählen.
3. Klicken Sie auf Anwenden. Wenn das Zertifikat ungültig ist, wird eine Fehlermeldung angezeigt.

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

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

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

Serverzertifikat anzeigen

Auf der Seite **SSL-Hauptmenü** wählen Sie **Server-Zertifikat anzeigen** und klicken dann auf **Weiter**. Die Seite **Serverzertifikat anzeigen** wird angezeigt.

Tabelle 5-28 erläutert die Felder und zugehörigen Beschreibungen, die im **Zertifikat**-Fenster aufgeführt werden.

Tabelle 5-28. Zertifikatinformationen

Feld	Beschreibung
Seriell	Seriennummer des Zertifikats
Bewerber	Vom Antragsteller eingegebene Zertifikatsattribute

Aussteller	Vom Aussteller zurückgegebene Zertifikatsattribute
nicht vor	Ausgabedatum des Zertifikats
nicht nach	Ablaufdatum des Zertifikats

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

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

Sitzungen verwalten

Die Seite **Sitzungen** zeigt alle aktuellen Verbindungen zum Gehäuse an und ermöglicht Ihnen, beliebige aktive Sitzungen zu beenden.

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

So beenden Sie eine Sitzung:

1. Melden Sie sich über die Webschnittstelle bei der CMC an.
2. Klicken Sie auf die Registerkarte **Netzwerk/Sicherheit** und dann auf die Unterregisterkarte **Sitzungen**.
3. Wählen Sie auf der Seite **Sitzungen** die zu beendenden Sitzungen aus und klicken Sie auf das Papierkorbsymbol.

So verwalten Sie Sitzungen:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf **Chassis** (Gehäuse).
3. Klicken Sie auf die Registerkarte **Netzwerk/Sicherheit**.
4. Klicken Sie auf die Unterregisterkarte Sitzungen. Die Seite Sitzungen wird angezeigt.

Tabelle 5-29. Sitzungseigenschaften

Eigenschaft	Beschreibung
Sitzungs-ID	Zeigt die sequenziell erstellte ID-Nummer für die einzelnen Instanzen einer Anmeldung an.
Benutzername	Zeigt den Anmeldenamen eines Benutzers an (lokaler Benutzer oder Active Directory-Benutzer). Beispiele von Active Directory-Benutzernamen sind *Name@Domäne.com*, *Domäne.com/Name*, *Domäne.com\Name*.
IP-Adresse	Zeigt die IP-Adresse des Benutzers an.
Sitzungstyp	Beschreibt den Sitzungstyp: Telnet, seriell, SSH, Remote-RACADM, SMASH CLP, WSMAN oder eine GUI-Sitzung.
Beenden	Ermöglicht Ihnen, eine beliebige aufgelistete Sitzung zu beenden (außer Ihrer eigenen). Klicken Sie auf das Papierkorbsymbol , um die entsprechende Sitzung zu beenden. Diese Spalte wird nur angezeigt, wenn Sie die Berechtigung zum **Gehäusekonfigurations-Administrator** besitzen.

Um eine Sitzung zu beenden, klicken Sie in der Zeile, die die Sitzung beschreibt, auf das Papierkorbsymbol.

Dienste konfigurieren

Der CMC enthält einen Web Server, der dazu konfiguriert ist, das SSL-Sicherheitsprotokoll des Industriestandards zu verwenden, um verschlüsselte Daten über das Internet von Clients zu empfangen bzw. sie an sie zu übermitteln. Der Web Server enthält ein von Dell selbstsigniertes digitales SSL-Zertifikat (Server-ID) und ist dafür verantwortlich, sichere HTTP-Aufforderungen von Clients zu empfangen bzw. auf sie zu antworten. Dieser Dienst wird von der Webschnittstelle und dem Remote-CLI-Hilfsprogramm zur Kommunikation mit dem CMC benötigt.

ANMERKUNG: Das Remote-CLI-Hilfsprogramm (RACADM) und die Webschnittstelle verwenden den Web Server. Im Falle, dass der Web Server nicht aktiv ist, stehen Remote-RACADM und die Webschnittstelle nicht zur Verfügung.

ANMERKUNG: Im Falle eines Webserver-Resets warten Sie mindestens eine Minute, bis die Dienste wieder verfügbar werden. Ein Web Server wird normalerweise auf Grund eines der folgenden Ereignisse zurückgesetzt: die Netzwerkkonfiguration oder Netzwerksicherheitseigenschaften wurden über die CMC-Webbenutzeroberfläche oder RACADM geändert; die Web Server- Schnittstellenkonfiguration wurde über die Webbenutzeroberfläche oder RACADM geändert; der CMC wurde zurückgesetzt; ein neues SSL-Serverzertifikat wurde hochgeladen.

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

So konfigurieren Sie die CMC-Dienste:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie auf die Registerkarte **Netzwerk/Sicherheit**.
3. Klicken Sie auf die Unterregisterkarte Dienste. Die Seite Dienste wird angezeigt.
4. Konfigurieren Sie die folgenden Dienste nach Bedarf:
   - Serielle-CMC-Konsole (Tabelle 5-30)
   - Web Server (Tabelle 5-31)
   - SSH (Tabelle 5-32)
   - Telnet (Tabelle 5-33)
   - Remote-RACADM (Tabelle 5-34)
   - SNMP (Tabelle 5-35)
   - Remote-Syslog (Tabelle 5-36)
5. Klicken Sie **Anwenden; dies aktualisiert all Standard-Zeitüberschreitungen und maximale Zeitüberschreitungsgrenzen**.

Tabelle 5-30. Einstellungen der seriellen CMC-Konsole

Einstellung	Beschreibung
Aktiviert	Aktiviert die Telnet-Konsolenschnittstelle auf dem CMC. Standardeinstellung: Nicht markiert (deaktiviert)
Umleitung aktiviert	Ermöglicht die serielle bzw. Text-Konsolenumleitung vom CMC zum Server über den seriellen/Telnet/SSH-Client. Der CMC verbindet mit dem iDRAC, der intern mit dem Server COM2-Anschluss verbunden ist. Konfigurationsoptionen: Markiert (aktiviert), nicht markiert (deaktiviert) Standardeinstellung: Markiert (aktiviert).
Zeitüberschreitung wegen Leerlauf	Zeigt die Anzahl der Sekunden an, bevor die Verbindung als eine sich im Leerlauf befindende serielle Sitzung automatisch unterbrochen wird. Eine Änderung an der Einstellung Zeitüberschreitung wird bei der nächsten Anmeldung wirksam; sie wirkt sich nicht auf die aktuelle Sitzung aus. Zeitüberschreitungsspanne: 0 oder 60 bis 10800 Sekunden. Um die Funktion der Zeitüberschreitung zu deaktivieren, geben Sie 0 ein. Standardeinstellung: 1800 Sekunden
Baudrate	Zeigt die Datengeschwindigkeit auf der externen seriellen Schnittstelle des CMC an. Konfigurationsoptionen: 9600, 19200, 28800, 38400, 57600 und 115200 Bit/s. Standardeinstellung: 115200 Bit/s
Authentifizierung deaktiviert	Aktiviert die Anmeldungsauthentifizierung der seriellen CMC-Konsole. Standardeinstellung: Nicht markiert (deaktiviert)
Escape-Taste	Ermöglicht Ihnen, die Escape-Tastenkombination festzulegen, die eine serielle bzw. Text-Konsolenumleitung beendet, wenn Sie den Befehl connect oder racadm connect verwenden. Standardeinstellung: ^\ (Halten Sie die Taste <Strg> gedrückt, und geben Sie einen umgekehrten Schrägstrich (\) ein). **ANMERKUNG:** Das Caret-Zeichen ^ steht für die Taste <Strg>. Konfigurationsoptionen: - Dezimalwert (Beispiel: 95) - Hexadezimalwert (Beispiel: 0x12) - Oktalwert (Beispiel: 007)

	• ASCII-Wert (Beispiel: ^a) ASCII-Werte können anhand der folgenden Escape-Tastencodes repräsentiert werden: • Esc, gefolgt von einem beliebigen alphabetischen Zeichen (a-z, A-Z) • Esc, gefolgt von den folgenden Sonderzeichen: [ ] \ ^ _ • Maximal zulässige Länge: 4
Größe des Verlaufspuffers	Zeigt die maximale Größe des seriellen Verlaufspuffers an, der die letzten Zeichen enthält, die an die serielle Konsole geschrieben wurden. Standardeinstellung: 8192 Zeichen
Anmeldungsbefehl	Bestimmt den seriellen Befehl, der automatisch ausgeführt wird, wenn sich ein Benutzer an der seriellen CMC-Konsolenschnittstelle anmeldet. Beispiel: connect server-1 Standardeinstellung: [Null]

Tabelle 5-31. Web Server-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert Web Server-Dienste (Zugriff über Remote-RACADM und die Webschnittstelle) für den CMC. Standardeinstellung: Markiert (aktiviert)
Max. Sitzungen	Zeigt die maximale Anzahl der für das Gehäuse zulässigen gleichzeitigen Sitzungen der Web-Benutzeroberfläche an. Eine Änderung an der Eigenschaft Max. Sitzungen wird bei der nächsten Anmeldung wirksam; sie hat keine Auswirkung auf die aktuellen aktiven Sitzungen (einschließlich Ihrer eigenen). Remote-RACADM ist von der Eigenschaft Max. Sitzungen für den Web Server nicht betroffen. Zugelassener Bereich: 1-4 Standardeinstellung: 4 **ANMERKUNG:** Wenn Sie die Eigenschaft Max. Sitzungen auf einen Wert unter dem Wert der aktuellen Anzahl an aktiven Sitzungen abändern und sich dann abmelden, können Sie sich nicht erneut anmelden, bevor die anderen Sitzungen beendet wurden oder abgelaufen sind.
Zeitüberschreitung wegen Leerlauf	Zeigt die Anzahl von Sekunden an, bevor die Verbindung zu einer sich im Leerlauf befindenden Web-Benutzeroberflächensitzung automatisch abgebrochen wird. Eine Änderung an der Einstellung Zeitüberschreitung wird bei der nächsten Anmeldung wirksam; sie wirkt sich nicht auf die aktuelle Sitzung aus. Der Zeitüberschreitungsbereich ist 60 bis 10800 Sekunden. Standardeinstellung: 1800 Sekunden
HTTP-Anschlussnummer	Zeigt die Standardschnittstelle an, die vom CMC verwendet wird, der eine Serververbindung abhört. **ANMERKUNG:** Wenn Sie die HTTP-Adresse im Browser angeben, führt der Web Server automatisch eine Umleitung aus und verwendet HTTPS. Wenn die Standard-HTTP-Schnittstellennummer (80) geändert wurde, müssen Sie in der Adresse im Adressenfeld des Browsers die Schnittstellennummer wie gezeigt angeben: http://<IP-Adresse>:<Schnittstellennummer> wobei IP-Adresse die IP-Adresse für das Gehäuse ist und Schnittstellennummer die HTTP-Schnittstellennummer ein anderer als der Standardwert 80 ist. Konfigurationsbereich:10 - 65535. Standardeinstellung: 80
HTTPS-Anschlussnummer	Zeigt die Standardschnittstelle an, die vom CMC verwendet wird, der eine sichere Serververbindung abhört. Wenn die Standard-HTTPS-Anschlussnummer (443) geändert wurde, müssen Sie in der Adresse im Adressenfeld des Browsers die Schnittstellennummer wie gezeigt angeben: https://<IP-Adresse>:<Anschlussnummer> wobei IP-Adresse die IP-Adresse für das Gehäuse ist und Schnittstellennummer die HTTPS-Schnittstellennummer ein anderer als der Standardwert 443 ist. Konfigurationsbereich:10 - 65535. Standardeinstellung: 443

Tabelle 5-32. SSH-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert SSH auf dem CMC. Standardeinstellung: Markiert (aktiviert)
Max. Sitzungen	Die maximale Anzahl gleichzeitiger, auf dem Gehäuse zulässiger SSH-Sitzungen. Eine Änderung an dieser Eigenschaft wird mit der nächsten Anmeldung wirksam; sie hat keine Auswirkung auf die aktuellen aktiven Sitzungen (einschließlich Ihrer eigenen). Konfigurierbarer Bereich: 1–4 Standardeinstellung: 4 **ANMERKUNG:** Wenn Sie die Eigenschaft Max. Sitzungen auf einen Wert unter dem Wert der aktuellen Anzahl an aktiven Sitzungen abändern und sich dann abmelden, können Sie sich nicht erneut anmelden, bevor die anderen Sitzungen beendet wurden oder abgelaufen sind.
Zeitüberschreitung wegen Leerlauf	Zeigt die Anzahl von Sekunden an, bevor die Verbindung zu einer sich im Leerlauf befindenden SSH-Sitzung automatisch unterbrochen wird. Eine Änderung an der Einstellung Zeitüberschreitung wird bei der nächsten Anmeldung wirksam; sie wirkt sich nicht auf die aktuelle Sitzung aus. Der Zeitüberschreitungsbereich ist 0 oder 60 bis 10800 Sekunden. Um die Funktion der Zeitüberschreitung zu deaktivieren, geben Sie 0 ein. Standardeinstellung: 1800 Sekunden
Anschlussnummer	Vom CMC verwendete Schnittstelle, die eine Serververbindung abhört. Konfigurationsbereich:10 - 65535. Standardeinstellung: 22

Tabelle 5-33. Telnet-Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert die Telnet-Konsolenschnittstelle auf dem CMC. Standardeinstellung: Nicht markiert (deaktiviert)
Max. Sitzungen	Zeigt die für das Gehäuse maximal zulässige Anzahl gleichzeitiger Telnet-Sitzungen an. Eine Änderung an dieser Eigenschaft wird mit der nächsten Anmeldung wirksam; sie hat keine Auswirkung auf die aktuellen aktiven Sitzungen (einschließlich Ihrer eigenen). Zugelassener Bereich: 1–4 Standardeinstellung: 4 **ANMERKUNG:** Wenn Sie die Eigenschaft Max. Sitzungen auf einen Wert unter dem Wert der aktuellen Anzahl an aktiven Sitzungen abändern und sich dann abmelden, können Sie sich nicht erneut anmelden, bevor die anderen Sitzungen beendet wurden oder abgelaufen sind.
Zeitüberschreitung wegen Leerlauf	Zeigt die Anzahl von Sekunden an, bevor die Verbindung zu einer sich im Leerlauf befindenden Telnet-Sitzung automatisch abgebrochen wird. Eine Änderung an der Einstellung Zeitüberschreitung wird bei der nächsten Anmeldung wirksam; sie wirkt sich nicht auf die aktuelle Sitzung aus. Der Zeitüberschreitungsbereich ist 0 oder 60 bis 10800 Sekunden. Um die Funktion der Zeitüberschreitung zu deaktivieren, geben Sie 0 ein. Standardeinstellung: 1800 Sekunden
Anschlussnummer	Zeigt die vom CMC verwendete Schnittstelle an, die eine Serververbindung abhört. Standardeinstellung: 23

Tabelle 5-34. Remote-RACADM- Einstellungen

Einstellung	Beschreibung
Aktiviert	Aktiviert den Zugriff des Remote-RACADM-Dienstprogramms auf den CMC. Standardeinstellung: Markiert (aktiviert)
Max. Sitzungen	Zeigt die maximal für das Gehäuse zulässige Anzahl gleichzeitiger RACADM-Sitzungen an. Eine Änderung an dieser Eigenschaft wird mit der nächsten Anmeldung wirksam; sie hat keine Auswirkung auf die aktuellen aktiven Sitzungen (einschließlich Ihrer eigenen).

	Zugelassener Bereich: 1–4 Standardeinstellung: 4 **ANMERKUNG:** Wenn Sie die Eigenschaft Max. Sitzungen auf einen Wert unter dem Wert der aktuellen Anzahl an aktiven Sitzungen abändern und sich dann abmelden, können Sie sich nicht erneut anmelden, bevor die anderen Sitzungen beendet wurden oder abgelaufen sind.
Zeitüberschreitung wegen Leerlauf	Zeigt die Anzahl der Sekunden an, bevor die Verbindung als eine sich im Leerlauf befindenden racadm-Sitzung automatisch unterbrochen wird. Bei der nächsten Anmeldung wird eine Änderung an der Einstellung Zeitüberschreitung wegen Leerlauf wirksam; sie wirkt sich nicht auf die aktuelle Sitzung aus. Geben Sie zur Deaktivierung der Funktion Zeitüberschreitung wegen Leerlauf den Wert 0 ein. Zeitüberschreitungsspanne: 0 oder 10 bis 1920 Sekunden. Um die Funktion der Zeitüberschreitung zu deaktivieren, geben Sie 0 ein. Standardeinstellung: 30 Sekunden

Tabelle 5-35. SNMP-Konfiguration

Einstellung	Beschreibung
Aktiviert	Aktiviert SNMP auf dem CMC. **Gültige Werte:** Markiert (aktiviert), nicht markiert (deaktiviert) **Standardeinstellung**: Nicht markiert (deaktiviert)
Community-Name	Gibt die Community-Zeichenfolge an, die verwendet wird, um Daten von SNMP-Deamon des CMC zu erhalten.

Tabelle 5-36. Remote-Syslog-Konfiguration

Einstellung	Beschreibung
Aktiviert	Ermöglicht Übertragung und Fernerfassung des Systemprotokolls (Syslog) auf den angegebenen Servern. **Gültige Werte:** Markiert (aktiviert), nicht markiert (deaktiviert) **Standardeinstellung**: Nicht markiert (deaktiviert)
Syslog Server 1	Der erste von drei möglichen Servern, die eine Kopie des Syslog verwalten können. Spezifiziert als Hostname, eine IPv6-Adresse oder eine IPv4-Adresse.
Syslog Server 2	Der zweite von drei möglichen Servern, die eine Kopie des Syslog verwalten können. Spezifiziert als Hostname, eine IPv6-Adresse oder eine IPv4-Adresse.
Syslog Server 3	Der dritte von drei möglichen Servern, die eine Kopie des Syslog verwalten können. Spezifiziert als Hostname, eine IPv6-Adresse oder eine IPv4-Adresse.
Syslog-Anschlussnummer	Spezifiziert die Anschlussnummer auf dem Remote-Server für den Empfang einer Kopie des Syslog. Die gleiche Anschlussnummer wird für alle drei Server verwendet. Eine gültige Syslog-Anschlussnummer liegt im Bereich von 10-65535. **Standardeinstellung**: 514

Strombudget konfigurieren

Sie können mit dem CMC die Stromversorgung des Gehäuses budgetieren und verwalten. Der Stromverwaltungsdienst optimiert den Stromverbrauch und weist den verschiedenen Modulen je nach Bedarf Strom zu.

Für Anweisungen zur Stromkonfiguration über den CMC, siehe Konfiguration und Verwaltung der Energieeinstellungen.

Für weitere Informationen zu den Strommanagementdiensten des CMC, siehe Stromverwaltung.

Firmwareaktualisierungen verwalten

Dieser Abschnitt beschreibt, wie Sie die Webschnittstelle zum Aktualisieren der CMC-Firmware verwenden. Die folgenden Komponenten können über die GUI oder RACADM-Befehle aktualisiert werden:

- CMC - Primär und Stand-by
- iKVM
- iDRAC
- EAM Infrastrukturgeräte

Bei der Aktualisierung von Firmware stets das empfohlene Verfahren einhalten, um Verlust des Dienstes zu vermeiden, falls die Aktualisierung fehlschlägt. Beachten Sie Installieren oder Aktualisieren der CMC-Firmware für einzuhaltende Richtlinien, bevor Sie die Anweisungen dieses Abschnittes anwenden.

Aktuelle Firmware-Versionen anzeigen

Die Seite Aktualisierung zeigt die aktuelle Version aller Komponenten im Gehäuse an, die aktualisiert werden können. Dies kann die iKVM-Firmware, primäre CMC-Firmware, (falls erforderlich) die Standby-CMC-Firmware, die iDRAC-Firmware und die Firmware der EAM-Infrastrukturgeräte beinhalten; weitere Informationen sind unter "Aktualisierung der Firmware des EAM-Infrastrukturgeräts" zu finden. Durch Klicken auf entweder den Gerätenamen oder das Kontrollkästchen Alle auswählen/abwählen und dann die Schaltfläche Aktualisierung anwenden, wird eine Aktualisierungsseite für die ausgewählten Geräte angezeigt.

Wenn sich im Gehäuse ein Server einer früheren Generation befindet, dessen iDRAC im Wiederherstellungsmodus ausgeführt wird, oder wenn der CMC beschädigte iDRAC-Firmware erkennt, wird der iDRAC einer früheren Generation ebenfalls auf der Seite **Aktualisierbare Komponenten** aufgeführt. "iDRAC-Firmware mittels CMC wiederherstellen" enthält die Schritte zur Wiederherstellung von iDRAC-Firmware mit dem CMC.

So zeigen Sie die Komponenten an, die aktualisiert werden können:

1. Melden Sie sich bei der Webschnittstelle an (siehe "Auf die CMC- Webschnittstelle zugreifen").
2. Klicken Sie in der Systemstruktur auf **Chassis** (Gehäuse).
3. Klicken Sie auf die Registerkarte Update (Aktualisieren). Die Seite Updatable Components (Aktualisierbare Komponenten) wird angezeigt.

Firmware aktualisieren

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

ANMERKUNG: Die Firmware-Aktualisierung übernimmt die derzeitigen CMC- und iKVM-Einstellungen.

ANMERKUNG: Wenn eine Benutzersitzung an der Webschnittstelle verwendet wird, um eine Systemkomponenten zu aktualisieren, müssen die Einstellungen für die **Zeitüberschreitung Leerlauf** hoch genug gesetzt sein, um dem Dateitransfer zu entsprechen. In einigen Fällen kann die Übertragungszeit der Firmware bis zu 30 Minuten betragen. Zur Einstellungen des Wertes für **Zeitüberschreitung Leerlauf** beachten Sie bitte "Dienste konfigurieren".

Die Seite Aktualisierbare Komponenten zeigt die aktuelle Version der Firmware für jede aufgeführte Komponente an und ermöglicht Ihnen, die Firmware mit der neuesten Revision zu aktualisieren. Die grundlegenden Schritte zur Aktualisierung der Geräte-Firmware sind:

- Geräte zur Aktualisierung auswählen
- Auf die Schaltfläche Anwenden unter der Gruppierung klicken
- Auf Durchsuchen klicken, um das Firmware-Image auszuwählen
- Auf Firmware-Aktualisierung starten klicken, um den Aktualisierungsvorgang zu starten. Die Meldung Datei-Image übertragen wird angezeigt, gefolgt von einer Statusfortschrittsseite.

ANMERKUNG: Stellen Sie sicher, dass Sie die neueste Firmware-Version besitzen. Sie können die neueste Firmware-Image-Datei von der Dell Support-Website herunterladen.

CMC-Firmware aktualisieren

ANMERKUNG: Während der Aktualisierung der CMC-Firmware auf einem Server, laufen einige oder alle Lüftereinheiten im Gehäuse mit 100 %. Dies ist normal.

ANMERKUNG: Der aktive CMC (primär) wird zurückgesetzt und ist vorübergehend nicht verfügbar, nachdem die Firmware erfolgreich hochgeladen wurde. Ist ein Stand-by-CMC vorhanden, werden die Rollen Stand-by und Aktiv getauscht; der Stand-by-CMC (sekundär) wird der aktive CMC (primär).

Wird eine Aktualisierung lediglich für den aktiven (primärer) CMC durchgeführt, wird der aktive CMC nach einem Reset nicht das aktualisierte Image abspielen; lediglich der Stand-by-CMC (sekundär) wird dieses Image haben.

ANMERKUNG: Um zu vermeiden, dass die Verbindung von anderen Benutzern während des Resets unterbrochen wird, benachrichtigen Sie berechtigte Benutzer, die sich am CMC anmelden könnten und überprüfen Sie auf aktive Sitzungen, indem Sie die Seite **Sitzungen** aufrufen. Um die Seite Sitzungen zu öffnen, wählen Sie in der Struktur Gehäuse, klicken auf die Registerkarte Netzwerk/Sicherheit und dann die Unterregisterkarte Sitzungen. Hilfe zu dieser Seite finden Sie über den Link Hilfe, der sich auf dieser Seite ganz oben rechts in der Ecke befindet.

ANMERKUNG: Wenn Sie Dateien zum und vom CMC übertragen, dreht sich während der Übertragung das Dateiübertragungssymbol. Wenn das Symbol nicht animiert ist, überprüfen Sie, ob der Browser so konfiguriert ist, dass Animationen zugelassen sind. Anleitungen finden Sie unter "Animationen im Internet Explorer erlauben" auf Seite 37.

ANMERKUNG: Wenn beim Herunterladen von Dateien vom CMC mit dem Internet Explorer Probleme auftreten, aktivieren Sie die Option **Verschlüsselte Seiten nicht auf der Festplatte speichern**. Anleitungen finden Sie unter "Dateien mit dem Internet Explorer vom CMC herunterladen" auf Seite 36.

1. Auf der Seite Aktualisierbare Komponenten, wählen Sie die zu aktualisierende(n) CMC(s) aus, indem Sie das Kontrollkästchen Ziele aktualisieren für die CMC(s) auswählen. Beide CMCs können gleichzeitig aktualisiert werden.
2. Klicken Sie auf die Schaltfläche CMC-Aktualisierung anwenden unterhalb der CMC-Komponentenliste.

   ANMERKUNG: Das standardmäßige Firmware-Image heißt firmimg.cmc. Die CMC-Firmware sollte zuerst, vor der Firmware der EAM-Infrastrukturgeräte, aktualisiert werden.

3. Im Feld Firmware-Image geben Sie den Pfad zur Firmware-Imagedatei auf Ihrer Managementstation oder dem gemeinsam genutzten Netzwerk ein oder klicken Sie Durchsuchen, um zum Dateispeicherort zu navigieren.
4. Klicken Sie auf Firmware-Aktualisierung beginnen. Der Abschnitt Fortschritt der Firmware-Aktualisierung bietet Statusinformationen zur Firmwareaktualisierung. Ein Statusindikator wird auf der Seite während des Aktualisierungsvorganges angezeigt. Die Zeit des Dateitransfers kann je nach Verbindungsgeschwindigkeit deutlich variieren. Wenn der interne Aktualisierungsprozess beginnt, aktualisiert sich die Seite automatisch und zeigt die Dauer der Firmwareaktualisierung. Zusätzliche Informationen:
   - Verwenden Sie während der Dateiübertragen nicht den Button Aktualisieren und navigieren nicht Sie zu einer anderen Seite.
   - Um den Prozess abzubrechen, klicken Sie auf Dateiübertrag und Aktualisierung abbrechen - diese Option ist nur während der Dateiübertragung verfügbar.
   - Der Status der Aktualisierung wird im Feld Aktualisierungsstatus angezeigt; diese Feld wird automatisch während der Dateiübertragung aktualisiert.

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

5. Bei einem Stand-by-CMC (sekundär) zeigt das Aktualisierungs- Zustandsfeld den Status "Erledigt", wenn die Aktualisierung abgeschlossen wurde. Bei einem aktiven (primären) CMC wird die Browsersitzung und die Verbindung zum CMC während der abschließenden Phase der Firmware-Aktualisierung vorübergehend unterbrochen, da der aktive (primäre) CMC offline genommen wird. Sie müssen sich nach einigen Minuten neu anmelden, wenn der aktive (primäre) CMC neu gestartet hat.

Nach dem Reset des CMC wird die neue Firmware auf der Seite Aktualisierbare Komponenten angezeigt.

ANMERKUNG: Nach dem Firmware-Upgrade löschen Sie den Cache des Internet-Browsers. Beachten Sie zum Löschen des Browser-Cache die Online-Hilfe Ihres Web-Browsers.

Aktualisieren der iKVM-Firmware

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

1. Melden Sie sich erneut bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf Chassis (Gehäuse).
3. Klicken Sie auf die Registerkarte Update (Aktualisieren). Die Seite Updatable Components (Aktualisierbare Komponenten) wird angezeigt.
4. Wählen Sie die zu aktualisierende iKVM, indem Sie das Kontrollkästchen Ziele aktualisieren für das iKVM auswählen.
5. Klicken Sie auf die Schaltfläche iKVM-Aktualisierung anwenden unterhalb der CMC-Komponentenliste.
6. Im Feld Firmware-Image geben Sie den Pfad zur Firmware-Imagedatei auf Ihrer Managementstation oder dem gemeinsam genutzten Netzwerk ein oder klicken Sie Durchsuchen, um zum Dateispeicherort zu navigieren.

ANMERKUNG: Der Standardname des iKVM-Firmware-Imagees ist ikvm.bin; der Dateiname des iKVM-Firmware-Imagees kann jedoch vom Benutzer verändert werden.

7. Klicken Sie auf Firmware-Aktualisierung beginnen.
8. Klicken Sie auf Yes (Ja), um fortzufahren. Der Abschnitt Fortschritt der Firmware-Aktualisierung bietet Statusinformationen zur Firmwareaktualisierung. Ein Statusindikator wird auf der Seite während des Aktualisierungsvorganges angezeigt. Die Zeit des Dateitransfers kann je nach Verbindungsgeschwindigkeit deutlich variieren. Wenn der interne Aktualisierungsprozess beginnt, aktualisiert sich die Seite automatisch und zeigt die Dauer der Firmwareaktualisierung. Zusätzliche Informationen:
   - Verwenden Sie während der Dateiübertragen nicht den Button Aktualisieren und navigieren nicht Sie zu einer anderen Seite.

- Um den Prozess abzubrechen, klicken Sie auf Dateiübertrag und Aktualisierung abbrechen - diese Option ist nur während der Dateiübertragung verfügbar.
- Der Status der Aktualisierung wird im Feld Aktualisierungsstatus angezeigt; diese Feld wird automatisch während der Dateiübertragung aktualisiert.

ANMERKUNG: Die Aktualisierung für das iKVM kann bis zu zwei Minuten dauern.

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

Aktualisierung der Firmware des EAM-Infrastrukturgeräts

Das Ausführen dieser Aktualisierung führt dazu, dass die Firmware für eine Komponente des EAM-Geräts aktualisiert wird, aber nicht die Firmware des EAM-Geräts selbst; die Komponente ist die Schnittstellenschaltung zwischen dem EAM-Gerät und dem CMC. Das Aktualisierungs-Image für die Komponente befindet sich im CMC-Dateisystem und die Komponente wird nur als aktualisierbares Gerät auf der CMC-Web-GUI angezeigt, wenn die aktuelle Revision auf der Komponente und das Komponenten-Image nicht übereinstimmen.

1. Melden Sie sich erneut bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf Chassis (Gehäuse).
3. Klicken Sie auf die Registerkarte Update (Aktualisieren). Die Seite Updatable Components (Aktualisierbare Komponenten) wird angezeigt.
4. Wählen Sie das zu aktualisierende EAM-Gerät, indem Sie das Kontrollkästchen Ziele markieren für dieses EAM-Gerät markieren.
5. Klicken Sie auf die Schaltfläche EAM-Aktualisierung anwenden unterhalb der CMC-Komponentenliste.

   ANMERKUNG: Das Feld **Firmware-Image** wird für ein EAM- Infrastrukturgerät-Ziel (IOMINF) nicht angezeigt, da sich das benötigte Image auf dem CMC befindet. Die CMC-Firmware sollte zuerst, vor der IONINF- Firmware, aktualisiert werden.

   IOMINF-Aktualisierungen werden vom CMC zugelassen, wenn der CMC erkennt, dass die IOMINF-Firmware gegenüber dem im CMC-Dateisystem enthaltenen Image veraltet ist. Falls die IOMINF-Firmware auf dem neuesten Stand ist, verhindert der CMC IOMINF-Aktualisierungen. Aktualisierte IOMINF-Geräte sind als aktualisierbare Geräte aufgelistet.
6. Klicken Sie auf Firmware-Aktualisierung beginnen. Der Abschnitt Fortschritt der Firmware-Aktualisierung bietet Statusinformationen zur Firmwareaktualisierung. Ein Statusindikator wird auf der Seite während des Aktualisierungsvorganges angezeigt. Die Zeit des Dateitransfers kann je nach Verbindungsgeschwindigkeit deutlich variieren. Wenn der interne Aktualisierungsprozess beginnt, aktualisiert sich die Seite automatisch und zeigt die Dauer der Firmwareaktualisierung. Zusätzliche Informationen:
   - Verwenden Sie während der Dateiübertragung nicht die Schaltfläche Aktualisieren und navigieren Sie nicht zu einer anderen Seite.
   - Der Status der Aktualisierung wird im Feld Aktualisierungsstatus angezeigt; diese Feld wird automatisch während der Dateiübertragung aktualisiert.

ANMERKUNG: Es wird bei der IOMINF-Firmware-Aktualisierung kein Zeitgeber angezeigt. Der Aktualisierungsprozess kann kurzzeitigen Verlust der Verbindungen verursachen, da das Gerät einen Neustart durchführt, wenn die Aktualisierung abgeschlossen ist.

Wenn die Aktualisierung abgeschlossen ist, wird die neue Firmware auf der Seite Aktualisierbare Komponenten angezeigt, und das aktualisierte System ist auf dieser Seite nicht mehr vorhanden.

iDRAC-Firmware aktualisieren

ANMERKUNG: Der iDRAC (auf einem Server) wird zurückgesetzt und vorübergehend nicht verfügbar, nachdem die Firmware-Aktualisierung erfolgreich geladen wurde.

ANMERKUNG: Die iDRAC-Firmware muss Version 1.4 oder höher für Server mit iDRAC, oder 2.0 oder höher für Server mit iDRAC6 Enterprise sein.

1. Melden Sie sich erneut bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf Chassis (Gehäuse).
3. Klicken Sie auf die Registerkarte Update (Aktualisieren). Die Seite Updatable Components (Aktualisierbare Komponenten) wird angezeigt.
4. Wählen Sie die zu aktualisierende(n) iDRAC(s), indem Sie das Kontrollkästchen Ziele aktualisieren für diese Geräte wählen.
5. Klicken Sie auf die Schaltfläche iDRAC-Aktualisierung anwenden unterhalb der CMC-Komponentenliste.
6. Im Feld Firmware-Image geben Sie den Pfad zur Firmware-Imagedatei auf Ihrer Managementstation oder dem gemeinsam genutzten Netzwerk ein oder klicken Sie Durchsuchen, um zum Dateispeicherort zu navigieren.
7. Klicken Sie auf Firmware-Aktualisierung beginnen. Der Abschnitt Fortschritt der Firmware-Aktualisierung bietet Statusinformationen zur Firmwareaktualisierung. Ein Statusindikator wird auf der Seite während des Aktualisierungsvorganges angezeigt. Die Zeit des Dateitransfers kann je nach Verbindungsgeschwindigkeit deutlich variieren. Wenn der interne Aktualisierungsprozess beginnt, aktualisiert sich die Seite automatisch und zeigt die Dauer der Firmwareaktualisierung an. Zusätzliche Informationen:

- Verwenden Sie während der Dateiübertragung nicht die Schaltfläche Aktualisieren und navigieren Sie nicht zu einer anderen Seite.
- Um den Prozess abzubrechen, klicken Sie auf Dateiübertrag und Aktualisierung abbrechen - diese Option ist nur während der Dateiübertragung verfügbar.
- Der Status der Aktualisierung wird im Feld Aktualisierungsstatus angezeigt; diese Feld wird automatisch während der Dateiübertragung aktualisiert.

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

iDRAC-Firmware mittels CMC wiederherstellen

iDRAC-Firmware wird normalerweise mit dem iDRAC, z. B. über die iDRAC-Webschnittstelle, die SM-CLP-Befehlszeilenschnittstelle oder mit betriebssystemspezifischen Aktualisierungspaketen, die von der Website **support.dell.com** heruntergeladen wurden, aktualisiert. Wie Sie die iDRAC-Firmware aktualisieren, erfahren Sie im *Benutzerhandbuch zur iDRAC-Firmware*.

Frühere Generationen von Servern können beschädigte Firmware aufweisen, die unter Verwendung des kürzlich aktualisierten iDRAC-Firmware-Prozesses wiederhergestellt werden. Wenn der CMC beschädigte iDRAC-Firmware erkennt, wird der Server auf der Seite **Aktualisierbare Komponenten** aufgeführt.

Führen Sie diese Schritte aus, um die iDRAC-Firmware zu aktualisieren.

1. Laden Sie die neueste iDRAC-Firmware von **support.dell.com** auf den Verwaltungscomputer herunter.
2. Melden Sie sich bei der Webschnittstelle an (siehe "Auf die CMC- Webschnittstelle zugreifen").
3. Klicken Sie in der Systemstruktur auf **Chassis** (Gehäuse).
4. Klicken Sie auf die Registerkarte Update (Aktualisieren). Die Seite Updatable Components (Aktualisierbare Komponenten) wird angezeigt.
5. Wählen Sie die zu aktualisierende(n) iDRAC(s) auf demselben Modell, indem Sie das Kontrollkästchen Ziele aktualisieren für diese Geräte wählen.
6. Klicken Sie auf die Schaltfläche iDRAC-Aktualisierung anwenden unterhalb der CMC-Komponentenliste.
7. Klicken Sie auf **Durchsuchen**, und suchen Sie nach dem von Ihnen heruntergeladenen iDRAC-Firmware-Image. Klicken Sie dann auf **Öffnen**.

   ANMERKUNG: Der Standardname für das iDRAC-Firmware-Image ist **firmimg.imc**.

8. Klicken Sie auf **Firmware-Aktualisierung beginnen**. Zusätzliche Informationen:
   - Verwenden Sie während der Dateiübertragung nicht die Schaltfläche Aktualisieren und navigieren Sie nicht zu einer anderen Seite.
   - Um den Prozess abzubrechen, klicken Sie auf Dateiübertrag und Aktualisierung abbrechen - diese Option ist nur während der Dateiübertragung verfügbar.
   - Der Status der Aktualisierung wird im Feld Aktualisierungsstatus angezeigt; diese Feld wird automatisch während der Dateiübertragung aktualisiert.

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

---

iDRAC verwalten

Der CMC stellt die Seite iDRAC bereitstellen bereit, um dem Benutzer die Konfiguration von installierten und neu eingefügten iDRAC-Netzwerkkonfigurationseinstellungen des Servers zu ermöglichen. Ein Benutzer kann ein oder mehrere installierte iDRAC-Geräte von dieser Seite aus konfigurieren. Der Benutzer kann außerdem die Standard- iDRAC-Netzwerkkonfigurationseinstellungen und das Stammkennwort für Server, die zu einem späteren Zeitpunkt installiert werden, konfigurieren; diese Standardeinstellungen sind die Einstellungen der schnellen iDRAC Bereitstellung.

Weitere Informationen zum iDRAC-Verhalten finden Sie in den *iDRAC-Benutzerhandbüchern* auf der Dell Support-Website unter **support.dell.com**.

Schnelle iDRAC Bereitstellung

Der Abschnitt Schnelle iDRAC Bereitstellung auf der Seite iDRAC bereitstellen enthält Netzwerkkonfigurationseinstellungen, die auf neu eingefügte Server angewendet werden. Diese Einstellungen können dazu verwendet werden, die Tabelle iDRAC-Netzwerkeinstellungen, die sich unter dem Abschnitt Schnelle Bereitstellung befindet, automatisch zu bestücken. Wenn Schnelle Bereitstellung aktiviert ist, werden die Einstellungen der schnellen Bereitstellung auf Server angewendet, wenn dieser Server installiert wird.

Befolgen Sie diese Schritte um die Einstellung der schnellen iDRAC-Bereitstellung zu aktivieren und einzustellen:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf Servers (Server).
3. Klicken Sie auf die Registerkarte Setup. Die Seite iDRAC bereitstellen wird angezeigt.
4. Stellen Sie die Einstellungen zur schnellen Bereitstellung entsprechend ein.

Tabelle 5-37. Einstellungen zur schnellen Bereitstellung

Einstellung	Beschreibung
Schnelle Bereitstellung aktiviert	Aktiviert/deaktiviert die Funktion Schnelle Bereitstellung, welche die iDRAC-Einstellungen, die auf dieser Seite konfiguriert sind, auf neu eingefügte Server anwendet; die automatische Konfiguration muss lokal auf der LCD-Konsole bestätigt werden. **ANMERKUNG:** Dies schließt das Stammbenutzerkennwort ein, wenn das Kontrollkästchen iDRAC-Stammkennwort bei Servereinfügung einstellen markiert ist. Standardeinstellung: Nicht markiert (deaktiviert)
iDRAC-Stammkennwort bei Servereinfügung einstellen	Gibt an ob das iDRAC-Stammkennwort eines Servers zu dem Wert geändert werden soll, der in das Textfeld iDRAC-Stammkennwort eingegeben wird, wenn der Server eingefügt wird.
iDRAC-Stammkennwort	Wenn iDRAC-Stammkennwort bei Servereinfügung einstellen und Schnelle Bereitstellung aktiviert markiert sind, wird der Kennwortwert einem Server-iDRAC-Stammbenutzerkennwort zugewiesen, wenn der Server in das Gehäuse eingefügt wird. Das Kennwort kann 1 bis 20 druckbare (einschließlich Leerzeichen) Zeichen haben.
iDRAC-Stammkennwort bestätigen	Bestätigt das Kennwort, das in das Feld iDRAC-Stammkennwort eingegeben wurde.
iDRAC LAN aktivieren	Aktiviert/deaktiviert den iDRAC LAN-Kanal. Standardeinstellung: Nicht markiert (deaktiviert)
iDRAC IPv4 aktivieren	Aktiviert/deaktiviert IPv4 auf dem iDRAC. Die Standardeinstellung lautet "aktiviert".
IPMI-Über-LAN aktivieren	Aktiviert/deaktiviert den IPMI-über-LAN-Kanal für jeden iDRAC, der sich in dem Gehäuse befindet. Standardeinstellung: Nicht markiert (deaktiviert)
iDRAC DHCP aktivieren	Aktiviert/deaktiviert DHCP für jeden iDRAC, der sich in dem Gehäuse befindet. Wenn diese Option aktiviert ist, sind die Felder Schnelle Bereitstellung-IP, Schnelle Bereitstellung-Subnetzmaske und Schnelle Bereitstellung-Gateway deaktiviert und können nicht geändert werden, da DHCP verwendet wird, um diese Einstellungen automatisch für jeden iDRAC zuzuweisen. Standardeinstellung: Nicht markiert (deaktiviert)
iDRAC-IPv4-Adresse (Steckplatz 1) starten	Gibt die statische IP-Adresse des iDRAC des Servers in Steckplatz 1 des Gehäuses an. Die IP-Adresse jedes folgenden 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 der Gateway werden nicht wie die IP-Adresse erhöht. Wenn zum Beispiel die ursprüngliche IP-Adresse 192.168.0.250 und die Subnetzmaske 255.255.0.0 ist, dann ist die schnelle Bereitstellungs-IP-Adresse für Steckplatz 15: 192.168.0.265. Wenn die Subnetzmaske 255.255.255.0 wäre, würde die Fehlermeldung Schneller Bereitstellungs-IP-Adressenbereich befindet sich nicht vollständig innerhalb des schnellen Bereitstellungs-Subnetzes angezeigt werden, wenn entweder die Schaltfläche Einstellungen zur schnellen Bereitstellung oder die Schaltfläche Mit Einstellungen zur schnellen Bereitstellung automatisch bestücken gedrückt werden.
iDRAC IPv4-Netzmaske	Gibt die schnelle Bereitstellungs-Subnetzmaske an, die allen neu eingefügten Servern zugewiesen ist.
iDRAC IPv4-Gateway	Gibt den schnellen Bereitstellungs-Standard-Gateway an, der allen iDRACs, die sich im Gehäuse befinden, zugewiesen ist.
iDRAC IPv6 aktivieren	Aktiviert IPv6-Adressierung für jeden iDRAC, der sich in dem Gehäuse befindet und IPv6-fähig ist.
iDRAC IPv6 AutoConfiguration aktivieren	Aktiviert den iDRAC zur Beschaffung von IPv6-Einstellungen (Adresse und Präfixlänge) von einem DHCPv6-Server und aktiviert auch statuslose automatische Adresskonfiguration. Die Standardeinstellung lautet "aktiviert".
iDRAC IPv6-Gateway	Gibt das Standard-IPv6-Gateway an, das den iDRACs zugewiesen wird. Die Standardeinstellung ist "::".
iDRAC IPv6-Präfixlänge	Gibt die Präfixlänge an, die den IPv6-Adressen auf dem iDRAC zugewiesen wird. Die Standardeinstellung ist 64.

5. Um die Auswahl zu speichern, drücken Sie die Schaltfläche Einstellungen zur schnellen Bereitstellung speichern. Wenn Sie jegliche Änderungen an den Einstellungen des iDRAC-Netzwerkes vorgenommen haben, klicken Sie auf die Schaltfläche iDRAC-Netzwerkeinstellungen anwenden, um die Einstellungen zur iDRAC bereitzustellen.
6. Um die Tabelle zu den zuletzt gespeicherten Einstellungen zur schnellen Bereitstellung zu aktualisieren und die iDRAC-Netzwerkeinstellungen zu den aktuellen Werten für jeden installierten Server wiederherzustellen, klicken Sie auf Aktualisieren.

ANMERKUNG: Durch das Klicken auf die Schaltfläche Aktualisieren werden alle schnellen iDRAC-Bereitstellungs- und iDRAC-Netzwerkkonfigurationseinstellungen gelöscht, die nicht gespeichert wurden.

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

ANMERKUNG: Wenn eine LAN- oder LAN-über- IPMI-Abweichung vorhanden ist, wird der Benutzer aufgefordert, die Einstellungen der schnellen Bereitstellungs-IP- Adresse anzunehmen. Wenn der Unterschied in der DHCP-Einstellung liegt, wird der Benutzer aufgefordert, die Einstellungen der schnellen DHCP-Bereitstellung anzunehmen.

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

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

iDRAC-Netzwerkeinstellungen

Der Abschnitt **iDRAC-Netzwerkeinstellungen** auf der Seite **iDRAC bereitstellen** enthält eine Tabelle, die die iDRAC IPv4- und IPv6-Netzwerkkonfigurationseinstellungen aller installierten Server aufführt. Mithilfe dieser Tabelle können Sie die iDRAC-Netzwerkkonfigurationseinstellungen für jeden installierten Server konfigurieren. Die anfänglichen Werte, die für jedes Feld angezeigt werden, sind die aktuellen vom iDRAC gelesenen Werte. Durch Ändern eines Felds und Klicken auf iDRAC-Netzwerkeinstellungen anwenden werden die geänderten Felder auf dem iDRAC gespeichert. Befolgen Sie diese Schritte, um die iDRAC-Netzwerkeinstellungen zu aktivieren und einzustellen:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Klicken Sie in der Systemstruktur auf Servers (Server).
3. Klicken Sie auf die Registerkarte Setup.

Die Seite iDRAC bereitstellen wird angezeigt.

4. Wählen Sie das Kontrollkästchen Schnelle Bereitstellung aktiviert, um die Einstellungen zur schnellen Bereitstellung zu aktivieren.
5. Stellen Sie die restlichen iDRAC-Netzwerkeinstellungen entsprechend ein.

Tabelle 5-38. iDRAC-Netzwerkeinstellungen

Einstellung	Beschreibung
Steckplatz	Zeigt den vom Server im Gehäuse besetzten Steckplatz an. Steckplatznummern sind sequenzielle IDs von 1 bis 16 (für die 16 im Gehäuse verfügbaren Steckplätze), mit denen die Position des Servers im Gehäuse identifiziert werden kann. **ANMERKUNG:** Wenn weniger als 16 Steckplätze mit Servern belegt sind, werden nur die mit Servern bestückten Steckplätze angezeigt.
Name	Zeigt den Servernamen des Servers in jedem Steckplatz an. Standardmäßig heißen die Steckplätze STECKPLATZ-01 bis STECKPLATZ-16. **ANMERKUNG:** Der Steckplatzname kann nicht leer oder NULL sein.
LAN aktivieren	Aktiviert (markiert) oder deaktiviert (nicht markiert) den LAN-Kanal. **ANMERKUNG:** Wenn LAN nicht ausgewählt ist (deaktiviert), werden alle anderen Netzwerkkonfigurationseinstellungen (IPMI-über-LAN, DHCP, IP-Adresse Subnetzmaske und Gateway) nicht verwendet. Diese Felder sind nicht zugreifbar.
Stammkennwort ändern	Aktiviert (wenn markiert) die Möglichkeit, das Kennwort des iDRAC-Stammbenutzers zu ändern. Die Felder iDRAC-Stammkennwort und iDRAC-Stammkennwort bestätigen müssen ausgefüllt sein, damit dieser Vorgang erfolgreich ist.
DHCP	Wenn markiert, wird DHCP verwendet, um IP-Adresse, Subnetzmaske und Standard-Gateway des iDRAC zu erwerben. Ansonsten werden die in den iDRAC-Netzwerkkonfigurationsfeldern definierten Werte verwendet. LAN muss aktiviert sein, um dieses Feld einzustellen.
IPMI über LAN	Aktiviert (markiert) oder deaktiviert (nicht markiert) den LAN-Kanal. LAN muss aktiviert sein, um dieses Feld einzustellen.
IP-Adresse	Die statische IPv4- oder IPv6-Adresse, die dem iDRAC in diesem Steckplatz zugewiesen ist.
Subnetzmaske	Gibt die Subnetzmaske an, die dem in diesem Steckplatz installierten iDRAC zugewiesen ist.
Gateway	Gibt den Standard-Gateway an, der dem in diesem Steckplatz installierten iDRAC zugewiesen ist.
IPv4 aktivieren	Aktiviert den iDRAC im Steckplatz für die Verwendung des IPv4-Protokolls im Netzwerk. Diese Option kann nur aktiv sein, wenn Sie die Option **LAN aktivieren** auswählen. Die Standardeinstellung lautet "aktiviert".
IPv6 aktivieren	Aktiviert den iDRAC im Steckplatz für die Verwendung des IPv6-Protokolls im Netzwerk. Diese Option kann nur aktiv sein, wenn Sie die Option **LAN aktivieren** auswählen und die **AutoConfiguration**-Option deaktivieren. Die Standardeinstellung lautet "deaktiviert". **ANMERKUNG:** Diese Option ist nur verfügbar, wenn der Server IPv6-fähig ist.
AutoConfiguration	Aktiviert den iDRAC zur Beschaffung von IPv6-Einstellungen (Adresse und Präfixlänge) von einem DHCPv6-Server und aktiviert auch statuslose automatische Adresskonfiguration. **ANMERKUNG:** Diese Option ist nur verfügbar, wenn der Server IPv6-fähig ist.
Präfixlänge	Gibt die Länge des IPv6-Subnetzes (in Bit) an, zu dem dieser iDRAC gehört.

6. Um die Einstellung auf dem iDRAC bereitzustellen, klicken Sie auf die Schaltfläche iDRAC-Netzwerkeinstellungen anwenden. Wenn Sie Änderungen an den Einstellungen zur schnellen Bereitstellung vorgenommen haben, werden diese ebenfalls gespeichert.

7. Um die iDRAC-Netzwerkeinstellungen zu den aktuellen Werten für jedes installierte Blade wiederherzustellen und die Tabelle der schnellen Bereitstellung zu den zuletzt gespeicherten Einstellungen der schnellen Bereitstellungen zu aktualisieren, klicken Sie auf Aktualisieren.

ANMERKUNG: Durch das Klicken auf die Schaltfläche Aktualisieren werden alle schnellen iDRAC-Bereitstellungs- und iDRAC-Netzwerkkonfigurationseinstellungen gelöscht, die nicht gespeichert wurden.

Die Tabelle iDRAC-Netzwerkeinstellungen zeigt zukünftige Netzwerkkonfigurationseinstellungen; die für installierte Blades angezeigten Werte können die gleichen sein, wie die Werte der zurzeit installierten iDRAC-Netzwerkkonfigurationseinstellungen. Drücken Sie die Schaltfläche Aktualisieren, um die Seite iDRAC-Bereitstellung mit jeder installierten iDRAC-Netzwerkkonfigurationseinstellung zu aktualisieren, nachdem Äderungen vorgenommen wurden.

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

iDRAC mit Einzelanmeldung starten

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

Um die iDRAC-Verwaltungskonsole von der Seite Server zu starten, führen Sie die folgenden Schritte aus:

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Wählen Sie in der Systemstruktur Server aus. Die Seite Servers Status (Serverstatus) wird angezeigt.
3. Klicken Sie auf das Symbol iDRAC GUI starten für den Server, den Sie verwalten wollen.

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

1. Melden Sie sich bei der CMC-Webschnittstelle an.
2. Erweitern Sie in der Systemstruktur Server. Es werden alle Server (1–16) in der erweiterten Liste der Server angezeigt.
3. Klicken Sie auf den Server, den Sie anzeigen möchten. Die Seite Serverstatus wird angezeigt.
4. Klicken Sie auf das Symbol iDRAC GUI starten.

Ein Benutzer kann die iDRAC GUI starten ohne sich ein zweites Mal anzumelden, da diese Funktion die Einzelanmeldung verwendet. Die Richtlinien der Einzelanmeldung sind nachfolgend beschrieben.

- Ein CMC-Benutzer, der Serveradministratorberechtigungen hat, wird automatisch mit der Einzelanmeldung 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 hat.
- Ein CMC-Benutzer der KEINE Serveradministratorrechte hat, aber dasselbe Konto auf iDRAC besitzt, wird automatisch mit der Einzelanmeldung 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 der Einzelanmeldung bei iDRAC angemeldet. Dieser Benutzer wird zur iDRAC-Anmeldungsseite umgeleitet, wenn die Schaltfläche iDRAC GUI starten geklickt wird.

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

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

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

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

FlexAddress

Dieser Abschnitt beschreibt die FlexAddress®-Webschnittstellenbildschirme. FlexAddress ist eine optionale Erweiterung, die es ermöglicht, die werkseitig zugewiesenen WWN/MAC-IDs der Servermodule mit einer WWN/MAC-ID des Gehäuses zu ersetzen.

ANMERKUNG: Sie müssen die FlexAddress-Erweiterung kaufen und installieren, um Zugriff auf die Konfigurationsbildschirme zu haben. Wenn das Upgrade nicht gekauft und installiert wurde, wird der folgende Text in der Webschnittstelle angezeigt:

```
Optional feature not installed. See the Dell Chassis Management Controller Users Guide for information on the chassis-based WWN and MAC address administration feature.

(Optionale Funktion nicht installiert. Nutzen Sie das Dell Benutzerhandbuch zur Gehäuseverwaltung für Informationen bezüglich der Administratorfunktion der Gehäuse-basierten WWN und MAC-Adresse.)


To purchase this feature, please contact Dell at www.dell.com.

(Um diese Funktion zu erstehen, kontaktieren Sie Dell bitte unter www.dell.com.)
```

Anzeigen des FlexAddress-Status

Sie können die Webschnittstelle nutzen, um Statusinformationen zu FlexAddress anzuzeigen. Sie können die Statusinformationen für das gesamte Gehäuse oder für einen einzelnen Server anzeigen lassen. Die angezeigten Informationen beinhalten:

- Architekturkonfiguration
- FlexAddress aktiv/nicht aktiv
- Steckplatznummer und -name
- Gehäuse-zugewiesene und Server-zugewiesene Adressen
- Verwendete Adressen

ANMERKUNG: Sie können den Status von FlexAddress auch über die Befehlszeile der Schnittstelle einsehen. Weitere Befehlsinformationen finden Sie unter "FlexAddress verwenden".

Anzeigen des Status Gehäuse FlexAddress

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

Verwenden Sie die folgenden Schritte, um zu sehen, ob FlexAddress für das Gehäuse aktiviert ist:

1. Melden Sie sich bei der Webschnittstelle an (siehe "Auf die CMC- Webschnittstelle zugreifen").
2. Klicken Sie in der Systemstruktur auf **Chassis** (Gehäuse).
3. Klicken Sie auf die Registerkarte Setup. Die Seite Allgemeine Einstellungen erscheint. Der Eintrag für FlexAddress wird einen Wert Aktiv oder Nicht Aktiv haben; ein Eintrag "aktiv" bedeutet, dass die Funktion für das Gehäuse installiert wurde. Ein Wert "nicht aktiv" bedeutet, dass die Funktion nicht für das Gehäuse installiert wurde und nicht verwendet wird.

Verwenden Sie die folgenden Schritte um einen FlexAddress-Statusüberblick für jedes Servermodul anzuzeigen:

1. Melden Sie sich bei der Webschnittstelle an (siehe "Auf die CMC- Webschnittstelle zugreifen").
2. Erweitern Sie in der Systemstruktur Server. Klicken Sie auf die Registerkarte Eigenschaften und dann die Unterregisterkarte WWN/MAC.
3. Die Seite FlexAddress-Zusammenfassung wird angezeigt. Diese Seite erlaubt Ihnen, die WWN-Konfiguration und die MAC-Adressen für alle Steckplätze im Gehäuse anzuzeigen.

Die Statusseite zeigt die folgenden Informationen:

Architekturkonfiguration	Architektur A, Architektur B und Architektur C zeigen den Typ der installierten Eingabe/Ausgabe-Architektur. **iDRAC** zeigt die Server Management MAC-Adresse an. **ANMERKUNG:** Wenn Architektur A aktiviert ist, werden die nicht bestückten Steckplätze Gehäuse-zugewiesene MAC-Adressen für Architektur A, und MAC oder WWNs für Architektur B und C anzeigen, wenn diese von den bestückten Steckplätzen verwendet werden.

WWN / MAC-Adressen	Zeigt die FlexAddress-Konfiguration für jeden Steckplatz im Gehäuse an. Die angezeigten Informationen beinhalten: • Der iDRAC Management Controller ist keine Architektur, doch seine FlexAddress wird wie eine Architektur behandelt. • Steckplatznummer und -position • FlexAddress-Status aktiv/nicht aktiv • Architekturtyp • Server-zugewiesene und Gehäuse-zugewiesene, verwendete WWN/MAC-Adressen Ein grünes Häkchen zeigt den aktiven Adresstyp, entweder Server-zugewiesen oder Gehäuse-zugewiesen.

4. Für weitere Informationen klicken Sie auf den Hilfe-Link und lesen Sie "FlexAddress verwenden".

Anzeigen des Status' Server FlexAddress

FlexAddress-Statusinformationen können auch für jeden einzelnen Server angezeigt werden. Die Server-Levelinformation zeigt den FlexAddress-Status überblickartig für jenen Einschubserver an.

Nutzen Sie die folgenden Schritte, um die FlexAddress-Serverinformationen anzuzeigen:

1. Melden Sie sich bei der Webschnittstelle an (siehe Auf die CMC- Webschnittstelle zugreifen).
2. Erweitern Sie in der Systemstruktur Server. Es werden alle Server (1–16) in der erweiterten Liste der Server angezeigt.
3. Klicken Sie auf den Server, den Sie anzeigen möchten. Die Seite Serverstatus wird angezeigt.
4. Klicken Sie die Registerkarte Einstellungen und dann die Unterregisterkarte FlexAddress. Die Seite FlexAddress-Status wird angezeigt. Diese Seite erlaubt Ihnen, die WWN-Konfiguration und die MAC-Adressen für ausgewählten Server anzuzeigen.

Die Statusseite zeigt die folgenden Informationen:

FlexAddress aktiviert	Zeigt, ob die Funktion FlexAddress für einen bestimmten Steckplatz entweder aktiviert oder deaktiviert ist.		
Aktueller Zustand	Zeigt die derzeitige FlexAddress-Konfiguration: • Gehäuse-zugewiesen - die ausgewählte Steckplatz-Adresse ist mittels FlexAddress dem Gehäuse zugewiesen. Die Steckplatz-basierten WWN/MAC-Adressen bleiben die gleiche, selbst wenn ein neuer Server installiert wird. • Server-zugewiesen - der Server verwendet eine Server-zugewiesen Adresse oder die standardmäßig in die Controller-Hardware eingebettete Adresse.		
Stromzustand	Zeigt den aktuellen Stromzustand der Server an; Werte sind:Ein, Einschalten, Ausschalten, Aus und k.A. (wenn ein Server nicht erkannt wird).		
Funktionszustand		OK	Zeigt an, dass FlexAddress aktiv ist und liefert den Status an den CMC. Im Falle eines Fehlers bei der Datenübertragung zwischen dem CMC und FlexAddress, kann der CMC den Funktionszustand für die Netzteileinheit weder abrufen noch anzeigen.
		Zur Information	Zeigt Informationen über FlexAddress an, wenn beim Funktionsstatus (OK, Warnung, Schwerwiegend) keine Änderung eingetreten ist.
		Warnung	Zeigt an, dass Warnungen ausgegeben wurden und Korrekturmaßnahmen ergriffen werden müssen. Wenn innerhalb des vom Administrator festgelegten Zeitraums keine Korrekturmaßnahmen vorgenommen werden, könnten kritische oder schwerwiegende Fehler auftreten, die sich wiederum auf die Integrität des Servers auswirken können.
		Schwerwiegend	Zeigt an, dass mindestens eine Fehlerwarnung ausgegeben wurde. Ein schwerwiegender Status repräsentiert einen Systemfehler auf dem Server. Es müssen umgehend Korrekturmaßnahmen getroffen werden.
		Kein Wert	Wenn FlexAddress nicht verfügbar ist, werden keine Informationen zum Funktionszustand geliefert.
iDRAC Firmware	Zeigt die derzeit auf dem Server installierte iDRAC-Version an.		
BIOS-Version	Zeigt die derzeit auf dem Servermodul installierte BIOS-Version an.		
Steckplatz	Steckplatznummer des Server, der mit der Architektur-Position verbunden ist, an.		
Standort	Zeigt die Position des Eingabe/Ausgabe (E/A) Moduls im Gehäuse nach		

	Gruppennummer (A, B oder C) und Steckplatznummer (1 oder 2) an. Steckplatznamen: A1, A2, B1, B2, C1 oder C2.
Architektur	Zeigt die Architektur an.
Server-zugewiesen	Zeigt die dem Server zugewiesenen WWN/MAC-Adressen an, die in die Hardware der Steuerung eingebettet sind.
Gehäuse-zugewiesen	Zeigt die dem Gehäuse zugewiesenen WWN/MAC-Adressen an, die für einen bestimmten Steckplatz verwendet werden.

5. Für weitere Informationen klicken Sie den Hilfe-Link und lesen Sie FlexAddress verwenden.

FlexAddress konfigurieren

Wenn Sie FlexAddress mit dem Gehäuse bestellt haben, ist es beim Einschalten des Systems installiert und aktiviert. Wenn Sie FlexAddress zu einem späteren Zeitpunkt erwerben, müssen Sie die SD-Funktionskarte gemäß den Anweisungen im Dokument CMC Secure Digital (SD) Card Technical Specification installieren. Sie finden dieses Dokument unter support.dell.com.

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

Für die ausgewählten Steckplätze wird FlexAddress für alle Architekturen aktiviert, die auch aktiviert sind. So ist es zum Beispiel nicht möglich, Architektur-A und -B zu aktivieren und FlexAddress auf Steckplatz 1 nur für Architektur-A, nicht aber für Architektur-B, zu aktivieren.

ANMERKUNG: Sie können den Status von FlexAddress auch über die Befehlszeile der Schnittstelle einsehen. Weitere Befehlsinformationen finden Sie unter FlexAddress verwenden.

Konfiguration der FlexAddress Architektur und Steckplatz auf Gehäuseebene

Auf Gehäuseebene können Sie FlexAddress für Architekturen und Steckplätze aktivieren oder deaktivieren FlexAddress ist jeweils für eine Architektur zu aktivieren und dann werden die Steckplätze, die davon betroffen sein sollen, ausgewählt. Sowohl Architekturen, als auch Steckplätze müssen für einen erfolgreiche FlexAddress-Konfiguration aktiviert sein.

Führen Sie folgende Schritte durch, um Architekturen und Steckplätze für die Nutzung von FlexAddress zu aktivieren oder zu deaktivieren:

1. Melden Sie sich bei der Webschnittstelle an (siehe "Auf die CMC- Webschnittstelle zugreifen").
2. Erweitern Sie in der Systemstruktur **Server**.
3. Klicken Sie auf der Registerkarte Setup auf die Unterregisterkarte → **FlexAddress**. Die Seite FlexAddress-Zusammenfassung wird angezeigt.
4. Der Abschnitt Architektur auswählen für gehäuseseitige WWN/MACs zeigt ein Kontrollkästchen für Architektur A, Architektur B, Architektur C und iDRAC.
5. Klicken Sie das Kontrollkästchen für jede Architektur, für die Sie FlexAddress aktivieren möchten. Um eine Architektur zu deaktivieren, klicken Sie auf das Kontrollkästchen, um die Auswahl zu löschen.

ANMERKUNG: Sind keine Architekturen ausgewählt, wird FlexAddress nicht für die gewählt Steckplätze aktiviert.

Die Seite Steckplatz auswählen für gehäuseseitige WWN/MACs zeigt ein aktiviertes Kontrollkästchen für jeden Steckplatz im Gehäuse (1-16).

6. Klicken Sie das Aktiviert-Kontrollkästchen für jeden Steckplatz, für den Sie FlexAddress aktivieren möchten. Wenn Sie alle Steckplätze auswählen möchten, verwenden Sie das Kontrollkästchen Alle auswählen/abwählen. Um einen Steckplatz zu deaktivieren, klicken Sie auf das Aktiviert-Kontrollkästchen, um die Auswahl zu löschen.

ANMERKUNG: Ist ein Einschubserver im Steckplatz vorhanden, muss dieser zunächst ausgeschaltet werden, bevor die Funktion FlexAddress für diesen Steckplatz aktiviert werden kann.

ANMERKUNG: Sind keine Steckplätze ausgewählt, wird FlexAddress nicht für die gewählten Architekturen aktiviert.

7. Klicken Sie auf Apply (Übernehmen), um die Änderungen zu speichern.

Für weitere Informationen klicken Sie auf den Hilfe-Link und lesen Sie "FlexAddress verwenden".

Serverseitige FlexAddress-Steckplatzkonfiguration

Auf Serverebene können Sie FlexAddress für einzelne Steckplätze aktivieren oder deaktivieren

Führen Sie die folgenden Schritte durch, um einen einzelnen Steckplatz für FlexAddress zu aktivieren oder zu deaktivieren:

1. Melden Sie sich bei der Webschnittstelle an (siehe "Auf die CMC- Webschnittstelle zugreifen").
2. Erweitern Sie in der Systemstruktur Server. Es werden alle Server (1 - 16) in der erweiterten Liste der Server angezeigt.
3. Klicken Sie auf den Server, den Sie anzeigen möchten. Die Seite Serverstatus wird angezeigt.
4. Klicken Sie die Registerkarte Einstellungen und dann die Unterregisterkarte FlexAddress. Die Seite FlexAddress-Status wird angezeigt.
5. Verwenden Sie das Ausklappmenü für FlexAddress aktiviert, um Ihre Auswahl zu treffen; wählen Sie Yes (Ja), um FlexAddress zu aktivieren oder wählen Sie No (Nein), um FlexAddress zu deaktivieren.
6. Klicken Sie auf Apply (Übernehmen), um die Änderungen zu speichern. Für weitere Informationen klicken Sie auf den Hilfe-Link und lesen Sie "FlexAddress verwenden".

Remote-Dateifreigabe

Die Option Remote-Dateifeigabe für virtuelle Datenträger ordnet ein Freigabelaufwerk im Netzwerk über den CMC einem oder mehreren Blades 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: Floppy-Laufwerke und CD/DVD-Laufwerke.

1. Melden Sie sich bei der Webschnittstelle an (siehe "Auf die CMC- Webschnittstelle zugreifen").
2. Erweitern Sie in der Systemstruktur Server.
3. Klicken Sie auf die Registerkarte Einstellungen und dann die Unterregisterkarte Remote-Dateifreigabe. Die Seite Remote- Dateifreigabe **bereitstellen** wird angezeigt.
4. Legen Sie die Einstellungen für die Remote-Dateifreigabe fest.

Tabelle 5-39. Remote-Dateifreigabe-Einstellungen

Einstellung	Beschreibung
Image-Dateipfad	Image-Dateipfad ist nur erforderlich für Verbindungs- und Bereitstellungsvorgänge. Die Einstellung wirkt sich nicht auf Trennvorgänge aus. Der Pfadname des Netzwerklaufwerks wird über ein Windows-SMB- oder Linux/Unix-NFS-Protokoll auf dem Server eingebunden. Beispiel für Verbindung zu CIFS: //<IP to connect for CIFS file system>/<Dateipfad>/<Imagename> Beispiel für Verbindung zu NFS: //<IP to connect for NFS file system>/<Dateipfad>/<Imagename> Dateinamen, die mit **.img** enden, sind als virtuelle Floppys verbunden. Dateinamen, die mit **.iso** enden, sind als virtuelle CDs/DVDs verbunden. Die maximale Zeichenzahl beträgt 511.
Benutzername	Benutzername ist nur erforderlich für Verbindungs- und Bereitstellungsvorgänge. Die Einstellung wirkt sich nicht auf Trennvorgänge aus. Sie können in diesem Feld maximal 40 Zeichen angeben.
Kennwort	Kennwort ist nur erforderlich für Verbindungs- und Bereitstellungsvorgänge. Die Einstellung wirkt sich nicht auf Trennvorgänge aus. Sie können in diesem Feld maximal 40 Zeichen angeben.
Steckplatz	Identifiziert den Standort des Steckplatzes. Steckplatznummern sind sequenzielle IDs von 1 bis 16 (für die 16 im Gehäuse verfügbaren Steckplätze).
Name	Identifiziert den Namen des Steckplatzes. Steckplätze werden nach ihrer Position im Gehäuse benannt.
Model	Zeigt den Modellnamen des Servers an.
Stromzustand	Zeigt den Stromzustand des Servers: **k.A.** – Der CMC hat die Stromversorgung des Servers noch nicht bestimmt. **Aus** – Entweder der Server oder das Gehäuse sind ausgeschaltet. **Ein** – Sowohl das Gehäuse als auch der Server sind eingeschaltet. **Einschalten –** Vorübergehender Zustand zwischen Aus und Ein. Ein erfolgreich, der Stromzustand ist Ein. **Ausschalten** – Vorübergehender Zustand zwischen Ein und Aus. Ein erfolgreich, der Stromzustand ist Aus.
Verbindungsstatus	Zeigt den Verbindungsstatus der Remote-Dateifreigabe an.
Alle auswählen/Auswahl rückgängig	Wählen Sie diese Option aus, bevor Sie einen Remote-Dateifreigabe-Vorgang initiieren. Remote-Dateifreigabe-Vorgänge sind: Verbinden, Trennen und Bereitstellen.

5. Klicken Sie auf **Verbinden**, um eine Verbindung zu einer Remote- Dateifreigabe herzustellen. Um eine Verbindung zu einer Remote- Dateifreigabe

herzustellen, müssen Sie den Pfad, den Benutzernamen und das Kennwort angeben. Ein erfolgreicher Vorgang ermöglicht den Zugriff auf den Datenträger.

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

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

ANMERKUNG: Speichern Sie alle Arbeitsdateien, bevor Sie den Befehl `Bereitstellen` ausführen, da diese Aktion den Server neu startet.

Dieser Befehl schließt Folgendes ein:

- Die Remote-Dateifreigabe wird verbunden.
- Die Datei wird als das erste Startgerät für die Server ausgewählt.
- Der Server ist wird neu gestartet.
- Strom wird an den Server angelegt, falls der Server ausgeschaltet ist.

Häufig gestellte Fragen

Tabelle 5-40 enthält eine Liste mit häufig gestellten Fragen und Antworten.

Tabelle 5-40. Remote-System verwalten und wiederherstellen: Häufig gestellte Fragen

Frage	Antwort
Wenn ich auf die CMC-Schnittstelle zugreife, erhalte ich eine Sicherheitswarnung, die besagt, dass der Host-Name des SSL-Zertifikats nicht mit dem Host-Namen des CMC übereinstimmt.	Der CMC enthält ein Standard-CMC-Serverzertifikat, um Netzwerksicherheit für die Webschnittstelle und die Remote-RACADM-Funktionen zu gewährleisen. 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 Sicherheitsbedenken 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, stellen Sie sicher, dass der allgemeine Name (CN) des CSR der IP-Adresse des CMC (z. B. 192.168.0.120) oder dem eingetragenen DNS-CMC-Namen entspricht. So stellen Sie sicher, dass die CSR dem eingetragenen DNS-CMC-Namen entspricht: 1. Kicken Sie in der **Systemstruktur** auf **System**. 2. Klicken Sie auf die Registerkarte **Netzwerk / Sicherheit** und dann auf **Netzwerk**. Die Seite **Netzwerkkonfiguration** wird angezeigt. 3. Aktivieren Sie das Kontrollkästchen **CMC auf DNS registrieren**. 4. Geben Sie den CMC-Namen in das Feld **DNS-CMC-Name** ein. 5. Klicken Sie auf **Änderungen übernehmen**. Weitere Informationen über die Erstellung von Zertifikatsignierungsanforderungen und zur Ausgabe von Zertifikaten finden Sie unter "Sichere CMC-Datenübertragung mit SSL und digitalen Zertifikaten".
Warum sind die Remote-RACADM- und webbasierten Dienste nach einer Eigenschaftsänderung nicht verfügbar?	Es kann etwa eine Minute dauern, bis die Remote-RACADM-Dienste und die Webschnittstelle nach einem Reset des CMC-Web Servers wieder verfügbar sind. Der CMC-Web Server führt nach den folgenden Ereignissen einen Reset durch: - Wenn die Netzwerkkonfiguration oder Netzwerksicherheitseigenschaften über die CMC-Webschnittstelle geändert werden. - Wenn die Eigenschaft **cfgRacTuneHttpsPort** geändert wird (einschließlich der Änderung durch eine config -f-<Konfigurationsdatei>) - Wenn **racresetcfg** verwendet wird - Wenn der CMC zurückgesetzt wird. - Wenn ein neues SSL-Serverzertifikat hochgeladen wird
Warum registriert mein DNS-Server meinen CMC nicht?	Einige DNS-Server registrieren nur Namen mit 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 Sicherheitsbedenken zu beseitigen, laden Sie ein CMC-Serverzertifikat von einer vertrauenswürdigen Zertifizierungsstelle (z. B. Thawte oder Verisign) hoch. Für weitere Informationen zur Herausgabe von Zertifikaten, siehe Sichere CMC-Datenübertragung mit SSL und digitalen Zertifikaten.
Die folgende Meldung wird aus unbekannten Gründen angezeigt:	Als Teil der Ermittlung versucht IT Assistant, die Get- und Set-Community-Namen des Geräts zu überprüfen. Im IT Assistant gibt es den Get-Community-Name = public und den Set-Community-Name = private. Standardmäßig ist der Community-Name für den CMC-Agenten "public". Wenn IT Assistant eine Set-Aufforderung sendet, erstellt der CMC-Agent den SNMP-Authentifizierungsfehler, weil er nur

Remote Access: SNMP Authentication Failure (Remote-Zugriff: SNMP-Authentifizierungsfehler)
 	
Warum geschieht dies?
	Aufforderungen von Community = public akzeptieren kann.
	
	Sie können den CMC-Community-Namen mit RACADM ändern.
	
	Um den CMC Community-Namen zu sehen, verwenden Sie den folgenden Befehl:
	
	`racadm getconfig -g cfgOobSnmp`
	
	Um den CMC Community-Namen anzugeben, verwenden Sie den folgenden Befehl:
	
	`racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <Community-Name>`
	
	Um SNMP-Authentifizierungs-Traps daran zu hindern erstellt zu werden, müssen Sie Community-Namen eingeben, die vom Agenten akzeptiert werden. Da der CMC nur einen Community-Namen zulässt, müssen Sie den gleichen Get- und Set-Community-Namen für das IT Assistant-Ermittlungs-Setup eingeben.

Fehlerbehebung beim CMC

Die CMC-Webschnittstelle enthält Hilfsprogramme zum Erkennen, Diagnostizieren und Beheben von Problemen mit dem Gehäuse. Weitere Informationen zur Problembehandlung finden Sie unter "Fehlerbehebung und Wiederherstellung".

Zurück zum Inhaltsverzeichnis