Dell PowerEdge M1000e Chassis Management Controller ファームウェア バージョン 4.45 ユーザーズガイド

メモ、注意、警告

メモ: コンピュータを使いやすくするための重要な情報を説明しています。

注意: ハードウェアの損傷やデータの損失の可能性を示し、その問題を回避するための方法を説明しています。

警告: 物的損害、けが、または死亡の原因となる可能性があることを示しています。

2013 - 08

Rev. A00

目次

1

概要

Dell PowerEdge M1000e シャーシ用 Dell Chassis Management Controller（CMC）は、複数の Dell サーバーシャーシを管理するためのシステム管理ハードウェアおよびソフトウェアソリューションです。これは、Dell PowerEdge M1000e シャーシの背面に取り付けられるホットプラグ対応カードです。 CMC は独自のマイクロプロセッサとメモリを備えており、差し込んだモジュラシャーシから電源が供給されます。

CMC により、IT 管理者は以下を行うことが可能になります。

- インベントリの表示
- タスクの設定および監視
- リモートでのサーバーの電源投入または切断
- M1000e シャーシ内のサーバーおよびコンポーネント上のイベントのためのアラートの有効化

M1000e シャーシは、1 つの CMC で構成することも、冗長 CMC で構成することもできます。冗長 CMC 構成では、プライマリ CMC が M1000e シャーシまたは管理ネットワークとの通信を失うと、スタンバイ CMC がシャーシ管理を引き継ぎます。

CMC は、サーバーのために複数のシステム管理機能を提供します。電源および温度の管理が CMC の基本的な機能です。

- エンクロージャレベルのリアルタイム自動電力 / 温度管理。
  - CMC はシステム電力要件を監視し、オプションの動的電源供給モードをサポートします。このモードでは、負荷および冗長要件に基づいて電源装置をスタンバイに設定することにより、CMC による電力効率の改善を可能にします。
  - CMC はリアルタイムの消費電力を報告します（タイムスタンプ付きの高低ポイントも記録されます）。
  - CMC は、オプションでエンクロージャの最大電力限度の設定をサポートしています。これを設定すると、設定された最大電力限度値以下に保つために、サーバーモジュールの調整や新しいブレードの電源オンの防止など、アラートが生成されたり処置が実行されたりします。
  - CMC は、実際の周囲温度と内部温度を測定して、ファンの冷却を監視し、自動制御します。
  - CMC は総合的なエンクロージャのインベントリ、および状態またはエラーレポートを提供します。
- CMC は、次に対する一元的な設定のためのメカニズムを提供します。
  - M1000e エンクロージャのネットワークおよびセキュリティ設定。
  - 電源冗長性と電力上限値設定。
  - I/O スイッチと iDRAC ネットワークの設定。
  - サーバー上の最初の起動デバイス。
  - I/O モジュールとサーバー間の I/O ファブリック整合性チェック。CMC はシステムハードウェアを保護するために、必要に応じてコンポーネントの無効化も行います。
  - ユーザーアクセスセキュリティ。

温度、ハードウェアの誤った設定、停電、およびファン速度関連の警告またはエラーについて、E-メールアラートまたは SNMP トラップアラートを送信するように CMC を設定することができます。

本リリースの新機能

CMC の本リリースは、次をサポートします。

- 4*10G KR Broadcom bNDC および Mellanox 10G KR メザニンカードのハードウェア有効
- 標準オプションとしての DC 電源装置
- DC 電源が存在している場合のファームウェアダウングレードのブロック
- シャーシグループのシャーシサーバーおよびコンポーネントインベントリの表示
- 固有の SSL 証明書生成変更
- スロットに対するプロファイルの Quick Deploy
- プロファイルを介したサーバー設定管理（バックアップ、復元、複製）。サーバープロファイル複製については、利用可能な設定のすべてがサポートされています。
- Dell PowerEdge M1000e I/O アグリゲータ の FCoE セッション情報の表示
- Dell PowerEdge M1000e I/O アグリゲータのアップリンクおよびダウンリンク状態の表示
- PMUX モードの Dell PowerEdge M1000e I/O アグリゲータのサポート
- Dell PowerEdge M1000e I/O アグリゲータの管理 VLAN 設定
- Dell PowerEdge M I/O アグリゲータのスタッキング情報
- 証明書生成時における、FQDN または PQDN の使用（既存の CMC デフォルト SRVTAG 固有名の代替）
- デフォルトの資格情報チェックおよび GUI、CLI、および SNMP アラートによるユーザーへの警告表示
- ログイン失敗後のユーザーおよび IP アドレスのブロック
- DNS 名を使用した iDRAC の起動
- OMPC のための追加の WSMAN サポート
- アクティブなエラーをクエリするための RACADM サポート

主な機能

CMC の機能は、管理とセキュリティ機能のグループに分けられます。

管理機能

CMC は次の管理機能を提供します。

- 冗長 CMC 環境。
- IPv4 および IPv6 のダイナミック DNS（DDNS）登録。
- SNMP、Web インタフェース、iKVM、Telnet、または SSH 接続を利用したリモートシステム管理と監視。
- 監視 — システム情報やコンポーネントのステータスへのアクセスを提供。
- システムイベントログへのアクセス — ハードウェアログと CMC ログへのアクセスを提供。
- 各種シャーシコンポーネントのファームウェアアップデート — CMC、サーバー、iKVM、I/O モジュールインフラデバイスのファームウェアアップデートが可能。
- シャーシ内の複数サーバーで、BIOS、ネットワークコントローラ、ストレージコントローラなどのサーバーコンポーネントを、Lifecycle Controller を使用してファームウェアアップデート可能。
- Dell OpenManage ソフトウェア統合 — Dell OpenManage Server Administrator または IT Assistant から CMC ウェブインタフェースを起動。
- CMC アラート — E メールメッセージまたは SNMP トラップを使って管理対象ノードに関する潜在的な問題を通知。
- リモート電源管理 — シャーシコンポーネントのシャットダウンやリセットなどのリモート電源管理機能を管理コンソールから提供。

- 電源使用率の報告。
- Secure Sockets Layer（SSL）暗号化 — Web インタフェースからセキュアなリモートシステム管理を提供。
- Integrated Dell Remote Access Controller（iDRAC）ウェブインタフェースの起動ポイント。
- WS-Management のサポート。
- FlexAddress 機能 — 特定のスロットに対して、工場で割り当てられたワールドワイドネーム / メディアアクセスコントロール（WWN/MAC）ID のシャーシに割り当てられた WWN/MAC ID への置き換え
- シャーシのコンポーネントステータスおよび状態のグラフィック表示。
- 単一およびマルチスロットサーバーのサポート。
- LCD iDRAC 設定ウィザードによる iDRAC ネットワーク設定のサポート。
- iDRAC シングルサインオン。
- ネットワークタイムプロトコル（NTP）対応。
- サーバーサマリ、電力レポート、電力制御ページの強化。
- 強制 CMC フェールオーバー、およびサーバーの仮想再装着。
- オペレーティングシステムの再起動なしでの iDRAC リセット
- RACADM を使用したストレージアレイ設定のサポート — RACADM を使用して IP の設定、グループへの参加または作成、およびストレージアレイ用のファブリックの選択を行う事ができます。
- マルチシャーシ管理：
  - リーダーシャーシから最大 8 台のその他シャーシを表示する機能。
  - リーダーシャーシからシャーシ設定プロパティを選択し、グループメンバーにプッシュする機能。
  - グループメンバーがシャーシ設定をリーダーシャーシと同期化させた状態を保つ機能。
- サーバー設定および構成情報をハードディスクに保存し、同じまたは異なるサーバーに復元する機能。

セキュリティ機能

CMC は次のセキュリティ機能を提供しています。

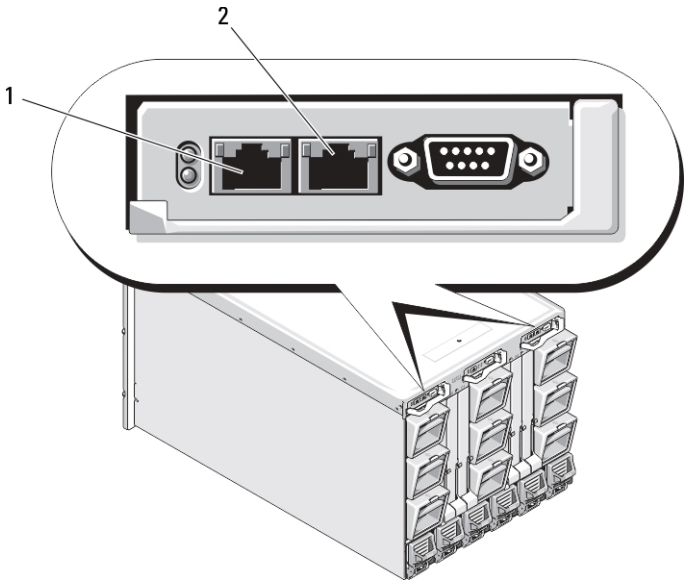
- パスワードレベルのセキュリティ管理 — リモートシステムへの無許可のアクセスを防止。
- 次による一元ユーザー認証：
  - 標準スキーマまたは拡張スキーマ（オプション）を使用する Active Directory。
  - ハードウェアに保存されたユーザー ID とパスワード。
- 役割ベースの権限 — システム管理者が各ユーザーに特定の権限を設定可能。
- ウェブインタフェースを介してのユーザー ID とパスワードの設定。

  メモ: ウェブインタフェースは 128 ビット SSL 3.0 暗号化と 40 ビット SSL 3.0 暗号化（128 ビットが使用できない国向け）をサポート。

  メモ: Telnet は SSL 暗号化をサポートしていません。
- 設定可能な IP ポート（該当する場合）。
- IP アドレスごとのログイン失敗数の制限による、制限を超えた IP アドレスのログインの阻止。
- 設定可能なセッション自動タイムアウトおよび複数の同時セッション数。
- CMC に接続するクライアントの IP アドレス範囲を限定。
- 暗号化層を使用してセキュリティを強化するセキュアシェル（SSH）。
- シングルサインオン、二要素認証、公開キー認証。

シャーシの概要

次の図は、CMC（差し込み）の前面図とシャーシ内の CMC スロット位置を表示しています。



1	GB ポート
2	STK ポート

CMC ポート情報

次の TCP/IP ポートは、ファイアウォールを介してリモートで CMC にアクセスするために必要です。これらのポートは、CMC が接続のためにリッスンするポートです。

表 1. CMC サーバーリスニングポート

ポート番号	機能
22*	SSH
23*	Telnet
80*	HTTP
161	SNMP エージェント
443*	HTTPS

*設定可能なポート

次の表に、CMC がクライアントとして使用するポートを示します。

表 2. CMC クライアントポート

ポート番号	機能
25	SMTP
53	DNS

ポート番号	機能
68	DHCP で割り当てた IP アドレス
69	TFTP
162	SNMP トラップ
514*	リモート Syslog
636	LDAPS
3269	グローバルカタログ（GC）用 LDAPS

*設定可能なポート

CMC の必要最低バージョン

次の表には、リストされたブレードサーバーを有効化するために必要な最低限の CMC バージョンがリストされています。

表 3. ブレードサーバー用 CMC の必要最低バージョン

サーバー	CMC の最低バージョン
PowerEdge M600	CMC 1.0
PowerEdge M605	CMC 1.0
PowerEdge M805	CMC 1.2
PowerEdge M905	CMC 1.2
PowerEdge M610	CMC 2.0
PowerEdge M610x	CMC 3.0
PowerEdge M710	CMC 2.0
PowerEdge M710HD	CMC 3.0
PowerEdge M910	CMC 2.3
Power Edge M915	CMC 3.2
PowerEdge M420	CMC 4.1
PowerEdge M520	CMC 4.0
PowerEdge M620	CMC 4.0
PowerEdge M820	CMC 4.11
PowerEdge PSM4110	CMC 4.11

次の表には、リストされた IOM を有効化するために必要な最低限の CMC バージョンがリストされています。

表 4. IOM 用 CMC の必要最低バージョン

IOM スイッチ	CMC の最低バージョン
PowerConnect M6220	CMC 1.0
PowerConnect M6348	CMC 2.1

IOM スイッチ	CMC の最低バージョン
PowerConnect M8024	CMC 1.2
PowerConnect M8024-k	CMC 3.2
PowerConnect M8428-k	CMC 3.1
Dell 10/100/1000 Mb イーサネットパススルー	CMC 1.0
Dell 4Gbps FC パススルーモジュール	CMC 1.0
Dell 8/4Gbps FC SAN モジュール	CMC 1.2
Dell 10Gb イーサネットパススルー	CMC 2.1
Dell 10 Gb イーサネットパススルー II	CMC 3.0
Dell 10Gb イーサネットパススルー -k	CMC 3.0
Brocade M4424	CMC 1.0
Brocade M5424	CMC 1.2
Cisco Catalyst CBS 3130X-S	CMC 1.0
Cisco Catalyst CBS 3130G	CMC 1.0
Cisco Catalyst CBS 3032	CMC 1.0
Dell Force10 MXL 10/40 GbE	CMC 4.11
Dell PowerEdge M I/O Aggregator	CMC 4.2
Mellanox M2401G DDR Infiniband スイッチ	CMC 1.0
Mellanox M3601Q QDR Infiniband スイッチ	CMC 2.0
Mellanox M4001F/M4001Q FDR/QDR Infiniband スイッチ	CMC 4.0
Mellanox M4001T FDR10 Infiniband スイッチ	CMC 4.1
Brocade M6505	CMC 4.3
Cisco Nexus B22DELL	CMC 4.3

本リリースの最新ファームウェア

次の表には、リストされたサーバーをサポートする BIOS、iDRAC、および Lifecycle Controller 用の最新ファームウェアバージョンが記載されています。

表 5. BIOS、iDRAC、および Lifecycle Controller 用の最新ファームウェアバージョン

サーバー	BIOS	iDRAC	Lifecycle Controller
PowerEdge M600	2.4.0	1.65	適用なし
PowerEdge M605	5.4.1	1.65	適用なし
PowerEdge M805	2.3.3	1.65	適用なし
PowerEdge M905	2.3.3	1.65	適用なし
PowerEdge M610	6.3.0	3.50	1.6

サーバー	BIOS	iDRAC	Lifecycle Controller
PowerEdge M610x	6.3.0	3.50	1.6
PowerEdge M710	6.3.0	3.50	1.6
PowerEdge M710HD	7.0.0	3.50	1.6
PowerEdge M910	2.7.9	3.50	1.6
Power Edge M915	3.0.4	3.50	1.6
PowerEdge M420	1.5.1	1.40.40	1.1.5
PowerEdge M520	1.7.4	1.40.40	1.1.5
PowerEdge M620	1.7.4	1.40.40	1.1.5
PowerEdge M820	1.5.1	1.40.40	1.1.5

メモ: PowerEdge PSM4110 は、Array Software バージョン 6.0.4 によってサポートされています。

対応リモートアクセス接続

次の表で、サポートされているリモートアクセスコントローラをリストします。

表 6. 対応リモートアクセス接続

接続	機能
CMC ネットワークインタフェースポート	• GB ポート：CMC ウェブインタフェース専用のネットワークインタフェース。2 個の 10/100/1000 Mbps ポートがあり、一方は管理用、他方はシャーシ対シャーシのケーブル統合用です。 • STK：シャーシ対シャーシ管理ネットワークケーブル統合用のアップリンクポート。 • CMC GbE ポート経由での 10Mbps/100Mbps/1Gbps Ethernet 接続。 • DHCP サポート。 • SNMP トラップおよび E-メールイベント通知。 • iDRAC および I/O モジュール（IOM）用のネットワークインタフェース。 • システム起動、リセット、電源投入、シャットダウンコマンドを含む Telnet/SSH コマンドコンソールおよび RACADM CLI コマンドのサポート。
シリアルポート	• システム起動、リセット、電源投入、シャットダウンコマンドを含む シリアルコンソールおよび RACADM CLI コマンドのサポート。 • 特定タイプの IOM へのバイナリプロトコルによる通信を行うために特別に設計されたアプリケーション用バイナリ交換のサポート。 • シリアルポートは、connect（または racadm connect）コマンドを使ってサーバーのシリアルコンソールまたは I/O モジュールに内部的に接続可能。
その他の接続	• Avocent 内蔵 KVM スイッチモジュール（iKVM）経由での Dell CMC コンソールへのアクセス。

対応プラットフォーム

CMC は、PowerEdge M1000e プラットフォーム用に設計されたモジュラーシステムをサポートします。CMC との互換性の詳細については、デバイスのマニュアルを参照してください。
最新の対応プラットフォームについては、**dell.com/support/manuals** で『*Readme*』を参照してください。

対応ウェブブラウザ

対応ウェブブラウザについての最新情報は、**dell.com/support/manuals** で『*Readme*』を参照してください。

他言語の CMC ウェブインタフェースの表示

CMC ウェブインタフェースのローカライズバージョンを表示するには：

1. Windows の **コントロールパネル** を開きます。
2. **地域のオプション** アイコンをダブルクリックします。
3. **ロケーション（オプション）** ドロップダウン メニューで対象となる場所を選択します。

対応管理コンソールアプリケーション

CMC は、Dell OpenManage IT Assistant と統合することができます。詳しくは、Dell サポートサイト **dell.com/support/manuals** から入手可能な IT Assistant マニュアルセットを参照してください。

その他の必要マニュアル

本ガイドに加え、**dell.com/support/manuals** で利用できる次のガイドにもアクセスすることができます。**すべてのデル製品のリストから選択する** を選択し、**続行** をクリックします。**ソフトウェア モニタ周辺機器およびアクセサリ → ソフトウェア** とクリックします。

- **リモートエンタープライズシステム管理** をクリックし、**Dell Chassis Management Controller Version 4.45** をクリックして次を表示します。
  - 『*CMC オンラインヘルプ*』では、ウェブインタフェースの使用方法について説明しています。
  - 『*Chassis Management Controller（CMC）セキュアデジタル（SD）カード技術仕様*』は、BIOS およびファームウェアの最小バージョン、インストール方法および使用方法についての情報を提供します。
  - 『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』には、RACADM サブコマンド、サポートされているインタフェース、およびプロパティデータベースグループとオブジェクト定義に関する情報が記載されています。
  - 『Chassis Management Controller バージョン 4.45 リリースノート』には、専門知識をお持ちのユーザーまたは技術者向けのシステムの最新アップデート、マニュアル、または高度な参考技術資料が提供されています。
- **リモートエンタープライズシステム管理** をクリックしてから、必要な iDRAC7 バージョン番号をクリックして、管理下システムに iDRAC をインストールし、設定およびメンテナンスを行うための情報が記載された『*Integrated Dell Remote Access Controller 7（iDRAC7）ユーザーズガイド*』を表示します。
- **エンタープライズシステム管理** をクリックしてから、製品名をクリックして次のマニュアルを表示します。
  - 『*Dell OpenManage Server Administrator ユーザーズガイド*』には、Server Administrator のインストールと使用方法について記載されています。

– 『*Dell Update Packages ユーザーズガイド*』は、システムアップデート対策の一環としての Dell Update Packages の入手方法と使い方を説明しています。

dell.com/support/manuals で利用できる次のシステムマニュアルは、CMC がインストールされたシステムについての詳細情報を提供します。

- システムに付属している「安全にお使いただくために」には安全や規制に関する重要な情報が記載されています。規制に関する詳細な情報については、**www.dell.com/regulatory_compliance** にある 法規制の順守ホームページを参照してください。保証に関する情報は、このマニュアルに含まれているか、別の文書として同梱されています。
- 『*ラック取り付けガイド*』および『*ラック取り付け手順*』では、システムをラックに取り付ける方法を説明しています。
- 『*ハードウェアオーナーズマニュアル*』では、システムの機能、トラブルシューティングの方法、およびコンポーネントの取り付け方や交換方法について説明しています。
- システム管理ソフトウェアのマニュアルでは、システム管理ソフトウェアの機能、動作要件、インストール、および基本操作について説明しています。
- 別途購入されたコンポーネントのマニュアルでは、これらのオプション装置の取り付けや設定について説明しています。
- システムやマニュアルの最新のアップデート情報、または専門知識をお持ちのユーザーや技術者向けの高度な技術上の参考資料が記載されたリリースノートや readme ファイルが含まれている場合があります。
- IOM ネットワーク設定の詳細については、『*Dell PowerConnect M6220 スイッチ重要情報*』マニュアルおよび『*Dell PowerConnect 6220 シリーズポートアグリゲータホワイトペーパー*』を参照してください。
- サードパーティ製管理コンソールアプリケーションのマニュアル

システム、ソフトウェア、またはマニュアルの変更について記載されたアップデート情報がシステムに付属していることがあります。このアップデート情報には他の文書の内容を差し替える情報が含まれていることがあるので、必ず最初にお読みください。

デルへのお問い合わせ

メモ: お使いのコンピュータがインターネットに接続されていない場合は、購入時の納品書、出荷伝票、請求書、またはデルの製品カタログで連絡先をご確認ください。

デルでは、オンラインまたは電話によるサポートとサービスのオプションを複数提供しています。サポートやサービスの提供状況は国や製品ごとに異なり、国 / 地域によってはご利用いただけないサービスもございます。デルのセールス、テクニカルサポート、またはカスタマーサービスへは、次の手順でお問い合わせいただけます。

1. **dell.com/support** にアクセスします
2. サポートカテゴリを選択します。
3. ページの上部にある 国 / 地域の選択 ドロップダウンメニューで、お住まいの国または地域を確認します。
4. 必要なサービスまたはサポートのリンクを選択します。

ソーシャルメディアリファレンス

Dell ソリューションおよびサービスの製品、ベストプラクティス、情報に関してより知るには、Dell TechCenter および YouTube などのソーシャルメディアプラットフォームにアクセスすることができます。
www.delltechcenter.com/cmc の CMC ウィキページからは、ブログ、フォーラム、ホワイトペーパー、ハウツービデオなどにアクセスすることができます。次の CMC 4.45 向けハウツービデオをご利用いただけます。

- Replicating Server Configuration Profile in a PowerEdge M1000E Chassis（PowerEdge M1000E シャーシでのサーバー設定プロファイルの複製）

- Assigning Profiles to Server Slots Using Quick Deploy Feature（Quick Deploy 機能を使用したプロファイルのサーバースロットへの割り当て）
- Resetting iDRACs Without OS Reboot（OS の再起動なしでの iDRAC のリセット）
- Multi-chassis management（マルチシャーシ管理）

これらのハウツービデオは、YouTube でも閲覧可能です。

CMC マニュアルおよびその他の関連ファームウェア文書については、**www.dell.com/esmmanuals** を参照してください。

2

CMC のインストールと設定

本項では、PowerEdge M1000e Chassis Management Controller（CMC）ハードウェアの取り付け、CMC へのアクセス確立、CMC を使用するための管理環境の設定、および CMC の設定の各種方法について説明します。

- CMC への初期アクセスの設定。
- ネットワーク経由の CMC へのアクセス。
- CMC ユーザーの追加と設定。
- CMC ファームウェアのアップデート。

冗長 CMC 環境の取り付けと設定の詳細については、「冗長 CMC 環境について」を参照してください。

作業を開始する前に

CMC 環境をセットアップする前に、**support.dell.com** から最新バージョンの CMC ファームウェアをダウンロードしてください。
また、システム付属の『*Dell Systems Management Tools およびマニュアル*』DVD があることを確認してください。

CMC ハードウェアの取り付け

CMC はシャーシに事前に取り付けられているため、取り付けは必要ありません。2 台目の CMC を取り付けて、アクティブ CMC のスタンバイとして使用できます。

関連リンク

冗長 CMC 環境について

シャーシ設定のチェックリスト

次の手順を参照して、シャーシを正確に設定してください。

1. CMC とブラウザを使用する管理ステーションが、管理ネットワークと呼ばれる同じネットワーク上にあることを確認してください。Ethernet ネットワークケーブルを、**GB** とラベル付けされた CMC ポートから管理ネットワークに接続します。

   メモ: STK とラベル付けされた CMC Ethernet ポートにはケーブルを接続しないでください。STK ポートのケーブル接続の詳細については、冗長 CMC 環境について を参照してください。
2. シャーシに I/O モジュールを取り付けてからケーブルで接続します。
3. シャーシにサーバーを挿入します。
4. シャーシを電源に接続します。
5. 手順 7 を完了したら、シャーシの左下隅にある電源ボタンを押すか、CMC GUI からシャーシの電源を入れます。

   メモ: サーバーの電源は入れないでください。
6. システムの前面にある LCD パネルを使用して、CMC に静的 IP アドレスを指定するか、それを DHCP 用に設定します。

7. CMC の IP アドレスに接続して、デフォルトのユーザー名（root）およびパスワード（calvin）を入力します。
8. CMC ウェブインタフェースで各 iDRAC に IP アドレスを指定し、LAN と IPMI インタフェースを有効にします。

   メモ: デフォルトでは、一部のサーバーの iDRAC LAN インタフェースは無効になっています。
9. CMC ウェブインタフェースで各 I/O モジュールに IP アドレスを指定します。
10. 各 iDRAC に接続して、iDRAC の最終設定を行います。デフォルトのユーザー名は *root*、パスワードは *calvin* です。
11. ウェブブラウザを使用して各 I/O モジュールに接続し、I/O モジュールの最終設定を行います。
12. サーバーの電源を入れ、オペレーティングシステムをインストールします。

CMC の基本的なネットワーク接続

注意: STK ポートを管理ネットワークに接続すると、予期しない結果が生じるおそれがあります。GB と STK を同じネットワーク（ブロードキャストドメイン）に接続すると、ブロードキャストストームが生じる場合があります。

最大限の冗長性を得るためには、使用可能な各 CMC を管理ネットワークに接続してください。

各 CMC には 2 つの RJ-45 イーサネットポートがあり、**GB**（アップリンクポート）および **STK**（スタッキングまたはケーブル統合ポート）とラベルが付いています。基本的なケーブル配線では、GB ポートを管理ネットワークに接続し、STK ポートは使用しません。

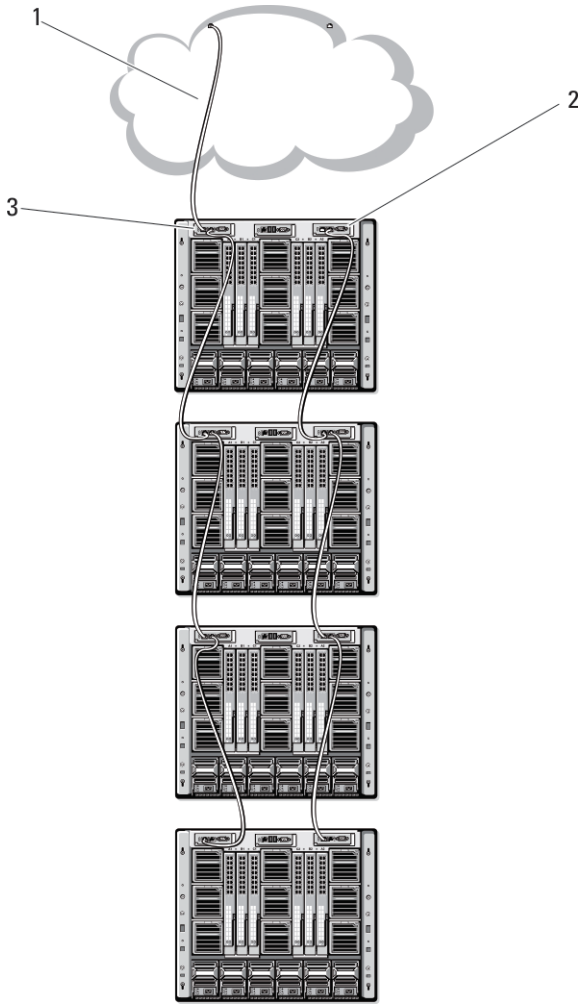
デイジーチェーン CMC ネットワーク接続

ラックに複数のシャーシがある場合は、最大 4 台のシャーシをまとめてデイジーチェーンに接続して、管理ネットワークへの接続数を減らすことができます。4 台の各シャーシに冗長 CMC がある場合は、デイジーチェーンにすることで、必要とされる管理ネットワーク接続の数を 8 から 2 に減らすことができます。各シャーシに CMC が 1 台しかない場合は、必要とされる接続の数を 4 から 1 に減らすことができます。

シャーシをまとめてデイジーチェーンにする場合、GB はアップリンクポート、STK はスタッキング（ケーブル統合）ポートとなります。GB ポートを管理ネットワークまたはネットワークに近いシャーシの CMC の STK ポートに接続します。STK ポートはチェーンまたはネットワークから遠い GB ポートにのみ接続してください。

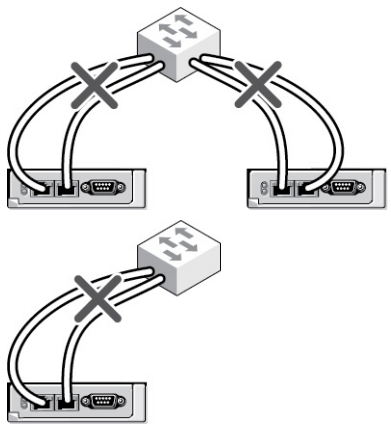
アクティブ CMC スロットにある CMC とセカンダリ CMC スロットにある CMC は、個別にデイジーチェーン接続します。

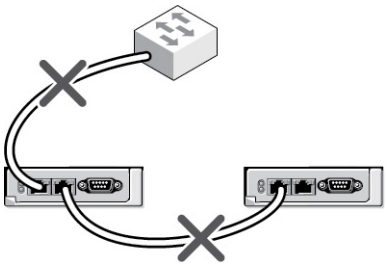
下図は、それぞれアクティブとスタンバイの CMC がある 4 台のシャーシをデイジーチェーンに接続したケーブル配線を示したものです。



1	管理ネットワーク
2	スタンバイ CMC
3	アクティブ CMC

次の図は、CMC の誤ったケーブル配線の例を示しています。





4 台までのシャーシをデイジーチェーンで接続するには、次の手順を実行します。

1. 最初のシャーシのアクティブ CMC の GB ポートを管理ネットワークに接続します。
2. 2 つ目のシャーシのアクティブ CMC の GB ポートを最初のシャーシのアクティブ CMC の STK ポートに接続します。
3. 3 つ目のシャーシがある場合は、そのシャーシのアクティブ CMC の GB ポートを 2 つ目のシャーシのアクティブ CMC の STK ポートに接続します。
4. 4 つ目のシャーシがある場合は、そのシャーシのアクティブ CMC の GB ポートを 3 つ目のシャーシの STK ポートに接続します。
5. シャーシ内に冗長 CMC がある場合は、上記と同じように、それぞれ相互に接続します。

   注意: CMC 上の STK ポートは管理ネットワークに接続してはいけません。STK ポートは、別のシャーシ上の GB ポートにしか接続できません。STK ポートを管理ネットワークに接続すると、ネットワークに支障をきたし、データの損失を招く恐れがあります。GB と STK を同じネットワーク（ブロードキャストドメイン）に接続すると、ブロードキャストストームが生じる場合があります。

   メモ: アクティブ CMC をスタンバイ CMC に接続しないでください。

   メモ: STK ポートが別の CMC にチェーン接続されている CMC をリセットすると、チェーン後方の CMC のネットワークに支障を来たす可能性があります。チェーン後方の CMC は、ネットワーク接続が失われたことをログ記録し、冗長 CMC にフェールオーバーする場合があります。
6. CMC の利用を開始するには、「管理ステーションへのリモートアクセスソフトウェアのインストール」を参照してください。

管理ステーションへのリモートアクセスソフトウェアのインストール

Telnet、セキュアシェル（SSH）、またはオペレーティングシステム付属のシリアルコンソールユーティリティなどのリモートアクセスソフトウェア、またはウェブインタフェースを使用して、管理ステーションから CMC にアクセスできます。

管理ステーションからリモート RACADM を使用するには、システムに付随する『*Dell Systems Management Tools およびマニュアル DVD*』を使用してリモート RACADM をインストールします。この DVD には、次の Dell OpenManage コンポーネントが含まれます。

- DVD ルート - Dell System Build and Update Utility が含まれます。
- SYSMGMT - Dell OpenManage Server Administrator を含むシステム管理ソフトウェアの製品が含まれます。
- Docs: このディレクトリには、システム、システム管理ソフトウェア製品、周辺機器および RAID コントローラのマニュアルが入っています。
- SERVICE - システムを設定するために必要なツールやシステムの最新の診断および Dell 最適化ドライバが含まれます。

Dell OpenManage ソフトウェアコンポーネントのインストールの詳細については、DVD または **dell.com/support/manuals** にある『*Dell OpenManage のインストールとセキュリティユーザーガイド*』を参照してください。Dell DRAC ツールの最新バージョンは、デルのサポートサイト **dell.com/support** からもダウンロードできます。

RACADM の Linux 管理ステーションへのインストール

1. 管理下システムコンポーネントを取り付けようとしている、サポートされた Red Hat Enterprise Linux または SUSE Linux Enterprise Server オペレーティングシステムを実行するシステムに、root 権限でログインします。
2. DVD ドライブに『*Dell Systems Management Tools およびマニュアル*』DVD を挿入します。
3. DVD を必要なロケーションにマウントするには、mount コマンドまたは類似のコマンドを使用します。

   メモ: Red Hat Enterprise Linux 5 オペレーティングシステムでは、DVD が `-noexec mount` オプションで自動的にマウントされます。このオプションは DVD からの実行ファイルの実行を許可せず、DVD-ROM を手動でマウントしてから、これらの実行ファイルを実行する必要があります。
4. **SYSMGMT/ManagementStation/linux/rac** ディレクトリに移動します。RAC ソフトウェアをインストールするには、次のコマンドを入力します。

   ```
   rpm -ivh *.rpm
   ```
5. RACADM コマンドのヘルプを表示するには、前のコマンドを入力した後 `racadm help` と入力します。RACADM の詳細については、『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

   メモ: RACADM リモート機能を使うとき、ファイル操作を含む RACADM サブコマンドを使用する対象となるフォルダへの書き込み権限が必要です。例：`racadm getconfig -f <file name>`

Linux 管理ステーションから RACADM のアンインストール

1. 管理ステーション機能をアンインストールするシステムに、root でログインします。
2. 次の rpm クエリコマンドを使用して、インストールされている DRAC ツールのバージョンを確認します。

   ```
   rpm -qa | grep mgmtst-racadm
   ```
3. アンインストールするパッケージバージョンを確認し、`-e rpm -qa | grep mgmtst-racadm` コマンドを使って機能をアンインストールします。

ウェブブラウザの設定

シャーシに取り付けられている CMC、サーバー、モジュールはウェブブラウザを使って設定および管理することができます。**dell.com/support/manuals** にある『*Readme*』で「*対応ブラウザ*」の項を参照してください。

CMC とブラウザを使用する管理ステーションは同じネットワーク上にあることが必要です。このネットワークを *管理ネットワーク*と呼びます。セキュリティ要件によっては、管理ネットワークをセキュリティ上、安全な分離されたネットワークにすることができます。

メモ: ファイアウォールやプロキシサーバーなどの管理ネットワークのセキュリティ対策によって、ウェブブラウザから CMC へのアクセスが妨げられることがないことを確認してください。

また、ブラウザの一部の機能が接続性や性能に支障をきたすことがあります。特に管理ネットワークがインターネットへの経路を持たない場合はご注意ください。管理ステーションで Windows オペレーティングシステムが稼動している場合は、コマンドラインインタフェースを使って管理ネットワークにアクセスする場合でも Internet Explorer の設定により接続が妨げられることがあります。

関連リンク

プロキシサーバー
Microsoft フィッシングフィルタ
証明書失効リスト（CRL）のフェッチ
Internet Explorer を使用した CMC からのファイルのダウンロード
Internet Explorer でのアニメーションの有効化

プロキシサーバー

管理ネットワークにアクセスしていないプロキシサーバーから閲覧するには、管理ネットワークアドレスをブラウザの例外リストに追加します。これは、ブラウザに対して管理ネットワークにアクセスする際にプロキシサーバーを迂回する指示を出します。

Internet Explorer

Internet Explorer の例外リストを編集するには、次の手順を実行します。

1. Internet Explorer を起動します。
2. **ツール → インターネットオプション → 接続** をクリックします。
3. **ローカル エリア ネットワーク（LAN）設定** セクションで、**LAN の設定** をクリックします。
   ローカルエリアネットワーク（LAN）設定 ダイアログボックスが表示されます。
4. **ローカルエリアネットワーク（LAN）設定** ダイアログボックスで **プロキシサーバー** セクションに進みます。**LAN にプロキシサーバーを使用する** オプションを選択します。
   詳細設定 オプションが有効になります。
5. **詳細設定** をクリックします。
6. **例外** セクションのリストに管理ネットワーク上の CMC と iDRAC のアドレスをセミコロンで区切って追加します。エントリに DNS 名やワイルドカードを使用できます。

Mozilla Firefox

Mozilla Firefox バージョン 3.0 で例外リストを編集するには：

1. Mozilla Firefox を起動します。
2. **ツール → オプション**（Windows を実行しているシステム）または **編集 → プリファレンス**（Linux を実行しているシステム）をクリックします。
3. **詳細**、**ネットワーク** タブの順にクリックします。
4. **設定** をクリックします。
5. **手動プロキシ設定**を選択します。
6. **プロキシなしの接続** フィールドに、管理ネットワーク上の CMC と iDRAC のアドレスをカンマで区切ったリストとして追加します。エントリには DNS 名およびワイルドカードを使用できます。

Microsoft フィッシングフィルタ

Microsoft フィッシング詐欺検出機能が管理システムの Internet Explorer 7 で有効になっており、また CMC がインターネットにアクセスできない場合、CMC は数秒遅れる可能性があります。この遅延は、ブラウザやリモート RACADM などの他のインタフェースを使用中に生じる可能性があります。次の手順に従って、フィッシング詐欺検出機能を無効にしてください。

1. Internet Explorer を起動します。
2. **ツール → フィッシング詐欺検出機能** をクリックしてから、**フィッシング詐欺検出機能**の設定をクリックします。
3. **フィッシング詐欺検出機能を無効にする** チェックボックスを選択し、**OK** をクリックします。

証明書失効リスト（CRL）のフェッチ

CMC にインターネットへのアクセスがない場合は、Internet Explorer の 証明書失効リスト（CRL）のフェッチ機能を無効にしてください。この機能では、CMC ウェブサーバーなどのサーバーが、インターネットから取得する無効な証明書リストにある証明書を使用しているかどうかをテストします。インターネットにアクセ

スできない場合、ブラウザまたはリモート RACADM などのコマンドラインインタフェースを使って CMC にアクセスするときに、この機能が数秒の遅延の原因となる可能性があります。

CRL フェッチを無効化するには、次の手順を実行します。

1. Internet Explorer を起動します。
2. **ツール → インターネット オプション** をクリックしてから、 **詳細設定** をクリックします。
3. **セキュリティ** セクションにスクロールして、**発行元証明書の取り消しを確認する** チェックボックスをクリアし、**OK** をクリックします。

Internet Explorer を使用した CMC からのファイルのダウンロード

Internet Explorer を使って CMC からファイルをダウンロードするとき、**暗号化されたページをディスクに保存しない** オプションが有効になっていないと問題が発生する場合があります。

暗号化されたページをディスクに保存しない オプションを有効にするには、次の手順を実行します。

1. Internet Explorer を起動します。
2. **ツール → インターネットオプション → 詳細** をクリックします。
3. **セキュリティ** セクションにスクロールして、**暗号化されたページをディスクに保存しない** を選択します。

Internet Explorer でのアニメーションの有効化

ファイルをウェブインタフェース間で転送する際、ファイル転送アイコンが回転して転送アクティビティを示します。Internet Explorer を使用する場合は、アニメーションを再生するようにブラウザを設定する必要があります。

アニメーションを再生するように Internet Explorer を設定するには、次の手順を実行します。

1. Internet Explorer を起動します。
2. **ツール → インターネットオプション → 詳細** をクリックします。
3. **マルチメディア** セクションにスクロールして、**Web ページのアニメーションを再生する** を選択します。

CMC への初期アクセスのセットアップ

CMC をリモートで管理するには、CMC を管理ネットワークに接続してから CMC ネットワーク設定を行います。

メモ: M1000e ソリューションを管理するには、管理ネットワークに接続している必要があります。

CMC のネットワーク設定の詳細については、「CMC の初期ネットワーク設定」を参照してください。この初期設定によって、CMC へのアクセスを可能にする TCP/IP ネットワークパラメータが割り当てられます。

各サーバーとスイッチ I/O モジュールのネットワーク管理ポートにある CMC と iDRAC は、M1000e シャーシ内の共通の内部ネットワークに接続されていることを確認してください。これにより、管理ネットワークをサーバーデータネットワークから分離することができます。中断のないシャーシ管理へのアクセスには、このトラフィックを分離することが重要です。

CMC は管理ネットワークに接続されます。CMC と iDRAC への外部アクセスはすべて CMC を介して確立できます。一方、管理サーバーへのアクセスは I/O モジュール（IOM）へのネットワーク接続を介して行われます。これによって、アプリケーションネットワークを管理ネットワークから分離できます。

シャーシ管理とデータネットワークを分離することを推奨します。Dell は、ユーザー環境に不適切に統合されたシャーシのアップタイムのサポートまたは保証はできません。データネットワーク上の潜在的なトラフィックのため、内部管理ネットワーク上の管理インタフェースはサーバー向けのトラフィックにより飽和状態になる可能性があります。このため、CMC と iDRAC 間の通信に遅延が発生します。遅延が起こると、iDRAC

が稼動中であっても CMC が iDRAC をオフライン状態と見なしたりするなどの予期しないシャーシ動作が発生し、他の不要な動作が発生する原因になります。管理ネットワークを物理的に分離することができない場合は、CMC および iDRAC トラフィックをそれぞれ異なる VLAN に分離するというオプションもあります。CMC と個々の iDRAC ネットワークインタフェースは、VLAN を使用するように設定することもできます。

シャーシが 1 つの場合は、CMC およびスタンバイ CMC を管理ネットワークに接続します。冗長 CMC の場合は、別のネットワークケーブルを使用して GB CMC ポートを管理ネットワークの 2 番目のポートに接続します。

シャーシが複数存在する場合は、各 CMC を管理ネットワークに接続する基本接続か、シャーシを直列式に接続し、1 つの CMC のみを管理ネットワークに接続するデイジーチェーン接続のいずれかを選択できます。基本接続タイプは管理ネットワーク上のポートの使用数が多く、冗長性が高いという特徴を持ちます。デイジーチェーン接続タイプでは管理ネットワーク上のポート数は少なくなりますが、CMC 間の依存性が生じるため、システムの冗長性が低くなります。

メモ: CMC の冗長構成において、適切にケーブル接続しないと、管理ができなくなり、ブロードキャストストームが発生する場合があります。

関連リンク

CMC の基本的なネットワーク接続
デイジーチェーン CMC ネットワーク接続
初期 CMC ネットワークの設定

初期 CMC ネットワークの設定

メモ: CMC のネットワーク設定を変更すると、現在のネットワーク接続が切断される可能性があります。

CMC の初期ネットワーク設定は、CMC に IP アドレスが与えられる前後のどちらでも実行可能です。IP アドレスが与えられる前に CMC の初期ネットワーク設定を行う場合は、次のいずれかのインタフェースを使用できます。

- シャーシの前面にある LCD パネル
- Dell CMC シリアルコンソール

CMC に IP アドレスが与えられた後に初期ネットワーク設定を行うには、次のいずれかのインタフェースを使用できます。

- シリアルコンソール、Telnet、SSH などのコマンドラインインタフェース（CLI）、または iKVM 経由の Dell CMC コンソール
- リモート RACADM
- CMC ウェブインタフェース

CMC では、IPv4 と IPv6 の両方のアドレス指定モードがサポートされています。IPv4 と IPv6 の設定は、互いに独立しています。

LCD パネルインタフェースを使用した CMC ネットワークの設定

メモ: LCD パネルを使用して CMC を設定するオプションは、CMC が導入されるまで、またはデフォルトパスワードが変更されるまで使用可能です。パスワードが変更されていなければ、セキュリティリスクの可能性のある CMC の設定をリセットするために引き続き LCD を使用することができます。

LCD パネルはシャーシ前面の左下の角にあります。

LCD パネルインタフェースを使用してネットワークを設定するには、次の手順に従います。

1. シャーシの電源ボタンを押してオンにします。
   電源がオンになる過程で、LCD 画面に一連の初期化画面が表示されます。準備ができると、**言語のセットアップ** 画面が表示されます。

2. 方向ボタンを使って言語を選択し、中央のボタン押して **承認する / はい** を選択してから、中央のボタンを再度押します。

   エンクロージャ 画面が開き、「**エンクロージャを設定しますか?**」という質問が表示されます。

   - 中央のボタンを押して、**CMC ネットワーク設定** 画面に進みます。手順 **4** を参照してください。
   - **エンクロージャの設定** メニューを終了するには、いいえのアイコンを選択し、中央のボタンを押します。手順 **9** を参照してください。

3. 中央のボタンを押して、**CMC ネットワーク設定** 画面に進みます。
4. 下矢印ボタンを使って、ネットワーク速度（10Mbps、100Mbps、自動（1Gbps））を選択します。

   ネットワークのスループットを効果的にするには、ネットワーク速度 の設定をネットワーク設定に合わせる必要があります。ネットワーク速度 をネットワーク設定の速度より下げると、帯域幅の消費が増えてネットワーク通信が遅くなります。**使用しているネットワークがネットワーク速度を超える速度をサポートしているかどうかを判断し、それに従って設定してください**。ネットワーク設定がこれらの値のどれにも一致しない場合は、オートネゴシエーション（**自動** オプション）を使用するか、ネットワーク装置のメーカーに問い合わせてください。

   中央のボタンを押して、**CMC ネットワーク設定** 画面に進みます。

5. 使用しているネットワーク環境に適した二重モード（半二重または全二重）を選択します。

   メモ: メモ：オートネゴシエーションがオンかまたは 1000MB（1Gbps）が選択されている場合には、ネットワーク速度と二重モードの設定はできません。

   オートネゴシエーションを 1 台のデバイスでオンにし、別の 1 台でオフにすると、オートネゴシエーションはもう一つのデバイスのネットワーク速度を判別できますが、二重モードを判別できません。この場合、二重モードはオートネゴシエーション中にデフォルトで半二重の設定になります。このような二重モードの不一致は、ネットワーク接続を低速化します。

   中央のボタンを押して、**CMC ネットワーク設定** 画面に進みます。

6. CMC に使用するインターネットプロトコル（IPv4、IPv6、または両方）を選択し、中央のボタンを押して次の **CMC ネットワーク設定** 画面へ進みます。
7. CMC の NIC IP アドレスを取得するモードを選択します。

動的ホスト構成プロトコル（DHCP）	CMC は IP 設定（IP アドレス、マスク、ゲートウェイ）をネットワーク上の DHCP サーバーから自動的に取得します。CMC には、ネットワーク上で割り振られた固有の IP アドレスが割り当てられます。DHCP オプションを選択した場合は、中央のボタンを押します。**iDRAC7 の設定** の画面が表示されたら、手順 **9** に進みます。
静的	続く画面に、IP アドレス、ゲートウェイ、サブネットマスクを手動で入力します。 **静的** オプションを選択した場合は、中央のボタンを押して次の **CMC ネットワーク設定** 画面に進みます。 – 左右の矢印キーを使って位置を移動し、上下の矢印キーを使って各位置の数値を選択することで、**静的 IP アドレス** を設定します。**静的 IP アドレス** の設定を終えたら、中央のボタンを押して先に進みます。 – サブネットマスクを設定してから中央のボタンを押します。 – サブネットマスクを設定してから中央のボタンを押します。**ネットワークの概要** 画面が表示されます。 **ネットワークの概要** 画面には、入力した **静的 IP アドレス**、**サブネットマスク**、および **ゲートウェイ** の設定が表示されます。設定が正確であることを確認してください。設定を修正するには、左矢印キーで移動し、中央のボタンを押して、対象の設定画面に戻ります。修正を終えたら、中央のボタンを押します。 – 入力した設定が正しいことを確認してから、中央のボタンを押します。**DNS を登録しますか?** 画面が表示されます。

メモ: CMC IP 構成に DHCP（動的ホスト設定プロトコル）モードを選択すると、デフォルトで DNS 登録も有効になります。

8. 前の手順で **DHCP** を選択した場合は、手順 10 に進みます。

   DNS サーバーの IP アドレスを登録するには、中央のボタンを押して先に進みます。DNS がない場合は、右矢印キーを押します。**DNS を登録しますか?** の画面が表示されたら、手順 10 に進みます。

   左右の矢印キーを使って位置を移動し、上下の矢印キーを使って各位置の数値を選択することで、**DNS IP アドレス** を設定します。DNS IP アドレス の設定を終えたら、中央のボタンを押して先に進みます。

9. iDRAC を設定するかどうかを指定します。

   - **いいえ**: 手順 13 に進みます。
   - **はい**：中央のボタンを押して先に進みます。

   また、CMC GUI から iDRAC を設定できます。

10. サーバーに使用するインターネットプロトコル（IPv4、IPv6、または両方）を選択します。

動的ホスト構成プロトコル（DHCP）	iDRAC は IP 設定（IP アドレス、マスク、ゲートウェイ）をネットワーク上の DHCP サーバーから自動的に取得します。iDRAC には、ネットワーク上で割り振られた固有の IP アドレスが割り当てられます。中央のボタンを押してください。
静的	すぐ後に続く画面で、IP アドレス、ゲートウェイ、サブネットマスクを手動で入力する必要があります。 **静的** オプションを選択した場合は、中央のボタンを押して次の **iDRAC ネットワーク設定** 画面に進みます。 – 左右の矢印キーを使って位置を移動し、上下の矢印キーを使って各位置の数値を選択することで、**静的 IP アドレス** を設定します。このアドレスは、最初のスロットに装着された iDRAC の静的 IP アドレスです。後続の iDRAC の固定 IP アドレスは、この IP アドレスを増分したスロット番号として算出されます。**静的 IP アドレス** の設定を終えたら、中央のボタンを押して先に進みます。 – サブネットマスクを設定してから中央のボタンを押します。 – サブネットマスクを設定してから中央のボタンを押します。

   - IPMI LAN チャンネルを **有効** または **無効** にするかを選択します。 中央のボタンを押して続行します。
   - **iDRAC 構成** 画面で、インストールされているサーバーにすべての iDRAC ネットワーク設定を適用するには、**承諾する / はい** アイコンをハイライト表示して、中央のボタンを押します。インストールされているサーバーに iDRAC ネットワーク設定を適用するには、**いいえ** アイコンを反転表示させてから、中央のボタンを押して手順 c を続けます。
   - 次の **iDRAC 構成** 画面で、新しくインストールされたサーバーにすべての iDRAC ネットワーク設定を適用するには、承認する / はい アイコンをハイライト表示してから、中央のボタンを押します。新しいサーバーがシャーシに挿入されると、以前に設定したネットワーク設定 / ポリシーを使ってサーバーを自動展開するかどうかを尋ねるメッセージが、LCD に表示されます。新しくインストールされたサーバーに iDRAC ネットワーク設定を適用しない場合は、**いいえ** アイコンをハイライト表示してから中央のボタンを押します。新しいサーバーがシャーシに挿入されても、iDRAC ネットワーク設定は構成されません。

11. **エンクロージャ** 画面で、すべてのエンクロージャ設定を適用するには、**承諾する / はい** アイコンをハイライト表示させてから中央のボタンを押します。エンクロージャの設定を適用するには、**いいえ** アイコンをハイライト表示させてから中央のボタンを押します。
12. **IP の概要** 画面で、設定した IP アドレスが正しいことを確認します。設定を修正するには、左矢印キーで移動し、中央のボタンを押して、対象の設定画面に戻ります。修正を終えたら、中央のボタンを押します。必要に応じて、右矢印キーで移動し、中央のボタンを押して、**IP の概要** 画面に戻ります。

入力した設定がすべて正しいことを確認したら、中央のボタンを押します。設定ウィザードが閉じて、**メインメニュー** 画面に戻ります。

メモ: はい / 承認する を選択している場合は、**待機** 画面が表示されてから、**IP の概要** 画面が表示されます。

これで CMC と iDRAC は、ネットワークでも利用できるようになりました。ウェブインタフェース、シリアルコンソール、Telnet、SSH などの CLI を使用して、割り当てられた IP アドレスの CMC にアクセスできます。

メモ: LCD 設定ウィザードを使ってネットワークの設定を終えた後は、ウィザードが使用できなくなります。

CMC にアクセスするためのインタフェースおよびプロトコル

CMC ネットワーク設定を終えた後、さまざまなインタフェースを使って CMC にリモートアクセスできます。次の表に、リモートで CMC にアクセスするために使用できるインタフェースを示します。

メモ: Telnet は他のインターフェースほどセキュアではないため、デフォルトでは無効です。Telnet は、ウェブ、ssh またはリモート RACADM を使用して有効にします。

メモ: 複数のインタフェースを同時に使用すると、予期しない結果が生じることがあります。

表 7. CMC インタフェース

インタフェース	説明
ウェブインタフェース	グラフィカルユーザーインタフェースを使って CMC へのリモートアクセスを提供します。ウェブインタフェースは CMC のファームウェアに組み込まれ、管理ステーションで対応ウェブブラウザから NIC インタフェースを介してアクセスします。 対応するウェブブラウザのリストは、デルサポートサイト **dell.com/support/manuals** にある『*Readme*』で対応ブラウザの項を参照してください。
リモート RACADM コマンドラインインタフェース	このコマンドラインユーティリティを使用して、CMC とそのコンポーネントを管理します。リモートまたはファームウェア RACADM を使用できます。 • リモート RACADM は、管理ステーションで実行されるクライアントユーティリティです。これは、管理下システムで RACADM コマンドを使用するために帯域外ネットワークインタフェースを使用し、HTTP チャネルも使用します。`-r` オプションは、ネットワークで RACADM コマンドを実行します。 • ファームウェア RACADM には、SSH または telnet を使用して CMC にログインすることでアクセスできます。CMC IP、ユーザー名、またはパスワードを指定しなくても、ファームウェア RACADM コマンドを実行できます。 RACADM プロンプトが開いたら、racadm プリフィックスなしで直接コマンドを実行できます。
シャーシ LCD パネル	前面パネルの LCD を使用して、次の操作を行うことができます。 • アラート、CMC IP または MAC アドレス、ユーザーによるプログラムが可能な文字列の表示 • DHCP の設定 • CMC 静的 IP の設定

インタフェース	説明
	サーバーを再起動しないで CMC をリセットするには、システム識別  ボタンを 16 秒間押し続けます。
Telnet	ネットワーク経由でコマンドラインによる CMC へのアクセスを提供します。RACADM コマンドライン インタフェースとサーバーまたは IO モジュールのシリアル コンソールの接続に使われる connect コマンドは、CMC コマンド ラインから実行できます。 **メモ:** Telnet は、セキュアなプロトコルではなく、デフォルトで無効になっています。Telnet は、パスワードのプレーンテキストでの送信を含む、すべてのデータを伝送します。機密情報を伝送する場合は、SSH インタフェースを使用してください。
SSH	SSH を使用して RACADM コマンドを実行します。 高度なセキュリティを実現するために暗号化されたトランスポート層を使用して、Telnet コンソールと同じ機能を提供します。デフォルトで SSH サービスは CMC で有効になっており、無効にすることができます。
WS-MAN	LC-Remote Services は、WS-Management プロトコルに基づいて一対多のシステム管理タスクを実行します。LC-Remote Services 機能を使用するには、WinRM クライアント（Windows）や OpenWSMAN クライアント（Linux）などの WS-MAN クライアントを使用する必要があります。Power Shell および Python を使用して、WS-MAN インタフェースに対してスクリプトを実行することもできます。 Web Services for Management（WS-Management）は、システム管理に使用する SOAP（Simple Object Access Protocol）ベースのプロトコルです。CMC は、WS-Management を使用して、Distributed Management Task Force（DMTF）の Common Information Model（CIM）ベースの管理情報を伝達します。CIM 情報は、管理化システムで変更できるセマンティックや情報の種類を定義します。 CMC WS-MAN の実装は、トランスポートセキュリティに対してポート 443 の SSL を使用し、基本認証をサポートしています。WS-Management で使用できるデータは、DMTF プロファイルおよび拡張プロファイルにマップされている、CMC 計装インタフェースによって提供されます。 詳細については、次の文書を参照してください。 • MOF およびプロファイル — **delltechcenter.com/page/DCIM.Library** • DTMF ウェブサイト — **dmtf.org/standards/profiles/** • WS-MAN リリースノートまたは Read Me ファイル。 • **www.wbemsolutions.com/ws_management.html** • DMTF WS-Management 仕様：**www.dmtf.org/standards/wbem/wsman** ウェブサービスインタフェースは、Windows WinRM や Powershell CLI、WSMANCLI などのオープンソースユーティリティ、Microsoft .NET などのアプリケーションプログラミング環境といったクライアントインフラストラクチャを活用することで、使用できます。 Microsoft WinRM を使用してクライアント接続を行うには、最低バージョン 2.0 が必要です。詳細については、Microsoft の記事 <**support.microsoft.com/kb/968929**> を参照してください。

メモ: CMC デフォルトユーザー名は **root**、デフォルトパスワードは **calvin** です。

その他のシステム管理ツールを使用した CMC の起動

Dell Server Administrator または Dell OpenManage IT Assistant を使って CMC を起動することもできます。

Dell Server Administrator を使って CMC インタフェースにアクセスするには、管理ステーションで Server Administrator を起動します。Server Administrator ホームページの左ペインにあるシステムツリーで、**システム → メインシステムシャーシ → モートアクセスコントローラ** の順にクリックします。詳細については、『*Dell Server Administrator ユーザーズガイド*』を参照してください。

CMC ファームウェアのダウンロードとアップデート

CMC ファームウェアをダウンロードするには、「DCMC ファームウェアのダウンロード」を参照してください。

CMC ファームウェアをアップデートするには、「DCMC ファームウェアのアップデート」を参照してください。

シャーシの物理的な場所とシャーシ名の設定

ネットワーク上でシャーシを識別するために、データセンターでのシャーシの物理的な場所とシャーシ名（デフォルト名は **Dell Rack System**）を設定できます。たとえば、シャーシ名での SNMP クエリで、設定した名前が返されます。

ウェブインタフェースを使用したシャーシの物理的位置およびシャーシ名の設定

CMC ウェブインタフェースを使用してシャーシの位置およびシャーシ名を設定するには、次の手順を実行します。

1. システムツリーで、**シャーシの概要** へ移動し、**セットアップ → 一般** をクリックします。
   シャーシの一般設定 ページが表示されます。
2. 場所のプロパティとシャーシ名を入力します。詳細については、『*CMC オンラインヘルプ*』を参照してください。

   メモ: シャーシの場所 フィールドはオプションです。**データセンター**、**通路**、**ラック**、および **ラックスロット** フィールドを使用して、シャーシの物理的な場所を示すことを推奨します。
3. **適用** をクリックします。設定が保存されます。

RACADM を使用したシャーシの物理的な場所とシャーシ名の設定

コマンドラインインタフェースを使ってとシャーシ名または場所、日付と時刻を設定するには、**setsysinfo** および **setchassisname** コマンドを参照してください。詳細は、『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

CMC の日付と時刻の設定

日付や時刻を手動で設定でき、あるいはネットワーク時間プロトコル（NTP）サーバーと日付と時刻を同期させることができます。

CMC ウェブインタフェースを使用した CMC の日付と時刻の設定

CMC ウェブインタフェースを使用して CMC の日付と時刻を設定するには：

1. システムツリーで、シャーシの概要へ移動し、**セットアップ → 日付 / 時刻** をクリックします。
   日付 / 時刻 ページが表示されます。
2. 日時をネットワーク時間プロトコル（NTP）サーバーと同期するには、**NTP を有効にする** を選択し、NTP サーバーを 3 台まで指定します。
3. 日時を手動で設定するには、**NTP を有効にする** を選択解除し、**日付** と **時刻** の各フィールドを編集して、ドロップダウンメニューから **タイムゾーン** を選択した後、**適用** をクリックします。

RACADM を使用した CMC の日付と時刻の設定

コマンドラインインタフェースを使って日付と時刻を設定するには、『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』の config コマンドと `cfgRemoteHosts` データベースプロパティグループの項を参照してください。

シャーシ上のコンポーネントを識別するための LED の設定

すべてのまたは個別のコンポーネント（シャーシ、サーバー、IOM）のコンポーネント LED を点滅させてシャーシ上のコンポーネントを識別することができます。

メモ: これらの設定を変更するには、**シャーシ設定システム管理者** の権限が必要です。

CMC ウェブインタフェースを使用した LED 点滅の設定

CMC ウェブインタフェースを使用して 1 つ、複数、またはすべての LED 点滅を有効にするには、次の手順を実行します。

1. 次のいずれかのページに移動します。
   - **シャーシの概要 → トラブルシューティング → 識別**。
   - **シャーシの概要 → シャーシコントローラ → トラブルシューティング → 識別**。
   - **シャーシの概要 → サーバーの概要 → トラブルシューティング → 識別**。

     メモ: このページではサーバーのみを選択できます。
   - **シャーシの概要 → I/O モジュールの概要 → トラブルシューティング → 識別**。
     識別 ページが表示されます。
2. コンポーネント LED の点滅を有効にするには、必要なコンポーネントを選択して **点滅** をクリックします。
3. コンポーネント LED の点滅を無効にするには、必要なコンポーネントの選択を解除して **点滅解除** をクリックします。

RACADM を使用した LED の点滅の設定

シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインした後、次を入力します。

```
racadm setled -m <モジュール> [-l <ledState>]
```

ここで、*<モジュール>* は LED の設定を行うモジュールを指定します。設定オプション：

- `server-nx`（*n* = 1〜8 および *x* = a、b、c、または d）

- switch-n（*n*=1～6）
- cmc-active

および *<ledState>* は LED を点滅させるかどうかを指定します。

- 0 — 点滅なし（デフォルト）
- 1 — 点滅

CMC プロパティの設定

ウェブインタフェースまたは RACADM を使って、電力バジェット、ネットワーク設定、ユーザー、SNMP および E-メールアラートなどの CMC プロパティを設定することができます。

CMC ウェブインタフェースを使用した iDRAC 起動方法の設定

シャーシの一般設定 ページから iDRAC 起動方法を設定するには、次の手順を実行します。

1. システムツリーで **シャーシ概要** → **設定** をクリックします。
   シャーシの一般設定 ページが表示されます。
2. **iDRAC 起動方法** プロパティのドロップダウンメニューで、**IP アドレス** または **DNS** を選択します。
3. **適用** をクリックします。

   メモ: DNS ベースの起動は、以下の場合のみ、特定の iDRAC に使われます。

   - シャーシ設定が DNS である。
   - 特定の iDRAC が DNS 名で設定されていることを CMC が検出した。

RACADM を使用した iDRAC 起動方法の設定

RACADM を使用して CMC ファームウェアをアップデートするには、cfgRacTuneIdracDNSLaunchEnable サブコマンドを使用します。詳細については、『iDRAC7 および CMC 用 RACADM コマンドラインリファレンスガイド』を参照してください。

CMC ウェブインタフェースを使用したログインロックアウトポリシー属性の設定

メモ: 次の手順を行うには、**シャーシ設定システム管理者**の権限が必要です。

ログインセキュリティ により、CMC ウェブインタフェースを使用した CMC ログインの IP 範囲属性の設定が可能になります。CMC ウェブインタフェースを使用して IP 範囲属性を設定するには、以下の手順を実行します。

1. システムツリーで **シャーシ概要** へ移動し、**ネットワーク** → **ネットワーク** をクリックします。
   ネットワーク設定ページが表示されます。
2. IPv4 設定セクションで、**詳細設定** をクリックします。あるいは、**ログインセキュリティ** ページにアクセスするには、システムツリーで **シャーシ概要** に移動して、**セキュリティ** → **ログイン** をクリックします。
   ログインセキュリティ ページが表示されます。
3. ユーザーブロックまたは IP ブロック機能を有効にするには、**ログインロックアウトポリシー** セクションで、**ユーザー名によるロックアウト** または **IP アドレス（IPV4）によるロックアウト** を選択します。
   その他のログインロックアウトポリシー属性を設定するオプションがアクティブになります。

4. アクティブになったフィールドで、ログインロックアウトポリシー属性に必要な値 — **ロックアウト失敗回数**、**ロックアウト失敗時間枠**、および **ロックアウトペナルティ時間** を入力します。 詳細については、『CMC オンラインヘルプ』を参照してください。
5. これらの設定を保存するには、**適用**をクリックします。

RACADM を使用したログインロックアウトポリシー属性の設定

RACADM を指定して、以下の機能にログインロックアウトポリシー属性を設定することができます。

- ユーザーブロック
- IP アドレスブロック
- 許容されるログイン試行回数
- ロックアウト失敗回数が生じる期間
- ロックアウトペナルティ時間

- ユーザーブロック機能を有効化するには、以下を使用します。
  `racadm config -g cfgRacTuning -o cfgRacTuneUserBlkEnable <0|1>`
- IP ブロック機能を有効化するには、以下を使用します。
  `racadm config -g cfgRacTuning -o cfgRacTuneIPBlkEnable <0|1>`
- ログイン試行回数を指定するには、以下を使用します。
  `racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount`
- ロックアウト失敗回数が生じる必要がある期間を指定するには、以下を使用します。
  `racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow`
- ロックアウトペナルティ時間の値を指定するには、以下を使用します。
  `racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime`

これらのオブジェクトの詳細に関しては、**dell.com/support/manuals** にある『iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド』を参照してください。

冗長 CMC 環境について

アクティブ CMC に障害が発生した場合に、フェイルオーバーするためのスタンバイ CMC を取り付けられます。冗長 CMC は、事前に取り付けることも、後日取り付けることもできます。CMC ネットワークを適切にケーブル接続し、完全冗長性またはベストパフォーマンスを確保することが大切です。

フェイルオーバーは、次のような場合に行われます。

- RACADM **cmcchangeover** コマンドを実行した場合（『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』の **cmcchangeover** コマンドの項を参照してください）。
- アクティブ CMC で RACADM racreset コマンドを実行した場合（『*iDRAC6 および CMC 向け RACADM コマンドラインリファレンスガイド*』の **racreset** コマンドの項を参照してください）。
- ウェブインタフェースでアクティブ CMC をリセットした場合。（電力制御操作の実行 に説明される **電力制御操作** の **CMC のリセット** オプションを参照。）
- アクティブ CMC からネットワークケーブルを外した場合。
- シャーシからアクティブ CMC を取り外した場合。
- アクティブ CMC で CMC ファームウェアフラッシュアップデートを行った場合 。
- アクティブ CMC が機能していない場合

  メモ: CMC フェイルオーバーが発生すると、すべての iDRAC 接続およびすべてのアクティブな CMC セッションが失われます。セッションを失ったユーザーは、新しいアクティブ CMC に再接続する必要があります。

関連リンク

スタンバイ CMC について

スタンバイ CMC はアクティブ CMC と同一で、そのミラーとして維持されています。アクティブ CMC とスタンバイ CMC には共に同じファームウェアリビジョンがインストールされている必要があります。ファームウェアリビジョンが異なる場合、冗長性劣化として報告されます。

スタンバイ CMC はアクティブ CMC と同じ設定とプロパティを引き継ぎます。CMC のファームウェアリビジョンは同じでなければなりませんが、スタンバイ CMC に設定を複製する必要はありません。

メモ: スタンバイ CMC の取り付けに関する詳細は、『*ハードウェアオーナーズマニュアル*』を参照してください。スタンバイ CMC に CMC ファームウェアをインストールする手順については、「ファームウェアのアップデート」を参照してください。

CMC フェイルセーフモード

フェイルセーフモードでは、冗長 CMC によるフェイルオーバー保護と同様、M1000e エンクロージャでもフェイルセーフモードによってブレードと I/O モジュールを障害から保護することができます。フェイルセーフモードは、シャーシを制御している CMC がない時に有効になります。CMC のフェイルオーバー中、または単一の CMC 管理が失われている間には、次の状態が発生します。

- 新たに取り付け足したブレードの電源を入れることができない
- 既存のブレードにリモートでアクセスできません。
- コンポーネントの熱保護のため、シャーシの冷却ファンが 100% 稼動
- CMC の管理が復旧するまで、電力消費制限のためにブレードのパフォーマンスが低下

CMC 管理の喪失につながる状況のいくつかを以下に示します。

- CMC の取り外し — シャーシの管理は、CMC の交換またはスタンバイ CMC へのフェイルオーバー後に再開されます。
- CMC ネットワークケーブルの取り外しまたはネットワーク接続の損失 — シャーシの管理はスタンバイ CMC へのフェイルオーバー後に再開されます。ネットワークフェイルオーバーは冗長 CMC モードでのみ有効になります。
- CMC のリセット — CMC が再起動したあと、またはシャーシがフェイルオーバーしてスタンバイ CMC に引き継がれたあとに、シャーシ管理が再開します。
- CMC フェイルオーバーコマンドの発行 — シャーシの管理はスタンバイ CMC へのフェイルオーバー後に再開されます。
- CMC ファームウェアのアップデート — CMC が再起動したあと、またはシャーシがフェイルオーバーしてスタンバイ CMC に引き継がれたあとに、シャーシ管理が再開します。フェイルオーバーイベントが 1 つだけになるように、先にスタンバイ CMC をアップデートすることをお勧めします。
- CMC エラー検出と修正 — CMC のリセット後、またはシャーシがフェイルオーバーしてスタンバイ CMC に引き継がれたあとに、シャーシ管理が再開します。

  メモ: エンクロージャは、1 つの CMC で構成することも、冗長 CMC で構成することもできます。冗長 CMC 構成では、プライマリ CMC がエンクロージャまたは管理ネットワークとの通信を失うと、スタンバイ CMC がシャーシ管理を引き継ぎます。

アクティブ CMC の選択プロセス

2 つの CMC スロットには違いはありません。つまり、スロットによってアクティブかスタンバイかが決まるわけではありません。最初に取り付けた、または起動した CMC がアクティブ CMC になります。CMC が 2 つ

取り付けられている場合に AC 電源を入れると、CMC シャーシスロット 1（左側）に取り付けられている CMC がアクティブ CMC になります。アクティブ CMC は青色 LED で示されます。

既に電源が入っているシャーシに 2 台の CMC を挿入した場合、自動アクティブ / スタンバイネゴシエーションに 2 分間までかかることがあります。ネゴシエーションが完了したら、通常のシャーシの動作が再開されます。

冗長 CMC の正常性ステータスの取得

ウェブインタフェースでスタンバイ CMC の正常性ステータスを表示できます。ウェブインタフェースで CMC の正常性ステータスにアクセスする詳細については、「シャーシ情報の表示およびシャーシとコンポーネントの正常性の監視」を参照してください。

3

CMC へのログイン

CMC には、CMC ローカルユーザー、Microsoft Active Directory ユーザー、または LDAP ユーザーとしてログインできます。デフォルトのユーザー名とパスワードは、それぞれ root および calvin です。シングルサインオンまたはスマートカードを使用してログインすることもできます。

関連リンク

CMC ウェブインタフェースへのアクセス
ローカルユーザー、Active Directory ユーザー、または LDAP ユーザーとしての CMC へのログイン
スマートカードを使用した CMC へのログイン
シングルサインオンを使用した CMC へのログイン
シリアル、Telnet、または SSH コンソールを使用した CMC へのログイン
RACADM を使用した CMC へのアクセス
公開キー認証を使用した CMC へのログイン

CMC ウェブインタフェースへのアクセス

ウェブインタフェースを使用して CMC にログインする前に、サポートされているウェブブラウザ（Internet Explorer または Firefox）が設定されており、必要な権限を持つユーザーアカウントが作成されていることを確認してください。

メモ: プロキシ経由の接続で Microsoft Internet Explorer を使用している場合、エラーメッセージ「XML ページを表示できません」が表示されたときは、プロキシを無効にする必要があります。

CMC ウェブインタフェースにアクセスするには：

1. サポートされているウェブブラウザのウィンドウを開きます。
   対応ウェブブラウザについての最新情報は、**dell.com/support/manuals** で『*Readme*』を参照してください。
2. **アドレス** フィールドに次の URL を入力し、<Enter> を押します。
   - IPv4 アドレスを使用して CMC にアクセスするには：`https://<CMC IP アドレス>`
     デフォルトの HTTPS ポート番号（ポート 443）が変更されている場合は、次のように入力します：`https://<CMC IP アドレス>:<ポート番号>`
   - IPv6 アドレスを使用して CMC にアクセスするには：`https://[<CMC IP アドレス>]`
     デフォルトの HTTPS ポート番号（ポート 443）が変更されている場合は、次のように入力します：`https://[<CMC IP アドレス>]:<ポート番号>`

     メモ: IPv6 を使用する場合は、*<CMC の IP アドレス>* を角かっこ（[ ]）で囲む必要があります。

     <CMC の IP アドレス> は CMC の IP アドレス、*<ポート番号>* は HTTPS のポート番号です。

     CMC の ログイン ページが表示されます。

関連リンク

ウェブブラウザの設定
ローカルユーザー、Active Directory ユーザー、または LDAP ユーザーとしての CMC へのログイン
スマートカードを使用した CMC へのログイン

シングルサインオンを使用した CMC へのログイン

ローカルユーザー、Active Directory ユーザー、または LDAP ユーザーとしての CMC へのログイン

CMC にログインするには、**CMC へのログイン** 権限を持つ CMC アカウントが必要です。デフォルトの CMC ユーザー名は root、パスワードは calvin です。ルートアカウントは、CMC 出荷時のデフォルトの管理者アカウントです。

メモ: セキュリティを強化するために、初期設定時に root アカウントのデフォルトパスワードを変更することを強くお勧めします。

CMC では、ß、å、é、ü などの拡張 ASCII 文字、および主に英語以外の言語で使用されるその他の文字がサポートされていません。

1 台のワークステーション上で複数のブラウザウィンドウを開き、異なるユーザー名を利用してウェブインタフェースにログインすることはできません。

ローカルユーザー、Active Directory ユーザー、または LDAP ユーザーとしてログインするには、次の手順を実行します。

1. **ユーザー名** フィールドにユーザー名を入力します。
   - CMC ユーザー名: <ユーザー名>
   - Active Directory ユーザー名 : <ドメイン>\<ユーザー名>、<ドメイン>/<ユーザー名> または <ユーザー>@<ドメイン>
   - LDAP ユーザー名: <ユーザー名>

   メモ: このフィールドでは大文字と小文字が区別されます。Active Directory ユーザーとしてログインするには、次の手順を実行します。
2. **パスワード** フィールドにユーザーパスワードを入力します。

   メモ: このフィールドでは大文字と小文字が区別されます。
3. オプションとしてセッションタイムアウトを選択します。これは、自動的にログアウトするまで操作を行わずにログインしたままにできる時間を指します。デフォルト地は、ウェブサービスアイドルタイムアウトです。
4. **OK** をクリックします。

   必要なユーザー権限で CMC にログインしました。

関連リンク

ユーザーアカウントと権限の設定
CMC ウェブインタフェースへのアクセス

スマートカードを使用した CMC へのログイン

スマートカードを使用して CMC にログインできます。スマートカードでは、次の 2 層構造のセキュリティを実現する 2 要素認証（TFA）が提供されます。

- 物理的なスマートカードデバイス。
- パスワードや PIN などの秘密コード。

ユーザーは、スマートカードと PIN を使用して自身の資格情報を検証する必要があります。

メモ: スマートカードにログインには、IP アドレスを使って、 CMC にログインすることはできません。Kerberos は、完全修飾ドメイン名（FQDN）を基にユーザーの資格情報を検証します。

スマートカードを使用して Active Directory ユーザーとしてログインする前に、次を実行する必要があります。

- 信頼できる認証局（CA）証明書（CA 署名付き Active Directory 証明書）を CMC にアップロードします。
- DNS サーバーを設定します。
- Active Directory ログインを有効にします。
- スマートカードログインを有効にします。

スマートカードを使用して CMC に Active Directory ユーザーとしてログインするには、次の手順を実行します。

1. 次のリンクを使用して CMC にログインします。 `https://<cmcname.domain-name>`
   CMC ログイン ページが表示され、スマートカードを挿入するプロンプトが表示されます。

   メモ: デフォルトの HTTPS ポート番号（ポート 80）を変更した場合は、`<cmcname.domain-name>:<port number>` を使って CMC ウェブページにアクセスします。ここで、**cmcname** は CMC の CMC ホスト名、**domain-name** はドメイン名、**port number** は HTTPS のポート番号をそれぞれ表します
2. スマートカードを挿入し、**ログイン** をクリックします。
   PIN ポップアップが表示されます。
3. PIN を入力し、**送信** をクリックします。

   メモ: スマートカードユーザーが Active Directory に存在する場合、Active Directory のパスワードは必要ありません。

   Active Directory の資格情報で CMC にログインされます。

関連リンク

Active Directory ユーザーに対する CMC SSO またはスマートカードログインの設定

シングルサインオンを使用した CMC へのログイン

シングルサインオン（SSO）を有効にすると、ユーザー名やパスワードなどのドメインユーザー認証資格情報を入力せずに、CMC にログインできます。

メモ: IP アドレスを使って、シングルサインオンにログインすることはできません。Kerberos は、完全修飾ドメイン名（FQDN）に対してユーザーの資格情報を検証します。

シングルサインオンを使用して CMC にログインする前に、次を確認してください。

- 有効な Active Directory ユーザーアカウントを使用して、システムにログインしている。
- Active Directory の設定時に、シングルサインオンオプションを有効にしている。

シングルサインオンを使用して CMC にログインするには、次の手順を実行します。

1. ネットワークアカウントを使ってクライアントシステムにログインします。
2. `https://<cmcname.domain-name>` を使用して CMC ウェブインタフェースにアクセスします。
   例：**cmc-6G2WXF1.cmcad.lab,** ここで、**cmc-6G2WXF1** は cmc 名、**cmcad.lab** はドメイン名です。

   メモ: デフォルトの HTTPS ポート番号（ポート 80）を変更した場合は、`<cmc 名.ドメイン名>:<ポート番号>` の書式で CMC ウェブインタフェースにアクセスします。ここで、**cmc 名** は CMC の CMC ホスト名、ドメイン名 はドメイン名、ポート番号 は HTTPS のポート番号をそれぞれ表します。

   CMC は、有効な Active Directory アカウントを使ってログインしたときにブラウザによってキャッシュされた Kerberos 資格情報でユーザーをログインします。ログインに失敗すると、ブラウザは通常の CMC ログインページにリダイレクトされます。

メモ: Active Directory ドメインにログインしないで Internet Explorer 以外のブラウザを使用している場合は、ログインに失敗し、ブラウザには空白ページのみが表示されます。

関連リンク

Active Directory ユーザーに対する CMC SSO またはスマートカードログインの設定

シリアル、Telnet、または SSH コンソールを使用した CMC へのログイン

シリアル、Telnet、または SSH 接続、あるいは iKVM 上の Dell CMC コンソールを使って CMC にログインできます。

管理ステーションのターミナルエミュレータソフトウェアおよび管理下ノード BIOS を設定した後、次の手順に従って CMC にログインします。

1. 管理ステーションのターミナルエミュレーションソフトウェアを使って、CMC に接続します。
2. CMC ユーザー名とパスワードを入力して、<Enter> を押します。

   これで、CMC にログインできます。

関連リンク

CMC にコマンドラインコンソールの使用を設定する方法

Dell CMC コンソールからの iKVM へのアクセスの有効化

RACADM を使用した CMC へのアクセス

RACADM は、テキストベースのインタフェースを通して CMC の設定と管理を行えるコマンド群を提供します。RACADM には、Telnet/SSH またはシリアル接続の使用、iKVM 上で Dell CMC コンソールの使用、あるいは管理ステーションにインストールされた RACADM コマンドラインインタフェースのリモート使用によってアクセスできます。

RACADM インタフェースは、次のように分類されます。

メモ: リモート RACADM は、『Dell Systems Management ツールおよびマニュアル DVD』に含まれており、管理ステーションにインストールされます。

- リモート RACADM — -r オプションと CMC の DNS 名または IP アドレスを使って、管理ステーション上で RACADM コマンドを実行できます。
- ファームウェア RACADM — Telnet、SSH、シリアル接続、または iKVM を使って CMC にログインできます。ファームウェア RACADM では、CMC ファームウェアの一部である RACADM を実行することになります。

リモート RACADM コマンドをスクリプトで使用して、複数 CMC を設定することができます。CMC はスクリプトに対応していないため、スクリプトを直接 CMC で実行することはできません。

RACADM の詳細については、『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

複数の CMC を設定する方法については、「RACADM を使用した複数の CMC の設定」を参照してください。

公開キー認証を使用した CMC へのログイン

パスワードを入力せずに SSH 経由で iDRAC7 にログインできます。また、1 つの RACADM コマンドをコマンドライン引数として SSH アプリケーションに送信できます。コマンドの完了後にセッションが終了するため、コマンドラインオプションはリモート RACADM と同様に動作します。

SSH 経由で iDRAC7 にログインする前に、公開キーがアップロードされていることを確認してください。

たとえば、次のとおりです。

- **ログイン**: `ssh service@<ドメイン>` または `ssh service@<IP_address>` ここで、IP_address は CMC IP アドレスです。
- **RACADM コマンドの送信**: `ssh service@<ドメイン> racadm getversion` および `ssh service@<ドメイン> racadm getsel`

サービスアカウントへのログイン時に、パスフレーズが公開 / 秘密キーペアを作成するときに設定された場合は、そのパスフレーズの再入力を求めるメッセージが表示される場合があります。パスフレーズをキーと一緒に使用している場合は、Windows および Linux の両方のクライアントには、その操作を自動化する方法が用意されています。Windows クライアントでは、Pageant アプリケーションを使用できます。このアプリケーションはバックグラウンドで実行され、パスフレーズの入力操作は透過的に行われます。Linux クライアントでは、 sshagent を使用できます。これらのいずれかのアプリケーションを設定および使用するには、そのアプリケーションに付属のマニュアルを参照してください。

関連リンク

SSH 経由の公開キー認証の設定

複数の CMC セッション

次の表では、各種インタフェースを使用して実行できる複数の CMC セッションのリストを提供します。

表 8. 複数の CMC セッション

インタフェース	セッション数
CMC ウェブインタフェース	4
RACADM	4
Telnet	4
SSH	4

デフォルトログインパスワードの変更

デフォルトパスワードの変更を求める警告メッセージは、以下の場合に表示されます。

- **ユーザー設定** 権限で CMC にログインする。
- デフォルトパスワード警告機能が有効になっている。
- 現在有効なアカウントのデフォルトユーザー名およびパスワードが、それぞれ `root` および `calvin` である。

Active Directory または LDAP でログインしても同じ警告メッセージが表示されます。ローカルアカウントが資格情報として `root` および `calvin` を持っているかどうかを判別するときに Active Directory および LDAP アカウントは考慮されません。警告メッセージは、SSH、Telnet、リモート RACADM、またはウェブインタフェースを使用して CMC にログインするときにも表示されます。リモート RACADM の場合、警告メッセージは各コマンドで表示されます。

資格情報を変更するには、**ユーザー設定** 権限が必要です。

メモ: CMC **ログイン** ページで **今後この警告を表示しない** オプションが選択されている場合、CMC ログメッセージが生成されます。

ウェブインタフェースを使用したデフォルトログインパスワードの変更

CMC ウェブインタフェースにログインするときに、**デフォルトパスワード警告** ページが表示された場合、パスワードを変更できます。これを行うには、次の手順を実行します。

1. **デフォルトパスワードの変更** オプションを選択します。
2. **新しいパスワード** フィールドに、新しいパスワードを入力します。
   パスワードの最大文字数は 20 文字です。文字はマスクされます。次の文字がサポートされています。
   - 0～9
   - A～Z
   - a～z
   - 特殊文字 : +、&、?、>、-、}、|、.、!、(、'、,、_、[、"、@、#、)、*、;、$、]、/、§、%、=、<、:、{、`、\
3. **パスワードの確認** フィールドに、もう一度パスワードを入力します。
4. **続行** をクリックします。新しいパスワードが設定され、CMC にログインされます。

   メモ: 続行 は、**新しいパスワード** フィールドと **パスワードの確認** フィールドに入力されたパスワードが一致した場合にのみ有効化されます。

   この他のフィールドについての詳細は、『CMC オンラインヘルプ』を参照してください。

RACADM を使用したデフォルトログインパスワードの変更

パスワードを変更するには、次の RACADM コマンドを実行します。

```
racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i <index> <newpassword>
```

ここで <index> は 1 から 16 の値（ユーザーアカウントを示す）、および <newpassword> は新しいユーザー定義のパスワードです。

詳細に関しては、『iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド』を参照してください。

デフォルトパスワード警告メッセージの有効化または無効化

デフォルトパスワード警告メッセージの表示を有効または無効にすることができます。これを行うには、ユーザー設定権限が必要です。

ウェブインタフェースを使用したデフォルトパスワード警告メッセージの有効化または無効化

iDRAC にログインした後にデフォルトパスワード警告メッセージを有効または無効にするには、次の手順を実行します。

1. **シャーシコントローラ → ユーザー認証 → ローカルユーザー** に進みます。
   ユーザー ページが表示されます。
2. **デフォルトパスワード警告** セクションで、**有効** を選択し、次に **適用** をクリックして、CMC へのログイン時における **デフォルトパスワード警告** ページの表示を有効にします。これを行わない場合は、**無効** を選択します。
   または、この機能が有効になっていて、今後のログイン操作で警告メッセージを表示したくない場合は、**デフォルトパスワード警告** ページで、**今後この警告を表示しない** オプションを選択し、**適用** をクリックします。

RACADM を使用したデフォルトログインパスワードの変更のための警告メッセージの有効化または無効化

RACADM を使用してデフォルトログインパスワードの変更のための警告メッセージを有効化するには、`racadm config -g cfgRacTuning -o cfgRacTuneDefCredentialWarningEnable<0> or <1>` オブジェクトを使用します。詳細については、**dell.com/support/manuals** にある、『iDRAC7 および CMC 向け RACADM コマンドラインレファレンスガイド』を参照してください。

4

ファームウェアのアップデート

以下のファームウェアをアップデートできます。

- CMC — アクティブとスタンバイ
- iKVM
- IOM

以下のサーバーコンポーネントのファームウェアをアップデートできます。

- iDRAC - iDRAC6 より前の iDRAC では、リカバリインタフェースを使用してアップデートする必要があります。iDRAC6 ファームウェアもリカバリインタフェースでアップデートできますが、iDRAC6 およびそれ以降のバージョンでは廃止されています。
- BIOS
- Unified Server Configurator
- 32 ビット診断
- オペレーティングシステムドライバパック
- ネットワークインタフェースコントローラ
- RAID コントローラ

関連リンク

CMC ファームウェアのダウンロード
現在インストールされているファームウェアのバージョンの表示
CMC ファームウェアのアップデート
iKVM ファームウェアのアップデート
サーバー iDRAC ファームウェアのアップデート
サーバーコンポーネントファームウェアのアップデート
CMC を使用した iDRAC ファームウェアのリカバリ
IOM インフラストラクチャデバイスファームウェアのアップデート

CMC ファームウェアのダウンロード

ファームウェアのアップデートを開始する前に、デルサポートサイト **support.dell.com** から最新のファームウェアバージョンをダウンロードし、ローカルシステムに保存します。

CMC ファームウェアパッケージには、次のソフトウェアコンポーネントが含まれています。

- コンパイルされた CMC ファームウェアコードとデータ
- ウェブインタフェース、JPEG、および他のユーザーインタフェースデータファイル
- デフォルト設定ファイル

現在インストールされているファームウェアのバージョンの表示

You can view the currently installed firmware versions using the CMC ウェブインタフェースまたは RACADM を使用して、現在インストールされているファームウェアのバージョンを表示できます。

CMC ウェブインタフェースを使用した現在インストールされているファームウェアバージョンの表示

現在インストールされているファームウェアバージョンを表示するには、CMC ウェブインタフェースで次のいずれかのページに移動します。

- **シャーシの概要 → アップデート**
- **シャーシの概要 → シャーシコントローラ → アップデート**
- **シャーシの概要 → サーバーの概要 → アップデート**
- **シャーシの概要 → I/O モジュール概要 → アップデート**
- **シャーシの概要 → iKVM → アップデート**

ファームウェアアップデート ページには、一覧表示された各コンポーネントに対するファームウェアの現行バージョンが表示され、ファームウェアを最新バージョンにアップデートできます。
シャーシに iDRAC がリカバリ モードにある前世代のサーバーが存在する場合、または iDRAC のファームウェアが破損していることを CMC が検出した場合には、これらの前世代 iDRAC も ファームウェアのアップデートページに表示されます。

RACADM を使用した現在インストールされているファームウェアバージョンの表示

RACADM を使用して現在インストールされているファームウェアバージョンを表示するには、**getkvminfo** サブコマンドを使用します。詳細については、『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

CMC ファームウェアのアップデート

CMC ウェブインタフェースまたは RACADM を使用して、CMC ファームウェアをアップデートできます。ファームウェアアップデートは、デフォルトで現在の CMC 設定を保持します。アップデート処理中に、CMC 構成設定を工場出荷時のデフォルト設定にリセットすることができます。

メモ: CMC 上でファームウェアをアップデートするには、シャーシ設定システム管理者 の権限が必要です。

システムコンポーネントのファームウェアをアップデートするためにウェブユーザーインタフェースのセッションを利用する場合、ファイル転送時間を十分に許容できるようにアイドルタイムアウト時間を設定する必要があります。ファームウェアのファイル転送に 30 分までもかかることがあります。アイドルタイムアウト値を設定するには、「サービスの設定」を参照してください。
CMC ファームウェアのアップデート中、シャーシ内の冷却ファンの一部または全部が全速回転します。
シャーシに冗長 CMC がある場合、両方とも同じファームウェアバージョンにアップデートすることをお勧めします。ファームウェアのバージョンが異なる場合、フェイルオーバーが起きた際、不測の結果が生じます。
ファームウェアが正常にアップロードされた後、Active CMC がリセットされ、一時的に使用不可になります。スタンバイ CMC が存在する場合、スタンバイとアクティブの役割が入れ替わり、スタンバイ CMC がアクティブ CMC になります。アクティブ CMC のみにアップデートが適用される場合、リセット完了後、アクティブ CMC はそのアップデートされたイメージを実行しません。スタンバイ CMC だけがそのイメージを所持します。一般に、アクティブとスタンバイの CM C の同一ファームウェアバージョンを保存することをお勧めします。
スタンバイ CMC をアップデートし終えたら、CMC の役割を交代させて新しくアップデートした CMC をアクティブにし、古いバージョンのファームウェアの CMC がスタンバイになるようにします。『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』の `cmcchangeover` コマンドセクションで、役割の交代についての情報を参照してください。これにより、2 番目の CMC のファームウェアをアップデートする前に、アップデートが正常に完了し、新しいファームウェアが正しく機能していることを確認できま

す。両方の CMC をアップデートしたら、cmcchangeover コマンドを使用して CMC をそれぞれ元の役割に戻すことができます。CMC Firmware revision 2.x は、 cmcchangeover コマンドを使用せずに、プライマリ CMC と冗長 CMC の両方をアップデートします。

リセット中に他のユーザーが切断されないように、CMC にログインしている可能性のあるすべてのユーザーに通知し、セッション ページを表示して、アクティブなセッションを確認してください。**セッション** ページを開くには、ツリーから **シャーシ** を選択し、**ネットワーク** タブをクリックしてから、**セッション** サブタブをクリックします。

CMC との間でのファイルの転送中は、ファイル転送アイコンが回転します。アイコンが回転する場合は、ブラウザでアニメーションが有効になっているか確認してください。手順については、 Internet Explorer でアニメーションの再生 を参照してください。

Internet Explorer を使って CMC からファイルをダウンロードするときに問題が起きた場合は、暗号化されたページをディスクに保存しない オプションを有効にしてください。手順については、Internet Explorer で CMC からファイルのダウンロード を参照してください。

関連リンク

CMC ファームウェアのダウンロード
現在インストールされているファームウェアのバージョンの表示

ウェブインタフェースを使用した CMC ファームウェアのアップデート

CMC ウェブインタフェースを使用して CMC ファームウェアをアップデートするには、次の手順を実行します。

1. 次のいずれかのページに移動します。
   - **シャーシ概要 → アップデート**
   - **シャーシ概要 → シャーシコントローラ → アップデート**
   - **シャーシ概要 → I/O モジュール概要 → アップデート**
   - **シャーシ概要 → iKVM → アップデート**

   ファームウェアのアップデート ページが表示されます。
2. **CMC ファームウェア** セクションで、ファームウェアをアップデートする CMC または複数の CMC（スタンバイ CMC がある場合）の **ターゲットのアップデート** 列にあるチェックボックスを選択して、**CMC アップデートの適用** をクリックします。
3. **ファームウェアイメージ** フィールドに、管理ステーションまたは共有ネットワーク上のファームウェアのイメージファイルへのパスを入力するか、**参照** をクリックし、ファイルの保存場所にナビゲートします。デフォルトの CMC ファームウェアイメージ名は、firmimg.cmc です。
4. **ファームウェアアップデートを開始する** をクリックして、次に **はい** をクリックして続行します。**ファームウェアアップデートの進行状況** セクションでは、ファームウェアアップデートのステータス情報を提供します。イメージファイルがアップロードされる間、ページにステータスインジケータが表示されます。ファイルの転送時間は、接続速度によって異なります。内部更新処理が始まると、ページは自動的に更新され、ファームウェア アップデートのタイマーが表示されます。

   メモ: DC PSU によってサポートされるシャーシでは、DC PSU 非対応バージョンのファームウェアにアップデートしようとすると、エラーメッセージが表示されます。
5. 補足的指示：
   - ファイル転送時に、**更新** アイコンをクリックしたり、他のページへ移動しないでください。
   - アップデートプロセスをキャンセルするには、**ファイル転送およびアップデートのキャンセル** をクリックします。このオプションは、ファイル転送時にのみ、利用可能です。
   - **アップデート状態** フィールドにファームウェアのアップデート状態が表示されます。

   メモ: CMC のアップデートには数分かかる場合があります。

6. スタンバイ CMC の場合、アップデートが完了すると、**アップデート状態** フィールドに **完了** と表示されます。アクティブ CMC の場合、ファームウェアのアップデート処理の最終段階では、アクティブ CMC はオフラインになることから、ブラウザセッションと CMC への接続が一時的に失われます。アクティブ CMC の再起動後、数分経過したら、再びログインする必要があります。CMC がリセットされた後、新しいファームウェアが **ファームウェアアップデート** ページに表示されます。

   メモ: ファームウェアアップグレード後、ウェブベースブラウザのキャッシュをクリアします。ブラウザのキャッシュをクリアする手順については、ウェブブラウザのオンラインヘルプを参照してください。

RACADM を使用した CMC ファームウェアのアップデート

RACADM を使用して CMC ファームウェアをアップデートするには、`fwupdate` サブコマンドを使用します。詳細については、『iDRAC7 および CMC 用 RACADM コマンドラインリファレンスガイド』を参照してください。

iKVM ファームウェアのアップデート

ファームウェアが正常にアップロードされると、iKVM がリセットされ、一時的に使用できなくなります。

関連リンク

CMC ファームウェアのダウンロード
現在インストールされているファームウェアのバージョンの表示

CMC ウェブインタフェースを使用した iKVM ファームウェアのアップデート

CMC ウェブインタフェースを使用して iKVM ファームウェアをアップデートするには：

1. 次のいずれかのページに移動します。
   - **シャーシの概要 → アップデート**
   - **シャーシの概要 → シャーシコントローラ → アップデート**
   - **シャーシの概要 → iKVM → アップデート**

   ファームウェアのアップデート ページが表示されます。
2. **iKVM ファームウェア** セクションで、ファームウエアをアップデートする **iKVM** の **ターゲットを更新する** 列のチェックボックスを選択して、**iKVM の更新を適用する** をクリックします。
3. **ファームウェアイメージ** フィールドに、管理ステーションまたは共有ネットワーク上のファームウェアのイメージファイルへのパスを入力するか、**参照** をクリックし、ファイルの保存場所にナビゲートします。iKVM ファームウェアイメージのデフォルト名は **iKVM.bin** です。
4. **ファームウェアアップデートを開始する** をクリックし、**はい** をクリックして続行します。

   ファームウェアアップデートの進行状況 セクションでは、ファームウェアアップデートのステータス情報を提供します。イメージファイルがアップロードされる間、ページにステータスインジケータが表示されます。ファイルの転送時間は、接続速度によって異なります。内部更新処理が始まると、ページは自動的に更新され、ファームウェア アップデートのタイマーが表示されます。
5. 次の補足的指示に従って下さい。
   - ファイル転送時に、**更新** アイコンをクリックしたり、他のページへ移動しないでください。
   - アップデートプロセスをキャンセルするには、**ファイル転送およびアップデートのキャンセル** をクリックします。このオプションは、ファイル転送時にのみ、利用可能です。
   - **アップデート状態** フィールドにファームウェアのアップデートステータスが表示されます。

   メモ: iKVM のアップデートに最高 2 分かかる場合があります。

アップデートが完了すると、iKVM がリセットし、新しいファームウェアが **ファームウェアのアップデート** ページに表示されます。

RACADM を使用した iKVM ファームウェアのアップデート

RACADM を使用して iKVM ファームウェアをアップデートするには、`fwupdate` サブコマンドを使用します。詳細については、『*iDRAC7 および CMC 用 RACADM コマンドラインリファレンスガイド*』を参照してください。

IOM インフラストラクチャデバイスファームウェアのアップデート

このアップデートを実行することにより、IOM デバイスのコンポーネント用のファームウェアがアップデートされますが、IOM デバイス自体のファームウェアはアップデートされません。コンポーネントとは、IOM デバイスと CMC の間のインタフェース回路です。コンポーネントのアップデートイメージは、CMC ファイルシステムに常駐しており、コンポーネントは、コンポーネントの現行バージョンと CMC のコンポーネントイメージが一致しない場合に限り、CMC ウェブインタフェースにアップデート可能デバイスとして表示されます。

IOM インフラストラクチャデバイスファームウェアをアップデートする前に、CMC ファームウェアがアップデートされていることを確認してください。

メモ:

CMC ファイルシステムに含まれているイメージを用いて、IOMINF ファームウェアが古いと判断された場合にのみ、IOMINF のアップデートが CMC により許可されます。IOMINF ファームウェアが最新である場合、CMC は IOMINF のアップデートを許可しません。最新の IOMINF デバイスはアップデート可能なデバイスとして一覧表示されません。

関連リンク

CMC ファームウェアのダウンロード
現在インストールされているファームウェアのバージョンの表示
CMC ウェブインタフェースを使用した IOM ソフトウェアのアップデート

CMC ウェブインタフェースを使用した IOM ファームウェアのアップデート

CMC ウェブインタフェースから IOM インフラストラクチャデバイスファームウェアをアップデートするには、次の手順を実行します。

1. **シャーシ概要 → I/O モジュール概要 → アップデート** と移動します。
   IOM ファームウェアとソフトウェア ページが表示されます。
   または、次のいずれかのページに移動します。
   - **シャーシの概要 → アップデート**
   - **シャーシの概要 → シャーシコントローラ → アップデート**
   - **シャーシの概要 → iKVM → アップデート**

   IOM ファームウェアとソフトウェア ページへのリンクが記載された**ファームウェアアップデート** ページが表示されます。
2. **IOM ファームウェアとソフトウェア** ページの **IOM ファームウェア** セクションで、ファームウェアをアップデートする IOM の **アップデート** 列のチェックボックスを選択して、**ファームウェアアップデートの適用** をクリックします。
   アップデート状態 セクションでは、ファームウェアアップデートのステータス情報を提供します。イメージファイルがアップロードされる間、ページにステータスインジケータが表示されます。ファイルの

転送時間は、接続速度によって異なります。内部更新処理が始まると、ページは自動的に更新され、ファームウェアアップデートのタイマーが表示されます。

メモ: ファイル転送時に、**更新** アイコンをクリックしたり、他のページへ移動しないでください。

メモ: IOMINF ファームウェアのアップデート時には、ファイル転送タイマーは表示されません。

アップデートが完了すると、IOM デバイスがリセットされて新しいファームウェアが **IOM ファームウェアとソフトウェア** ページに表示されるため、IOM デバイスとの接続が一時的に失われます。

RACADM を使用した IOM ファームウェアのアップデート

RACADM を使用して IOM インフラストラクチャデバイスのファームウェアをアップデートするには、fwupdate サブコマンドを使用します。詳細については、『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

サーバー iDRAC ファームウェアのアップデート

You can update firmware for iDRAC6 および iDRAC7 のファームウェアをアップデートできます。

iDRAC ファームウェアは iDRAC を搭載したサーバーではバージョン 1.4 以降、iDRAC6 Enterprise を搭載したサーバーではバージョン 2.0 以降である必要があります。iDRAC ファームウェアを iDRAC 2.3 より前のバージョンから 3.0 以降にアップデートする場合は、iDRAC ファームウェアをバージョン 3.0 以降にアップデートする前にバージョン 2.3 にアップデートする必要があります。

ファームウェアアップデートのアップロードが正常に行われると、（サーバー上の）iDRAC はリセットされ、一時的に利用できなくなります。

関連リンク

CMC ファームウェアのダウンロード
現在インストールされているファームウェアのバージョンの表示

ウェブインタフェースを使用したサーバー iDRAC ファームウェアのアップデート

CMC ウェブインタフェースを使用してサーバーの iDRAC ファームウェアをアップデートするには、次の手順を実行します。

1. 次のいずれかのページに移動します。
   - **シャーシの概要 → アップデート**
   - **シャーシの概要 → シャーシコントローラ → アップデート**
   - **シャーシの概要 → iKVM → アップデート**

   ファームウェアのアップデート ページが表示されます。

   また、**シャーシの概要 → サーバーの概要 → アップデート** からでもサーバー iDRAC ファームウェアをアップデートできます。詳細は、「サーバーコンポーネントファームウェアのアップデート」を参照してください。
2. iDRAC6 ファームウェアをアップデートするには、**iDRAC6 エンタープライズファームウェア** セクションで、ファームウェアをアップデートする iKVM の **ターゲットを更新する** 列のチェック ボックスを選択し、**iDRAC6 エンタープライズアップデートの適用** をクリックして手順 4 に進みます。
3. iDRAC7 ファームウェアをアップデートするには、**iDRAC7 エンタープライズファームウェア** セクションで、ファームウェアをアップデートするサーバーの **アップデート** リンクをクリックします。

   サーバーコンポーネントのアップデート ページが表示されます。続行するには、「サーバーコンポーネントファームウェアのアップデート」のセクションを参照してください。

4. **ファームウェアイメージ** フィールドに、管理ステーションまたは共有ネットワーク上のファームウェアのイメージファイルへのパスを入力するか、**参照** をクリックし、ファイルの保存場所にナビゲートします。デフォルトの iDRAC ファームウェアイメージ名は **firmimg.imc** です。
5. **ファームウェアアップデートを開始する** をクリックし、**はい** をクリックして続行します。

   ファームウェアアップデートの進行状況 セクションでは、ファームウェアアップデートのステータス情報を提供します。イメージファイルがアップロードされる間、ページにステータスインジケータが表示されます。ファイルの転送時間は、接続速度によって異なります。内部更新処理が始まると、ページは自動的に更新され、ファームウェア アップデートのタイマーが表示されます。
6. 次の補足的指示に従って下さい。
   - ファイル転送時に、**更新** アイコンをクリックしたり、他のページへ移動しないでください。
   - アップデートプロセスをキャンセルするには、**ファイル転送およびアップデートのキャンセル** をクリックします。このオプションは、ファイル転送時にのみ、利用可能です。
   - **アップデート状態** フィールドにファームウェアのアップデートステータスが表示されます。

   メモ: iDRAC ファームウェアのアップデートには、最大 10 分かかることがあります。

   アップデートが完了すると、iKVM がリセットし、新しいファームウェアが **ファームウェアのアップデート** ページに表示されます。

RACADM を使用したサーバー iDRAC ファームウェアのアップデート

RACADM を使用してサーバー iDRAC ファームウェアをアップデートするには、**fwupdate** サブコマンドを使用します。詳細については、『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

サーバーコンポーネントファームウェアのアップデート

Lifecycle Controller は、iDRAC6 および iDRAC7 を通してモジュールアップデートをサポートします。サーバーコンポーネントファームウェアモジュールのアップデート前に CMC ファームウェアをアップデートすることをお勧めします。CMC ファームウェアをアップデートした後、CMC ウェブインタフェースの **シャーシ概要 → サーバー概要 → アップデート → サーバーコンポーネントアップデート** ページでサーバーコンポーネントファームウェアをアップデートすることができます。また、アップデートするサーバーのコンポーネントモジュールをすべて一緒に選択することもお勧めします。これによって、Lifecycle Controller は最適化されたアルゴリズムを使用してファームウェアをアップデートすることが可能になり、再起動回数が削減されます。

メモ: この機能をサポートするには、iDRAC6 ファームウェアがバージョン 3.2 以降である必要があります。

サーバー上で Lifecycle Controller が無効になっている場合、**コンポーネント / デバイスのファームウェアインベントリ** セクションで *Lifecycle Controller が有効化されていない可能性があります*と表示されます。

メモ: サーバーコンポーネントファームウェアのアップデートに関する詳細は、「PowerEdge Servers のアップデートの実行で推奨されるワークフロー」を参照してください。

関連リンク

Lifecycle Controller の有効化
ファームウェアアップデートのためのコンポーネントのフィルタ
ファームウェアインベントリの表示
Lifecycle Controller のジョブ操作
IOM インフラストラクチャデバイスファームウェアのアップデート

Lifecycle Controller の有効化

サーバーの起動プロセス中に Lifecycle Controller サービスを有効にできます。

- iDRAC6 サーバーの場合は、起動コンソールで、「リモートアクセスセットアップを行う場合は 5 秒以内に <CTRL-E> を押してください。」というメッセージが表示されたら、<CTRL-E> を押します。次に、セットアップ画面で、**システムサービス** を有効にします。
- iDRAC7 サーバーの場合は、起動コンソールで F2 を選択してシステムセットアップを表示します。セットアップ画面で、**iDRAC 設定** を選択して、次に **システムサービス** を選択します。

  システムサービスをキャンセルすると、 保留中のすべてのスケジュール済みジョブがキャンセルされ、それらがキューから削除されます。

Lifecycle Controller とサーバーコンポーネント、およびデバイスファームウェアの管理についての詳細は、次を参照してください。

- 『*Lifecycle Controller Remote Services ユーザーズガイド*』
- **delltechcenter.com/page/Lifecycle+Controller**

サーバーコンポーネントのアップデート ページでは、お使いのシステムにあるさまざまなファームウェアコンポーネントをアップデートすることができます。このページの機能を使用するには、次が必要です。

- CMC：**サーバー管理者** 権限。
- iDRAC：**iDRAC の設定** 権限および **iDRAC へのログイン** 権限。

権限が不十分である場合には、サーバー上のコンポーネントおよびデバイスのファームウェアインベントリの表示のみが可能となります。そのサーバーでは、どのような Lifecycle Controller 操作にも、選択できるコンポーネントまたはデバイスはありません。

ファームウェアアップデートのためのコンポーネントのフィルタ

全サーバーのコンポーネントおよびデバイスすべての情報は、一度に取得されます。この大量な情報に対処するため、Lifecycle Controller はさまざまなフィルタリング機構を提供しています。これらのフィルタにより、次が可能になります。

- 簡単に表示できるよう、1 つまたは複数のカテゴリーのコンポーネントやデバイスを選択。
- サーバー全体のコンポーネントおよびデバイスのファームウェアのバージョンを比較。
- 選択されたコンポーネントおよびデバイスを自動的にフィルタリングして、タイプやモデルに基づいた特定のコンポーネントやデバイスのカテゴリの絞り込みを実施。

  メモ: 自動フィルタリング機能は、Dell アップデートパッケージ（DUP）を使用する際に重要です。DUP のアップデートプログラミングは、コンポーネントやデバイスのタイプまたはモデルにもとづいて行うことができます。自動フィルタリングの動作は、最初の選択を行った後は、その後の選択決定を最小化するように設計されています。

例

次に、フィルタリング機構の適用例をいくつか示します。

- BIOS フィルタが選択されると、全サーバーの BIOS インベントリのみが表示されます。複数サーバーモデルで構成される一連のサーバーがあり、そのうちの 1 つのサーバーが BIOS アップデートの対象として選択された場合、自動フィルタリングロジックにより、選択されたサーバーのモデルと異なるモデルのサーバーはすべて自動的に除外されます。これにより、選択された BIOS ファームウェアのアップデートイメージ（DUP）が、正しいサーバーモデルとの互換性を持っていることを確実にします。

  場合よっては、1 つの BIOS ファームウェアアップデートイメージが複数のサーバーモデルと互換性を持つことがあります。この互換性が将来失われる場合に備え、このような最適化は無視されます。
- 自動フィルタリングは、ネットワークインタフェースコントローラ（NIC）や RAID コントローラのファームウェアアップデートにおいて重要です。これらのデバイスカテゴリには、種々のタイプやモデルが存在します。同様に、ファームウェアアップデートイメージ（DUP）が最適化された形式（ある特定のカテゴリ内の複数のタイプまたはモデルのデバイスをアップデートできるように DUP がプログラムされている）で利用できる場合もあります。

CMC ウェブインタフェースを使用したファームウェアアップデートのためのコンポーネントのフィルタ

デバイスをフィルタするには、次の手順を実行します。

1. システムツリーで、**サーバーの概要** へ移動し、**アップデート → サーバーコンポーネントのアップデート** をクリックします。
   サーバーコンポーネントのアップデート ページが表示されます。
2. **コンポーネント/デバイスのアップデートフィルタ** セクションで、次の 1 つまたは複数を選択します。
   - BIOS
   - iDRAC
   - Lifecycle Controller
   - 32 ビット診断
   - オペレーティングシステムのドライバパック
   - ネットワーク I/F コントローラ
   - RAID コントローラ

   ファームウェアインベントリ セクションには、シャーシ内に存在する全サーバーで一致するコンポーネントまたはデバイスのみが表示されます。このフィルタは、パスフィルタです。すなわち、フィルタ条件に一致するコンポーネントやデバイスのみが許可され、それ以外はすべて除外されます。

   フィルタされたコンポーネントやデバイスがインベントリセクションに表示された後、コンポーネントまたはデバイスがアップデート対象として選択された場合には、さらにフィルタリングが行われる場合があります。たとえば、BIOS フィルタが選択されると、インベントリセクションにはすべてのサーバーとその BIOS コンポーネントのみが表示されます。それらのうちの 1 つのサーバーの BIOS コンポーネントが選択されると、インベントリがさらにフィルタされ、選択されたサーバーと同じモデル名のサーバーのみが表示されます。

   フィルタが選択されず、インベントリセクションでコンポーネントまたはデバイスのアップデート用選択が行われた場合には、その選択に関連するフィルタが自動的に有効になります。モデル、タイプ、またはその他の識別要素において選択されたコンポーネントに一致するすべてのサーバーがインベントリセクションに表示される、さらなるフィルタリングが行われる場合もあります。たとえば、1 つのサーバーの BIOS コンポーネントがアップデート対象として選択された場合、フィルタがこの BIOS に自動的に設定され、インベントリセクションには、選択されたサーバーのモデル名に一致するサーバーが表示されます。

RACADM を使用したファームウェアアップデート用コンポーネントのフィルタ

RACADM を使用してファームウェアアップデート用コンポーネントをフィルタするには、getversion コマンドをしようします。

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

詳細については、**dell.com/support/manuals** にある iDRAC7 および CMC 向け RACADM コマンドライン リファレンスガイドを参照してください。

ファームウェアインベントリの表示

シャーシ内に現在存在するすべてのサーバーについて、すべてのコンポーネントおよびデバイスのファームウェアバージョンの概要の他それらの状態を表示することができます。

CMC ウェブインタフェースを使用したファームウェアインベントリの表示

ファームウェアインベントリを表示するには、次の手順を実行します。

1. システムツリーで、**サーバーの概要** へ移動し、**アップデート → サーバーコンポーネントのアップデート** をクリックします。

   サーバーコンポーネントのアップデート ページが表示されます。

2. **コンポーネント/デバイスのファームウェアインベントリ** セクションに、ファームウェアインベントリの詳細が表示されます。表には、

   – 現在 Lifecycle Controller によってサポートされていないサーバーは、**未対応** としてリストされます。iDRAC ファームウェアのみを直接にアップデートすることができる代替ページへのハイパーリンクが表示されます。このページでは、iDRAC ファームウェアアップデートのみをサポートし、サーバー上のコンポーネントおよびデバイスのアップデートは一切サポートしていません。iDRAC ファームウェアアップデートは Lifecycle Controller サービスには依存しません。

   – サーバーが **準備中** と表示されている場合は、ファームウェアインベントリを取得した時点でサーバー上の iDRAC がまだ初期化中であったことを示します。iDRAC が完全に作動するまで待ち、ファームウェアインベントリが再度検索されるまで、ページを更新します。

   – インベントリに表示されるコンポーネントやデバイスの内容が、サーバーに物理的にインストールされている内容を正しく反映していないときは、サーバーの起動プロセス中に Lifecycle Controller を起動する必要があります。これは、コンポーネントおよびデバイスの内部情報を更新するために役立ち、現在インストールされているコンポーネントやデバイスを検証できるようにします。この状況は、次の場合に発生します。

     * サーバー管理に新たに Lifecycle Controller 機能を導入するために、サーバーの iDRAC ファームウェアがアップデートされた。
     * サーバーに新しいデバイスが挿入された。

     このアクションを自動化するため、iDRAC 構成ユーティリティ（iDRAC6 用）または iDRAC 設定ユーティリティ（iDRAC6 用）は、ブートコンソールからアクセス可能なオプションを提供します。

     * iDRAC6 サーバーの場合は、起動コンソールで、「リモートアクセスセットアップを行う場合は 5 秒以内に <CTRL-E. を押してください。」というメッセージが表示されたら、<CTRL-E> を押します。次に、セットアップ画面で、**再起動時にシステムインベントリを収集** を有効にします。
     * iDRAC7 サーバーの場合は、起動コンソールで F2 を選択してシステムセットアップを表示します。セットアップ画面で、iDRAC 設定を選択して、次にシステムサービス（USC）を選択します。セットアップ画面で、**再起動時にシステムインベントリを収集** を有効にします。

   – アップデート、ロールバック、再インストール、およびジョブの削除などの、Lifecycle Controller のさまざまな操作のオプションを実行するオプションが利用可能です。一度に実行できる操作は 1 種類のみです。サポートされていないコンポーネントとデバイスがインベントリの一部としてリストされる可能性がありますが、Lifecycle Controller 操作を許可しないでください。

次の図にサーバーのコンポーネントおよびデバイス情報を示します。

表 9. : コンポーネントおよびデバイス情報

フィールド	説明
スロット	シャーシでサーバーが装着されているスロットを示します。スロット番号は 1～16（シャーシには使用できるスロットが 16 個あります）の連番 ID で、シャーシ内のサーバーの場所を識別します。スロットに装着されているサーバーが 16 未満の場合は、サーバーが装着されているスロットのスロット番号のみが表示されます。
名前	各スロット内のサーバーの名前を表示します。

フィールド	説明
モデル	サーバーのモデルを表示します。
コンポーネント / デバイス	サーバーのコンポーネントおよびデバイスの情報を示します。列幅が狭すぎる場合、マウスオーバーツールを使うと説明が表示されます。
現在のバージョン	サーバー上のコンポーネントとデバイスの現在のバージョンを表示します。
ロールバックバージョン	サーバー上のコンポーネントとデバイスのロールバックバージョンを表示します。
ジョブ状態	そのサーバー上でスケジュールされているすべての操作のジョブステータスを表示します。ジョブステータスは継続して動的にアップデートされます。状態が 完了 となっているジョブの完了が検出されると、コンポーネントまたはデバイスのいずれかにおいてファームウェアバージョンが変更された場合に備えて、これらのサーバー上のコンポーネントおよびデバイスのファームウェアバージョンが自動的に更新されます。現在の状態の隣には、情報アイコンも表示され、現在のジョブステータスに関する追加情報を提供します。このアイコンをクリックするか、またはカーソルを置くと、情報を表示できます。
アップデート	サーバーで、ファームウェアアップデート対象のコンポーネントまたはデバイスを選択します。

RACADM を使用したファームウェアインベントリの表示

RACADM を使用してファームウェアインベントリを表示するには、getversion コマンドを使用します。

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

詳細については、**dell.com/support/manuals** にある『RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド』を参照してください。

Lifecycle Controller のジョブ操作

次のような Lifecycle Controller 操作が可能です。

- 再インストール
- ロールバック
- アップデート
- ジョブの削除

一度に実行できる操作は 1 種類のみです。サポートされていないコンポーネントとデバイスがインベントリの一部としてリストされる可能性がありますが、Lifecycle Controller 操作を許可しないでください。

Lifecycle Controller 操作を実行するには、以下が必要です。

- CMC：サーバー管理者権限。
- iDRAC：iDRAC の設定 権限および iDRAC へのログイン権限。

サーバーでスケジュールされた Lifecycle Controller 操作は、完了に 10～15 分かかる場合があります。このプロセスでは、ファームウェアのインストールが実行されるサーバーの再起動が数回行われ、これにはファームウェアの検証ステージも含まれます。この処理の進行状況を、サーバーコンソールで表示することができます。サーバー上にアップデートの必要があるコンポーネントまたはデバイスが複数ある場合、すべてのアップデートを 1 つの操作に統合してスケジュールすることにより、再起動の必要回数を最小限に減らすことができます。

時折、操作が、他のセッションまたはコンテキストを介してスケジュールのため送信されている時に、別の操作が試行されることがあります。この場合、その状況、および操作が送信されないことを示す確認のポップアップメッセージが表示されます。処理中の操作が完了するのを待って、再度送信してください。

スケジュールのために操作を送信した後は、他のページに移動しないでください。他のページに移動しようとすると、ページ移動をキャンセルするための確認のポップアップメッセージが表示されます。キャンセルしない場合は、操作が中断されます。操作の中断、特にアップデート操作中の中断は、ファームウェアイメージファイルのアップロードが正しく完了せずに終了する原因となる可能性があります。スケジュールのために操作を送信した後は、その操作のスケジュールが正常に行われたことを示すポップアップメッセージを確認するようにしてください。

関連リンク

サーバーコンポーネントファームウェアの再インストール
サーバーコンポーネントファームウェアのロールバック
サーバーコンポーネントファームウェアのアップデート
スケジュールされたサーバーコンポーネントファームウェアジョブの削除

サーバーコンポーネントファームウェアの再インストール

1 つまたは複数のサーバー上の選択されたコンポーネントまたはデバイスの、現在インストールされているファームウェアのファームウェアイメージを再インストールできます。

ウェブインタフェースを使用したサーバーコンポーネントファームウェアの再インストール

サーバーコンポーネントファームウェアを再インストールするには：

1. システムツリーで、**サーバーの概要** へ移動し、**アップデート → サーバーコンポーネントのアップデート → をクリック**します。
   サーバーコンポーネントのアップデート ページが表示されます。
2. コンポーネントまたはデバイスをフィルタします（オプション）。
3. **現在のバージョン** 列で、ファームウェアを再インストールするコンポーネントまたはデバイスのチェックボックスを選択します。
4. 次のオプションのいずれかを選択します。
   - **今すぐ再起動** - ただちに再起動します。
   - **後で再起動** - 後で手動で再起動します。
5. **再インストール** をクリックします。選択されたコンポーネントまたはデバイスのファームウェアバージョンが再インストールされます。

サーバーコンポーネントファームウェアのロールバック

1 つまたは複数のサーバー上の、選択されたコンポーネントまたはデバイスに以前インストールされたファームウェアの、ファームウェアイメージをインストールすることができます。ファームウェアイメージは、ロールバック 操作のために Lifecycle Controller 内で使用可能です。これら機能の可用性は、Lifecycle Controller のバージョン互換性ロジックによって異なります。Lifecycle Controller はまた、以前のバージョンのアップデートが Lifecycle Controller によって行われたものとみなします。

CMC ウェブインタフェースを使用したサーバーコンポーネントファームウェアのロールバック

サーバーコンポーネントファームウェアバージョンを以前のバージョンにロールバックするには：

1. CMC ウェブインタフェースでシステムツリーを展開し、**サーバーの概要** へ移動して **アップデート → サーバーコンポーネントのアップデート** をクリックします。
   サーバーコンポーネントのアップデート ページが表示されます。
2. コンポーネントまたはデバイスをフィルタします（オプション）。
3. **ロールバックバージョン** 列で、ファームウェアをロールバックするコンポーネントまたはデバイスのチェックボックスを選択します。
4. 次のオプションのいずれかを選択します。

- **今すぐ再起動** - ただちに再起動します。
- **次回の起動時** - サーバーを後で手動で再起動します。

5. **ロールバック** をクリックします。以前インストールされたファームウェアのバージョンが、選択されたコンポーネントまたはデバイスに再インストールされます。

サーバーコンポーネントファームウェアのアップデート

1 つまたは複数のサーバー上の選択されたコンポーネントまたはデバイスの、次世代のファームウェアイメージをインストールすることができます。ファームウェアイメージは、ロールバック 操作のために Lifecycle Controller 内で使用可能です。

メモ: iDRAC および OS ドライバパックファームウェアのアップデートでは、拡張ストレージ機能が有効になっていることを確認してください。

サーバーコンポーネントのファームウェアアップデートを開始する前に、ジョブキューをクリアしておくことをお勧めします。サーバー上の全ジョブのリストは、Lifecycle Controller ジョブ ページで利用できます。このページで、単一または複数のジョブを削除したり、サーバー上のすべてのジョブを削除することができます。「リモートシステムの Lifecycle Controller ジョブの管理」のトラブルシューティングの項を参照してください。

BIOS アップデートは、サーバーのモデルに特有なものです。選択ロジックは、この動作にもとづいています。サーバー内で単一のネットワークインタフフェースコントローラ（NIC）デバイスがファームウェアのアップデート対象として選択されていたとしても、そのサーバーのすべての NIC にアップデートが適用されることもあります。このような動作は Lifecycle Controller の機能性、とりわけ Dell アップデートパッケージ（DUP）に含まれるプログラミングに固有です。現時点では、サイズが 48MB 未満の Dell アップデートパッケージ（DUP）がサポートされています。

アップデートファイルのイメージサイズがより大きい場合、ジョブステータスはダウンロードが失敗したことを示します。サーバーで複数のサーバーコンポーネントのアップデートが試行された場合、すべてのファームウェアアップデートファイルの合計サイズが 48M を超えることがあります。このような場合には、それらのアップデートファイルの 1 つのファイルサイズが切り詰められ、そのファイルによるアップデートが失敗します。1 つのサーバー上で複数のコンポーネントをアップデートする場合、最初に Lifecycle Controller および 32-Bit Diagnostics のコンポーネントをまとめてアップデートすることをお勧めします。これらのコンポーネントのアップデートは、サーバーを再起動する必要がなく、比較的短時間で完了します。その後、それ以外のコンポーネントをまとめてアップデートすることができます。

すべての Lifecycle Controller アップデートは、即時に実行するようにスケジュールされます。ただし、システムサービスにより、これらの実行が遅延されることもあります。そのような状況では、CMC にホストされているリモート共有が実行時に利用不可となり、その結果アップデートが失敗します。

CMC ウェブインタフェースを使用したサーバーコンポーネントファームウェアのアップデート

ファームウェアバージョンを次のバージョンにアップデートするには、次の手順を実行します。

1. CMC ウェブインタフェースのシステムツリーで、**サーバーの概要** へ移動し、**アップデート → サーバーコンポーネントのアップデート** をクリックします。

   サーバーコンポーネントのアップデート ページが表示されます。

2. コンポーネントまたはデバイスをフィルタします（オプション）。

3. **アップデート** 列で、次のバージョンにアップデートするコンポーネントまたはデバイスのチェックボックスを選択します。CRTL キーのショートカットを使用して、アップデート対象のコンポーネントまたはデバイスのタイプを、該当する全サーバーで選択できます。CRTL キーを押し下げたままにすると、すべてのコンポーネントが黄色でハイライト表示されます。CRTL キーを押し下げた状態で、**アップデート** 列のチェックボックスを有効にすると、そのコンポーネントまたはデバイスがアップデート対象として選択されます。

   選択されたタイプのコンポーネントまたはデバイスおよび、ファームウェアのイメージファイルのセレクタをリストにした、2 つ目の表が表示されます。各コンポーネントタイプに対して 1 つのファームウェアイメージファイルのセレクタが表示されます。

ネットワークインタフェースコントローラ（NIC）および RAID コントローラのようなデバイスによっては、多くのタイプとモデルがあります。アップデートの選択ロジックは、最初に選択されたデバイスに基づいて、関連するデバイスタイプやモデルを自動的にフィルタします。このような自動的なフィルタ動作の一番の理由は、カテゴリに対して指定できるのが 1 個のファームウェアイメージファイルのみであるということです。

メモ: 拡張ストレージ機能がインストールされ、有効になっている場合には、1 つの DUP、 または DUP の組み合わせにのどちらについてもサイズの制限が無視されます。拡張ストレージの有効化については、「CMC 拡張ストレージカードの設定」を参照してください。

4. 選択されたコンポーネントまたはデバイスのファームウェアイメージファイルを指定します。これは Microsoft Windows Dell Update Package（DUP）ファイルです。
5. 次のオプションのいずれかを選択します。
   - **今すぐ再起動** - ただちに再起動します。
   - **次の再起動時** - 後で手動で再起動します。

   メモ: この手順は、Lifecycle Controller および 32 ビット診断のファームウェアアップデートでは無効となります。これらのデバイスでは、サーバーの再起動はただちに実行されます。
6. **アップデート** をクリックします。選択されたコンポーネントまたはデバイスのファームウェアバージョンがアップデートされます。

スケジュールされたサーバーコンポーネントファームウェアジョブの削除

1 つ、または複数のサーバーで選択されたコンポーネントおよびデバイスにスケジュールされたジョブを削除できます。

ウェブインタフェースを使用したスケジュール済みサーバーコンポーネントファームウェアジョブの削除

スケジュール済みサーバーコンポーネントファームウェアジョブを削除するには：

1. CMC ウェブインタフェースのシステムツリーで、**サーバーの概要** に移動し、**アップデート → サーバーコンポーネントのアップデート** とクリックします。

   サーバーコンポーネントのアップデート ページが表示されます。
2. コンポーネントまたはデバイスをフィルタします（オプション）。
3. **ジョブステータス** 列で、ジョブステータスの横にチェックボックスが表示されている場合は、Lifecycle Controller ジョブが現在実行中および 表示中の状態であることを示します。これは、ジョブの削除 操作にも選択できます。
4. **ジョブの削除** をクリックします。 選択されたコンポーネントまたはデバイスのジョブが削除されます。

CMC を使用した iDRAC ファームウェアのリカバリ

iDRAC ファームウェアは通常、iDRAC ウェブインタフェース、SM-CLP コマンドラインインタフェース、**support.dell.com** からダウンロードしたオペレーティングシステム固有のアップデートパッケージ などの iDRAC インタフェースを使ってアップデートします。詳細については、iDRAC ユーザーズガイドを参照してください。

初期世代のサーバーは、iDRAC ファームウェアの新規更新処理により破損したファームウェアを回復できます。CMC が iDRAC ファームウェアの破損を検知すると、**ファームウェアのアップデート** ページにそのサーバーをリストします。説明された手順でファームウェアをアップデートします。

5

シャーシ情報の表示とシャーシとコンポーネントの正常性状態の監視

以下の情報の表示と正常性の監視ができます。

- アクティブとスタンバイの CMC
- すべてのサーバーと個々のサーバー
- ストレージアレイ
- すべての IO モジュール（IOM）と個々の IOM
- ファン
- iKVM
- 電源装置（PSU）
- 温度センサー
- LCD アセンブリ

シャーシコンポーネント概要の表示

CMC ウェブインタフェースにログインすると、**シャーシの正常性** ページにシャーシの正常性とそのコンポーネントを表示できます。そこでは、シャーシとそのコンポーネントがライブでグラフィカルに表示されます。表示は動的にアップデートされ、現在の状況を反映するようにコンポーネントサブグラフィックの色およびテキストヒントも自動的に変更されます。

図 1. ウェブインタフェースにおけるシャーシグラフィックスの例

シャーシの正常性を表示するには、**シャーシの概要 → プロパティ → 正常性** と移動します。そこでは、シャーシ、アクティブおよびスタンドバイ CMC、サーバーモジュール、IO モジュール（IMO）、ファン、iKVM、電源装置（PSU）、温度センサーおよび LCD アセンブリの全体的な正常性ステータスが表示されます。各コンポーネントの詳細情報は、そのコンポーネントをクリックすると表示されます。さらに、CMC ハードウェアログの最新イベントも表示されます。詳細は、『*CMC オンラインヘルプ*』を参照してください。

お使いのシャーシがグループリードとして設定されている場合は、ログイン後に **グループの正常性** ページが表示されます。シャーシレベルの情報とアラートが表示されます。すべての重要および非重要アラートが表示されます。

シャーシの図解

シャーシは、前面図と背面図で表示されます（上部と下部のイメージ）。サーバーと LCD は前面図で、残りのコンポーネントは背面図で表示されます。コンポーネントを選択するとブルーで表示され、必要なコンポーネントイメージをクリックするとコントロールできます。シャーシにコンポーネントがある場合、そのコンポーネントのタイプのアイコンが、コンポーネントが設置されている場所（スロット）を示す図に表示されます。空の場所は、背景色がチャコールグレーで表示されます。コンポーネントアイコンは、コンポーネントの状態を視覚的に示します。その他のコンポーネントでは、物理コンポーネントを視覚的に表すアイコンが表示されます。 ダブルサイズのコンポーネントが設置されると、サーバーと IOM のアイコンは、複数のスロットにまたがります。コンポーネント上にカーソルを移動すると、そのコンポーネントに関するツールチップが表示されます。

表 10. ：サーバーアイコンの状況

アイコン	説明
	サーバーの電源が入り、正常に動作しています。
	サーバーの電源がオフです。
	サーバーは非重要なエラーを報告しています。
	サーバーは重要なエラーを報告しています。

アイコン	説明
	サーバーがありません。

選択したコンポーネントの情報

選択したコンポーネントの情報は、次の 3 つの独立した項で表示されます。

- 正常性、パフォーマンスおよびプロパティ — ハードウェアログで表示されるアクティブな重要および重要ではないイベントと、時間によって変化するパフォーマンスのデータが表示されます。
- プロパティ— 時間により変化しない、またはほとんど変化しないコンポーネントのプロパティが表示されます。
- クイックリンク— 最も頻繁にアクセスするページと最も頻繁に実行される操作へ移動できるリンクが提供されます。選択したコンポーネントに適用されるリンクのみが、この項に表示されます。

サーバー モデル名とサービス タグの表示

各サーバーのモデル名とサービス タグは、次の手順で簡単に表示することができます。

1. システム ツリーで サーバー を展開します。展開されたサーバーリストにすべてのサーバー（0〜16）が表示されます。サーバーなしのスロットは名前がグレー表示されます。
2. カーソルをサーバーのスロット名またはスロット番号の上に重ねると、ツールチップとしてサーバーのモデル名とサービス タグ番号が表示されます（存在する場合）。

シャーシ概要の表示

シャーシにインストールされたコンポーネントの概要を表示することができます。

シャーシ概要の情報を表示するには、**シャーシ概要 → プロパティ → 概要** と移動します。

シャーシ概要 ページが表示されます。詳細については、『*CMC オンラインヘルプ*』を参照してください。

シャーシコントローラの情報とステータスの表示

シャーシコントローラの情報とステータスを表示するには、CMC ウェブインタフェースで、**シャーシの概要 → シャーシコントローラ → プロパティ → ステータス** と移動します。

シャーシコントローラのステータス ページが表示されます。詳細については、『*CMC オンラインヘルプ*』を参照してください。

すべてのサーバーの情報および正常性ステータスの表示

すべてのサーバーの正常性ステータスを表示するには、次のいずれかを実行します。

1. **シャーシの概要 → → 正常性** と移動します。

シャーシ正常性 ページは、シャーシに取り付けられたすべてのサーバーのグラフィック表示を提供します。サーバーの正常性ステータスは、サーバーサブグラフィックの色で示されます。詳細は、『*CMC オンラインヘルプ*』を参照してください。

2. **シャーシの概要 → サーバーの概要 → プロパティ → ステータス** と移動します。
   サーバーステータス ページには、シャーシ内のサーバーの概要が表示されます。詳細は、『*CMC オンラインヘルプ*』を参照してください。

個々のサーバーの正常性状態と情報の表示

個々のサーバーの正常性状態を表示するには、次のいずれかを実行します。

1. **シャーシの概要 → プロパティ → 正常性** と移動します。
   シャーシ正常性 ページは、シャーシに取り付けられたすべてのサーバーのグラフィック表示を提供します。サーバーの正常性ステータスは、サーバーサブグラフィックの色で示されます。カーソルをそれぞれのサーバーのサブグラフィックに置きます。そのサーバーに対応するテキストのヒントまたはスクリーンのヒントが追加の情報を提供します。サーバーのサブグラフィックをクリックすると、IOM 情報が右側に表示されます。詳細については、『*CMC オンラインヘルプ*』を参照してください。

2. システムツリーで、**シャーシの概要** へ移動し、**サーバーの概要** を展開します。展開されたリストにすべてのサーバー（1～16）が表示されます。表示するサーバー（スロット）をクリックします。
   サーバーステータス ページ（**サーバーステータス** ページとは別）には、シャーシ内のサーバーの正常性状態および、サーバーの管理に使用されるファームウェアである iDRAC 用のウェブインタフェースの起動ポイントが表示されます。詳細については、『*CMC オンラインヘルプ*』を参照してください。

   メモ: iDRAC ウェブインタフェースを使用するには、iDRAC ユーザー名とパスワードが必要です。iDRAC および iDRAC ウェブ インタフェースの使い方の詳細は、『*Integrated Dell Remote Access Controller ファームウェアユーザーズガイド*』を参照してください。

ストレージアレイステータスの表示

ストレージサーバーの正常性状態を表示するには、次のいずれかを実行します。

1. **シャーシの概要 → プロパティ → 正常性** と移動します。
   シャーシ正常性 ページは、シャーシに取り付けられたすべてのサーバーのグラフィック表示を提供します。サーバーの正常性ステータスは、サーバーサブグラフィックの色で示されます。カーソルをそれぞれのサーバーのサブグラフィックに置きます。そのサーバーに対応するテキストのヒントまたはスクリーンのヒントで追加の情報が提供されます。サーバーのサブグラフィックをクリックすると、IOM 情報が右側に表示されます。詳細については、『*CMC オンラインヘルプ*』を参照してください。

2. システムツリーで、**シャーシの概要** へ移動し、**サーバーの概要** を展開します。展開されたリストにすべてのサーバー（1～16）が表示されます。ストレージアレイが挿入されているスロットをクリックします。
   ストレージアレイステータスページにストレージアレイの正常性状態とプロパティが表示されます。詳細については、『*CMC オンラインヘルプ*』を参照してください。

すべての IOM の情報および正常性ステータスの閲覧

CMC ウェブインタフェースで IOM の正常性ステータスを閲覧するには、次のいずれかを実行します。

1. **シャーシの概要 → プロパティ → 正常性** をクリックします。
   シャーシの正常性 ページが表示されます。**シャーシグラフィックス** の下側のセクションには、シャーシの背面図が描写され、IOM の正常性ステータスが表示されます。IOM の正常性ステータスは、IOM のサ

ブグラフィックの色で示されます。カーソルをそれぞれの IOM のサブグラフィックに置きます。テキストヒントは、IOM に関する追加情報を提供します。IOM のサブグラフィックをクリックすると、IOM の情報が右側に表示されます。

2. **シャーシの概 要 → I/O モジュールの概要 → プロパティ → ステータス** と移動します。
   I/O モジュールステータス ページに、シャーシに関連のあるすべての IOM の概要が表示されます。詳細は、『*CMC オンラインヘルプ*』を参照してください。

個々の IOM の情報と正常性状態の表示

個々の IOM の正常性状態を表示するには、次のいずれかを実行します。

1. **シャーシの概要 → プロパティ → 正常性** へ移動します。
   シャーシの正常性 ページが表示されます。シャーシグラフィックス の下方のセクションには、シャーシの背面図と IOM の正常性ステータスが表示されます。IOM の正常性ステータスは、IOM のサブグラフィックの色で示されます。カーソルをそれぞれの IOM のサブグラフィックに置きます。テキストヒントは、IOM に関する追加情報を提供します。IOM のサブグラフィックをクリックすると、IOM 情報が右側に表示されます。

2. **シャーシの概要** へ移動し、システムツリーで **I/O モジュールの概要** を展開します。すべての IOM（1〜6）が展開されたリストに表示されます。表示する IOM （スロット）をクリックします。
   その IOM 固有の **I/O モジュールステータス** ページ（全般的な **I/O モジュールステータス** ページとは別）が表示されます。詳細は、『*CMC オンラインヘルプ*』を参照してください。

ファンの情報と正常性状態の表示

ファンの速度を調整する CMC は、システム全体のイベントに基づいてファンの速度を自動的に増減します。次のイベントが起きた場合、CMC は警告を生成し、ファン速度を上げます。

- CMC の周辺温度がしきい値を超えた。
- ファンが故障した。
- シャーシからファンが取り外された。

メモ: サーバーの CMC または iDRAC ファームウェアを更新中に、シャーシ内のファンの一部またはすべてが 100 パーセントの速度で回転します。これは正常な動作です。

CMC ウェブインタフェースでファンの正常性状態を表示するには、次のいずれかを実行します。

1. **シャーシの概要 → → 正常性** と移動します。
   シャーシの正常性 ページが表示されます。シャーシグラフィックスの下方のセクションには、シャーシの背面図とシャーシの正常性ステータスが表示されます。ファンの正常性ステータスは、ファンのサブグラフィックの色で示されます。カーソルをファンのサブグラフィックに移動します。テキストヒントは、ファンに関する追加情報を提供します。ファンのサブグラフィックをクリックすると、ファンの情報が右側に表示されます。

2. **シャーシの概要 → ファン → プロパティ** と移動します。
   ファンス テータス ページには、シャーシ内のファンの状態と速度の測定値（RPM）が表示されます。ファンは 1 台または複数台です。

   メモ: CMC とファン装置間で通信障害が発生した場合は、CMC はサーバーの正常性ステータスを取得または表示できません。

   詳細については、『*CMC オンラインヘルプ*』を参照してください。

iKVM の情報と正常性状態の表示

Dell M1000e サーバーシャーシのローカルアクセス KVM モジュールは Avocent 内蔵 KVM スイッチモジュールまたは iKVM と呼ばれます。

シャーシに関連した iKVM の正常性状態を表示するには、次のいずれかを実行します。

1. **シャーシの概要 → → 正常性** と移動します。

   シャーシの正常性 ページが表示されます。シャーシグラフィックスの下方のセクションには、シャーシの背面図と iKVM の正常性状態が表示されます。iKVM の正常性ステータスは、iKVM サブグラフィックの色で示されます。カーソルを iKVM サブグラフィック上に移動すると、対応するテキストヒントまたは画面ヒントが表示されます。テキストヒントは、iKVM に関する追加情報を提供します。iKVM サブグラフィックをクリックすると、iKVM 情報が右側に表示されます。

2. **シャーシの概要 → iKVM → プロパティ** と移動します。

   iKVM ステータス ページには、シャーシに関連付けられている iKVM の状態が表示されます。詳細については、『*CMC オンラインヘルプ*』を参照してください。

PSU の情報および正常性状態の表示

シャーシに関連のある電源装置ユニット（PSU） の正常性状態を表示するには、次のいずれかを実行します。

1. **シャーシの概要 → プロパティ → 正常性** と移動します。

   シャーシの正常性 ページが表示されます。シャーシグラフィックス の下側のセクションには、シャーシの背面図とすべての PSU の正常性状態が表示されます。PSU の正常性状態は、PSU サブグラフィックの色で示されます。それぞれの PSU のサブグラフィックにマウスのカーソルを移動すると、該当するテキストヒントまたは画面ヒントが表示されます。テキストヒントは、対象 PSU に関する追加情報を提供します。PSU サブグラフィックをクリックすると、PSU 情報が右側に表示されます。

2. **シャーシの概要 → 電源装置** と移動します。

   電源装置ステータス ページには、シャーシに関連付けられている PSU の状態が表示されます。ここでは、全般的な電源の正常性、システムの電源状態、および電源装置冗長性の状態が示されます。詳細は、『*CMC オンラインヘルプ*』を参照してください。

温度センサーの情報と正常性状態の表示

温度センサーの正常性状態を表示するには、次の手順を実行します。

シャーシの概要 → 温度センサー と移動します。

温度センサー状態 ページでは、シャーシ全体（シャーシとサーバー）の温度プローブの状態と値が表示されます。詳細については、『*CMC オンラインヘルプ*』を参照してください。

メモ: 温度プローブの値を変更することはできません。しきい値を超えるとアラートが生成され、ファン速度が変化します。たとえば、CMC 周囲温度プローブがしきい値を超えると、シャーシ内のファンの速度が上昇します。

LCD の情報と正常性の表示

LCD の正常性状態を表示するには：

1. CMC ウェブインタフェースのシステムツリーで、**シャーシの概要** へ移動し、**プロパティ → 正常性** をクリックします。

シャーシの正常性 ページが表示されます。シャーシグラフィックの情報のセクションでは、シャーシの前面図が表示されます。LCD の正常性状態は、LCD のサブグラフィックの色で示されます。

2. カーソルを LCD のサブグラフィックに移動します。対応するテキストのヒントまたはスクリーンのヒントに、LCD の追加情報が表示されます。
3. LCD サブグラフィックをクリックすると、LCD 情報が右側に表示されます。詳細については、『*CMC オンラインヘルプ*』を参照してください。

6

CMC の設定

CMC では、リモート管理タスクを実行するために CMC プロパティの設定、ユーザーのセットアップ、およびアラートのセットアップを行うことができます。

CMC の設定を始める前に、まず CMC ネットワーク設定を指定し、CMC がリモート管理できるようにする必要があります。この初期設定によって、CMC へのアクセスを可能にするための TCP/IP ネットワークパラメータが割り当てられます。詳細については、「CMC への初期アクセスのセットアップ」を参照してください。

ウェブインタフェースまたは RACADM を使って CMC を設定できます。

メモ: 最初の CMC の設定を行う際は、リモートシステム上での RACADM コマンドの実行に root ユーザーとしてログインする必要があります。CMC の設定権限を持つ別のユーザーを作成することもできます。

CMC を設定して基本的な設定が終わったら、以下を実行できます。

- 必要に応じてネットワーク設定を変更します。
- CMC にアクセスするインタフェースを設定します。
- LED 表示を設定します。
- 必要に応じてシャーシグループを設定します。
- サーバー、IOM、または iKVM を設定します。
- VLAN を設定します。
- 必要な証明書を取得します。
- CMC ユーザーを追加し、権限を設定します。
- E-メールアラートおよび SNMP トラップを設定して有効化します。
- 必要に応じて電力制限ポリシーを設定します。

関連リンク

CMC へのログイン
CMC ネットワーク LAN 設定の表示と変更
CMC ネットワークおよびログインセキュリティ設定の実行
CMC の仮想 LAN タグプロパティ
サービスの設定
シャーシ上のコンポーネントを識別するための LED の設定
シャーシグループのセットアップ
サーバーの設定
I/O ファブリックの管理
iKVM の設定と使用
証明書の取得
ユーザーアカウントと権限の設定
アラートを送信するための CMC の設定
電力の管理と監視
RACADM を使用した複数の CMC の設定

CMC ネットワーク LAN 設定の表示と変更

コミュニティ文字列や SMTP サーバー IP アドレスなどの LAN 設定は、CMC およびシャーシの外部設定に影響します。

シャーシに CMC が 2 つあり（アクティブとスタンバイ）、ネットワークに接続されている場合は、フェイルオーバーが生じた場合、スタンバイ CMC は自動的にアクティブ CMC のネットワーク設定を引き継ぎます。

IPv6 が起動時に有効になると、3 つのルーターの要請が 4 秒ごとに送信されます。外部ネットワークのスイッチがスパニングツリープロトコル（SPT）を実行している場合、外部スイッチポートが 12 秒超ブロックされ、IPv6 の要請が送信されます。このような場合、ルーター広告が IPv6 ルーターによって送信されるまで、接続が制限される期間があります。

メモ: CMC のネットワーク設定を変更すると、現在のネットワーク接続が切断される可能性があります。

メモ: CMC ネットワーク設定を指定するには、**シャーシ設定システム管理者** の権限が必要です。

CMC ウェブインタフェースを使用した CMC ネットワーク LAN 設定の表示と変更

CMC ウェブインタフェースを使用して CMC ネットワーク LAN 設定を表示および変更するには：

1. システムツリーで、**シャーシの概要?** へ移動し、**ネットワーク → ネットワーク** をクリックします。**ネットワーク設定** に現在のネットワーク設定ページが表示されます。
2. 必要に応じて、全般、IPv4 または IPv6 の設定を変更します。詳細は、『*CMC オンラインヘルプ*』を参照してください。
3. 各セクションで **変更の適用** をクリックして、設定を適用します。

RACADM を使用した CMC ネットワーク LAN 設定の表示と変更

IPv4 設定を表示するには、次のサブコマンドおよびオブジェクトを使用します。

- `getniccfg`
- `getconfig`
- cfgCurrentLanNetworking

IPv6 設定を表示するには、次のサブコマンドおよびオブジェクトを使用します。

- `getconfig`
- cfgIPv6LanNetworking

シャーシの IPv4 と IPv6 アドレス指定情報を表示するには、`getsysinfo` サブコマンドを使用します。

サブコマンドおよびオブジェクトの詳細については、『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

CMC ネットワークインタフェースの有効化

CMC ネットワークインタフェースで IPv4 と IPv6 を有効 / 無効にするには、次を入力します。

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

メモ: CMC NIC はデフォルトで有効になっています。

CMC IPv6 アドレス指定を有効 / 無効にするには、次を入力します。

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

メモ: CMC IPv4 アドレス設定 はデフォルトで有効になっています。

CMC IPv6 アドレス指定を有効 / 無効にするには、次を入力します。

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

メモ: CMC IPv6 アドレス指定はデフォルトで無効になっています。

IPv4 では、CMC はデフォルトで DHCP サーバーから自動的に CMC IP アドレスを要求して取得します。この機能を無効にして、CMC の静的 IP アドレス、ゲートウェイ、サブネットマスクを指定できます。

IPv4 ネットワークで DHCP を無効にして、CMC の静的 IP アドレス、ゲートウェイ、サブネットマスクを指定するには、次を入力します。

```
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0 racadm config -g
cfgLanNetworking -o cfgNicIpAddress <静的 IP アドレス> racadm config -g
cfgLanNetworking -o cfgNicGateway <静的ゲートウェイ> racadm config -g
cfgLanNetworking -o cfgNicNetmask <静的サブネットマスク>
```

デフォルトで、IPv6 では、CMC は IPv6 自動設定メカニズムを使用して CMC IP アドレスを自動的に要求し取得します。

IPv6 ネットワークにおいて、自動設定機能を無効にし、静的 CMC IPv6 アドレス、ゲートウェイ、プレフィックス長を指定するには、次を入力します。

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

CMC ネットワークインタフェースアドレスの DHCP を有効または無効にする

有効にすると、CMC の DHCP を使って NIC アドレスを取得する機能は、動的ホスト構成プロトコル（DHCP）サーバーから自動的に IP アドレスを要求して取得します。この機能はデフォルトでは有効になっています。

DHCP を使って NIC アドレスを取得する機能を無効にして、静的 IP アドレス、サブネットマスク、ゲートウェイを指定することもできます。詳細は、「CMC への初期アクセスのセットアップ」を参照してください。

DHCP を使用した DNS IP アドレスの取得機能の有効 / 無効化

CMC の DHCP を使って DNS アドレスを取得する機能はデフォルトで無効になっています。この機能を有効にすると、プライマリとセカンダリ DNS サーバーアドレスが DHCP サーバーから取得されます。この機能を使用すると、DNS サーバーの静的 IP アドレスを設定する必要はありません。

DHCP を使用した DNS アドレスの取得機能を無効にして、プライマリとセカンダリ DNS サーバーの静的アドレスを指定するには、次を入力します。

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

IPv6 で DHCP を使用した DNS アドレスの取得機能を無効にして、プライマリとセカンダリ DNS サーバーの静的サーバーアドレスを指定するには、次を入力します。

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6DNSServersFromDHCP6 0
```

DNS の静的 IP アドレスの設定

メモ: 静的 DNS IP アドレス設定は、DNS アドレス機能が無効ではない場合は、有効ではありません。

IPv4 でプライマリとセカンダリ DNS IP サーバーアドレスを設定するには、次を入力します。

```
racadm config -g cfgLanNetworking -o cfgDNSServer1 <IP アドレス> racadm config -
g cfgLanNetworking -o cfgDNSServer2 <IPv4 アドレス>
```

IPv6 でプライマリとセカンダリ DNS IP サーバーアドレスを設定するには、次を入力します。

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6DNSServer1 <IPv6 アドレス>
racadm config -g cfgIPv6LanNetworking -o cfgIPv6DNSServer2 <IPv6 アドレス>
```

DNS 設定のセットアップ（IPv4 と IPv6）

- **CMC 登録**—DNS サーバーで CMC を登録するには、次を入力します。

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

  メモ: 31 文字以内の名前しか登録できない DNS サーバーもあります。指定する名前が DNS で要求される上限以下であることを確認してください。

  メモ: 次の設定は、**cfgDNSRegisterRac** を 1 に設定することで DNS サーバー上に CMC を登録した場合にのみ有効です。
- **CMC 名** — デフォルトで、DNS サーバー上の CMC 名は cmc-<*service tag*> です。DNS サーバー上の CMC の名前を変更するには、次を入力します。

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

  ここで、<名前> は 63 文字以内の英数字とハイフンを使って指定します。例えば、次のようになります。e: cmc-1, d-345
- **DNS ドメイン名** — デフォルトの DNS ドメイン名は空白文字 1 文字です。DNS ドメイン名を設定するには、次を入力します。

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

  ここで、<名前> は 254 文字以内の英数字とハイフンを使って指定します。例えば、次のようになります。p45, a-tz-1, r-id-001

オートネゴシエーション、二重モード、ネットワーク速度の設定（IPv4 と IPv6）

オートネゴシエーション機能は、有効にした場合、最も近いルーターまたはスイッチと通信することで CMC が自動的に二重モードとネットワーク速度を設定するかどうかを判定します。オートネゴシエーションはデフォルトで有効になっています。

オートネゴシエーションを無効にして、二重モードとネットワーク速度を指定するには、次を入力します。

```
racadm config -g cfgNetTuning -o cfgNetTuningNicAutoneg 0 racadm config -g
cfgNetTuning -o cfgNetTuningNicFullDuplex <ニ重モード>
```

ここで、

<二重モード> は 0（半二重）または 1（全二重　、デフォルト）です。

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

ここで、

<速度> は 10 または 100（デフォルト）です。

最大転送単位（MTU）の設定（IPv4 と IPv6）

MTU プロパティでは、インタフェースを通して渡すことができるパケットの最大サイズを設定できます。MTU を設定するには、次を入力してください。

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

ここで、<mtu> は 576～1500 の数値です（両方を含む。デフォルトは 1500）。

メモ: IPv6 では最低 1280 の MTU が必要です。IPv6 が有効で、cfgNetTuningMtu の値がこれよりも低い値に設定されている場合、CMC は 1280 の MTU を使用します。

CMC ネットワークおよびログインセキュリティ設定の実行

CMC における IP アドレスブロックおよびユーザーブロック機能によって、パスワード推測の試みによるセキュリティ問題を防止することができます。この機能は、IP アドレス範囲と CMC にアクセスできるユーザーのブロックを可能にします。デフォルトで、CMC では IP アドレスブロック機能が有効になっています。

メモ: IP アドレスによるブロックは、IPV4 アドレスのみに適用されます。

CMC ウェブインタフェースまたは RACADM を使用して IP 範囲属性を設定できます。IP アドレスブロックおよびユーザーブロック機能を使用するには、CMC ウェブインタフェースまたは RACADM を使ってそのオプションを有効にしてください。ログインロックアウトポリシーを設定して、特定のユーザーまたは IP アドレスに対するログイン失敗回数を設定できるようにします。この限度を超えると、ブロックされたユーザーはペナルティ時間が経過しなければログインできません。

CMC ウェブインタフェースを使用した IP 範囲属性の設定

メモ: 次のタスクを行うには、**シャーシ設定システム管理者** の権限が必要です。

CMC ウェブインタフェースを使用して IP 範囲属性を設定するには、次を実行します。

1. システムツリーで、**シャーシ概要** に移動し、**ネットワーク → ネットワーク** をクリックします。**ネットワーク設定** ページが表示されます。
2. IPv4 設定セクションで、**詳細設定** をクリックします。
   ログインセキュリティ ページが表示されます。
   ログインセキュリティページにアクセスする別の方法は、システムツリーで **シャーシ概要** に移動して **セキュリティ → ログイン** をクリックします。
3. IP 範囲チェック機能を有効にするには、**IP 範囲** セクションで **IP 範囲有効** オプションを選択します。
   IP 範囲アドレス および **IP 範囲マスク** フィールドがアクティブになります。
4. **IP 範囲アドレス** および **IP 範囲マスク** フィールドで、CMC アクセスからブロックする IP アドレスの範囲と IP 範囲マスクを入力します。
   詳細については、『CMC オンラインヘルプ』を参照してください。
5. **適用** をクリックして設定を保存します。

RACADM を使用した IP 範囲属性の設定

RACADM を使用して、以下の CMC の IP 範囲属性を設定できます。

- IP 範囲チェック機能
- CMC アクセスからブロックする IP アドレスの範囲
- CMC アクセスからブロックする IP 範囲マスク

IP フィルタは、受信ログインの IP アドレスを指定された IP アドレス範囲と比較します。受信 IP アドレスからのログインは、以下の両方が一致したときのみ許可されます。

- **cfgRacTuneIpRangeMask**（ビットワイズ）および受信 IP アドレス
- **cfgRacTuneIpRangeMask**（ビットワイズ）および **cfgRacTuneIpRangeAddr** で指定された IP アドレス

メモ:

- IP 範囲チェック機能を有効化するには、 cfgRacTuning グループで次のプロパティを使用します。
  cfgRacTuneIpRangeEnable <0/1>
- CMC アクセスをブロックする IP アドレスの範囲を指定するには、 cfgRacTuning グループで次のプロパティを使用します。
  cfgRacTuneIpRangeAddr
- CMC アクセスをブロックする IP 範囲マスクを指定するには、 cfgRacTuning グループで次のプロパティを使用します。
  cfgRacTuneIpRangeMask

CMC の仮想 LAN タグプロパティ

VLAN を使用すると、複数の仮想 LAN が同じ物理ネットワーク上で共存でき、セキュリティやロード管理の目的でネットワークトラフィックを分離できます。VLAN 機能を有効にすると、各ネットワークパケットに VLAN タグが割り当てられます。

ウェブインタフェースを使用した CMC の仮想 LAN タグプロパティの設定

ウェブインタフェースを使用して CMC 用 LAN を設定するには：

1. 次のいずれかのページに移動します。
   - システムツリーで、 **シャーシの概要**? へ移動し、**ネットワーク → VLAN**?をクリックします。
   - システムツリーで、 **シャーシの概要 → サーバーの概要** へ移動し、**ネットワーク → VLAN**?をクリックします。

   VLAN タグ設定 ページが表示されます。VLAN タグはシャーシプロパティです。このタグは、コンポーネントを削除した後もシャーシに残ります。
2. **CMC** セクションで CMC 用に VLAN を有効にし、優先順位を設定して ID を割り当てます。フィールドについての詳細は、『*CMC オンラインヘルプ*』を参照してください。
3. 適用 をクリックします。VLAN のタグ設定が保存されます。
   シャーシの概要 → サーバー → 設定 → VLAN サブタブから、このページにアクセスすることもできます。

RACADM を使用した CMC 用仮想 LAN タグプロパティの設定

1. 外部シャーシ管理ネットワークの VLAN 機能を有効にします。
   racadm config -g cfgLanNetworking -o cfgNicVLanEnable 1
2. 外部シャーシ管理ネットワークの VLAN ID を指定します。
   racadm config -g cfgLanNetworking -o cfgNicVlanID <VLAN id>

   <VLAN id> に指定できる値は 1～4000、および 4021～4094 の範囲の数値です。デフォルトは 1 です。
   たとえば、次のとおりです。
   racadm config -g cfgLanNetworking -o cfgNicVlanID 1
3. 次に、外部シャーシ管理ネットワークの VLAN 優先順位を指定します。
   racadm config -g cfgLanNetworking -o cfgNicVLanPriority <VLAN 優先順位>

   <VLAN 優先順位> の有効値は 0～7 です。デフォルトは 0 です。
   たとえば、次のとおりです。
   racadm config -g cfgLanNetworking -o cfgNicVLanPriority 7

   また、1 つのコマンドで VLAN ID と VLAN 優先順位を指定できます。
   racadm setniccfg -v <VLAN id> <VLAN 優先順位>

たとえば、次のとおりです。

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

4. CMC VLAN を削除するには、外部シャーシ管理ネットワークの VLAN 機能を無効にします。

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

次のコマンドを使用しても、CMC VLAN を削除できます。

```
racadm setniccfg -v
```

サービスの設定

CMC では、次のサービスの設定と有効化ができます。

- CMC シリアルコンソール — シリアルコンソールを使用した CMC へのアクセスを有効にします。
- Web サーバー — CMC ウェブインタフェースへのアクセスを有効にします。Web サーバーのオプションを無効にすると、リモート RACADM も同時に無効になるので、Web サーバーを再度有効にするには、ローカル RACADM を使用します。
- SSH — ファームウェア RACADM を介した CMC へのアクセスを有効にします。
- Telnet — ファームウェア RACADM を介した CMC へのアクセスを有効にします。
- RACADM — RACADM を使用した CMC へのアクセスを有効にします。
- SNMP — イベントに対して SNMP トラップを送信するよう CMC を有効にします。
- リモート Syslog — イベントをリモートサーバーに記録するよう CMC を有効にします。

CMC には、インターネット経由でクライアント間で暗号化されたデータを受け入れて転送する業界標準の SSL セキュリティプロトコルを設定した Web Server がインストールされています。Web Server には、デルの自己署名 SSL デジタル証明書（サーバー ID）が含まれており、クライアントからのセキュア HTTP 要求を受け入れて応答します。このサービスは、ウェブインタフェースとリモート RACADM CLI ツールが CMC と通信するために必要です。

Web サーバーがリセットされた場合は、サービスが再び利用可能になるまで少なくとも 1 分間お待ちください。Web サーバーのリセットは通常、以下のいずれかのイベントが発生した結果です。

- ネットワーク設定またはネットワークセキュリティプロパティが CMC Web ユーザーインタフェースまたは RACADM を介して変更された。
- Web サーバーポートの設定が Web ユーザーインタフェースまたは RACADM を介して変更された。
- CMC がリセットされた。
- 新しい SSL サーバー証明書がアップロードされた。

メモ: サービスの設定を変更するには、**シャーシ設定システム管理者**の権限が必要です。

リモートシスログは、追加の CMC ログターゲットです。リモートシスログを設定したら、新しい各ログエントリが CMC によって生成され、送信先に転送されます。

メモ: 転送されるログエントリのネットワークトランスポートは UDP であるため、ログエントリが確実に配信されるという保証もなければ、ログエントリが正常に受信されたかどうかを通知するフィードバックが CMC に送られることもありません。

CMC ウェブインタフェースを使用したサービスの設定

CMC ウェブインタフェースを使用して CMC サービスを設定するには、次の手順を実行します。

1. **シャーシの概要** へ移動し、**ネットワーク → サービス** をクリックします。**サービス** ページが表示されます。
2. 必要に応じて次のサービスを設定します。

- CMC シリアルコンソール
- ウェブサーバー
- SSH
- Telnet
- リモート RACADM
- snmp
- リモート Syslog

フィールドについての情報は、『*CMC オンラインヘルプ*』を参照してください。

3. **適用** をクリックし、すべてのデフォルトのタイムアウト値および最大タイムアウト制限値を更新します。

RACADM を使用したサービスの設定

さまざまなサービスを有効化し、設定するには、次の RACADM オブジェクトを使用します。

- `cfgRacTuning`
- `cfgRacTuneRemoteRacadmEnable`

これらのオブジェクトの詳細については、**dell.com/support/manuals** にある『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

ブレードサーバー上のファームウェアによって機能がサポートされていない場合は、その機能に関連するプロパティを設定するとエラーが表示されます。たとえば、RACADM を使用して非対応の iDRAC でリモート syslog を有効にしようとすると、エラーメッセージが表示されます。

同様に、RACADM getconfig コマンドを使用して iDRAC プロパティを表示しようとすると、ブレードサーバーで非対応の機能に対するプロパティ値には 該当なし と表示されます。

たとえば、次のとおりです。

```
$ 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
```

CMC 拡張ストレージカードの設定

拡張不揮発性ストレージとして使用するため、オプションのリムーバブルフラッシュメディアの設定を有効化または修復することができます。CMC の機能のなかには、動作が拡張不揮発性ストレージに依存するものもあります。

CMC ウェブインタフェースを使用してリムーバブルフラッシュメディアを有効化または修復するには：

1. システムツリーで、**シャーシの概要** へ移動し、**シャーシコントローラ → フラッシュメディア** をクリックします。リムーバブルフラッシュメディア ページが表示されます。
2. ドロップダウンメニューから、必要に応じて次のいずれかを選択します。
   - シャーシデータの保存用にフラッシュメディアを使用する
   - アクティブコントロールメディアを修復する
   - メディア間のデータの複製を開始する
   - メディア間のデータの複製を停止する
   - シャーシデータの保存用にフラッシュメディアを使用しない

   これらのオプションの詳細については、『*CMC オンラインヘルプ*』を参照してください。

3. **適用** をクリックして選択したオプションを適用します。

   シャーシ内に 2 台の CMC がある場合は、両方の CMC にフラッシュメディアが装着されている必要があります。フラッシュメディアに依存する CMC 機能（Flexaddress を除く）は、デル承認のメディアをインストールして、このページで有効化するまで、正しく動作しません。

シャーシグループのセットアップ

CMC では、単一のリードシャーシから複数のシャーシを監視することが可能になります。シャーシグループを有効にした場合、リードシャーシの CMC は、リードシャーシおよびそのシャーシグループ内のすべてのメンバーシャーシのステータスのグラフィカル表示を生成します。

シャーシグループの機能は以下のとおりです。

- **シャーシグループ** ページには、リーダーおよび各メンバーシャーシの前面と背面を描写した画像がそれぞれ 1 セットずつ表示されます。
- グループのリーダーおよび各メンバーの正常性に関する懸念がある場合、その症状があるコンポーネントは赤色または黄色および X または ! で表示されます。詳細情報は、シャーシの画像または **詳細** をクリックすると、そのシャーシ画像の下に表示されます。
- メンバーシャーシまたはサーバーのウェブページを開くために、クィック起動のリンクを使用できます。
- グループに対する、ブレードと入出力のインベントリが可能です。
- 新しいメンバーがグループに追加されたときに、新しいメンバーのプロパティをリーダーのプロパティと同期させることができるオプションを選択できます。

1 つのシャーシグループには、最大 8 つのメンバーを含むことができます。また、リーダーおよび各メンバーは、1 つのグループにのみ参加できます。あるグループに属するシャーシを別のグループに参加させることは（リーダーまたはメンバーのどちらとしても）できません。そのシャーシをグループから削除すれば、後で別のグループに追加することはできます。

CMC ウェブインタフェースを使用してシャーシグループを設定するには、次の手順を実行します。

1. リーダーに予定しているシャーシに、シャーシ管理者権限でログインします。
2. **セットアップ → グループ管理** とクリックします。**シャーシグループ** ページが表示されます。
3. **シャーシグループ** ページの **役割** で、**リーダー** を選択します。グループ名を追加するフィールドが表示されます。
4. **グループ名** フィールドにグループの名前を入力して、**適用** をクリックします。

   メモ: ドメイン名に適用される規則と同じものが、グループ名にも適用されます。

   シャーシグループが作成されると、GUI が自動的に **シャーシグループ** ページに切り替わります。システムツリーはグループをグループ名で示し、リードシャーシと未実装のメンバーシャーシがシステムツリーに表示されます。

関連リンク

シャーシグループへのメンバーの追加
リーダーからのメンバーの削除
シャーシグループの無効化
メンバーシャーシでの個別のメンバーの無効化
メンバーシャーシまたはサーバーのウェブページの起動
リーダーシャーシプロパティのメンバーシャーシへの伝達

シャーシグループへのメンバーの追加

シャーシグループをセットアップした後、次の手順でそのグループにメンバーを追加することができます。

1. リーダーシャーシに、シャーシ管理者権限でログインします。
2. システムツリーでリードシャーシを選択します。
3. **セットアップ → グループ管理** とクリックします。
4. **グループ管理** にある **ホスト名 /IP アドレス** フィールドで、メンバーの IP アドレスまたは DNS 名を入力します。
5. **ユーザー名** フィールドに、そのメンバーシャーシのシャーシ管理者権限のあるユーザーの名前を入力します。
6. **パスワード** フィールドに、該当するパスワードを入力します。
7. **適用** をクリックします。
8. 手順 4 から手順 8 を繰り返して、最大 8 つまでのメンバーを追加します。 新しく追加したメンバーのシャーシ名が、**メンバー** ダイアログボックスに表示されます。

   ツリー内のグループを選択すると、新しいメンバーのステータスが表示されます。シャーシの画像または詳細ボタンをクリックすると、詳細情報が表示されます。

   メモ: メンバーに対して入力された資格情報は、セキュアにメンバーシャーシに受け渡され、そのシャーシとリードシャーシとの間の信頼関係が確立されます。この資格情報は、いずれのシャーシにも存続するものではなく、一度信頼関係が確立された後は、相互にやりとりされることはありません。

   リーダーシャーシプロパティのメンバーシャーシへの伝達についての情報は、「リーダーシャーシプロパティのメンバーシャーシへの伝達」を参照してください。

リーダーからのメンバーの削除

グループのメンバーをリードシャーシから削除することができます。メンバーを削除するには、次の手順を実行します。

1. リーダーシャーシに、シャーシ管理者権限でログインします。
2. システムツリーでリードシャーシを選択します。
3. **セットアップ → グループ管理** とクリックします。
4. **メンバーの削除** リストで、削除対象のメンバーの名前（1 つまたは複数）を選択し、**適用** をクリックします。

   その後、リードシャーシは、グループから削除されたメンバー（1 つまたは複数）との通信を行います。メンバー名が削除されます。ネットワーク上の問題によりリードとメンバー間の通信が妨げられている場合、メンバーシャーシがメッセージを受信しない場合があります。そのような場合には、メンバーシャーシからそのメンバーを無効にして削除を完了させてください。

関連リンク

メンバーシャーシでの個別のメンバーの無効化

シャーシグループの無効化

リードシャーシからグループを解除するには、次の手順を実行します。

1. リーダーシャーシに、管理者権限でログインします。
2. システムツリーでリードシャーシを選択します。
3. **セットアップ → グループ管理** とクリックします。

4. **シャーシグループ** ページの **役割** で **なし**を選択し、**適用** をクリックします。

   その後、リードシャーシはすべてのメンバーに、グループから削除された旨の通信を行います。最後にリードシャーシがそのグループのリードシャーシとしての役割を打ち切ります。この時点で、このシャーシは別のグループのメンバーまたはリーダーとしての役割を割り当てることができます。

   ネットワーク上の問題によりリードとメンバー間の通信が妨げられている場合、メンバーシャーシがメッセージを受信しない場合があります。そのような場合には、メンバーシャーシからそのメンバーを無効にして削除を完了させてください。

メンバーシャーシでの個別のメンバーの無効化

リードシャーシによるグループからのメンバーの削除を実行できない場合があります。このような状況は、メンバーへのネットワーク接続が失われた場合に発生します。メンバーシャーシでグループからメンバーを削除するには、次の手順を実行します。

1. メンバーシャーシに、シャーシ管理者権限でログインします。
2. **セットアップ → グループ管理** とクリックします。
3. **なし** を選択して、**適用** をクリックします。

メンバーシャーシまたはサーバーのウェブページの起動

グループ内のメンバーシャーシのウェブページ、サーバーのリモートコンソール、またはサーバー iDRAC のウェブページへのリンクは、リードシャーシのグループページから利用できます。メンバーデバイスにログインするには、リードシャーシにログインするときに使用したユーザー名とパスワードを使用できます。メンバーデバイスのログイン資格情報が同じ場合には、重ねてログインする必要はありません。同じでない場合は、メンバーデバイスのログインのログインページにリダイレクトされます。

メンバーデバイスに移動するには、次の手順を実行します。

1. リードシャーシにログインします。
2. ツリー内で **グループ：名前** を選択します。
3. 移動先がメンバーの CMC の場合には、目的のシャーシの **CMC の起動** を選択します。

   シャーシ内のサーバーが移動先の場合には、次の手順を実行します。

   a) 目的のシャーシの画像を選択します。
   b) **正常性とアラート** ペインの下に表示されるシャーシ画像内で、サーバーを選択します。
   c) **クィックリンク** という表題のボックスで、移動先デバイスを選択します。移動先ページ、またはログイン画面を表示する新しいウィンドウが開きます。

リーダーシャーシプロパティのメンバーシャーシへの伝達

グループのリーダーシャーシからメンバーシャーシにプロパティを伝達することができます。リーダープロパティとメンバーを同期化するには、次の手順を実行します。

1. リーダーシャーシに、管理者権限でログインします。
2. システムツリーでリードシャーシを選択します。
3. **セットアップ → グループ管理** とクリックします。
4. **シャーシプロパティ伝達** セクションで、伝達タイプのいずれかを選択します。

   - 変更時の伝達 — 選択したシャーシプロパティ設定の自動伝達には、このオプションを選択します。プロパティの変更は、リーダーのプロパティが変更されるたびに、現在のグループメンバーすべてに伝達されます。
   - 手動伝達 — シャーシグループリーダプロパティのメンバーへの手動伝達には、このオプションを選択します。リーダーシャーシのプロパティ設定は、リーダーシャーシの管理者が **伝達** をクリックした時にのみ、グループメンバーに伝達されます。

5. **伝達プロパティ** セクションで、メンバーシャーシに伝達されるリーダーの設定プロパティのカテゴリを選択します。
   シャーシグループのメンバー全体で同一に設定する設定カテゴリだけを選択します。 例えば、**ロギングとアラートプロパティ** カテゴリを選択して、グループ内の全シャーシがリーダーシャーシのロギングおよびアラート設定を共有するようにします。

6. **保存** をクリックします。
   変更時の伝達 が選択されている場合、メンバーシャーシはリーダーのプロパティを採用します。**手動伝達** が選択されている場合は、選んだ設定をメンバーシャーシに伝達したいときにいつでも **伝達** をクリックします。リーダーシャーシプロパティの伝達の詳細については、『*CMC オンラインヘルプ*』を参照してください。

マルチシャーシ管理グループのサーバーインベントリ

シャーシグループの正常性 ページには、すべてのメンバーシャーシが表示され、標準のブラウザダウンロード機能を使用して、サーバーインベントリレポートをファイルに保存することができます。レポートには以下のデータが含まれています。

- すべてのグループシャーシ（リーダーを含む）に現在あるすべてのサーバー。
- 空のスロットおよび拡張スロット（フルハイトおよびダブルワイドサーバーを含む）。

サーバーインベントリレポートの保存

CMC ウェブインタフェースを使用してサーバーインベントリレポートを保存するには、次の手順を実行します。

1. システムツリーで、**グループ** を選択します。
   シャーシグループ正常性 ページが表示されます。

2. **インベントリレポートの保存** をクリックします。
   ファイルを開くか保存するかをたずねる **ファイルのダウンロード** メッセージボックスが表示されます。

3. **保存** をクリックして、サーバーインベントリレポートのパスとファイル名 を指定します。

   メモ: 最も正確なサーバーインベントリレポートを入手するには、シャーシグループリーダー、メンバーシャーシ、および関連シャーシのサーバーが **オン** になっている必要があります。

エクスポートされたデータ

サーバーインベントリレポートには、シャーシグループのリーダーの通常のポーリング（30 秒ごと）で各シャーシグループのメンバーによって最近返されたデータが示されます。
最も正確なサーバーインベントリレポートを取得するには、以下の条件を満たしている必要があります。

- シャーシグループのリーダーシャーシとシャーシグループのすべてのメンバーシャーシが **シャーシ電源状態オン** になっている
- 関連シャーシ内のすべてのサーバーの電源がオンになっている

関連シャーシとサーバーのインベントリデータは、シャーシグループの一部のメンバーシャーシが以下の場合は、インベントリレポートに含まれない可能性があります。

- **シャーシ電源状態オフ**
- 電源オフ

  メモ: シャーシの電源がオフの状態でサーバーを挿入した場合、シャーシの電源がオンになるまで、モデル番号はウェブインタフェースに表示されません。

次の表は、各サーバーについてレポートされる特定のデータフィールドとフィールドの特定の要件を示しています。

表 11. : ブレードインベントリフィールドの説明

データフィールド	例
シャーシ名	データセンターのシャーシリーダー
シャーシ IP アドレス	192.168.0.1
スロットの場所	1
スロット名	SLOT-01
ホスト名	企業のウェブサーバー **メモ:** サーバー上で Server Administrator エージェントが実行されている必要があります。実行されていない場合は、何も表示されません。
オペレーティングシステム	Windows Server 2008 **メモ:** サーバー上で Server Administrator エージェントが実行されている必要があります。実行されていない場合は、何も表示されません。
モデル	PowerEdgeM610
サービスタグ	1PB8VF1
総システムメモリ容量	4.0 GB **メモ:** メンバー上に CMC 4.0 以上が必要です。これがない場合は、何も表示されません。
CPU の数	2 **メモ:** メンバー上に CMC 4.0 以上が必要です。これがない場合は、何も表示されません。
CPU 情報	Intel (R) Xeon (R) CPU E5502 @1.87GHzn **メモ:** メンバー上に CMC 4.0 以上が必要です。これがない場合は、何も表示されません。

データフォーマット

インベントリレポートは、Microsoft Excel などのさまざまなツールにインポートできるように、**.CSV** I ファイルフォーマットで生成されます。インベントリレポートの**.CSV** ファイルは、MS Excel で **データ → テキストファイル** を選択してテンプレートにインポートできます。インベントリレポートを MS Excel にインポートするとき、追加情報を求めるメッセージが表示される場合は、カンマ区切りを選択してファイルを MS Excel にインポートしてください。

シャーシグループインベントリとファームウェアバージョン

シャーシグループファームウェアバージョン ページは、シャーシ内のサーバーおよびサーバーコンポーネントのグループインベントリとファームウェアバージョンを表示します。このページでは、インベントリ情報を分類し、ファームウェアバージョン表示をフィルタすることも可能です。表示されるビューは、サーバーまたは以下のシャーシサーバーコンポーネントのいずれかに基づいたものです。

- BIOS
- iDRAC
- CPLD
- USC
- 診断
- OS ドライバ
- RAID
- NIC

メモ: シャーシグループ、メンバーシャーシ、サーバー、およびサーバーコンポーネントについて表示されるインベントリ情報は、グループに対するシャーシの追加または削除が行われるたびにアップデートされます。

シャーシグループインベントリの表示

CMC ウェブインタフェースを使用してシャーシグループを表示するには、システムツリーで **グループ** を選択します。**プロパティ → ファームウェアバージョン** をクリックします。**シャーシグループファームウェアバージョン** ページにグループ内のすべてのシャーシが表示されます。

ウェブインタフェースを使用した選択されたシャーシインベントリ表示

ウェブインタフェースを使用して選択されたシャーシインベントリを表示するには、次の手順を実行します。

1. システムツリーで **グループ** を選択します。**プロパティ → ファームウェアバージョン** をクリックします。
   シャーシグループファームウェアバージョン ページにグループ内のすべてのシャーシが表示されます。
2. **シャーシの選択** セクションで、インベントリを表示したいメンバーシャーシを選択します。
   ファームウェア表示フィルタ セクションに選択したシャーシのサーバーインベントリ、およびすべてのサーバーコンポーネントのファームウェアバージョンが表示されます。

ウェブインタフェースを使用した選択されたサーバーコンポーネントのファームウェアバージョンの表示

CMC ウェブインタフェースを使用して選択されたサーバーコンポーネントのファームウェアバージョンを表示するには、次の手順を実行します。

1. システムツリーで **グループ** を選択します。**プロパティ → ファームウェアバージョン** をクリックします。
   シャーシグループファームウェアバージョン ページにグループ内のすべてのシャーシが表示されます。
2. **シャーシの選択** セクションで、インベントリを表示したいメンバーシャーシを選択します。
3. **ファームウェア表示フィルタ** セクションで **コンポーネント** を選択します。
4. **コンポーネント** リストで、ファームウェアバージョンを表示させたい BIOS、iDRAC、CPLD、USC、診断、OS ドライブ、RAID デバイス（最大 2 台）、NIC デバイス（最大 6 台）といった必要コンポーネントを選択します。
   選択されたメンバーシャーシ内のすべてのサーバーに対する選択されたコンポーネントのファームウェアバージョンが表示されます。

メモ: 以下の場合、サーバーの USC、診断、OS ドライブ、RAID デバイス、NIC デバイスのファームウェアバージョンは表示できません。

- サーバーが第 10 世代の PowerEdge サーバーに属している。これらのサーバーは Lifecycle Controller をサポートしません。
- サーバーは第 11 世代の PowerEdge サーバーに属しているが、iDRAC ファームウェアが Lifecycle Controller をサポートしていない。
- メンバーシャーシの CMC ファームウェアバージョンがバージョン 4.45 より前である。この場合、サーバーが Lifecycle Controller をサポートしていても、このシャーシ内のサーバーのコンポーネントは全く表示されません。

証明書の取得

次の表に、ログインタイプに基づいた証明書のタイプを示します。

表 12. : ログインおよび証明書のタイプ

ログインタイプ	証明書タイプ	取得方法
Active Directory を使用したシングルサインオン	信頼できる CA 証明書	CSR を生成し、認証局の署名を取得します。
Active Directory ユーザーとしてのスマートカードログイン	• ユーザー証明書 • 信頼できる CA 証明書	• ユーザー証明書 — スマートカードベンダーが提供するカード管理ソフトウェアを使用して、スマートカードユーザー証明書を Base64 でエンコードされたファイルとしてエクスポートします。 • 信頼できる CA 証明書 — この証明書は、CA によって発行されます。
Active Directory ユーザーログイン	信頼できる CA 証明書	この証明書は、CA によって発行されます。
ローカルユーザーログイン	SSL 証明書	CSR を生成し、認証局の署名を取得します。 メモ: CMC はデフォルトの自己署名済み SSL サーバー証明書が同梱されて配送されます。CMC ウェブサーバーおよび仮想コンソールはこの証明書を使用します。

関連リンク

セキュアソケットレイヤー（SSL、Secure Sockets Layer）サーバー証明書

セキュアソケットレイヤー（SSL、Secure Sockets Layer）サーバー証明書

CMC には、インターネットで暗号化データを送信するための業界標準 SSL セキュリティプロトコルを使用する Web サーバーが備わっています。公開キーと秘密キーの暗号技術に基づく SSL は、クライアントとサーバー間に認証と暗号化を備えた通信を提供してネットワーク上の盗聴を防止するセキュリティ方式として広く受け入れられています。

SSL は、SSL を有効にしたシステムで次のタスクを実行します。

- SSL 対応クライアントに自らを認証する
- クライアントがサーバーに対して自らを認証できるようにする。
- 両システムが暗号化接続を確立できるようにする。

この暗号化プロセスは、高レベルなデータ保護を実現します。CMC には、北米のインターネットブラウザで一般的に使用できる暗号化形式の中でも最もセキュアな形式である 128 ビット SSL 暗号化標準が採用されています。

CMC Web サーバーには、デルが署名をした SSL デジタル証明書（サーバー ID）が含まれています。インターネットにおける高度なセキュリティを確保するため、新しい証明書署名要求（CSR）の生成要求を CMC に送信して、Web サーバーの SSL 証明書を置き換えてください。

以下の場合、起動時に新しい自己署名証明書が生成されます。

- カスタム証明書が存在しない
- 自己署名証明書が存在しない
- 自己署名証明書が破損している
- 自己署名証明書が失効している（30 日期間以内）

自己署名証明書が共有名を <cmcname.domain-name> として表示する。ここで、cmcname は CMC ホスト名で、domain-name はドメイン名です。ドメイン名がない場合は、部分的修飾ドメイン名（PQDN）のみ、すなわち CMC ホスト名を表示します。

証明書署名要求（CSR）

CSR はセキュアサーバー証明書の認証局（ウェブインタフェースでは CA という）へのデジタル要求です。セキュアサーバ証明書は、リモートシステムの身元を確認して、リモートシステムとやり取りする情報を他の人が閲覧または変更できないようにします。CMC のセキュリティを確保するため、CSR を生成して認証局に提出し、認証局から返された証明書をアップロードすることをお勧めします。

認証局（CA）は、IT 業界で認知されたビジネス組織で、高水準で信頼できる審査、身元確認、その他の重要なセキュリティ要件を提供しています。CA には、Thawte や VeriSign などがあります。認証局は CSR を受け取ると、CSR に含まれている情報を審査、検証します。申請者が認証局のセキュリティ標準を満たしていれば、ネットワークとインターネット上でトランザクションを行う申請者を一意に識別する証明書を発行します。

認証局が CSR を承認して証明書を送信したら、それを CMC ファームウェアにアップロードする必要があります。CMC ファームウェアに保管されている CSR 情報は、証明書に記載されている情報と一致する必要があります。

メモ: SSL を CMC 用に設定するには、**シャーシ設定システム管理者** の権限が必要です。

メモ: アップロードするサーバー証明書は最新で（期限が切れていない）、認証局が署名したものでなければなりません。

関連リンク

新しい証明書署名要求の生成
サーバー証明書のアップロード
サーバー証明書の表示

新しい証明書署名要求の生成

セキュリティ強化のため、セキュアなサーバー証明書を取得し、CMC にアップロードされることを強く推奨します。セキュアサーバー証明書は、リモートシステムの ID を確認し、リモートシステムとやり取りする情報を他者が表示したり変更したりできないようにします。セキュアサーバー証明書を使用しないと、CMC に許可のないユーザーが不正にアクセスする危険があります。

CMC のセキュアサーバー証明書を取得するには、利用する認証局に証明書署名要求（CSR）を送信する必要があります。CSR とは、組織に関する情報と一意の識別キーが含まれた署名入りのセキュアサーバー証明書を申請するデジタル要求です。

CSR が生成されると、管理ステーションまたは共有ネットワークにコピーを保存するように指示するメッセージが表示され、CSR の生成に使用した一意の情報が CMC に保存されます。この情報は、後で認証局から受け取るサーバー証明書の認証に使用されます。認証局からサーバー証明書を受け取った後、それを CMC にアップロードする必要があります。

メモ: 認証局から返されたサーバー証明書を CMC が受け入れるためには、新しい証明書の認証情報が、CSR 生成時に CMC に保存された情報と一致する必要があります。

注意: 新しい CSR が生成されると、CMC に保管されている古い CSR はすべて上書きされます。つまり、認証局からサーバー証明書が付与される前に保留中の CSR が上書きされた場合、証明書の認証に使用する情報が失われるため、CMC がサーバー証明書を受け入れなくなります。CSR を生成するとき、保留中の CSR を上書きしないように注意してください。

ウェブインタフェースを使用した新規証明書署名要求の生成

ウェブインタフェースを使用して CSR を生成するには：

1. システムツリーで、**シャーシの概要** へ移動し、**ネットワーク → SSL** をクリックします。**SSL メインメニュー** が表示されます。
2. **新規証明書署名要求（CSR）の生成** を選択して、**次へ** をクリックします。**証明書署名要求（CSR）の生成** ページが表示されます。
3. 各 CSR 属性値の値を入力します。
4. **生成** をクリックします。 **ファイルのダウンロード** ダイアログボックスが表示されます。
5. **csr.txt** ファイルを管理ステーションまたは共有ネットワークに保存します。（このままファイルを開いて、後で保存することも可能です。）このファイルを後で CA に提出する必要があります。

RACADM を使用した CSR の生成

CSR を生成するには、`cfgRacSecurityData` グループ内のオブジェクトを使用して値を指定し、`sslcsrgen` コマンドを使用して CSR を生成します。詳細については、**dell.com/support/manuals** にある『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

サーバー証明書のアップロード

CSR の生成後、署名された SSL サーバー証明書を CMC ファームウェアにアップロードできます。CMC は、証明書のアップロード後にリセットされます。CMC は、X509 Base-64 エンコードの Web サーバー証明書のみを受け入れます。

注意: 証明書のアップロード中は、CMC を使用できません。

CMC ウェブインタフェースを使用したサーバー証明書のアップロード

CMC ウェブインタフェースを使用してサーバー証明書をアップロードするには、次の手順を実行します。

1. システムツリーで、**シャーシの概要** へ移動し、**ネットワーク → SSL** をクリックします。**SSL メインメニュー** が表示されます。
2. **OSR に基づいて生成されたサーバー証明書のアップロード** オプションを選択して **次へ** をクリックします。
3. **ファイルの選択** をクリックして証明書ファイルを指定します。
4. **適用** をクリックします。証明書が無効の場合は、エラーメッセージが表示されます。

   メモ: アップロードする証明書の相対ファイルパスが **ファイルパス** の値に表示されます。フルパスと正しいファイル名とファイル拡張子を含む絶対ファイルパスを入力する必要があります。

RACADM を使用したサーバー証明書のアップロード

SSL サーバー証明書をアップロードするには、`sslcertupload` コマンドを使用します。詳細については、**dell.com/support/manuals** にある『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

ウェブサーバーキーと証明書のアップロード

Web Server キーおよび Web Server キーのサーバー証明書をアップロードします。サーバー証明書は、認証局（CA）から発行されます。

ウェブサーバー証明書は、暗号化プロセスに使用される重要なコンポーネントです。これは SSL 対応のクライアントに対して自身を認証し、クライアントがサーバーに対して自身を認証することを許可するため、両方のシステムが暗号化された接続を確立することを可能にします。

メモ: Web Server キーとサーバー証明書をアップロードするには、**シャーシ設定システム管理者** の権限が必要です。

CMC ウェブインタフェースを使用したウェブサーバーキーと証明書のアップロード

CMC ウェブインタフェースを使用してウェブサーバーキーと証明書をアップロードするには、次の手順を実行します。

1. システムツリーで、**シャーシの概要?** へ移動し、**ネットワーク → SSL** をクリックします。The **SSL メインメニュー** が表示されます。
2. **ウェブキーと証明書のアップロード** オプションを選択してから、**次へ** をクリックします。
3. **ファイルの選択** をクリックして、プライベートキーファイルと証明書ファイルを指定します。
4. 両ファイルがアップロードされたら、**適用** をクリックします。ウェブサーバーキーと証明書が一致しない場合、エラーメッセージが表示されます。

   メモ: CMC が受け入れるのは、X509、Base 64 エンコードの証明書のみです。DER など、他のエンコードスキームを使用している証明書は、受け入れられません。新しい証明書をアップロードすると、CMC で受け取ったデフォルトの証明書が置き換えられます。

   証明書が正常にアップロードされると、CMC がリセットされ、一時的に使用できなくなります。リセット中に他のユーザーが切断されないようにするため、CMC にログインしている可能性のある権限を持つユーザーに通知し、**ネットワーク** タブの **セッション** ページで、アクティブなセッションを確認してください。

RACADM を使用したウェブサーバーキーと証明書のアップロード

SSL キーをクライアントから iDRAC にアップロードするには、次のコマンドを入力します。

```
racadm sslkeyupload -t <タイプ> -f <ファイル名>
```

詳細については、**dell.com/support/manuals** にある『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

サーバー証明書の表示

現在 CMC で使用されている SSL サーバー証明書を表示できます。

ウェブインタフェースを使用したサーバー証明書の表示

CMC ウェブインタフェースで、**シャーシ概要 → ネットワーク → SSL** と移動し、**サーバー証明書の表示** を選択して **次へ** をクリックします。**サーバー証明書の表示** ページに、現在使用中の SSL サーバー証明書が表示されます。詳細については、『CMC オンラインヘルプ』を参照してください。

メモ: サーバー証明書では、共通名はドメイン名（存在する場合）が付加されたラック名として表示されます。ドメイン名がなければ、ラック名のみが表示されます。

RACADM を使用したサーバー証明書の表示

SSL サーバー証明書を表示するには、`sslcertview` コマンドを使用します。詳細に関しては、**dell.com/support/manuals** にある『iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド』を参照してください。

RACADM を使用した複数の CMC の設定

RACADM を使用すると、同じプロパティで 1 つまたは複数の CMC を設定できます。

グループ ID と オブジェクト ID を使って特定の CMC をクエリすると、RACADM は取得した情報から racadm.cfg 設定ファイルを作成します。ファイルを 1 つまたは複数の CMC にエクスポートして、同じプロパティのコントローラを最短の時間で設定できます。

メモ: 一部の設定ファイルには、他の CMC にファイルをエクスポートする前に変更しなければならない固有の CMC 情報（静的 IP アドレスなど）が含まれています。

1. 適切な設定を含むターゲット CMC に RACADM を使ってクエリします。

   メモ: 生成される設定ファイルは **myfile.cfg** です。このファイル名は変更できます。**.cfg** ファイルにはユーザー パスワードは含まれません。新しい CMC に **.cfg** ファイルをアップロードしたら、必ずすべてのパスワードを再度追加してください。
2. CMC への Telnet/SSH テキストコンソールを開いて、ログイン後、次を入力します。

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

   メモ: `getconfig -f` を使用して CMC の設定をファイルにリダイレクトする機能は、リモート RACADM インタフェースでのみサポートされています。
3. テキストのみのエディタ（オプション）を使用して設定ファイルを変更します。設定ファイルに特殊なフォーマット文字を使用すると、RACADM データベースが破損する可能性があります。
4. 新しく作成した設定ファイルを使ってターゲット CMC を変更します。 コマンドプロンプトで、次のコマンドを入力します。

   ```
   racadm getconfig -f myfile.cfg
   ```
5. 設定されたターゲット CMC をリセットします。コマンドプロンプトで、次のコマンドを入力します。

   ```
   racadm reset
   ```

   `getconfig -f myfile.cfg` サブコマンド（手順 1）は、アクティブ CMC の設定を要求し、**myfile.cfg** ファイルを生成します。必要に応じて、ファイル名を変更したり、別の場所に保存することができます。

   getconfig コマンドを使用して、次の操作を実行できます。

   - グループのすべての設定プロパティを表示する（グループ名とインデックスで指定）
   - ユーザーのすべての設定プロパティをユーザー名別に表示する

   `config` サブコマンドは、この情報をその他の CMC にロードします。サーバー管理者は `config` コマンドを使ってユーザーとパスワードのデータベースを同期します。

関連リンク

CMC 設定ファイルの作成

CMC 設定ファイルの作成

CMC 設定ファイル **<ファイル名>.cfg** を racadm config -f <ファイル名>.cfg コマンドで使用して、テキストファイルを作成します。このコマンドを使うと、（**.ini** ファイルに類似した）設定ファイルを作成し、このファイルから CMC を設定することができます。

ファイル名は自由に指定できます。ここでは拡張子 **.cfg** を付けて説明していますが、その必要はありません。

メモ: getconfig サブコマンドの詳細については、『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

RACADM は、CMC に初めてロードされたときに **.cfg** をパースして有効なグループとオブジェクト名が存在し、簡単な構文に適合していることを確認します。エラーには、検出された行番号のフラグと、その問題を説明したメッセージが付きます。正確性についてファイル全体がパースされ、すべてのエラーが表示されます。**.cfg** ファイルにエラーが発見された場合は、CMC への書き込みコマンドは送信されません。ユーザーは、設定を行う前に、すべてのエラーを訂正する必要があります。

設定ファイルを作成する前にエラーをチェックするには、-c オプションを config サブコマンドで使用します。-c オプションを使うと、config は構文を確認するだけで、CMC への書き込みは行いません。

.cfg ファイルを作成するときは、次のガイドラインに従ってください。

- パーサーがインデックス付けされたグループを見つけた場合、さまざまなインデックスの違いはアンカー付きオブジェクトの値で示されます。

  パーサーは、CMC からそのグループのすべてのインデックスを読み取ります。グループ内のオブジェクトは、CMC が設定されたときに修正されたものです。修正されたオブジェクトが新しいインデックスを表す場合、設定中 CMC にそのインデックスが作成されます。
- ユーザーは **.cfg** ファイルの必要なインデックスを指定できません。

  インデックスを作成したり、削除することができます。時間と共に、使用済みおよび未使用のインデックスでグループがフラグメント化される可能性があります。インデックスが存在する場合は、変更されます。インデックスが存在しない場合は、最初に使用できるインデックスが使用されます。

  この方法では、管理しているすべての CMC 間でインデックスの一致をとる必要がないので、インデックス エントリを柔軟に追加できます。新しいユーザーは、最初に使用可能なインデックスに追加されます。1 つの CMC で正しくパースおよび実行される **.cfg** ファイルは、すべてのインデックスが一杯で新しいユーザーを追加しなければならない場合に、別の CMC では正しく実行されない場合があります。
- 同等のプロパティを持つ CMC を両方共に設定するには、racresetcfg サブコマンドを使用します。

  racresetcfg サブコマンドを使って CMC をデフォルトにリセットした後、racadm config -f <filename>.cfg コマンドを実行します。**.cfg** ファイルに、必要なオブジェクト、ユーザー、インデックス、およびその他のパラメータがすべて含まれていることを確認します。オブジェクトとグループの完全なリストについては、『*iDRAC6 および CMC 向け RACADM コマンドラインリファレンスガイド*』のデータベースプロパティの章を参照してください。

  注意: racresetcfg サブコマンドを使用して、データベースと CMC ネットワークインタフェース設定を元のデフォルト設定にリセットし、すべてのユーザーとユーザー設定を削除します。root ユーザーは使用可能ですが、その他のユーザー設定もデフォルト設定にリセットされます。
- racadm getconfig -f <ファイル名> .cfg と入力すると、このコマンドは現在の CMC 設定のために **.cfg** ファイルを作成します。この設定ファイルは、固有の **.cfg** ファイルの使用例または開始点として利用できます。

関連リンク

構文解析規則

構文解析規則

- ハッシュ文字 (#) で始まる行はコメントとして取り扱われます。

  コメント行は一列目から記述する必要があります。その他の列の「#」文字は単に # 文字として扱われます。

  モデムパラメータでは文字列に # 文字が含まれている場合があります。エスケープ文字は必要ありません。racadm getconfig -f <filename> .cfg コマンドで **.cfg** を生成し、エスケープ文字を追加せずに、racadm config -f <filename> .cfg コマンドを異なる CMC 上で実行します。

  たとえば、次のとおりです。

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

- グループエントリはすべて大カッコ（[と]）で囲む必要があります。

  グループ名を示す右カッコ（[）は一列目になければなりません。このグループ名は、そのグループ内の他のオブジェクトよりも前に指定する必要があります。関連するグループ名が含まれていないオブジェクトは、エラーを生成します。構成データは、『*iDRAC6 および CMC 向け RACADM コマンドラインリファレンスガイド*』のデータベースプロパティの章で定義されているようにグループ化されます。次に、グループ名、オブジェクト、およびオブジェクトのプロパティ値の使用例を示します。

  ```
  [cfgLanNetworking] -{group name} cfgNicIpAddress=143.154.133.121 {object
  name} {object value}
  ```

- すべてのパラメータは、オブジェクト、=、または値の間に空白を入れずに「オブジェクト=値」のペアとして指定されます。値の後にあるスペースは無視されます。値の文字列内にあるスペースは変更されません。= の右側の文字はそのまま使用されます（例： 2 つ目の =、#、[、]、など）。これらの文字は、有効なモデムチャットスクリプト文字です。

  ```
  [cfgLanNetworking] -{group name} cfgNicIpAddress=143.154.133.121 {object
  name} {object value}
  ```

- **.cfg** パーサーはインデックスオブジェクトエントリを無視します。

  ユーザーは、使用するインデックスを指定できません。索引が既に存在する場合は、それが使用されます。索引がない場合は、そのグループで最初に使用可能な索引に新しいエントリが作成されます。

  racadm getconfig -f <filename>.cfg コマンドは、インデックスオブジェクトの前にコメントを配置するため、ここでコメントを確認できます。

  メモ: 次のコマンドを使用すると、インデックスグループを手動で作成できます。

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

- インデックス付きグループの行を **.cfg** ファイルから削除することはできません。この行をテキストエディタで削除すると、RACADM は設定ファイルをパースするときに停止し、エラー警告を発します。

  次のコマンドを使用して、手動でインデックスオブジェクトを削除する必要があります。

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

  メモ: NULL 文字列（2 つの " 文字で示される）は、指定したグループの索引を削除するように CMC に命令します。

  インデックス付きグループの内容を表示するには、次のコマンドを実行します。

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

- インデックス付きグループの場合、オブジェクトアンカーが [ ] ペアの後の最初のオブジェクトである必要があります。次に、現在のインデックス付きグループの例を示します。

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

- 設定グループをファイルにキャプチャするためにリモート RACADM を使用する際、グループ内でキープロパティが設定されていない場合は、設定グループは設定ファイルの一部として保存されません。別の CMC でこれらの設定グループをレプリケートするには、getconfig -f コマンドを実行する前に、キープロパティを設定します。あるいは、getconfig -f コマンドを実行した後で、欠落して

いるプロパティを手動で設定ファイルに入力します。これは、racadm インデックス付きグループのすべてに適用されます。
次は、この動作と対応するキープロパティを示したインデックス化されたグループを一覧にしたものです。

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

CMC IP アドレスの変更

設定ファイルで CMC の IP アドレスを変更する場合は、不必要なすべての <変数>=<値> エントリを削除します。IP アドレスの変更に関する 2 つの <変数>=<値> エントリを含む、[と] で囲まれた実際の変数グループのラベルのみが残ります。

例：

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

このファイルは次のように更新されます。

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

コマンド `racadm config -f <myfile>.cfg` はファイルを解析し、行番号によってすべてのエラーを識別します。正しいファイルは適切なエントリをアップデートします。また、前の例で示されたのと同じ `getconfig` コマンドを使用して、更新を確認することもできます。

このファイルを `racadm getconfig -f <myfile> .cfg<` と併用して、全社的な変更をダウンロードしたり、新しいシステムをネットワーク経由で設定することができます。

メモ: *アンカー*は予約語のため、**.cfg** ファイルでは使用しないでください。

CMC セッションの表示と終了

現在 iDRAC7 にログインしているユーザー数を表示し、ユーザーセッションを終了することができます。

メモ: セッションを終了するには、**シャーシ設定システム管理者** の権限が必要です。

ウェブインタフェースを使用した CMC セッションの表示と終了

ウェブインタフェースを使用してセッションを表示または終了するには：

1. システムツリーで、**シャーシ概要** へ移動し、**ネットワーク → セッション** をクリックします。
   セッション ページにはセッション ID、ユーザー名、IP アドレス、およびセッションタイプが表示されます。これらのプロパティの詳細については、『*CMC オンラインヘルプ*』を参照してください。
2. セッションを終了するには、セッションで **終了** をクリックします。

RACADM を使用した CMC セッションの表示と終了

RACADM を使用して CMC セッションを終了するには、システム管理者権限が必要です。

現在のユーザーセッションを表示するには、`getssninfo` コマンドを使用します。

ユーザーセッションを終了するには、`closessn` コマンドを使用します。

これらのコマンドの詳細については、**dell.com/support/manuals** にある『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

7

サーバーの設定

サーバーに対して以下を実行できます。

- スロット名の設定
- iDRAC ネットワークの設定
- iDRAC VLAN タグの設定
- 最初の起動デバイスの設定
- サーバー FlexAddress の設定
- リモートファイル共有の設定
- サーバークローンを使用した BIOS の設定

スロット名の設定

スロット名は個別のサーバーを識別するために使用します。スロット名を選択するとき、次のルールが適用されます。

- 名前には、非拡張 ASCII 文字（ASCII コード 32 から 126 まで）を**最大 15 文字**含めることができます。
- スロット名はシャーシ内で一意でなければなりません。複数のスロットに同じ名前を割り当てることはできません。
- スロット名では大文字と小文字は区別されません。`Server-1, server-1, and SERVER-1` はすべて同じ名前と見なされます。
- スロット名には、次の文字列で始まる名前を付けることはできません。
  - `Switch-`
  - `Fan-`
  - `PS-`
  - `KVM`
  - `DRAC`
  - `MC-`
  - `Chassis`
  - `Housing-Left`
  - `Housing-Right`
  - `Housing-Center`
- `Server-1` から `Server-16` までの文字列を使用することはできますが、対応するスロットに割り当てる必要があります。たとえば、`Server-3` はスロット **3** では有効ですが、スロット **4** では無効です。ただし、`Server-03` は、どのスロットに対しても有効な名前です。

  メモ: スロット名の変更は、必ず**シャーシ設定管理者**の権限で行ってください。

ウェブインタフェースでのスロット名の設定は、CMC 内でのみ保存されています。サーバーがシャーシから取り外されても、スロット名の設定はスロットに残ります。

スロット名の設定は、オプションの iKVM に対応していません。スロット名の情報は、iKVM FRU から入手可能です。

CMC ウェブインタフェースで設定したスロット名の設定は、iDRAC インタフェースに表示されている名前の変更に常に優先します。

CMC ウェブインタフェースを使用してスロット名を編集するには：

1. システムツリーで、**シャーシの概要** → **サーバーの概要** へ移動し、**セットアップ** → **スロット名** をクリックします。**スロット名** ページが表示されます。
2. **スロット名** フィールドでスロット名を編集します。名前を変更する各スロットについてこの手順を繰り返します。
3. サーバーのホスト名をスロット名として使用するには、**ホスト名を使用** を **スロット名** オプションで選択します。これにより、静的なスロット名がサーバーのホスト名（またはシステム名）で上書きされます。この操作には、サーバーに OMSA エージェントをインストールすることが必要です。OMSA エージェントの詳細については、『*Dell OpenManage Server Administrator ユーザーズガイド*』を参照してください。
4. 設定を保存するには、**適用** をクリックします。
5. サーバーに対してデフォルトのスロット名（サーバーのスロット位置に応じて **SLOT-01**～**SLOT-16**）に戻すには、**デフォルト値に戻す** をクリックします。

iDRAC ネットワークの設定

インストール済みの新規に挿入されたサーバーの iDRAC ネットワークの設定を行うことができます。ユーザーは、装着されている 1 つまたは複数の iDRAC デバイスを設定できます。また、後でインストールする予定のサーバーのデフォルトの iDRAC ネットワーク設定とルートパスワードを設定することもできます。このデフォルトの設定が iDRAC QuickDeploy 設定です。

iDRAC の詳細については、**dell.com/support/manuals** にある『*iDRAC ユーザーズガイド*』を参照してください。

関連リンク

iDRAC QuickDeploy ネットワーク設定
個々のサーバー iDRAC の iDRAC ネットワーク設定の変更
RACADM を使用した iDRAC ネットワーク設定の変更

iDRAC QuickDeploy ネットワーク設定

QuickDeploy 設定を使用して、新規に挿入されたサーバーに対するネットワーク設定を行います。QuickDeploy を有効にした後、サーバーがインストールされると QuickDeploy 設定がサーバーに適用されます。

CMC ウェブインタフェースを使用して iDRAC QuickDeploy 設定を有効にして設定するには、次の手順を実行します。

1. システムツリーで、**サーバー概要** に移動し、**セットアップ** → **iDRAC** をクリックします。**iDRAC の導入** ページが表示されます。
2. **QuickDeploy 設定** セクションで、次の表に示される設定を指定します。

表 13. ：QuickDeploy 設定

設定	説明
QuickDeploy の有効化	新規に挿入されたサーバーに対してこのページで設定した iDRAC に自動的に表示する **QuickDeploy** 機能を有効 / 無効にします。自動確認は必ずローカルの LCD パネルで確認します。

設定	説明
	メモ: これには、**サーバー追加時に iDRAC ルート パスワードを設定する** ボックスをチェックしたときのルートユーザーパスワードが含まれます。 このオプションはデフォルトでは無効になっています。
サーバープロファイル展開の有効化	プロファイルが **プロファイル** ページ上でスロットに割り当てられている場合は、LCD パネル上での確認後、新規に挿入されたサーバーへのプロファイルの導入が有効になります。
サーバー挿入で iDRAC root パスワードを設定	サーバーを挿入したとき、サーバーの iDRAC ルート パスワードを **iDRAC ルートパスワード** フィールドに表示される値に変更するかどうかを指定します。
iDRAC root パスワード	**サーバー挿入時に iDRAC ルートパスワードを設定する** および **QuickDeploy を有効にする** オプションが選択されている場合、シャーシにサーバーが挿入されたときに、このパスワードがサーバーの iDRAC ルート パスワードに割当てられます。パスワードは、印刷可能な 1～20 文字（スペース含む）で指定します。
iDRAC root パスワードの確認	**iDRAC ルート パスワード** フィールドに入力されたパスワードを確認します。
iDRAC LAN を有効にする	iDRAC LAN チャネルを有効または無効にします。このオプションはデフォルトでは無効になっています。
iDRAC IPv4 を有効にする	iDRAC での IPv4 を有効または無効にします。このオプションはデフォルトでは有効になっています。
iDRAC IPMI オーバー LAN を有効にする	シャーシに搭載されている各 iDRAC の IPMI オーバー LAN チャンネルを有効または無効にします。デフォルトでは無効になっています。
iDRAC DHCP を有効にする	シャーシに搭載されている各 iDRAC の IPMI オーバー LAN チャンネルを有効または無効にします。このオプションを有効にすると、**QuickDeploy IP** ゲートウェイ **QuickDeploy サブネットマスク**、および **QuickDeploy ゲートウェイ** フィールドが無効になります。これらの設定は、DHCP を使用して各 iDRAC に自動的に割り当てられるため、変更できません。このオプションはデフォルトでは無効になっています。
iDRAC IPv4 アドレス（スロット 1）をスタート中	エンクロージャのスロット 1 に搭載されているサーバーの iDRAC の固定 IP アドレスを指定します。各後続 iDRAC の IP アドレスは、スロットごとにスロット 1 の IP アドレスから 1 ずつ増加します。IP

設定	説明
	アドレスにスロット数を足した値がサブネットマスクより大きいと、エラー メッセージが表示されます。 **メモ:** サブネットマスクとゲートウェイは、IP アドレスのように増加しません。 たとえば、IP アドレスが 192.168.0.250 から始まり、サブネットマスクが 255.255.0.0 のとき、スロット 15 の QuickDeploy IP アドレスは 192.168.0.265 です。サブネットマスクが 255.255.255.0 のとき、**QuickDeploy 設定を保存する** または **QuickDeploy 設定を使用して自動入力する** をクリックすると、QuickDeploy IP address range is not fully within QuickDeploy Subnet というエラーメッセージが表示されます。
iDRAC IPv4 ネットマスク	新規に挿入されたすべてのサーバーに割当てられた QuickDeploy サブネットマスクを指定します。
iDRAC IPv4 ゲートウェイ	シャーシに搭載されているすべての iDRAC に割当てる QuickDeploy デフォルトゲートウェイを指定します。
iDRAC IPv6 を有効にする	IPv6 対応のシャーシ内にある各 iDRAC の IPv6 アドレス設定を有効にします。
iDRAC IPv6 自動設定を有効にする	iDRAC が DHCPv6 サーバーから IPv6 設定（アドレスおよびプレフィックス長）を取得できるようにします。また、ステートレスなアドレスの自動構成も有効にします。このオプションはデフォルトでは有効になっています。
iDRAC IPv6 ゲートウェイ	デフォルトの IPv6 ゲートウェイが iDRAC に割り当てられるように指定します。デフォルト値は "::" です。
iDRAC IPv6 プレフィックス長	プレフィックス長が iDRAC 上の IPv6 アドレスに対して割り当てられるように指定します。デフォルト値は 64 です。

3. **QuickDeploy 設定を保存する** をクリックして設定を保存します。iDRAC ネットワークの設定を変更した場合は、**iDRAC ネットワーク設定を適用する** をクリックして設定を iDRAC に導入します。

   QuickDeploy 機能は、有効にした場合および、シャーシにサーバーを挿入したときにのみ実行できます。**サーバー挿入時に iDRAC ルートパスワードを設定する** および **QuickDeploy を有効にする** が有効の場合、LCD インタフェースでパスワードの変更を有効にする（または無効にする）かどうかのメッセージが表示されます。現行の iDRAC 設定と異なるネットワーク構成がある場合は、変更を許可する（または許可しない）かどうかを尋ねるメッセージが表示されます。

   メモ: LAN または LAN オーバー IPMI が異なる場合は、QuickDeploy IP アドレス設定を許可するかどうかを尋ねるメッセージが表示されます。DHCP 設定が異なる場合は、DHCP QuickDeploy 設定を許可するかどうかを尋ねるメッセージが表示されます。

   QuickDeploy 設定を **iDRAC ネットワーク設定** セクションにコピーするには、**QuickDeploy 設定を使用して自動入力する** をクリックします。QuickDeploy ネットワーク構成設定が、 **iDRAC ネットワーク構成設定** テーブルの対応するフィールドにコピーされます。

メモ: QuickDeploy フィールドの変更は即座に実施されますが、1 つまたは複数の iDRAC サーバーネットワーク構成を変更した場合は、CMC から iDRAC に反映されるまで数分かかる場合があります。**更新** を押すタイミングが早すぎると、iDRAC サーバーのデータが部分的にしか正しく表示されない場合があります。

個々のサーバー iDRAC の iDRAC ネットワーク設定の変更

この表を使用すると、インストールされている各サーバーの iDRAC ネットワーク設定を行うことができます。各フィールドに表示される初期値は、iDRAC から読み込まれた現在の値です。

CMC ウェブインタフェースを使用して iDRAC ネットワーク設定を変更するには :

1. システムツリーで、**サーバーの概要** へ移動し、**セットアップ → iDRAC** をクリックします。 **iDRAC の導入** ページが表示されます。**iDRAC ネットワーク設定** セクションには、インストールされているすべてのサーバーの iDRAC IPv4 および IPv6 ネットワーク設定が表示されます。
2. サーバーの必要に応じて、iDRAC ネットワーク設定を変更します。

   メモ: IPv4 または IPv6 設定を指定するには、**LAN を有効にする** オプションを選択する必要があります。フィールドについての情報は、『iDRAC7 オンラインヘルプ』を参照してください。
3. iDRAC に設定を適用するには、**iDRAC ネットワーク設定を適用する** をクリックします。QuickDeploy 設定に変更を加えた場合は、それらも保存されます。

   iDRAC ネットワーク設定 表は、将来のネットワーク構成を反映するため、インストールされているサーバーに対して表示されている値は、現在インストールされている iDRAC ネットワーク構成と一致しない場合もあります。**更新** をクリックして変更後の iDRAC ネットワーク構成で **iDRAC の導入** ページを更新します。

   メモ: QuickDeploy フィールドの変更は即座に実施されますが、1 つまたは複数の iDRAC サーバーネットワーク構成を変更した場合は、CMC から iDRAC に反映されるまで数分かかる場合があります。**更新** をクリックするタイミングが早すぎると、1 つまたは複数の iDRAC サーバーのデータが部分的にしか正しく表示されない場合があります。

RACADM を使用した iDRAC ネットワーク設定の変更

RACADM `config` または `getconfig` コマンドでは、次の設定グループに対する `-m <モジュール>` オプションがサポートされています。

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

プロパティのデフォルト値および範囲の詳細は、『*RACADM コマンドライン iDRAC7 および CMC 向けリファレンスガイド*』を参照してください。

iDRAC VLAN タグの設定

VLAN を使用すると、複数の仮想 LAN が同じ物理ネットワーク上で共存でき、セキュリティやロード管理の目的でネットワークトラフィックを分離できます。VLAN 機能を有効にすると、各ネットワークパケットに VLAN タグが割り当てられます。VLAN タグはシャーシプロパティです。このタグは、コンポーネントを削除した後もシャーシに残ります。

ウェブインタフェースを使用した iDRAC VLAN タグの設定

CMC ウェブインタフェースを使用してサーバー用 VLAN を設定するには、次の手順を実行します。

1. 次のいずれかのページに移動します。
   - システムツリーで、**シャーシ概要**□ へ移動し、**ネットワーク → VLAN**□をクリックします。
   - システムツリーで、**シャーシ概要**□ **→ サーバー概要** へ移動し、 **ネットワーク → VLAN**□ をクリックします。**VLAN タグの設定** ページが表示されます。
2. **iDRAC** セクションで、サーバー用の VLAN を有効にし、優先順位を設定して ID を入力します。フィールドについての情報は、『*CMC オンラインヘルプ*』を参照してください。
3. 設定を保存するには、**適用** をクリックします。

RACADM を使用した iDRAC VLAN タグの設定

- 次のコマンドで、特定のサーバーの VLAN ID と優先順位を指定します。

  ```
  racadm setniccfg -m server-<n> -v <VLAN id> <VLAN priority>
  ```

  <n> の有効値は 1～16 です。

  <VLAN> に指定できる値は 1～4000、および 4021～4094 の範囲の数値です。デフォルトは 1 です。

  <VLAN priority> の有効値は 0～7 です。デフォルトは 0 です。

  たとえば、次のとおりです。

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

  たとえば、次のとおりです。

- サーバー VLAN を削除するには、指定したサーバーのネットワークの VLAN 機能を無効にします。

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

  <n> の有効値は 1～16 です。

  たとえば、次のとおりです。

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

最初の起動デバイスの設定

各サーバーについて、CMC の最初の起動デバイスを指定できます。これはサーバーの実際の最初の起動デバイスでなくてもよく、またそのサーバー上に存在するデバイスでなくてもかまいません。ここで指定するのは、CMC によってサーバーに送信されるデバイスであり、このデバイスはそのサーバーに対する最初の起動デバイスとして利用されます。

デフォルト起動デバイスを設定できるほか、Diagnostics（診断）の実行や OS の再インストールなどのタスクを実行するためのイメージから起動できるように、1 回限りの起動デバイスを設定することも可能です。

次回起動のみ、または後続のすべての再起動用に、最初の起動デバイスを選択できます。この選択に基づいて、サーバーの最初の起動デバイスを設定できます。システムは、次回および後続の再起動時に選択されたデバイスから起動し、そのデバイスは CMC ウェブインタフェースまたは BIOS 起動順序から再び変更されない限り、BIOS 起動順序に最初の起動デバイスとして保持されます。

メモ: CMC ウェブインタフェースで最初の起動デバイスの設定は、システム BIOS 起動設定を上書きします。

指定する起動デバイスは存在するもので、ブータブルメディアを含む必要があります。

次のデバイスについて、最初の起動デバイスを設定できます。

表 14. : 起動デバイス

起動デバイス	説明
PXE	ネットワークインタフェースカードの PXE (プレブート実行環境) プロトコルから起動します。
ハードドライブ	サーバーのハードディスクドライブから起動します。
ローカル CD/DVD	サーバー上の CD/DVD ドライブから起動します。
仮想フロッピー	仮想フロッピードライブから起動します。フロッピードライブ (またはフロッピーディスクイメージ) は管理ネットワーク上の別のコンピュータ上にあり、iDRAC GUI コンソールビューアで接続されます。
仮想 CD/DVD	仮想 CD/DVD ドライブまたは CD/DVD ISO イメージから起動します。この光学ドライブまたは ISO イメージファイルは管理ネットワーク上の別のコンピュータまたはディスク上にあり、iDRAC GUI コンソールビューアで接続されます。
iSCSI	iSCSI (インターネット小型コンピュータシステムインタフェース) デバイスから起動します。
ローカル SD カード	ローカル SD カードから起動します。(iDRAC6 および iDRAC7 システムをサポートするサーバーでのみ可能。)
フロッピー	ローカルのフロッピーディスクドライブにあるフロッピーディスクから起動します。
RFS	リモートファイル共有 (RFS) イメージから起動します。イメージファイルは iDRAC GUI コンソールビューアで接続されます。

関連リンク

CMC ウェブインタフェースを使用した複数サーバーの最初の起動デバイスの設定
CMC ウェブインタフェースを使用した個々のサーバーの最初の起動デバイスの設定
RACADM を使用した最初の起動デバイスの設定

CMC ウェブインタフェースを使用した複数サーバーの最初の起動デバイスの設定

メモ: サーバーの最初の起動デバイスを設定するには、**サーバー管理者** 特権または **シャーシ設定システム管理者** 特権、および **iDRAC ログイン**特権 を持っている必要があります。

CMC ウェブインタフェースを使用して複数サーバーの最初の起動デバイスを設定するには :

1. システムツリーで、**サーバーの概要** へ移動し、**セットアップ → 最初の起動デバイス** をクリックします。サーバーのリストが表示されます。
2. **最初の起動デバイス** 列のドロップダウンメニューから、各サーバーに使用する起動デバイスを選択します。
3. 選択した同じデバイスから毎回起動するようにサーバーを設定するには、そのサーバーの **1 回限りの起動** チェックボックスの選択を解除します。選択したデバイスから次回のみ起動するようにサーバーを設定するには、そのサーバーの **1 回限りの起動** チェックボックスを選択します。
4. 設定を保存するには、**適用** をクリックします。

CMC ウェブインタフェースを使用した個々のサーバーの最初の起動デバイスの設定

サーバーの第 1 起動デバイスを設定するには、**サーバー管理者** 特権または **シャーシ設定システム管理者** 特権、および **iDRAC ログイン特権** を持っている必要があります。

CMC ウェブインタフェースを使用して個々のサーバーの最初の起動デバイスを設定するには：

1. システムで **サーバーの概要** に移動し、最初の起動デバイスを設定するサーバーをクリックします。
2. **セットアップ → 最初の起動デバイス** に移動します。**最初の起動デバイス** ページが表示されます。
3. **最初の起動デバイス** ドロップダウンメニューで、各サーバーに使用する起動デバイスをリストボックスから選択します。
4. 選択した同じデバイスから毎回起動するようにサーバーを設定するには、そのサーバーの **ブートワンス** オプションの選択を解除します。選択したデバイスから次回のみ起動するようにサーバーを設定するには、そのサーバーの **ブートワンス** オプションを選択します。
5. **適用** をクリックして設定を保存します。

RACADM を使用した最初の起動デバイスの設定

最初の起動デバイスを設定するには、`cfgServerFirstBootDevice` オブジェクトを使用します。

デバイスで 1 度だけ起動することを有効にするには、`cfgServerBootOnce` オブジェクトを使用します。

これらのオブジェクトの詳細については、**dell.com/support/manuals** にある『*iDRAC および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

サーバーでの FlexAddress の設定

サーバーでの FlexAddress の設定に関する情報は、サーバーレベルスロットでの FlexAddress の設定 を参照してください。

リモートファイル共有の設定

リモート仮想メディアのファイル共有 機能は、ネットワーク上の共有ドライブのファイルを CMC を介して 1 つまたは複数のサーバーにマッピングし、オペレーティングシステムを導入または更新します。接続が完了すると、リモートファイルはローカルシステムにある場合と同様にアクセス可能になります。サポートされている 2 つのメディアの種類はフロッピーディスクと CD/DVD ドライブです。

リモートファイル共有操作（接続、切断、導入）を行うには、**シャーシ設定システム管理者** または **サーバー管理者** の権限が必要です。

CMC ウェブインタフェースを使用してリモートファイル共有を設定するには、次の手順を実行します。

1. システムツリーで **サーバー概要** に進み、次に **セットアップ → リモートファイル共有** とクリックします。
   リモートファイル共有の展開 ページが表示されます。

   メモ: スロット内のサーバーのいずれかが第 12 世代以降であり、適切なライセンスがない場合は、必要なライセンスが欠落している、または失効していることを示すメッセージが表示されます。適切なライセンスを取得してから再試行するか、サービスプロバイダに追加詳細についてお問い合わせいただく必要があります。
2. 必要な設定を指定します。詳細については、『*CMC オンラインヘルプ*』を参照してください。
3. **接続** をクリックしてリモートファイル共有に接続します。リモートファイル共有を接続するには、パス、ユーザー名、パスワードを指定する必要があります。操作に成功すると、メディアにアクセスできます。

接続解除 をクリックすると、前に接続したリモートファイル共有を接続解除できます。

導入 をクリックすると、メディアデバイスを導入できます。

メモ: この処置はサーバーを再起動させることから、メディアデバイスを導入するための **導入** オプションを選択する前に、すべての作業ファイルを保存してください。

この処置では、以下が行われます。

- リモートファイル共有が接続される。
- ファイルがサーバーの最初の起動デバイスとして選択される。
- サーバーが再起動される。
- サーバーの電源が切れている場合は、電源がサーバーに投入される。

サーバー設定複製を使用したプロファイル設定の実行

サーバー設定複製機能によって、特定のサーバーからすべてのプロファイル設定を 1 台または複数台のサーバーに適用することができます。変更可能で、サーバー全体で複製されることが目的とされているプロファイル設定のみが複製可能です。以下の 3 つのプロファイルグループが表示され、複製可能です。

- BIOS — このグループには、サーバーの BIOS 設定のみが含まれます。これらプロファイルは、 4.3 バージョンより前の CMC から生成されます。
- BIOS および起動 — このグループには、サーバーの BIOS および起動設定が含まれます。これらのプロファイルは、以下から生成されます。
  - CMC バージョン 4.3
  - 第 11 世代サーバーにおける CMC バージョン 4.45
  - CMC バージョン 4.45、およびバージョン 1.1 より前の Lifecycle Controller 2 を搭載した第 12 世代サーバー
- すべての設定 — このバージョンには、サーバーとそのサーバー上のコンポーネントのすべての設定が含まれます。これらプロファイルは CMC バージョン 4.45、および iDRAC7 with Lifecycle Controller 2 バージョン 1.1 以降を搭載した第 12 世代サーバーから生成されます。

サーバー設定複製機能は iDRAC6 サーバーおよび iDRAC7 サーバーをサポートします。古い世代の RAC サーバーがリストされますが、メインページではグレー表示になり、この機能の使用は有効になりません。

サーバー設定複製機能を使用するには、以下が必要です。

- iDRAC が必要最低限のバージョンになっている。iDRAC6 サーバーは 3.2、iDRAC7 サーバーは 1.00.00 が最低限必要なバージョンです。
- サーバーの電源がオンになっている。

サーバーバージョンおよびプロファイルの互換性は次のとおりです。

- iDRAC7 with Lifecycle Controller 2 バージョン 1.1 は、どのプロファイルバージョンにも対応します。
- iDRAC6 バージョン 3.2 および iDRAC7 with Lifecycle Controller 2 バージョン 1.0 は、BIOS または BIOS および起動プロファイルのみに対応します。
- iDRAC7 with Lifecycle Controller 2 バージョン 1.1 搭載のサーバーからプロファイルを保存すると、プロファイルはすべての設定プロファイルになります。iDRAC6 V3.2 および iDRAC7 with LC2V1 搭載のサーバーからプロファイルを保存すると、プロファイルは BIOS および起動プロファイルになります。

次の操作が可能です。

- サーバーまたは保存プロファイルからプロファイル設定を表示する。
- サーバーからのプロファイルを保存する。
- プロファイルを別のサーバーに適用する。

- リモートファイル共有から保存プロファイルをインポートする。
- プロファイルの名前と説明を編集する。
- 保存プロファイルをリモートファイル共有にエクスポートする。
- 保存プロファイルを削除する。
- **Quick Deploy** オプションを使って選択したプロファイルをターゲットデバイスに展開する。
- 最近のサーバープロファイルタスクのログアクティビティを表示する。

関連リンク

サーバープロファイルページへのアクセス
プロファイルの追加または保存
プロファイルの適用
プロファイル設定の表示
プロファイルログの表示
完了状態とトラブルシューティング

サーバープロファイルページへのアクセス

サーバープロファイル ページを使用して、1 つまたは複数のサーバーに対してサーバープロファイルの追加、管理、および適用を行うことができます。

CMC ウェブインタフェースを使用して **サーバープロファイル** ページにアクセスするには、システムツリーで **シャーシ概要 → サーバー概要** に移動します。**セットアップ → プロファイル** をクリックします。**サーバープロファイル** ページが表示されます。

関連リンク

プロファイルの追加または保存
プロファイルの適用
プロファイル設定の表示
プロファイルログの表示
完了状態とトラブルシューティング

プロファイルの追加または保存

サーバーのプロパティをクローンする前に、まずプロパティを保存プロファイルにキャプチャします。保存プロファイルを作成して、各プロファイルに名前および説明（オプション）を入力します。CMC 不揮発性拡張ストレージメディアには、最大 16 の保存プロファイルを保存することができます。

不揮発性ストレージメディアを取り外すか無効にすると、保存プロファイルにアクセスできなくなり、サーバークローニング機能が無効になります。

プロファイルを追加または保存するには、次の手順を実行します。

1. **サーバープロファイル** ページに進みます。**サーバープロファイル** セクションで、プロファイルの生成元となるサーバーを選択し、**プロファイルの保存** をクリックします。

   サーバープロファイルの保存 セクションが表示されます。

2. **プロファイル名** および **説明** フィールドに、プロファイル名と説明（オプション）を入力し、**プロファイルの保存** をクリックします。

   CMC が LC と通信して利用可能なサーバープロファイル設定を取得し、それらを命名したプロファイルとして保存します。

   進捗状況インジケータが、進行中の保存操作を示します。この処置が完了したら、「操作成功」メッセージが表示されます。

   メモ: 設定を収集するプロセスはバックグラウンドで実行されることから、新しいプロファイルが表示されるまでしばらく時間がかかることがあります。新しいプロファイルが表示されない場合、プロファイルログでエラーをチェックしてください。

関連リンク

サーバープロファイルページへのアクセス

プロファイルの適用

サーバークローニングは、サーバープロファイルが CMC 上の不揮発性メディアで保存プロファイルとして使用できる場合にのみ可能です。サーバークローニング操作を開始するには、保存プロファイルを 1 台または複数台のサーバーに適用することができます。

メモ: サーバーが Lifecycle Controller をサポートしていない場合や、シャーシの電源がオフになっている場合は、プロファイルをサーバーに適用できません。

プロファイルを 1 つ、または複数のサーバーに適用するには、次の手順を実行します。

1. **サーバープロファイル** ページに進みます。**プロファイルの保存と適用** セクションで、選択したプロファイルを適用するサーバーを 1 台または複数台選択します。
   プロファイルの選択 ドロップダウンメニューが有効化されます。
2. **プロファイルの選択** ドロップダウンメニューから、適用するプロファイルを選択します。
   プロファイルの適用 オプションが有効化されます。
3. **プロファイルの適用** をクリックします。
   新しいサーバープロファイルの適用は現在の設定を上書きし、選択したサーバーを再起動するという警告メッセージが表示されます。操作を続行する場合は、それを確認するプロンプトが表示されます。

   メモ: サーバークローニング操作をサーバーで実行するには、サーバーに対する CSIOR オプションが有効になっている必要があります。CSIOR オプションが無効の場合、CSIOR がサーバーに対して有効になっていないという警告メッセージが表示されます。ブレードのクローニング操作を完了するためには、サーバーで CSIOR オプションを有効化するようにしてください。
4. **OK** をクリックして、選択したサーバーにプロファイルを適用します。
   選択したプロファイルがサーバーに適用され、サーバーは必要に応じて直ちに再起動される場合があります。詳細については、『CMC オンラインヘルプ』を参照してください。

関連リンク

サーバープロファイルページへのアクセス

プロファイルのインポート

リモートファイル共有に保存されたサーバープロファイルを CMC にインポートすることができます。

リモートファイル共有に保存されたプロファイルをインポートするには、次の手順を実行します。

1. **サーバープロファイル** ページの **SD カード上のプロファイル** セクションで、**プロファイルのインポート** をクリックします。
   サーバープロファイルのインポート セクションが表示されます。
2. **参照** をクリックし、必要な場所からのプロファイルにアクセスしてから、**プロファイルのインポート** をクリックします。
   詳細については、『*CMC オンラインヘルプ*』を参照してください。

プロファイルのエクスポート

CMC 不揮発性メディア（SD カード）に保存された保存サーバープロファイルは、リモートファイル共有の指定されたパスにエクスポートすることができます。

保存されたプロファイルをエクスポートするには、次の手順を実行します。

1. **サーバープロファイル** ページに進みます。**SD カード上のプロファイル** セクションで、必要なプロファイルを選択してから **プロファイルのエクスポート** をクリックします。
   ファイルを開くか保存するかをたずねる **ファイルのダウンロード** メッセージが表示されます。
2. **保存** または **開く** をクリックして、プロファイルを必要な場所にエクスポートします。
   詳細については、『*CMC オンラインヘルプ*』を参照してください。

プロファイルの編集

CMC 不揮発性メディア（SD カード）に保存されたサーバープロファイルの名前と説明を編集することができます。
保存されたプロファイルを編集するには、次の手順を実行します。

1. **サーバープロファイル** ページに進みます。**SD カード上のプロファイル** セクションで、必要なプロファイルを選択してから **プロファイルの編集** をクリックします。
   BIOS プロファイルの編集 — <プロファイル名> セクションが表示されます。
2. 必要に応じてサーバープロファイルの名前と説明を編集し、**プロファイルの編集** をクリックします。
   詳細については、『*CMC オンラインヘルプ*』を参照してください。

プロファイルの削除

CMC 不揮発性メディア（SD カード）に保存されたサーバープロファイルを削除することができます。
保存されたプロファイルを削除するには、次の手順を実行します。

1. **サーバープロファイル** ページの **SD カード上のプロファイルの管理** セクションで、必要なプロファイルを選択してから **プロファイルの削除** をクリックします。
   プロファイルを削除すると選択したプロファイルが恒久的に削除されるという警告メッセージが表示されます。
2. **OK** をクリックして、選択したプロファイルを削除します。
   詳細については、『*CMC オンラインヘルプ*』を参照してください。

プロファイル設定の表示

選択したサーバーの **プロファイル設定** を表示するには、**サーバープロファイル** ページに進みます。**サーバープロファイル** セクションで、対象サーバーの **サーバープロファイル** 行で **表示** をクリックします。**表示の設定** ページが表示されます。
表示設定の詳細については、『CMC オンラインヘルプ』を参照してください。

メモ: CMC サーバークローニングアプリケーションは、CSIOR（**Collect System Inventory on Restart**）オプションが有効の場合に限り、特定のサーバーの設定を取得して表示します。

CSIOR を有効にするには、次の手順を実行します。

- 第 11 世代サーバー — サーバーを再起動した後、**Ctrl-E** セットアップから、**システムサービス** を選択して **CSIOR** を有効にし、変更を保存します。
- 第 12 世代サーバー — サーバーを再起動した後、**F2** セットアップから、**iDRAC 設定 → Lifecycle Controller** を選択して **CSIOR** を有効にし、変更を保存します。

関連リンク

サーバープロファイルページへのアクセス

保存プロファイル設定の表示

CMC 不揮発性メディア（SD カード）に保存されているサーバープロファイルのプロファイル設定を表示するには、**サーバープロファイル** ページに進みます。**SD カード上のプロファイル** セクションで、対象サーバーの **プロファイルの表示** 列で **表示** をクリックします。**設定の表示** ページが表示されます。設定の表示に関する詳細については、『CMC オンラインヘルプ』を参照してください。

プロファイルログの表示

プロファイルログを表示するには、**サーバープロファイル** ページで、**最近のプロファイルログ** セクションを確認します。このセクションは、サーバークローニング操作から 10 件の最新プロファイルログエントリを直接表示します。各ログエントリーには、重大度、サーバークローニング操作の実行日時、およびクローニングログメッセージの説明が表示されます。ログエントリは、RAC ログでも使用可能です。その他のエントリを表示するには、**プロファイルログに移動** をクリックします。**プロファイルログ** ページが表示されます。詳細に関しては『CMC オンラインヘルプ』を参照してください。

完了状態とトラブルシューティング

適用済みのサーバープロファイルの完了状態をチェックするには、次の手順を実行します。

1. **サーバープロファイル** ページで、 **最近のプロファイルログ** セクションから実行済みジョブのジョブ ID（JID）を書き取ります。
2. システムツリーで、**サーバー概要** に移動して **トラブルシューティング → Lifecycle Controller ジョブ** をクリックします。**ジョブ** 表で同じ JID を探します。

プロファイルの Quick Deploy

Quick Deploy 機能によって、保存プロファイルをサーバースロットに割り当てることができます。そのスロットに挿入されたサーバークローニング対応サーバーは、割り当てられたプロファイルを使用して設定されます。Quick Deploy 処置は、**iDRAC の導入** ページで **サーバープロファイル導入の有効化** オプションが有効になっている場合にのみ実行できます。**iDRAC の導入** ページに進むには、**サーバー概要 → セットアップ → iDRAC** と選択します。導入できるプロファイルは、SD カードに含まれています。

メモ:

Quick Deploy 用プロファイル をセットアップするには、**シャーシ管理者** 権限が必要です。

サーバープロファイルのスロットへの割り当て

サーバープロファイル ページでは、サーバープロファイルをスロットへ割り当てることができます。プロファイルをシャーシスロットへ割り当てるには、以下の手順を実行します。

1. **サーバープロファイル** ページで、 **Quick Deploy 用プロファイル** セクションに進みます。
   サーバープロファイル 行に含まれる選択ボックスに、スロットに対する現在のプロファイル割り当てが表示されます。、
2. ドロップダウンリストから、必要なスロットに割り当てるプロファイルを選択します。複数のスロットに適用するプロファイルを選択できます。
3. **割り当て** をクリックします。
   プロファイルが選択されたスロットに割り当てられます。

メモ: プロファイルが割り当てられていないスロットは、選択ボックスに表示される「プロファイル未選択」で示されます。

メモ: スロットからすべてのプロファイル割り当てを削除するには、ドロップダウンリストで **プロファイル未選択** を選択します。

メモ: Quick Deploy プロファイル 機能を使用してプロファイルがサーバーに展開されるときは、アプリケーションの進捗と結果がプロファイルログに維持されます。

シングルサインオンを使った iDRAC の起動

CMC は、サーバーなどの個別シャーシコンポーネントの限定された管理機能を提供します。これらの各コンポーネントを完全な管理のため、CMC は、サーバーの管理コントローラ（iDRAC）のウェブベースインタフェースの起動ポイントを提供しています。

この機能はシングルサインオンを活用するため、ユーザーは一度ログインすると、二度目からは、ログインをせずに iDRAC ウェブインタフェースを起動できます。シングルサインオンポリシーは以下のようになります。

- サーバー管理者の権限を持つ CMC のユーザーは、シングルサインオンで自動的に iDRAC にログインされます。iDRAC のサイトが表示されたら、そのユーザーに管理者権限が自動的に許可されます。これは、iDRAC のアカウントを持たない同じユーザーや、アカウントに管理者権限のない場合でも同様です。
- サーバー管理者の権限を **持たない** CMC ユーザーでも、iDRAC に同じアカウントがある場合は、シングルサインオンで iDRAC に自動ログインできます。iDRAC のサイトが表示されたら、iDRAC アカウントに対して作られた権限が許可されます。
- サーバー管理者の権限、または iDRAC に同じアカウントを持たない CMC ユーザーは、シングルサインオンで iDRAC に自動ログイン **されません**。このユーザーが **iDRAC GUI の起動** をクリックすると、iDRAC ログインページが表示されます。

  メモ: ここで言う「同じアカウント」とは、ユーザーが CMC および iDRAC にパスワードが一致する同じログイン名を持っているということです。同じログイン名で、パスワードが一致しないユーザーは、同じアカウントを持つと見なされます。

  メモ: その場合、ユーザーは、iDRAC のログインページが表示されます（前述のシングルサインオンの 3 つ目の項目参照）。

  メモ: iDRAC ネットワーク LAN が無効（LAN 無効＝オフ）の場合は、シングルサインオンは利用できません。

サーバーがシャーシから取り外された、iDRAC IP アドレスを変更した、または iDRAC ネットワーク接続にエラーが発生した場合、iDRAC GUI の起動をクリックするとエラーページが表示されることがあります。

関連リンク

サーバー状態ページからの iDRAC の起動
サーバーステータス ページからの iDRAC の起動

サーバー状態ページからの iDRAC の起動

サーバー状態 ページから iDRAC 管理コンソールを起動するには、次の手順を実行します。

1. システムツリーで **サーバー概要** をクリックします。**サーバー状態** ページが表示されます。
2. iDRAC ウェブインタフェースを起動するサーバーで **iDRAC の起動** をクリックします。

   メモ: iDRAC 起動は、IP アドレスまたは DNS 名を使用して設定することができます。デフォルトは、IP アドレスを使う方法です。

サーバーステータス ページからの iDRAC の起動

各サーバーに対する iDRAC 管理コンソールを起動するには：

1. システムツリーで **サーバーの概要** を展開します。すべてのサーバー（1～16）が展開された **サーバー** リストに表示されます。
2. iDRAC Web インタフェースを起動するサーバーをクリックします。 **サーバーステータス** ページが表示されます。
3. **iDRAC GUI の起動** をクリックします。iDRAC Web インタフェースが表示されます。

CMC ウェブインタフェースからのリモートコンソールの起動

サーバーでキーボード - ビデオ - マウス（KVM）セッションを直接起動できます。リモートコンソール機能は、次の条件がすべて満たされた場合のみサポートされます。

- シャーシに電源が入っている。
- サーバーが iDRAC6 と iDRAC7 をサポートしている
- サーバーの LAN インタフェースが有効である
- iDRAC のバージョンが 2.20 以降
- ホストシステムに JRE（Java Runtime Environment）6 アップデート 16 以降がインストールされている
- ホストシステム上のブラウザで、ポップアップウィンドウが許可されている（ポップアップブロッキングが無効）

リモートコンソールは、iDRAC ウェブインタフェースからも起動できます。詳細については、『*iDRAC ユーザーズガイド*』を参照してください。

関連リンク

シャーシの正常性ページからのリモートコンソールの起動
サーバーステータスページからのリモートコンソールの起動
サーバー状態ページからのリモートコンソールの起動

シャーシの正常性ページからのリモートコンソールの起動

CMC ウェブインタフェースからリモートコンソールを起動するには、次のいずれかを実行します。

1. システムツリーで、**シャーシの概要** へ移動し、**プロパティ → 正常性** をクリックします。**シャーシの正常性** ページが表示されます。
2. シャーシ図で指定したサーバーをクリックします。
3. **クイックリンク** セクションで、**リモートコンソールの起動** リンクをクリックしリモートコンソールを起動します。

サーバーステータスページからのリモートコンソールの起動

個別にサーバーのリモートコンソールを起動するには：

1. システムツリーで、**サーバーの概要** を展開します。
   展開されたサーバーリストにすべてのサーバー（1～16）が表示されます。
2. リモートコンソールを起動するサーバーをクリックします。
   サーバーステータス ページが表示されます。
3. **リモートコンソールの起動** をクリックします。

サーバー状態ページからのリモートコンソールの起動

サーバー状態 ページからサーバーリモートコンソールを起動するには、次の手順を実行します。

1. システムツリーで **サーバー概要** に移動し、**プロパティ → 状態** とクリックします。
   サーバー状態 ページが表示されます。
2. 必要なサーバーの **リモートコンソールの起動** をクリックします。

8

アラートを送信するための CMC の設定

管理下システムで発生した特定のイベント用にアラートおよび処置を設定することができます。システムコンポーネントの状態が事前定義された状態を超過すると、イベントが発生します。イベントがイベントフィルタに一致し、そのフィルタをアラートメッセージ（E-メールアラートまたは SNMP トラップ）を生成するように設定した場合、アラートが 1 つ、または複数の設定済みの宛先に送信されます。

アラートを送信するように CMC を設定するには、次の手順を実行します。

1. グローバルシャーシイベントアラートを有効にします。
2. オプションで、アラートが生成されるべきイベントを選択することができます。
3. E-メールアラートまたは SNMP トラップ設定を行います。

関連リンク

アラートの有効化または無効化
アラートの宛先設定

アラートの有効化または無効化

設定された送信先にアラートを送るには、グローバルアラートオプションを有効にする必要があります。このプロパティは個々のアラート設定を上書きします。

SNMP または E-メールアラートの送信先がアラートを受信するように設定されていることを確認してください。

CMC ウェブインタフェースを使用したアラートの有効化または無効化

アラートの生成を有効化または無効化するには、次の手順を実行します。

1. システムツリーで、**シャーシの概要** に移動し、**アラート → シャーシイベント** をクリックします。
   シャーシイベント ページが表示されます。
2. **シャーシイベントフィルタ設定** セクションで、**シャーシイベントアラートの有効化** オプションを選択してアラートの生成を有効にします。アラートの生成を無効にするには、このオプションをクリアします。
3. **シャーシイベントリスト** セクションで、次のいずれかを実行します。
   - アラートが生成されるべき個々のイベントを選択します。
   - 列の見出しで **アラートの有効化** オプションを選択して、すべてのイベントでアラートが生成されるようにします。それ以外は、このオプションを消去します。
4. **適用** をクリックして設定を保存します。

RACADM を使用したアラートの有効化または無効化

アラートの生成を有効化または無効化するには、**cfgIpmiLanAlertEnable** RACAM オブジェクトを使用します。詳細は、『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

アラートの宛先設定

管理ステーションは、シンプル ネットワーク 管理プロトコル（SNMP）を使用して CMC からデータを受信します。

IPv4 および IPv6 アラートの宛先設定、E-メール設定、SMTP サーバー設定を行い、これらの設定をテストすることができます。

E-メールアラートまたは SNMP トラップ設定を行う前に、**シャーシ設定システム管理者** 権限があることを確認してください。

関連リンク

SNMP トラップアラート送信先の設定
E-メールアラートの設定

SNMP トラップアラート送信先の設定

SNMP トラップを受信する IPv6 または IPv4 アドレスを設定できます。

CMC ウェブインタフェースを使用した SNMP トラップアラート送信先の設定

CMC ウェブインタフェースを使用して IPv4 または IPv6 アラート宛先を設定するには、次の手順を実行します。

1. システムツリーで、**シャーシの概要** へ移動し、**アラート → トラップ設定** をクリックします。
   シャーシイベントアラート送信先 ページが表示されます。
2. 以下を入力します。
   - **送信先** フィールドに、有効な IP アドレスを入力します。ドットで 4 つに区切られた IPv4 フォーマット、標準 IPv6 アドレス表記、または FQDN を使用します。例：**123.123.123.123**、**2001:db8:85a3::8a2e:370:7334**、**dell.com**
     ネットワーキング技術またはインフラストラクチャと一貫性のあるフォーマットを選択します。テストトラップ 機能では、現在のネットワーク設定に不適当な選択項目は検出されません（IPv4 専用の環境で IPv6 送信先を使用する場合など）。
   - **コミュニティ文字列** フィールドに、 送信先管理ステーションが属する有効なコミュニティ文字列 を入力します。
     このコミュニティ文字列は、**シャーシ → ネットワーク → サービス** ページのコミュニティ文字列とは異なります。SNMP トラップのコミュニティ文字列は、CMC が管理ステーション宛の送信トラップに使用するものです。 **シャーシ → ネットワーク → サービス** ページのコミュニティ文字列は、管理ステーションが CMC の SNMP デーモンにクエリを行うために使用します。
   - **有効** で、トラップ受信用に有効にする IP アドレスの、送信先 IP に対応するチェックボックスを選択します。IP アドレスは最大 4 つまで指定できます。
3. 設定を保存するには、**適用** をクリックします。
4. IP アドレスが SNMP トラップを受信しているかどうかを確認するには、**SNMP トラップのテスト** 列の **送信** をクリックします。
   IP アラート送信先が設定されます。

RACADM を使用した SNMP トラップアラート送信先の設定

RACADM を使用して IP アラート送信先を設定するには：

1. シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインします。

メモ: SNMP と E-メールアラートの両方とも、設定できるフィルタマスクは 1 つだけです。フィルタマスクを既に選択している場合は、手順 2 を省略することができます。

2. アラートの生成を有効にします。
```
racadm config -g cfgAlerting -o cfgAlertingEnable 1
```

3. アラートが生成されるべきイベントを指定します。
```
racadm config -g cfgAlerting -o cfgAlertingFilterMask <mask value>
```

ここで、<mask value> は 0x0 ～ 0xffffffff の 16 進値です。

マスク値を得るには、科学計算用電卓を 16 進モードで使い、<OR> キーで各マスクの第 2 値 (1、2、4、...) を追加します。

たとえば、バッテリプローブ警告（0x2）、電源装置エラー（0x1000）、KVM エラー（0x80000）用トラップ警告を有効にするには、2 <OR> 1000 <OR> 80000 を入力して <=> キーを押します。

結果の 16 進値は 81002 で、RACADM コマンドのマスク値は 0x81002 です。

表 15. イベントトラップのフィルタマスク

イベント	フィルタマスク値
ファンプローブエラー	0x1
バッテリプローブ警告	0x2
温度プローブ警告	0x8
温度プローブエラー	0x10
冗長性低下	0x40
冗長性喪失	0x80
電源装置警告	0x800
電源装置エラー	0x1000
電源装置がありません	0x2000
ハードウェアログエラー	0x4000
ハードウェアログ警告	0x8000
サーバーがありません	0x10000
サーバーエラー	0x20000
KVM がありません	0x40000
KVM エラー	0x80000
IOM がありません	0x100000
IOM エラー	0x200000
ファームウェアのバージョンが一致しません	0x400000
シャーシ電力しきい値エラー	0x1000000
SD カードがありません	0x2000000
SDCARD エラー	0x4000000
シャーシグループエラー	0x8000000

イベント	フィルタマスク値
サーバースリーブがありません	0x10000000
ファブリックの不一致	0x20000000

4. トラップアラートを有効にします。
   ```
   racadm config -g cfgTraps -o cfgTrapsEnable 1 -i <index>
   ```
   ここで、<index> は 1〜4 の値です。CMC はインデックス番号を使用して、トラップアラート用の設定可能送信先を最大 4 つまで識別します。送信先は適切にフォーマットされた数値アドレス（IPv6 または IPv4）、または完全修飾ドメイン名（FQDN）で指定できます。

5. トラップアラートの送信先 IP アドレスを指定します。
   ```
   racadm config -g cfgTraps -o cfgTrapsAlertDestIPAddr <IP address> -i <index>
   ```
   ここで、<IP address> は有効な IP アドレスで、<index> は手順 4 で指定したインデックス値です。

6. コミュニティ名を指定します。
   ```
   racadm config -g cfgTraps -o cfgTrapsCommunityName <community name> -i
   <index>
   ```
   ここで <community name> はシャーシが属する SNMP コミュニティの名前で、<index> は手順 4 および 5 で指定したインデックス値です。
   トラップアラートの送信先 IP アドレスを 4 つまで設定できます。送信先をさらに追加するには、手順 2〜6 を繰り返します。

   メモ: 手順 2〜6 のコマンドは、指定するインデックス（1〜4）の既存の設定をすべて上書きします。インデックスに既に値が設定されているかを調べるには、`racadm getconfig -g cfgTraps -i <index>` を入力します。インデックスが設定されていると、その値が **cfgTrapsAlertDestIPAddr** と **cfgTrapsCommunityName** オブジェクトに表示されます。

7. アラート送信先へのイベントトラップをテストするには、次を入力します。
   ```
   racadm testtrap -i <index>
   ```
   ここで、<index> は 1〜4 の値で、テストするアラート送信先を表します。
   インデックス番号がわからない場合は、次を入力します。
   ```
   racadm getconfig -g cfgTraps -i <index>
   ```

E-メールアラートの設定

CMC が環境についての警告やコンポーネント障害などのシャー シイベントを検出した場合、1 つ、または複数の E-メールアドレスに E-メールアラートを送信するように設定できます。

CMC の IP アドレスから送信された E-メールを受け入れるように SMTP E-メールサーバーを設定する必要があります。この機能は通常、セキュリティ上、ほとんどのメールサーバーでオフになっています。これをセキュアな方法で行うための手順は、SMTP サーバーに同梱のマニュアルを参照してください。

メモ: メールサーバーが Microsoft Exchange Server 2007 である場合、iDRAC7 から E-メールアラートを受信するには、そのメールサーバー用に iDRAC7 ドメイン名が設定されていることを確認してください。

メモ: E-メールアラートは IPv4 および IPv6 アドレスの両方をサポートします。IPv6 を使用する場合には、DRAC DNS ドメイン名を指定する必要があります。

ご利用のネットワークに定期的に IP アドレスを解放し、異なるアドレスで更新する SMTP サーバーが存在する場合、指定した SMTP サーバーの IP アドレスが変更されるときに、このプロパティ設定が機能しない期間が生じます。そのような場合は、DNS 名を使用してください。

CMC ウェブインタフェースを使用した E-メールアラートの設定

ウェブインタフェースを使用して E-メールアラートを設定するには、次の手順を実行します。

1. システムツリーで **シャーシ概要** に移動し、**アラート → E-メールアラート設定** をクリックします。
2. アラートの受信用 SMTP E-メールサーバー設定および E-メールアドレスを指定します。フィールドの詳細については、『CMC オンラインヘルプ』を参照してください。
3. 設定を保存するには、**適用** をクリックします。
4. **E-メールのテスト** で **送信** をクリックして、指定した E-メールアラートの宛先にテスト E-メールを送信します。

RACADM を使用した E-メールアラートの設定

RACADM を使用して E-メールアラートの送信先にテスト E-メールを送信するには、次の手順を実行します。

1. シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインします。
2. アラートの生成を有効にします。
   ```
   racadm config -g cfgAlerting -o cfgAlertingEnable 1
   ```
   メモ: SNMP と E-メールアラートの両方とも、設定できるフィルタマスクは 1 つだけです。フィルタマスクを既に設定している場合は、手順 3 を省略することができます。
3. アラートが生成されるべきイベントを指定します。
   ```
   racadm config -g cfgAlerting -o cfgAlertingFilterMask <mask value>
   ```
   ここで、<mask value> は 0x0～ 0xffffffff の 16 進数値で、0x で始まる形式である必要があります。Table イベントトラップのフィルタマスク は、各イベントタイプのフィルタマスクを提供します。有効にするフィルタマスクの 16 進値の計算方法は、「RACADM を使用した SNMP トラップアラート送信先の設定」の手順 3 を参照してください。
4. E-メールアラートの生成を有効にします。
   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable 1 -i <index>
   ```
   ここで、<index> は 1～4 の範囲の値です。CMC ではインデックス番号を使用して、設定可能な最大 4 つの送信先 E-メールアドレスを区別します。
5. E-メールアラートを受信する送信先 E-メールアドレスを指定します。
   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertAddress <email address> -i
   <index>
   ```
   ここで、<email address> は有効な E-メールアドレスで、<index> は手順 4 で指定したインデックス値です。
6. E-メールアラートを受信する人の名前を指定します。
   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEmailName <email name> -i
   <index>
   ```
   ここで、<email name> は、E-メールアラートを受信する人またはグループの名前で、<index> は手順 4 と 5 で指定したインデックス値です。E-メール名は、32 文字以内の英数字、ハイフン、下線、ピリオドで指定します。スペースは使用できません。
7. SMTP ホストを設定します。
   ```
   racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr host.domain
   ```
   ここで host.domain は FQDN です。

   E-メールアラートを受け取る送信先 E-メールアドレスは、最大 4 件設定できます。E-メールアドレスをさらに追加するには、手順 2～6 を繰り返します。

メモ: 手順 2〜6 のコマンドは、指定するインデックス（1〜4）の既存の設定をすべて上書きします。インデックスに既に値が設定されているかを調べるには、:x`racadm getconfig -g cfgEmailAlert – I <index>` を入力します。インデックスが設定されていると、その値が **cfgEmailAlertAddress** インデックスが設定されていると、その値が **cfgEmailAlertEmailName** オブジェクトに表示されます。

詳細については、**dell.com/support/manuals** にある『iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド』を参照してください。

9

ユーザーアカウントと権限の設定

特定の権限（*ロールベースの権限*）を持つユーザーアカウントをセットアップし、CMC を使用してシステムを管理したり、システムセキュリティを維持したりできます。デフォルトで、iDRAC7 はローカル管理者アカウントで設定されています。デフォルトユーザー名は *root* で、パスワードは *calvin* です。管理者として、他のユーザーが CMC にアクセスすることを許可するユーザーアカウントをセットアップできます。

最高 16 のローカルユーザーをセットアップ、または Microsoft Active Directory や LDAP などのディレクトリサービスを使用して、追加のユーザーアカウントをセットアップできます。ディレクトリサービスは、認証されたユーザーアカウントを管理するための一元管理地点を提供します。

CMC は、関連付けられた権限の一連を持つユーザーへの役割ベースのアクセスをサポートします。役割は、管理者、オペレータ、読み取り専用、またはなしです。これらは、利用可能な最大権限を定義します。

関連リンク

ユーザーのタイプ
ローカルユーザーの設定
Active Directory ユーザーの設定
汎用 LDAP ユーザーの設定
ルートユーザー管理者アカウント設定の変更

ユーザーのタイプ

ユーザーには 2 つのタイプがあります。

- CMC ユーザーまたはシャーシユーザー
- iDRAC ユーザーまたはサーバーユーザー（iDRAC がサーバーにあるため）

CMC および iDRAC ユーザーは、ローカルユーザーまたはディレクトリサービスユーザーにすることができます。

サーバーユーザーは CMC ユーザーとは独立して作成されるため、CMC ユーザーが **サーバー管理者** 権限 を持つ場合を除き、CMC ユーザーに与えられる権限はサーバー上の同じユーザーに自動的に転送されるわけではありません。つまり、CMC Active Directory ユーザーと iDRAC Active Directory ユーザーは、Active Directory ツリーの異なるブランチに位置することになります。ローカルサーバーユーザーを作成するには、ユーザー設定システム管理者は直接サーバーにログインする必要があります。ユーザー設定システム管理者は、CMC からサーバーユーザーまたはその逆を作成できません。このルールにより、サーバーのセキュリティと整合性は保護されます。

表 16. : ユーザーのタイプ

権限	説明
CMC ログインユーザー	ユーザーは CMC にログインし、全 CMC データを表示できますが、データの追加や修正、またはコマンドの実行はできません。 ユーザーは、CMC ログインユーザー権限を持たずに他の権限を持つこともできます。この機能は、ユーザーが一時的にログインを禁止されている場合に便利です。そのユーザーの CMC ログインユーザー権限が復元した場合にも、その前に与えられていたその他のすべての権限を保持できます。
シャーシ設定システム管理者	ユーザーは、次のデータの追加や変更ができます。

権限	説明
	• シャーシを識別する（シャーシ名やシャーシの位置など）。 • シャーシに特別に割り当てられている（IP モード（静的または DHCP）、静的 IP アドレス、静的ゲートウェイ、静的サブネットマスクなど）。 • シャーシにサービスを提供する（日時、ファームウェアアップデート、CMC リセットなど）。 • シャーシに関連している（スロット名やスロットの優先順位など）。これらのプロパティはサーバーに適用されますが、正確にはサーバーそのものでなくスロットに関連付けられるシャーシプロパティです。このため、スロット名とスロットの優先順位は、サーバーがスロットにあるなしに関係なく、追加または変更することができます。 サーバーが別のシャーシに移動されると、サーバーは新しいシャーシのそのスロットに割り当てられているスロット名と優先順位を継承します。前のスロット名と優先順位はそのまま前のシャーシに残ります。 **メモ: シャーシ設定システム管理者** 権限を持つ CMC ユーザーが電源設定を行うことができます。ただし、シャーシの電源オン、電源オフ、パワーサイクルなどのシャーシ電源操作を行うには、**シャーシ制御システム管理者** 権限が必要です。
ユーザー設定システム管理者	ユーザーは次の操作ができます。 • 新規ユーザーを追加する。 • ユーザーのパスワードの変更 • ユーザー権限の変更 • ユーザーのログイン権限を有効または無効にしますが、ユーザーの名前やデータベース内のその他の権限は保持されます。
ログのクリアシステム管理者	ユーザーはハードウェアログと CMC ログをクリアできます。
シャーシ制御システム管理者（電源コマンド）	**シャーシ電源システム管理者** の権限を持つ CMC ユーザーは、電源関連の操作をすべて行うことができます。電源オン、電源オフ、パワーサイクルなどのシャーシ電力操作を制御できます。 **メモ:** 電源設定を行うには、**シャーシ設定システム管理者** 権限が必要です。
Server Administrator	これは、CMC ユーザーにシャーシ内に存在する任意のサーバー上の任意の操作を実行する全権利を与える包括的な権限です。 **サーバーシステム管理者** 権限を持つユーザーがサーバー上で実行する処置を出すと、CMC ファームウェアはサーバー上のユーザーの権限を確認せずに、コマンドを対象のサーバーに送信します。つまり、**サーバーシステム管理者** 権限はサーバーにシステム管理者権限がない場合でもそれを無視してコマンドを送信します。 **サーバーシステム管理者** 権限がない場合、シャーシで作成されたユーザーは以下のすべての条件が満たされた場合にのみ、サーバー上でコマンドを実行することができます。 • 同じユーザー名がサーバー上に存在する • サーバー上の同じユーザー名は同じパスワードが所有する必要がある。 • ユーザーはコマンドを実行する権限を持っている **サーバーシステム管理者** 権限のない CMC ユーザーがサーバー上で実行する処置を出す場合、CMC はユーザーのログイン名とパスワードを入力して、対象のサーバーにコマンドを送信します。ユーザーがサー

権限	説明
	バー上に存在しない、またはパスワードが一致しない場合は、ユーザーは処置を実行することができません。 ユーザーが対象のサーバーに存在し、パスワードが一致する場合は、サーバーはユーザーがサーバー上で与えられた権限を使って応答します。CMC ファームウェアはサーバーから返された権限に基づいてユーザーに処置を実行する権利があるかどうかを決定します。 以下のリストに、サーバーシステム管理者が持っているサーバー上の権限と処置を示します。これらの権利は、シャーシユーザーがシャーシ上でサーバーシステム管理者権限を持っていない場合にのみ適用されます。 サーバー設定システム管理者： • IP アドレスの設定 • ゲートウェイの設定 • サブネットマスクの設定 • 最初の起動デバイスの設定 ユーザーの設定： • iDRAC ルートパスワードの設定 • iDRAC のリセット サーバー制御システム管理者： • 電源オン • 電源オフ • 電源の入れ直し • 正常なシャットダウン • サーバーの再起動
テストアラートユーザー	ユーザーはテストアラートメッセージを送信できます。
デバッグコマンドシステム管理者	ユーザーはシステム診断コマンドを実行できます。
ファブリック A システム管理者	ユーザーは、I/O スロットのスロット A1 またはスロット A2 に存在するファブリック A IOM を設定できます。
ファブリック B システム管理者	ユーザーは、I/O スロットのスロット B1 またはスロット B2 に存在するファブリック B IOM を設定できます。
ファブリック C システム管理者	ユーザーは、I/O スロットのスロット C1 またはスロット C2 に存在するファブリック C IOM を設定できます。

CMC ユーザーグループは、あらかじめ割り当てられたユーザー権限を持つ一連のユーザーグループを提供します。

メモ: システム管理者、パワーユーザー、またはゲストユーザーを選択し、事前に定義された設定から権限を追加または削除した場合、CMC グループ は自動的に カスタム に変更されます。

表 17. : CMC グループ権限

ユーザーグループ	特権
システム管理者	• CMC ログインユーザー • シャーシ設定システム管理者 • ユーザー設定システム管理者

ユーザーグループ	特権
	• ログのクリアシステム管理者 • Server Administrator • テストアラートユーザー • デバッグコマンドシステム管理者 • ファブリック A システム管理者 • ファブリック B システム管理者 • ファブリック C システム管理者
パワーユーザー	• ログイン • ログのクリアシステム管理者 • シャーシ制御システム管理者（電源コマンド） • Server Administrator • テストアラートユーザー • ファブリック A システム管理者 • ファブリック B システム管理者 • ファブリック C システム管理者
ゲストユーザー	ログイン
カスタム	次の権限を任意の組み合わせで選択します。 • CMC ログインユーザー • シャーシ設定システム管理者 • ユーザー設定システム管理者 • ログのクリアシステム管理者 • シャーシ制御システム管理者（電源コマンド） • Server Administrator • テストアラートユーザー • デバッグコマンドシステム管理者 • ファブリック A システム管理者 • ファブリック B システム管理者 • ファブリック C システム管理者
なし	権限の割り当てなし

表 18. : CMC システム管理者、パワーユーザー、ゲストユーザー間の権限の比較

権限セット	システム管理者のアクセス権	パワーユーザーの許可	ゲストユーザーのアクセス権
CMC ログインユーザー	はい	はい	はい
シャーシ設定システム管理者	はい	不可	不可
ユーザー設定システム管理者	はい	不可	不可
ログのクリアシステム管理者	はい	はい	不可

権限セット	システム管理者のアクセス権	パワーユーザーの許可	ゲストユーザーのアクセス権
シャーシ制御システム管理者（電源コマンド）	はい	はい	不可
Server Administrator	はい	はい	不可
テストアラートユーザー	はい	はい	不可
デバッグコマンドシステム管理者	はい	不可	不可
ファブリック A システム管理者	はい	はい	不可
ファブリック B システム管理者	はい	はい	不可
ファブリック C システム管理者	はい	はい	不可

ルートユーザー管理者アカウント設定の変更

セキュリティを強化するため、ルート（ユーザー 1）アカウントのデフォルトパスワードを変更することが強く推奨されます。ルートアカウントは、CMC に組み込まれているデフォルトの管理アカウントです。

CMC ウェブインタフェースを使用して root アカウントのデフォルトパスワードを変更するには、次の手順を実行します。

1. システムツリーで、**シャーシ概要** へ移動し、**ユーザー認証 → ローカルユーザー** をクリックします。
   ユーザー ページが表示されます。
2. **ユーザー ID** 列で、ユーザー ID 1 をクリックします。

   メモ: ユーザー ID 1 は CMC にデフォルトで組み込まれているルートユーザーアカウントです。これを変更することはできません。

   ユーザー設定 ページが表示されます。
3. **パスワードの変更** チェックボックスを選択します。
4. **パスワード** および **パスワードの確認** フィールドに新しいパスワードを入力します。
5. **適用** をクリックします。
   ユーザー ID 1 のパスワードが変更されました。

ローカルユーザーの設定

CMC では、特定のアクセス権限を持つローカルユーザーを最大 16 人設定できます。CMC ユーザーを作成する前に、現在のユーザーが存在するかどうかを確認してください。これらのユーザーには、ユーザー名、パスワード、および権限付きの役割を設定できます。ユーザー名とパスワードは、CMC でセキュア化された任意のインタフェース（つまり、ウェブインタフェース、RACADM、または WS-MAN）を使用して変更できます。

CMC ウェブインタフェースを使用したローカルユーザーの設定

ローカル CMC ユーザーを追加して設定するには、次の手順を実行します。

メモ: CMC ユーザーを作成するには、**ユーザーの設定** 権限が必要です。

1. システムツリーで、**シャーシ概要** へ移動し、**ユーザー認証 → ローカルユーザー** をクリックします。
   ユーザー ページが表示されます。
2. **ユーザー ID** 列で、ユーザー ID 番号をクリックします。

   メモ: ユーザー ID 1 は CMC にデフォルトで組み込まれているルートユーザーアカウントです。これを変更することはできません。

   ユーザー設定 ページが表示されます。
3. ユーザー ID を有効にして、そのユーザーのユーザー名、パスワード、およびアクセス権限を指定します。
   オプションの詳細については、『CMC オンラインヘルプ』を参照してください。
4. **適用** をクリックします。
   必要な権限を持つユーザーが作成されます。

RACADM を使用したローカルユーザーの設定

メモ: リモート Linux システム上で RACADM コマンドを実行するには、**root** ユーザーとしてログインする必要があります。

CMC のプロパティデータベースには 16 のユーザーを設定できます。CMC ユーザーを手動で有効にする前に、現在のユーザーが存在するか確認します。

新しい CMC を設定している場合や、RACADM の `racresetcfg` コマンドを実行した場合、現在のユーザーは、パスワードが `calvin` の `root` のみが存在します。`racresetcfg` サブコマンドは、すべての 設定パラメータを元のデフォルトにリセットします。それまでに行った変更がすべて失われます。

メモ: ユーザーをいつでも有効および無効に切り替えられますが、ユーザーを無効にしてもそのユーザーはデータベースから削除されません。

ユーザーが存在するかどうかを確認するには、CMC への Telnet/SSH テキストコンソールを開き、ログインしてから、1〜16 のインデックスごとに、次のコマンドを一度入力します。

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

メモ: `racadm getconfig -f <myfile.cfg>>` と入力して、CMC 設定パラメータのすべてが含まれる **myfile.cfg** ファイルの表示や編集を行うこともできます。

複数のパラメータとオブジェクト ID が、それぞれの現在の値と共に表示されます。重要な 2 つのオブジェクトは、次のとおりです。

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

`cfgUserAdminUserName` オブジェクトに値がない場合、`cfgUserAdminIndex` オブジェクトで示されるインデックス番号を使用できます。名前が「=」の後に表示されている場合、そのインデックスはそのユーザー名によって使用されています。

racadm `config` サブコマンドを使用してユーザーを手動で有効または無効にする場合は、`-i` オプションでインデックスを指定する **必要があります**。

コマンドオブジェクト内の「#」文字は、それが読み取り専用オブジェクトであることを示しています。また、`racadm config -f racadm.cfg` コマンドを使用して、書き込み用に任意の数のグループ / オブジェクトを指定する場合、インデックスは指定できません。新規ユーザーは最初の使用可能なインデックスに追加されます。この動作は、メイン CMC と同じ設定での第 2 の CMC の設定におけるより優れた柔軟性を可能にします。

RACADM を使用した CMC ユーザーの追加

新しいユーザーを CMC 設定に追加するには、次の手順を実行します。

1. ユーザー名を設定します。
2. パスワードを設定します。
3. ユーザー権限を設定します。ユーザー権限の詳細については、「ユーザーのタイプ」を参照してください。
4. ユーザーを有効にします。

例：

次の例は、パスワードが「123456」で CMC へのログイン権限のある「John」という新しいユーザーを追加する方法を示しています。

メモ: 特定のユーザー権限に対する有効なビットマスク値については、『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。デフォルトの権限値は 0 で、これはユーザーの権限が有効になっていないことを示します。

```
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
```

正しい権限を持つユーザーが追加されたことを確認するには、次のコマンドを使用します。

```
racadm getconfig -g cfgUserAdmin -i 2
```

RACADM コマンドの詳細については、**dell.com/support/manuals** にある『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

CMC ユーザーの無効化

RACADM を使用する場合、ユーザーは個別に手動で無効化する必要があります。設定ファイルを使用してユーザを削除することはできません。

CMC ユーザーを削除するためのコマンド構文は、次のとおりです。

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <インデックス>"" racadm
config -g cfgUserAdmin -i 2 -o cfgUserAdminPrivilege 0x0
```

二重引用符のヌル文字列（""）は、指定したインデックスでユーザー設定を削除して、ユーザー設定をオリジナルの工場出荷時デフォルトにリセットするように CMC に指示します。

許可を持つ iDRAC7 ユーザーの有効化

特定の管理許可（役割ベースの権限）を持つユーザーを有効にするには、次の手順を実行します。

1. 次のコマンド構文を使用して使用可能なユーザーインデックスを見つけます。

   ```
   racadm getconfig -g cfgUserAdmin -i <インデックス>
   ```

2. 新しいユーザー名とパスワードで次のコマンドを入力します。

   ```
   racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <インデックス> <ユーザー権限ビットマスク値>
   ```

   メモ: 特定ユーザー権限用の有効なビットマスク値のリストに関しては、**dell.com/support/manuals** にある『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。デフォルトの権限値は 0 で、ユーザーに有効な権限がないことを示します。

Active Directory ユーザーの設定

会社で Microsoft Active Directory ソフトウェアを使用している場合、CMC にアクセス権を付与するようにソフトウェアを設定することができます。これにより、ディレクトリサービスの既存ユーザーに CMC ユーザー権限を追加し、制御することが可能になります。これはライセンスが必要な機能です。

メモ: Microsoft Windows 2000 および Windows Server 2003 オペレーティングシステムでは、Active Directory を使用して CMC のユーザーを認識できます。IPv6 および IPv4 経由の Active Directory は、Windows 2008 でサポートされています。

CMC にログインするために、Active Directory を介してユーザー認証を設定できます。また、管理者が各ユーザーに特定の権限を設定できるようにする、役割ベースの権限を提供することもできます。

サポートされている Active Directory の認証機構

Active Directory を使用して、次の 2 つの方法を使用する CMC ユーザーアクセスを定義できます。

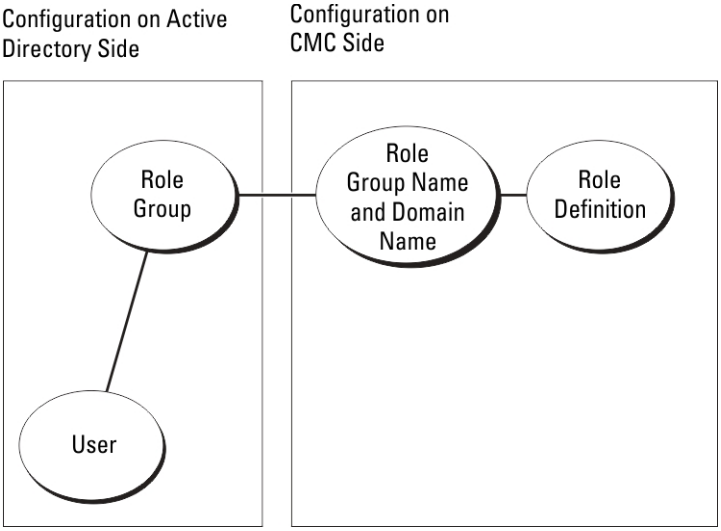
- Microsoft のデフォルトの Active Directory グループオブジェクトのみを使用する*標準*スキーマソリューション。
- デル提供のカスタマイズされた Active Directory オブジェクトを持つ*拡張*スキーマソリューション。アクセスコントロールオブジェクトはすべて Active Directory で管理されます。これにより、異なる CMC 上でさまざまな権限レベルを持つユーザーアクセスを設定するための最大限の柔軟性が実現します。

関連リンク

標準スキーマ Active Directory の概要
拡張スキーマ Active Directory の概要

標準スキーマ Active Directory の概要

次の図に示すように、標準スキーマを使用して Active Directory を統合する場合は、Active Directory と CMC の両方での設定が必要となります。



標準グループオブジェクトは、Active Directory では役割グループとして使用されます。CMC アクセスを持つユーザーは、役割グループのメンバーです。このユーザーに特定の CMC へのアクセスを与えるには、その特定 CMC に役割グループ名およびドメイン名を設定する必要があります。役割および権限のレベルは、Active

Directory ではなく、各 CMC で定義されます。各 CMC には最大 5 つまで役割グループを設定できます。次の表は、デフォルトの役割グループの権限を示します。

表 19. ：デフォルトの役割グループの権限

役割グループ	デフォルトの権限レベル	許可する権限	ビットマスク
1	なし	• CMC ログインユーザー • シャーシ設定システム管理者 • ユーザー設定システム管理者 • ログのクリアシステム管理者 • シャーシ制御システム管理者（電源コマンド） • Server Administrator • テストアラートユーザー • デバッグコマンドシステム管理者 • ファブリック A システム管理者 • ファブリック B システム管理者 • ファブリック C システム管理者	0x00000fff
2	なし	• CMC ログインユーザー • ログのクリアシステム管理者 • シャーシ制御システム管理者（電源コマンド） • Server Administrator • テストアラートユーザー • ファブリック A システム管理者 • ファブリック B システム管理者 • ファブリック C システム管理者	0x00000ed9
3	なし	CMC ログインユーザー	0x00000001
4	なし	権限の割り当てなし	0x00000000
5	なし	権限の割り当てなし	0x00000000

メモ: ビットマスク値は、RACADM で標準スキーマを設定する場合に限り使用されます。

メモ: ユーザー権限の詳細については、「ユーザーのタイプ」を参照してください。

標準スキーマ Active Directory の設定

Active Directory のログインアクセスのために CMC を設定するには、次の手順を実行します。

1. Active Directory サーバー（ドメインコントローラ）で、**Active Directory ユーザーとコンピュータスナップイン** を開きます。
2. CMC ウェブインタフェースまたは RACADM の使用：
   a) グループを作成するか、既存のグループを選択します。
   b) 役割権限を設定します。
3. CMC にアクセスするには、Active Directory ユーザーを Active Directory グループのメンバーとして追加します。

CMC ウェブインタフェースを使用した標準スキーマでの Active Directory の設定

メモ: さまざまなフィールドについての情報は、『*iDRAC7 オンラインヘルプ*』を参照してください。

1. システムツリーで、**シャーシの概要** へ移動し、**ユーザー認証 → ディレクトリサービス** をクリックします。**ディレクトリサービス** ページが表示されます。
2. Select **（標準スキーマ）** を選択します。標準スキーマ用の設定が同じページに表示されます。
3. 以下を指定します。
   - Active Directory の有効化、ルートドメイン名、およびタイムアウト値の入力。
   - ドメインコントローラとグローバルカタログの検索を直接呼び出す場合は、**検索する AD サーバーの検索（オプション）** オプションを選択して、ドメインコントローラとグローバルカタログの詳細を指定します。
4. 設定を保存するには、**適用** をクリックします。

   メモ: 続行する前に、設定を適用する必要があります。設定を適用しない場合、次のページへ移動したときに設定が失われます。
5. **標準スキーマの設定** セクションで、**役割グループ** をクリックします。**役割グループの設定** ページが表示されます。
6. 役割グループのグループ名、ドメイン、および権限を指定します。
7. **適用** をクリックして役割グループ設定を保存し、**ユーザー設定ページに戻る** をクリックします。
8. 証明書の検証を有効にした場合、ドメインフォレストのルート認証局の署名付き証明書を CMC にアップロードする必要があります。**証明書を管理** セクションで、証明書のファイルパスを入力するか、参照 をクリックして証明書ファイルを選択します。**アップロード** をクリックしてファイルを CMC にアップロードします。

   メモ: アップロードする証明書の相対ファイルパスが **ファイルパス** の値に表示されます。フルパスと正しいファイル名とファイル拡張子を含む絶対ファイルパスを入力する必要があります。

   ドメインコントローラの SSL 証明書は、ルート認証局の署名付き証明書で署名されていなければなりません。CMC にアクセスする管理ステーションで、ルート認証局の署名付き証明書が使用可能である必要があります。
9. シングルサインオン（SSO）を有効にした場合、**Kerberos Keytab** セクションで **参照** をクリックして keytab ファイルを指定し、**アップロード** をクリックします。アップロードを完了したら、アップロードに成功または失敗したかを通知するメッセージが表示されます。
10. **適用** をクリックします。**適用** をクリックした後、CMC ウェブサーバーが自動的に再起動します。
11. CMC Active Directory の設定を完了するには、ログアウトしてから CMC にログインします。
12. システムツリーで、**シャーシ** を選択し、**ネットワーク** タブへ移動します。**ネットワークの設定** ページが表示されます。
13. **ネットワーク設定** で **DHCP を使用（CMC ネットワークインターフェース IP アドレス用）** が選択されている場合、**DHCP を使用して DNS サーバーアドレスを取得** を選択します。

DNS サーバーの IP アドレスを手動で入力するには、**DHCP を使用して DNS サーバーアドレスを取得する** チェックボックスをオフにし、プライマリおよび代替 DNS サーバーの IP アドレスを入力します。

14. **変更の適用** をクリックします。
    これで、CMC 標準スキーマ Active Directory 機能の設定が完了します。

RACADM を使用した標準スキーマの Active Directory の設定

RACADM を使用した標準スキーマの CMC Active Directory を設定するには、次の手順を実行します。

1. CMC へのシリアル /Telnet/SSH テキスト コンソールを開いて、次を入力します。

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1 racadm config -g
cfgActiveDirectory -o cfgADType 2 racadm config -g cfgActiveDirectory -o
cfgADRootDomain <完全修飾ルートドメイン名> racadm config -g cfgStandardSchema -
i <インデックス> -o cfgSSADRoleGroupName <役割グループのコモンネーム> racadm
config -g cfgStandardSchema -i <インデックス>-o cfgSSADRoleGroupDomain <完全修飾
ドメイン名> racadm config -g cfgStandardSchema -i <インデックス> -o
cfgSSADRoleGroupPrivilege <特定ユーザー権限用のビットマスク番号> racadm
sslcertupload -t 0x2 -f <ADS ルート CA 証明書> racadm sslcertdownload -t 0x1 -
f <RAC SSL 証明書>
```

   メモ: ビットマスクの番号については、『*iDRAC6 および CMC 向け RACADM コマンドラインリファレンスガイド*』のデータベースプロパティの章を参照してください。

2. 次のいずれかのオプションを使用して DNS サーバーを指定します。
   - CMC で DHCP が有効化されており、DHCP サーバーによって自動取得される DNS アドレスを使用したい場合は、次のコマンドを入力します。

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

   - CMC で DHCP が無効になっている場合や、手動で DNS の IP アドレスを入力する場合は、次のコマンドを入力します。

     ```
     racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0 racadm
     config -g cfgLanNetworking -o cfgDNSServer1 <プライマリ DNS IP アドレス>
     racadm config -g cfgLanNetworking -o cfgDNSServer2 <セカンダリ DNS IP ア
     ドレス>
     ```

拡張スキーマ Active Directory の概要

拡張スキーマソリューションを使用する場合は、Active Directory スキーマの拡張が必要です。

Active Directory スキーマ拡張

Active Directory データは、*属性*と*クラス*の分散データベースです。Active Directory スキーマには、データベースに追加または挿入するデータタイプを決定する規則があります。データベースに格納されるクラスの一例として、ユーザークラスがあります。ユーザークラスの属性には、ユーザーの姓、名、電話番号などが含まれます。

特定の要件を満たす*属性*および*クラス*を追加して、データベースを拡張できます。デルでは、スキーマを拡張して、Active Directory を使用したリモート管理の認証と許可をサポートするために必要な変更を含めました。

既存の Active Directory スキーマに追加される各*属性*または*クラス*は、固有の ID で定義される必要があります。業界全体で固有の ID を保持するため、マイクロソフトでは Active Directory オブジェクト識別子（OID）のデータベースを維持しており、企業がスキーマに拡張を追加したときに、それらが固有であり、お互いに拮抗しないことを保証できるようにしています。マイクロソフトの Active Directory におけるスキーマの拡張

のため、Dell は、ディレクトリサービスに追加される属性およびクラス用に固有の OID、固有の名前拡張子、および固有にリンクされた属性 ID を取得しました。

- デルの拡張子：dell
- デルのベース OID：1.2.840.113556.1.8000.1280
- RAC LinkID の範囲： 12070 〜 12079

スキーマ拡張の概要

デルでは、*関連*、*デバイス*、および*権限*プロパティを取り入れるためにスキーマを拡張しました。*関連*プロパティは、特定の権限セットを持つユーザーまたはグループと、1 つ、または複数の RAC デバイスとをリンクするために使用されます。このモデルは、複雑な操作をほとんど行うことなく、ネットワーク上のユーザー、RAC 権限、および RAC デバイスの様々な組み合わせにおける最大の柔軟性をシステム管理者に提供します。

認証と承認を Active Directory と統合したい CMC が 2 つネットワーク上にある場合は、各 CMC につき少なくとも 1 つの関連オブジェクトと 1 つの RAC デバイスオブジェクトを作成する必要があります。関連オブジェクトは必要なだけいくつでも作成でき、各関連オブジェクトにリンクできるユーザー、ユーザーグループ、RAC デバイスオブジェクトの数にも制限はありません。ユーザーと RAC デバイスオブジェクトは、企業内のどのドメインのメンバでもかまいません。

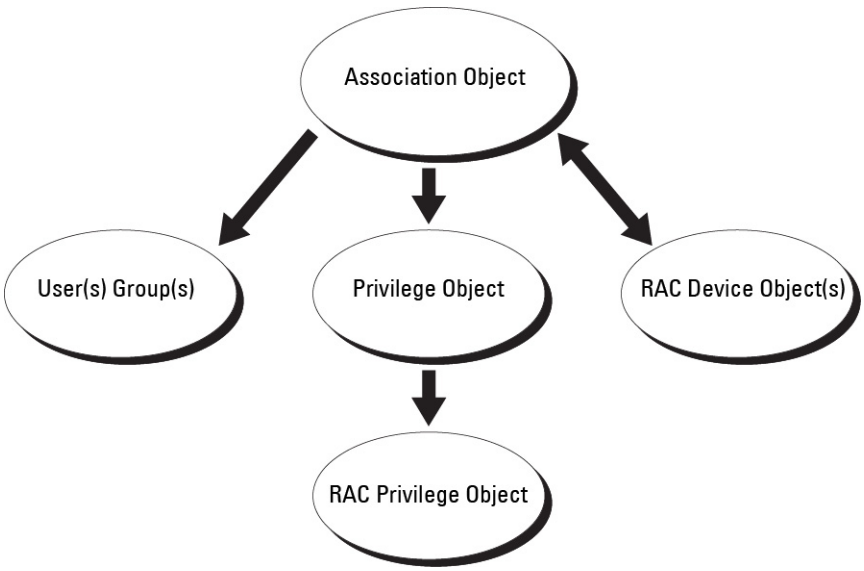
ただし、各関連オブジェクト（または、ユーザー、ユーザーグループ、あるいは RAC デバイスオブジェクト）は、1 つの権限オブジェクトにしかリンクすることができません。この例では、システム管理者が、特定の CMC で各ユーザーの権限をコントロールすることができます。

RAC デバイスオブジェクトは、Active Directory に照会して認証と許可を実行するための RAC ファームウェアへのリンクです。RAC をネットワークに追加した場合、システム管理者は RAC とそのデバイスオブジェクトをその Active Directory 名で設定して、ユーザーが Active Directory で認証と認可を実行できるようにする必要があります。さらに、ユーザーが認証できるように、RAC を少なくとも 1 つの関連オブジェクトに追加する必要があります。

次の図は、関連オブジェクトによって、認証と許可に必要な接続が提供されていることを示しています。

メモ: RAC 特権オブジェクトは DRAC 4、DRAC 5、および CMC に適用されます。

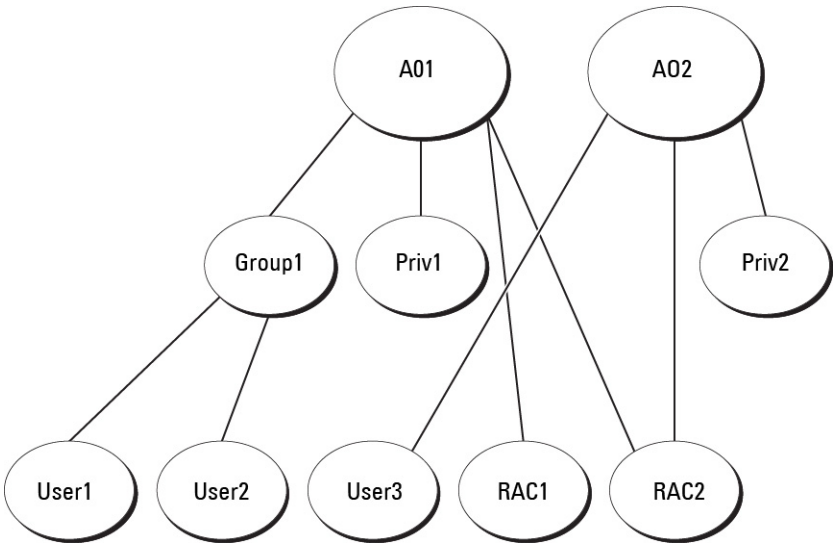
関連オブジェクトは、必要に応じて多くも少なくも作成できます。ただし、少なくとも 1 つの関連オブジェクトを作成する必要があり、Active Directory を統合するネットワーク上の RAC（CMC）ごとに、1 つの RAC デバイスオブジェクトが必要です。



関連オブジェクトは、必要な数だけのユーザーおよび / またはグループの他、RAC デバイスオブジェクトにも対応できます。ただし、関連オブジェクトには、関連オブジェクトにつき 1 つの権限オブジェクトしか含めることができません。関連オブジェクトは、RAC（CMC）に対して*権限*を持つユーザーを連結します。

また、Active Directory オブジェクトは、単一ドメイン、複数のドメインのいずれに設定することも可能です。たとえば、CMC が 2 つ（RAC1、RAC2）と、既存の Active Directory ユーザーが 3 つ（ユーザー 1、ユーザー 2、ユーザー 3）あるとし、ユーザー 1 とユーザー 2 に 両方の CMC へのシステム管理者特権を与え、ユーザー 3 に RAC2 カードへのログイン特権を与えたいとします。下の図 に、このシナリオで Active Directory オブジェクトを設定する方法を示します。

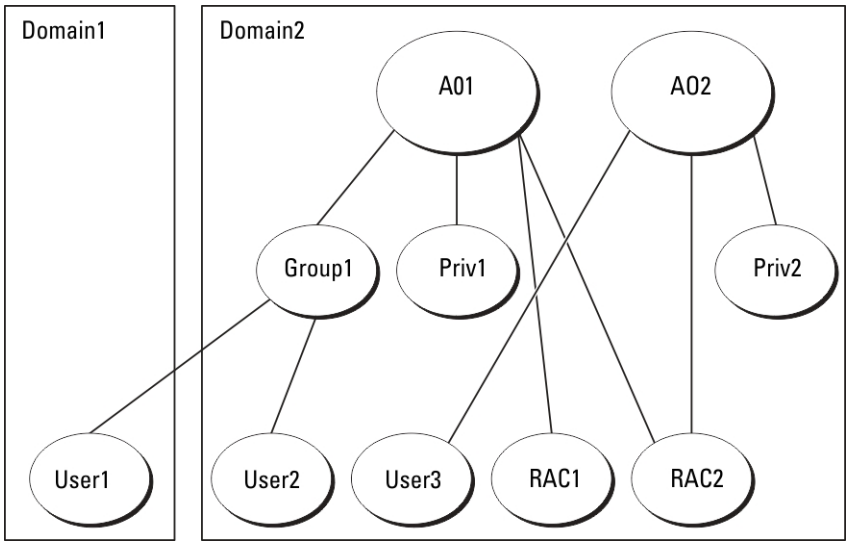
別のドメインからユニバーサルグループを追加するときは、ユニバーサルスコープを持つ関連オブジェクトを作成します。Dell Schema Extender ユーティリティによって作成されるデフォルトの関連オブジェクトは、ドメインローカルグループであり、他のドメインのユニバーサルグループとは連携しません。



単一ドメインのシナリオでオブジェクトを設定するには、次の手順を実行します。

1. 関連オブジェクトを 2 つ作成します。
2. 2 つの CMC を表す 2 つの RAC デバイスオブジェクト、RAC1 と RAC2 を作成します。
3. 2 つの特権オブジェクト、特権 1 と特権 2 を作成します。特権 1 にはすべての特権（システム管理者）、特権 2 にはログイン特権を与えます。
4. User1 と User2 を Group1 にまとめます。
5. グループ 1 を関連オブジェクト 1（A01）のメンバ、特権 1 を A01 の特権オブジェクトとして、RAC1 と RAC2 を A01 の RAC デバイスとして追加します。
6. ユーザー 3 を関連オブジェクト 2（A02）のメンバ、特権 2 を A02 の特権オブジェクト、RAC2 を A02 の RAC デバイスとして追加します。

下の図に、複数ドメインの Active Directory オブジェクトの例を示します。このシナリオでは、CMC が 2 つ（RAC1 と RAC2）と、既存の Active Directory ユーザーが 3 つ（ユーザー 1、ユーザー 2、ユーザー 3）あるとします。ユーザー 1 はドメイン 1 に存在し、ユーザー 2 とユーザー 3 はドメイン 2 に存在しています。このシナリオでは、ユーザー 1 とユーザー 2 に両方の CMC へのシステム管理者特権を持つように設定し、ユーザー 3 に RAC2 カードへのログイン特権を持つようにします。



複数ドメインのシナリオでオブジェクトを設定するには

1. ドメインのフォレスト機能がネイティブまたは Windows 2003 モードになっていることを確認します。
2. 2 つの関連オブジェクト A01（ユニバーサルスコープの）と A02 を任意のドメインに作成します。複数ドメインに Active Directory オブジェクトを設定している図では、オブジェクトがドメイン 2 に示されています。
3. 2 つの CMC を表す 2 つの RAC デバイスオブジェクト、RAC1 と RAC2 を作成します。
4. 2 つの特権オブジェクト、特権 1 と特権 2 を作成します。特権 1 にはすべての特権（システム管理者）、特権 2 にはログイン特権を与えます。
5. User1 と User2 を Group1 にまとめます。Group1 のグループスコープはユニバーサルである必要があります。
6. グループ 1 を関連オブジェクト 1（A01）のメンバ、特権 1 を A01 の特権オブジェクトとして、RAC1 と RAC2 を A01 の RAC デバイスとして追加します。
7. ユーザー 3 を関連オブジェクト 2（A02）のメンバ、特権 2 を A02 の特権オブジェクト、RAC2 を A02 の RAC デバイスとして追加します。

拡張スキーマ Active Directory の設定

Active Directory を設定して CMC にアクセスするには、次の手順を実行します。

1. Active Directory スキーマを拡張します。
2. Active Directory ユーザーとコンピュータスナップインを拡張します。
3. Active Directory に CMC ユーザーと権限を追加します。
4. 各ドメインコントローラ上で SSL を有効にします。
5. CMC ウェブインタフェースまたは RACADM を使用して、CMC Active Directory のプロパティを設定します。

関連リンク

Active Directory スキーマの拡張
Active Directory ユーザーとコンピュータスナップインへの Dell 拡張のインストール
Active Directory への CMC ユーザーと特権の追加
CMC ウェブインタフェースを使用した拡張スキーマの Active Directory の設定
RACADM を使用した拡張スキーマの Active Directory の設定

Active Directory スキーマの拡張

Active Directory スキーマを拡張すると、Active Directory スキーマに Dell の組織単位、スキーマクラスと属性、および権限例と関連オブジェクトが追加されます。スキーマを拡張する前に、ドメインフォレストのスキーママスタ Flexible Single Master Operation（FSMO）役割所有者におけるスキーマ管理者権限を所持していることを確認してください。

スキーマは、次のいずれかの方法を使用して拡張できます

- Dell Schema Extender ユーティリティ
- LDIF スクリプトファイル

LDIF スクリプトファイルを使用すると、Dell の組織単位はスキーマに追加されません。

LDIF ファイルと Dell Schema Extender はそれぞれ『*Dell Systems Management Tools およびマニュアル*』DVD の次のディレクトリに収録されています。

- **DVDdrive:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced \LDIF_Files**
- **<DVDdrive>:\SYSMGMT\ManagementStation\support\OMActiveDirector y_Tools \Remote_Management_Advanced\Schema Extender**

LDIF ファイルを使用するには、**LDIF_Files** ディレクトリにある readme の説明を参照してください。

Schema Extender または LDIF ファイルは、任意の場所にコピーして実行することができます。

Dell Schema Extender の使用

注意: Dell Schema Extender では、SchemaExtenderOem.ini ファイルを使用します。Dell Schema Extender ユーティリティが正常に機能することを確認するため、このファイルの名前は変更しないでください。

1. **ようこそ** 画面で、**次へ** をクリックします。
2. 警告を読み、理解した上で、もう一度 **次へ** をクリックします。
3. **現在のログイン資格情報を使用** を選択するか、スキーマ管理者権限でユーザー名とパスワードを入力します。
4. **次へ** をクリックして、Dell Schema Extender を実行します。
5. **終了** をクリックします。
   スキーマが拡張されます。スキーマ拡張子を確認するには、MMC と Active Directory スキーマスナップインを使用して、クラスと属性があることを確認します。クラスと属性に関する詳細は、「クラスと属性」を参照してください。MMC および Active Directory スキーマスナップインの使い方は、Microsoft のマニュアルを参照してください。

クラスと属性

表 20. : Active Directory スキーマに追加されたクラスのクラス定義

クラス名	割り当てられたオブジェクト識別番号（OID）
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

表 21. : dellRacDevice クラス

OID	1.2.840.113556.1.8000.1280.1.7.1.1
説明	Dell RAC7 デバイスを表します。Active Directory では、RAC7 は delliDRACDevice として設定される必要があります。この設定によって、CMC から Active Directory に Lightweight Directory Access Protocol（LDAP）クエリを送信できるようになります。
クラスの種類	構造体クラス
SuperClasses	dellProduct
属性	dellSchemaVersion dellRacType

表 22. : delliDRACAssociationObject クラス

OID	1.2.840.113556.1.8000.1280.1.7.1.2
説明	Dell 関連オブジェクトを表します。関連オブジェクトは、ユーザーとデバイス間の連結を可能にします。
クラスの種類	構造体クラス
SuperClasses	グループ
属性	dellProductMembers dellPrivilegeMember

表 23. : dellRAC4Privileges クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.3
説明	CMC デバイスの権限（承認権限）を定義します。
クラスの種類	補助クラス
SuperClasses	なし
属性	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsTestAlertUser dellIsDebugCommandAdmin dellPermissionMask1 dellPermissionMask2

表 24. : dellPrivileges クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.4
説明	デルの権限（許可権限）のコンテナクラスとして使用されます。
クラスの種類	構造体クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.4
SuperClasses	ユーザー
属性	dellRAC4Privileges

表 25. : dellProduct クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.5
説明	すべての Dell 製品が派生するメインクラス。
クラスの種類	構造体クラス
SuperClasses	コンピュータ
属性	dellAssociationMembers

表 26. : Active Directory スキーマに追加された属性のリスト

割り当てられた OID/ 構文オブジェクト識別子	単一値
属性：dellPrivilegeMember **説明**：この属性に属する dellPrivilege オブジェクトのリスト。 **OID:** 1.2.840.113556.1.8000.1280.1.1.2.1 **識別名**：（LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12）	FALSE
属性：dellProductMembers **説明**: この役割に属する dellRacDevices オブジェクトのリスト。この属性は、dellAssociationMembers バックワードリンクへのフォワードリンクです。 **リンク ID**：12070 **OID**：1.2.840.113556.1.8000.1280.1.1.2.2 **識別名**：（LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12）	FALSE
属性：dellIsCardConfigAdmin **説明**：ユーザーがデバイスの設定権限がある場合には TRUE。 **OID**： 1.2.840.113556.1.8000.1280.1.1.2.4 ブール（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE
属性：dellIsLoginUser **説明**：ユーザーがデバイスでログイン権限がある場合には TRUE。 **OID**：1.2.840.113556.1.8000.1280.1.1.2.3 ブール（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE
属性：dellIsUserConfigAdmin **説明**：ユーザーがデバイスのユーザー設定システム管理者権限がある場合には TRUE。 **OID**：1.2.840.113556.1.8000.1280.1.1.2.5 ブール（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE

割り当てられた OID/ 構文オブジェクト識別子	単一値
属性：delIsLogClearAdmin **説明**：ユーザーがデバイスのログのクリアシステム管理者権限がある場合には TRUE。 **OID**：1.2.840.113556.1.8000.1280.1.1.2.6 ブール（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE
属性：dellIsServerResetUser **説明**：ユーザーがデバイスのサーバーリセット権限がある場合には TRUE。 **OID**：1.2.840.113556.1.8000.1280.1.1.2.7 ブール（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE
属性：dellIsTestAlertUser **説明**：ユーザーがデバイスのテスト警告ユーザー権限がある場合には TRUE。 **OID**：1.2.840.113556.1.8000.1280.1.1.2.10 ブール（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE
属性：dellIsDebugCommandAdmin **説明**：ユーザーがデバイスのデバッグコマンドシステム管理者権限がある場合には TRUE。 **OID**：1.2.840.113556.1.8000.1280.1.1.2.11 ブール（LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7）	TRUE
属性：dellSchemaVersion **説明**：現在のスキーマバージョンを使用してスキーマをアップデートします。 **OID**：1.2.840.113556.1.8000.1280.1.1.2.12 大文字小文字を区別しない文字列（LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905）	TRUE
属性：dellRacType **説明**：この属性は dellRacDevice オブジェクトの現在の RAC タイプで、dellAssociationObjectMembers フォワードリンクへのバックワードリンクです。 **OID**：1.2.840.113556.1.8000.1280.1.1.2.13 大文字小文字を区別しない文字列（LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905）	TRUE
属性：dellAssociationMembers **説明**：この製品に属する dellAssociationObjectMembers のリスト。この属性は、dellProductMembers にリンクされた属性へのバックワードリンクです。 **リンク ID**：12071 **OID**：1.2.840.113556.1.8000.1280.1.1.2.14 識別名（LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12）	FALSE
属性：dellPermissionsMask1	

割り当てられた OID/ 構文オブジェクト識別子	単一値

OID：1.2.840.113556.1.8000.1280.1.6.2.1 整数（LDAPTYPE_INTEGER）

属性：dellPermissionsMask2

OID：1.2.840.113556.1.8000.1280.1.6.2.2 整数（LDAPTYPE_INTEGER）

Active Directory ユーザーとコンピュータスナップインへの Dell 拡張のインストール

Active Directory でスキーマを拡張する場合は、RAC（CMC）デバイス、ユーザーとユーザーグループ、RAC 関連、RAC 特権などを管理できるように、Active Directory ユーザーとコンピュータスナップインも拡張する必要があります。

『*Dell Systems Management Tools およびマニュアル*』DVD を使用してシステム管理ソフトウェアをインストールする場合、インストール手順の実行中に **Active Directory ユーザーとコンピュータスナップイン** オプションを選択して、スナップインを拡張できます。システム管理ソフトウェアのインストールに関する追加手順については、『*Dell OpenManage ソフトウェアクイックインストールガイド*』を参照してください。64 ビットの Windows オペレーティングシステムの場合、スナップインのインストーラは次の場所にあります。
<DVDdrive>:\SYSMGMT\ManagementStation\support\OMActiveDirect ory_SnapIn64

Active Directory ユーザーとコンピュータスナップインの詳細については、マイクロソフトのマニュアルを参照してください。

Active Directory への CMC ユーザーと特権の追加

Dell 拡張 Active Directory ユーザーとコンピュータスナップインを使用して、RAC デバイスオブジェクト、関連オブジェクト、および権限オブジェクトを作成することにより、CMC ユーザーおよび権限を追加できます。各オブジェクトを追加するには、次の操作を行います。

- RAC デバイスオブジェクトの作成
- 権限オブジェクトの作成
- 関連オブジェクトの作成
- 関連オブジェクトへのオブジェクトの追加

関連リンク

関連オブジェクトへのオブジェクトの追加
RAC デバイスオブジェクトの作成
権限オブジェクトの作成
関連オブジェクトの作成

RAC デバイスオブジェクトの作成

RAC デバイスオブジェクトを作成するには、次の手順を実行します。

1. **コンソールのルート（MMC）** ウィンドウでコンテナを右クリックします。
2. **新規 → Dell リモート管理オブジェクトの詳細設定** を選択します。
   新規オブジェクト ウィンドウが表示されます。
3. 新しいオブジェクトの名前を入力します。名前は、「CMC ウェブインタフェースを使用した拡張スキーマの Active Directory の設定」で入力した CMC 名と同じである必要があります。
4. **RAC デバイスオブジェクト** を選択し、**OK** をクリックします。

権限オブジェクトの作成

権限オブジェクトを作成するには、次の手順を実行します。

メモ: 権限オブジェクトは、関係のある関連オブジェクトと同じドメイン内に作成する必要があります。

1. **コンソールのルート（MMC）** ウィンドウでコンテナを右クリックします。
2. **新規 → Dell リモート管理オブジェクトの詳細設定** を選択します。
   新規オブジェクト ウィンドウが表示されます。
3. 新しいオブジェクトの名前を入力します。
4. **権限オブジェクト** を選択し、**OK** をクリックします。
5. 作成した権限オブジェクトを右クリックして **プロパティ** を選択します。
6. **RAC 権限** タブをクリックして、ユーザーまたはグループに対する権限を設定します。
   CMC ユーザー権限の詳細については、「ユーザーのタイプ」を参照してください。

関連オブジェクトの作成

関連オブジェクトはグループから派生したもので、グループタイプを含む必要があります。関連スコープは、関連オブジェクトのセキュリティグループタイプを指定します。関連オブジェクトを作成する際は、追加するオブジェクトのタイプに適用する関連スコープを選択してください。たとえば、ユニバーサルを選択すると、Active Directory ドメインがネイティブモードで機能している場合のみ、関連オブジェクトが使用可能になります。

関連オブジェクトを作成するには、次の手順を実行します。

1. **コンソールのルート（MMC）** ウィンドウでコンテナを右クリックします。
2. **新規 → Dell リモート管理オブジェクトの詳細設定** を選択します。
   この **新規オブジェクト** ウィンドウが表示されます。
3. 新規オブジェクトの名前を入力し、**関連オブジェクト** を選択します。
4. **関連オブジェクト** の範囲を選択し、**OK** をクリックします。

関連オブジェクトへのオブジェクトの追加

関連オブジェクトプロパティ ウィンドウを使用すると、ユーザーまたはユーザーグループ、権限オブジェクト、および RAC デバイスまたは RAC デバイスグループを関連付けることができます。お使いのシステムが Microsoft Windows 2000 以降のモードで稼働している場合は、ユニバーサルグループを使って、ユーザーまたは RAC オブジェクトでドメインをスパンします。

ユーザーおよび RAC デバイスのグループを追加できます。デル関連グループとデルに関連しないグループを作成する手順は同じです。

関連リンク

ユーザーまたはユーザーグループの追加
権限の追加
RAC デバイスまたは RAC デバイスグループの追加

ユーザーまたはユーザーグループの追加

ユーザーまたはユーザーグループを追加するには、次の手順を実行します。

1. **関連オブジェクト** を右クリックし、**プロパティ** を選択します。
2. **ユーザー** タブを選択して、**追加** を選択します。
3. ユーザーまたはユーザーグループの名前を入力し、**OK** をクリックします。

権限の追加

権限を追加するには、次の手順を実行します。

1. **権限オブジェクト** タブを選択し、**追加** をクリックします。
2. 権限オブジェクト名を入力し、**OK** をクリックします。

   権限オブジェクト タブをクリックして、RAC7 デバイスに対して認証を行うときにユーザーまたはユーザーグループの権限を定義する関連に、権限オブジェクトを追加します。関連オブジェクトに追加できる権限オブジェクトは、1 つだけです。

RAC デバイスまたは RAC デバイスグループの追加

RAC デバイスまたは RAC デバイスグループを追加するには、次の手順に従います。

1. **製品** タブを選択して **追加** をクリックします。
2. RAC デバイスまたは RAC デバイスグループの名前を入力し、**OK** をクリックします。
3. **プロパティ** ウィンドウで、**適用**、**OK** の順にクリックします。

   製品 タブをクリックして、1 台または複数台の RAC デバイスを関連に追加します。関連デバイスは、ネットワークに接続している RAC デバイスのうち、定義したユーザーまたはユーザーグループが使用できるものを指定します。関連オブジェクトには複数の RAC デバイスを追加できます。

CMC ウェブインタフェースを使用した拡張スキーマの Active Directory の設定

CMC ウェブインタフェースを使用して Active Directory を拡張スキーマで設定するには、次の手順を実行します。

メモ: さまざまなフィールドについての情報は、『*CMC オンラインヘルプ*』を参照してください。

1. システムツリーで、**シャーシの概要** へ移動し、**ユーザー認証 → ディレクトリサービス** をクリックします。
2. **Microsoft Active Directory （拡張スキーマ）** を選択します。

   拡張スキーマ用に設定される設定値が同じページに表示されます。
3. 以下を指定します。
   - Active Directory を有効化し、ルートドメイン名とタイムアウト値を入力します。
   - ドメインコントローラとグローバルカタログの検索を直接呼び出す場合は、**検索する AD サーバーの検索（オプション）** オプションを選択して、ドメインコントローラとグローバルカタログの詳細を指定します。

     メモ: IP アドレスを 0.0.0.0 に設定すると、CMC のサーバー検索が無効になります。

     メモ: コンマ区切りのドメインコントローラまたはグローバルカタログサーバーのリストを指定できます。CMC では、最大 3 個の IP アドレスまたはホスト名を指定できます。

     メモ: ドメインコントローラまたはグローバルカタログサーバーが、すべてのドメインとアプリケーションに対して正しく設定されていない場合は、既存のアプリケーション / ドメインの動作中に予期しない結果が生成される可能性があります。
4. 設定を保存するには、**適用** をクリックします。

   メモ: 先に進む前に、設定を適用する必要があります。設定を適用しない場合、次のページへ移動したときに設定が失われます。
5. **拡張スキーマ設定** セクションで、CMC デバイス名およびドメイン名を入力します。
6. 証明書の検証を有効にした場合、ドメインフォレストのルート認証局の署名付き証明書を CMC にアップロードする必要があります。**証明書を管理** セクションで、証明書のファイルパスを入力するか、参照 をクリックして証明書ファイルを選択します。**アップロード** をクリックしてファイルを CMC にアップロードします。

メモ: アップロードする証明書の相対ファイルパスが `File Path` の値に表示されます。フルパスと正しいファイル名とファイル拡張子を含む絶対ファイルパスを入力する必要があります。

ドメインコントローラの SSL 証明書は、ルート認証局の署名付き証明書で署名されていなければなりません。CMC にアクセスする管理ステーションで、ルート認証局の署名付き証明書が使用可能である必要があります。

注意: デフォルトでは、SSL 証明書の検証が必要です。この証明書を無効にするには危険が伴います。

7. Kerberos Keytab セクションでシングルサインオン（SSO）を有効にした場合、**参照** をクリックしてキータブファイルを指定し、**アップロード** をクリックします。

   アップロードを完了したら、アップロードに成功または失敗したかを通知するメッセージが表示されます。

8. **適用** をクリックします。

   CMC ウェブサーバーが自動的に再起動します。

9. CMC ウェブインタフェースにログインします。

10. システムツリーで **シャーシ** を選択し、**ネットワーク** タブをクリックしてから **ネットワーク** サブタブをクリックします。

    ネットワーク設定 ページが表示されます。

11. CMC ネットワークインターフェース の IP アドレスに **DHCP を使用** が有効の場合は、次のいずれかを選択します。

    - **DHCP を使用して DNS サーバーアドレスを取得する** オプションを選択して、DNS サーバーアドレスが DHCP サーバーによって自動的に取得されるようにします。
    - **DHCP を使用して DNS サーバーアドレスを取得する** オプションを選択せずに、DNS サーバーの IP アドレスを手動で設定します。表示されるフィールドにプライマリおよび代替 DNS サーバーの IP アドレスを入力します。

12. **変更の適用** をクリックします。

    拡張スキーマ用の Active Directory 設定が設定されます。

RACADM を使用した拡張スキーマの Active Directory の設定

RACADM を使用した拡張スキーマの CMC Active Directory を設定するには、次の手順を実行します。

1. シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインした後、次を入力します。

   ```
   racadm config -g cfgActiveDirectory -o cfgADEnable 1 racadm config -g cfgActiveDirectory -o cfgADType 1 racadm config -g cfgActiveDirectory -o cfgADRacDomain <CMC の完全修飾ドメイン名> racadm config -g cfgActiveDirectory -o cfgADRootDomain <完全修飾ルートドメイン名> racadm config -g cfgActiveDirectory -o cfgADRacName <CMC のコモンネーム> racadm sslcertupload -t 0x2 -f <ADS ルート CA 証明書> -r racadm sslcertdownload -t 0x1 -f <CMC の SSL 証明書>
   ```

   メモ: このコマンドはリモート RACADM を介してのみ使用できます。リモート RACADM の情報については、『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

   オプション : DNS サーバーから返されたサーバーを使用せずに、LDAP またはグローバルカタログサーバーを指定してユーザー名を検索する場合は、次の **サーバーの指定** オプションを有効にします。

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

   メモ: サーバーの指定 オプションを使用すると、認証局の署名付き証明書が、指定したサーバーの名前と照合されません。IP アドレスだけでなくホスト名も入力できるため、CMC システム管理者にとっては特に便利です。

サーバーの指定 オプションを有効にした後、サーバーの IP アドレスまたは完全修飾ドメイン名（FQDN）で LDAP サーバーとグローバルカタログを指定できます。FQDN はサーバーのホスト名とドメイン名で構成されます。

LDAP サーバーを指定するには次のように入力します。

```
racadm config -g cfgActiveDirectory -o cfgADDomainController <AD ドメインコントローラの IP アドレス>
```

グローバルカタログサーバーを指定するには次のように入力します。

```
racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog <AD グローバルカタログの IP アドレス>
```

メモ: IP アドレスを 0.0.0.0 に設定すると、CMC のサーバー検索が無効になります。

メモ: コンマ区切りの LDAP または グローバルカタログサーバーのリストを 指定できます。CMC では、最大 3 個の IP アドレスまたはホスト名を指定できます。

メモ: すべてのドメインとアプリケーションに LDAP が正しく設定されていないと、既存のアプリケーション / ドメインの機能中に予期せぬ結果を招くことがあります。

2. 次のいずれかのオプションを使用して DNS サーバーを指定します。

   - CMC で DHCP が有効化されており、DHCP サーバーによって自動取得される DNS アドレスを使用したい場合は、次のコマンドを入力します。

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

   - CMC で DHCP が無効になっている場合や、DHCP が有効でも DNS の IP アドレスを手動で指定したい場合は、次のコマンドを入力します。

     ```
     racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0 racadm config -g cfgLanNetworking -o cfgDNSServer1 <プライマリ DNS IP アドレス>
     racadm config -g cfgLanNetworking -o cfgDNSServer2 <セカンダリ DNS IP アドレス>
     ```

これで、拡張スキーマ機能の設定は完了しました。

汎用 LDAP ユーザーの設定

CMC は Lightweight Directory Access Protocol（LDAP）ベースの認証をサポートするための汎用ソリューションを提供します。この機能は、ディレクトリサービス上のどのスキーマ拡張にも必要です。

CMC 管理者は、LDAP サーバーのユーザーログインを CMC と統合することが可能です。この統合を行うには、LDAP サーバーと CMC の両方での設定が必要です。Active Directory 側では、標準グループオブジェクトが役割グループとして使用されます。CMC のアクセス権を持つユーザーは、役割グループのメンバーとなります。特権は、Active Directory サポートを伴う標準スキーマセットアップの動作に似た認証のため、CMC に引き続き保存されます。

LDAP ユーザーが特定の CMC カードにアクセスできるようにするには、その CMC カードに役割グループ名とそのドメイン名を設定する必要があります。各 CMC には、5 つまで役割グループを設定できます。ユーザーは、オプションでディレクトリサービス内に複数のグループを追加できます。 ユーザーが複数グループのメンバの場合、そのグループのすべての特権を取得します。

役割グループの特権レベルおよびデフォルトの役割グループ設定に関する詳細は、「ユーザータイプ」を参照してください。

次の図は、汎用 LDAP を伴う CMC の設定を示しています。

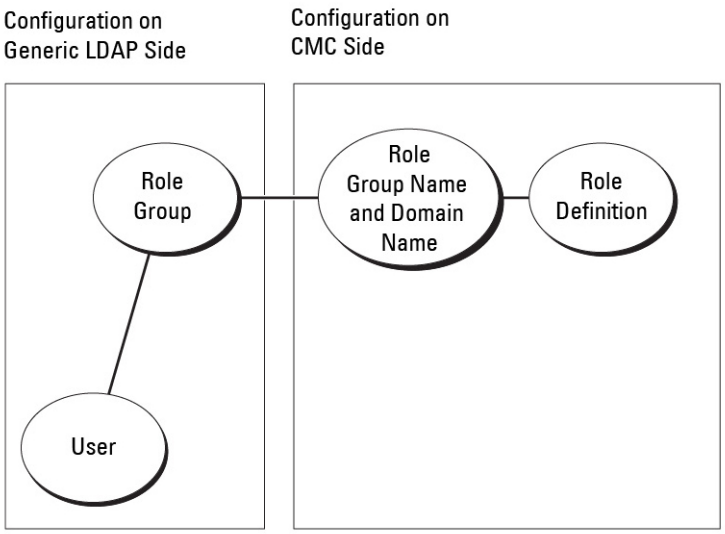


図 2. 汎用 LDAP を伴う CMC の設定

汎用 LDAP ディレクトリを設定した CMC へのアクセス

CMC の汎用 LDAP 実装では、ユーザーにアクセスを許可する際に、ユーザー認証とユーザー承認の 2 段階が行われます。

LDAP ユーザーの認証

一部のディレクトリサーバーでは、特定の LDAP サーバーに対して検索を行う前にバインドが必要です。ユーザーを認証するには、次の手順を実行します。

1. オプションでディレクトリサービスにバインドします。デフォルトは匿名バインドです。
2. ユーザーログインに基づきユーザーを検索します。デフォルトの属性は `uid` です。
   複数のオブジェクトが検出された場合、プロセスはエラーを返します。
3. バインドを解除してから、ユーザーの DN とパスワードを使ってバインド実行します。
   バインドできない場合は、ログインもできません。

これらの手順に問題がなければ、ユーザーは認証されています。

LDAP ユーザーの承認

ユーザーを承認するには、次の手順を実行します。

1. 設定された各グループで、`member or uniqueMember` 属性内のユーザーのドメイン名を検索します。
2. ユーザーがメンバーである各グループに対して、すべてのグループの権限がまとめられます。

CMC ウェブベースインタフェースを使用した汎用 LDAP ディレクトリサービスの設定

汎用 LDAP ディレクトリサービスを設定するには、次の手順を実行します。

メモ: シャーシ設定システム管理者 の権限が必要です。

1. システムツリーで、**シャーシの概要** へ移動し、**ユーザー認証 → ディレクトリサービス** をクリックします。
2. 汎用 **LDAP** を選択します。
   同じページに、標準スキーマ用に設定される設定が表示されます。
3. 以下を指定します。

   メモ: さまざまなフィールドについての情報は、『*CMC オンラインヘルプ*』を参照してください。

   - 共通設定
   - LDAP で使用するサーバー：
     * 静的サーバー — FQDN または IP アドレスおよび LDAP ポート番号を指定します。
     * DNS サーバー — DNS 内で SRV レコードを検索して、LDAP サーバーのリストを取得するための DNS サーバーを指定します。
       次の DNS クエリが SRV レコードに対して実行されます。
       `_[Service Name]._tcp.[Search Domain]`
       ここで、<*Search Domain*> は、クエリ内で使用するルートレベルドメインで、<*Service Name*> はクエリ内で使用するサービス名です。
       たとえば、次のとおりです。
       `_ldap._tcp.dell.com`
       ここで、`ldap` はサービス名、`dell.com` は検索ドメインです。
4. 設定を保存するには、**適用** をクリックします。

   メモ: 先に進む前に、設定を適用する必要があります。設定を適用しない場合、次のページへ移動したときに設定が失われます。
5. **グループ設定** セクションで、**役割グループ** をクリックします。**LDAP 役割グループの設定** ページが表示されます。
6. 役割グループのグループドメイン名と権限を指定します。
7. **適用** 役割グループの設定を保存し、**ユーザー設定ページに戻る** をクリックして **汎用 LDAP** を選択します。
8. **証明書の検証有効** オプションを選択した場合、 **証明書の管理** セクションで、SSL ハンドシェイク中に LDAP サーバー証明書を検証する CA 証明を指定し、**アップロード** をクリックします。
   証明書が CMC にアップロードされ、詳細が表示されます。
9. **適用** をクリックします。
   汎用 LDAP ディレクトリサービスが設定されました。

RACADM を使用した汎用 LDAP ディレクトリサービスの設定

ディレクトリサービスを設定するには、`cfgLdap` および `cfgLdapRoleGroup` RACADM グループにあるオブジェクトを使用します。

LDAP ログインの設定には、数多くのオプションがあります。大半の場合、デフォルト設定とともにいくつかのオプションを使います。

メモ: 初めてのセットアップで LDAP 設定をテストするには、`testfeature -f LDAP` コマンドを使用することをお勧めします。この機能は、IPv4 と IPv6 を両方サポートします。

必要なプロパティの変更には、LDAP ログインの有効化、サーバー FQDN または IP の設定、LDAP サーバーのベース DN の設定があります。

- `$ racadm config -g cfgLDAP -o cfgLDAPEnable 1`
- `$ racadm config -g cfgLDAP -o cfgLDAPServer 192.168.0.1`
- `$ racadm config -g cfgLDAP -o cfgLDAPBaseDN dc=company,dc=com`

オプションとして、DNS サーバーで SRW 記録のクエリを行うように CMC を設定できます。`cfgLDAPSRVLookupEnable` プロパティが有効の場合、`cfgLDAPServer` プロパティは無視されます。SRV レコードに対して DNS を検索する場合は、次のクエリが使用されます。

`_ldap._tcp.domainname.com`

上記のクエリの `ldap` は、`cfgLDAPSRVLookupServiceName` プロパティです。

`cfgLDAPSRVLookupDomainName` は、**domainname.com** に設定されます。

RACADM オブジェクトの詳細については、**dell.com/support/manuals** にある『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

10

シングルサインオンまたはスマートカードログイン用 CMC の設定

本項は、Active Directory ユーザーのスマートカードログインおよびシングルサインオン（SSO）ログイン用の CMC 設定に関する情報を提供します。

CMC バージョン 2.10 以降、CMC はスマートカードおよび SSO ログインに対応するため、Kerberos ベースの Active Directory 認証をサポートします。

SSO は認証方法として kerberos を使用するため、ドメインにサインインしたユーザーが Exchange など次に使用するアプリケーションに自動サインオンまたはシングルサインオンすることが可能になります。シングルサインオンでログインする場合、CMC はクライアントシステムの資格情報を使用します。この資格情報は、有効な Active Directory アカウントを使ってログインした後、オペレーティングシステムによってキャッシュされます。

2 要素認証ではユーザーがパスワードまたは PIN と秘密キーまたはデジタル証明書を含んだ物理カードを持っている必要があるため、高レベルのセキュリティを実現できます。Kerberos では、この 2 要素認証メカニズムを使用しており、これによってシステムはその信頼性を確認できます。

メモ: ログイン方法を選択しても、他のログインインタフェース（SSH など）に対してポリシー属性が設定されるわけではありません。他のログインインターフェースに対しては別のポリシー属性を設定する必要があります。すべてのログインインタフェースを無効にするには、**サービス** ページに移動してからすべて（または一部の）ログインインタフェースを無効にします。

Microsoft Windows 2000、Windows XP、Windows Server 2003、Windows Vista、Windows 7、および Windows Server 2008 は、Kerberos を SSO とスマートカード用の認証方法として使用することができます。

Kerberos の詳細については、Microsoft ウェブサイトを参照してください。

関連リンク

システム要件
シングルサインオンまたはスマートカードログインの前提条件
Active Directory ユーザーに対する CMC SSO またはスマートカードログインの設定

システム要件

Kerberos 認証を使用するには、ネットワークには以下が必要です。

- DNS サーバー
- Microsoft Active Directory Server

  メモ: Windows 2003 で Active Directory を使用している場合は、クライアントシステムに最新のサービスパックとパッチがインストールされていることを確認してください。Windows 2008 で Active Directory を使用している場合は、SP1 と次のホットフィックスがインストールされていることを確認してください。

  KTPASS ユーティリティ用 **Windows6.0-KB951191-x86.msu**。このパッチがないと、ユーティリティで不良な keytab ファイルが生成されます。

  LDAP バインド中に GSS_API および SSL トランザクションに使用する **Windows6.0-KB957072-x86.msu**。
- Kerberos キー配付センター（Active Directory サーバーソフトウェアに同梱）

- DHCP サーバー（推奨）
- DNS サーバー用のリバース（逆引き）ゾーンには Active Directory サーバーと CMC 用のエントリが必要です。

クライアントシステム

- Smart Card でログインする場合は、クライアントシステムには Microsoft Visual C++ 2005 再頒布可能なプログラムが必要です。詳細は、**www.microsoft.com/downloads/details.aspx?FamilyID=32BC1BEEA3F9-4C13-9C99-220B62A191EE&displaylang=en** を参照してください。
- シングルサインオンまたは Smart Card ログインでは、クライアントシステムは Active Directory ドメインと Kerberos 領域の一部である必要があります。

CMC

- CMC にはファームウェアバージョン 2.10 以降が必要
- 各 CMC には Active Directory アカウントが必要
- CMC は Active Directory ドメインと Kerberos Realm の一部である必要があります。

シングルサインオンまたはスマートカードログインの前提条件

SSO またはスマートカードログイン設定の前提条件は、次のとおりです。

- Active Directory（ksetup）の Kerberos レルムとキー配付センター（KDC）の設定
- クロックドリフトやリバースルックアップに伴う問題を回避するための強固な NTP および DNS インフラストラクチャ。
- 承認済みメンバーのある Active Directory 標準スキーマ役割グループに対する CMC の設定
- スマートカード用には、各 CMC の Active Directory を作成し、事前認証でなく Kerberos DES 暗号化を使用できるように設定します。
- SSO またはスマートカードのログインに使用するブラウザの設定
- Ktpass を使用して CMC ユーザーをキー配付センターに登録します（これにより、CMC にアップロードするキーも出力されます）。

関連リンク

標準スキーマ Active Directory の設定
拡張スキーマ Active Directory の設定
SSO ログイン用のブラウザの設定
Kerberos Keytab ファイルの生成
スマートカードのログインに使用するブラウザの設定

Kerberos Keytab ファイルの生成

SSO およびスマートカードログイン認証をサポートするために、CMC は Windows Kerberos ネットワークをサポートします。ktpass ツール（サーバーインストール CD/DVD の一部として Microsoft から提供）はユーザーアカウントにサービスプリンシパル名（SPN）バインドを作成して、信頼情報を MIT-スタイルの Kerberos keytab ファイルにエクスポートします。ktpass ユーティリティの詳細は、Microsoft のウェブサイトを参照してください。

keytab ファイルを生成する前に、ktpass コマンドの **-mapuser** オプションと使用する Active Directory ユーザーアカウントを作成する必要があります。さらに、このアカウントは、生成した keytab ファイルをアップロードする CMC DNS 名と同じ名前にする必要があります。

ktpass ツールを使用して keytab ファイルを生成するには、次の手順を実行します。

1. *ktpass* ユーティリティを、Active Directory 内のユーザーアカウントに CMC をマップするドメインコントローラ（Active Directory サーバー）上で実行します。
2. 次の ktpass コマンドを使用して、Kerberos keytab ファイルを作成します。

   ```
   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
   ```

   メモ: cmcname.domainname.com には RFC の要求に従って小文字を使用し、領域名 @REALM_NAME には大文字を使用します。さらに、CMC では Kerberos 認証用の DES-CBC-MD5 タイプの暗号化もサポートされています。

   CMC にアップロードする必要のある keytab ファイルが作成されます。

   メモ: keytab には暗号化キーが含まれているので、安全な場所に保管してください。*ktpass* ユーティリティの詳細については、**Microsoft** ウェブサイトを参照してください。

Active Directory スキーマ用の CMC の設定

Active Directory 標準スキーマ用の CMC の設定に関する情報は、「標準スキーマ Active Directory の設定」を参照してください。
Active Directory 拡張スキーマ用の CMC の設定に関する情報は、「拡張スキーマ Active Directory の概要」を参照してください。

SSO ログイン用のブラウザの設定

シングルサインオン（SSO）は、Internet Explorer バージョン 6.0 以降と Firefox バージョン 3.0 以降でサポートされています。

メモ: 次の手順は、CMC が Kerberos 認証でシングルサインオンを使用する場合にのみ適用されます。

Internet Explorer

Internet Explorer でシングルサインオンの設定を行うには、次の手順を実行します。

1. Internet Explorer で、**ツール → インターネットオプション** を選択します。
2. **セキュリティ** タブの **セキュリティ設定を表示または変更するゾーンを選択する** の下で、**ローカルイントラネット** を選択します。
3. **サイト** をクリックします。
   ローカルイントラネット ダイアログボックスが表示されます。
4. **詳細設定** をクリックします。
   ローカルイントラネットの詳細設定 ダイアログボックスが表示されます。
5. **このサイトをゾーンに追加する** に CMC の名前とそれが属するドメインを入力し、**追加** をクリックします。

   メモ: 対象ドメインでは、ワイルドカード（*）を使用してすべてのデバイスまたはユーザーを指定できます。

Mozilla Firefox

1. Firefox では、アドレスバーに **about:config** と入力します。

メモ: ブラウザに「**保証が無効になる場合があります**」という警告が表示された場合は、**注意することをお約束します** をクリックします。

2. **フィルタ** テキストボックスに、**negotiate** と入力します。
   ブラウザには、「negotiate」という単語を含んだプリファレンス名のリストが表示されます。
3. 表示されたリストから、**network.negotiate-auth.trusted-uris** をダブルクリックします。
4. **文字列値の入力** ダイアログボックスに、CMC のドメイン名を入力し、**OK** をクリックします。

スマートカードのログインに使用するブラウザの設定

Mozilla Firefox — CMC 2.10 では、Firefox ブラウザを使ってスマートカードにログインすることはできません。

Internet Explorer — インターネットブラウザが Active-X プラグインをダウンロードするように設定されていることを確認します。

Active Directory ユーザーに対する CMC SSO またはスマートカードログインの設定

CMC ウェブインタフェースまたは RACADM を使用して、 CMC SSO またはスマートカードログインを設定することができます。

関連リンク

シングルサインオンまたはスマートカードログインの前提条件
Keytab ファイルのアップロード

ウェブインタフェースを使用した Active Directory ユーザーの CMC SSO またはスマートカードログインの設定

CMC での Active Directory SSO またはスマートカードログインを設定するには、次の手順を実行します。

メモ: オプションの詳細については、『*CMC オンラインヘルプ*』を参照してください。

1. ユーザーアカウントをセットアップするために Active Directory を設定する際に、次の追加手順を実行しまうｓ。
   - keytab ファイルをアップロードします。
   - SSO を有効にするには、**シングルサインオンを有効にする** オプションを選択します。
   - スマートカードログインを有効にするには、**スマートカードログインの有効化** オプションを選択します。

     メモ: このオプションが選択された場合、セキュアシェル（SSH）、Telnet、シリアル、リモート RACADM など、すべてのコマンドライン帯域外インタフェースは変更されません。
2. **適用** をクリックします。
   設定が保存されます。
   RACADM コマンドを使用して、Kerberos 認証によって Active Directory をテストできます。

   ```
   testfeature -f adkrb -u <ユーザー>@<ドメイン>
   ```

   ここで、<ユーザー>は有効な Active Directory ユーザーアカウントを指します。

   コマンドが正常に実行されれば、CMC は Kerberos 資格情報を取得することができ、ユーザーの Active Directory アカウントにアクセスできることを示します。コマンドが正常に実行されない場合は、エラーを訂正してコマンドを実行し直してください。詳細については、デルサポートサイト **dell.com/support/manuals** の『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

Keytab ファイルのアップロード

Kerberos keytab ファイルは Kerberos データセンター（KDC）に対する CMC のユーザ名とパスワード資格情報として使用され、これによって Active Directory にアクセスすることができます。Kerberos 領域の各 CMC は Active Directory を使って登録し、一意の keytab ファイルがあることが必要です。

Active Directory Server 関連で生成される Kerberos Keytab をアップロードできます。**ktpass.exe** ユーティリティを実行すると、Active Directory Server から Kerberos Keytab を生成できます。この keytab は、Active Directory Server と CMC の間の信頼関係を確立します。

keytab ファイルをアップロードするには：

1. システムツリーで、**シャーシの概要** へ移動し、**ユーザー認証 → ディレクトリサービス** をクリックします。
2. **Microsoft Active Directory 標準スキーマ** を選択します。
3. **Kerberos Keytab** セクションで、**参照** をクリックして keytab ファイルを選択し、**アップロード** をクリックします。
   アップロードを完了したら、keytab ファイルのアップロードに成功または失敗したかを通知するメッセージが表示されます。

RACADM を使用した Active Directory ユーザー用 CMC SSO ログインまたはスマートカードログインの設定

SSO を有効にするには、Active Directory の設定中に実行する手順への追加として、次のコマンドを実行します。

```
racadm -g cfgActiveDirectory -o cfgADSSOEnable 1
```

スマートカードログインを有効にするには、Active Directory の設定中に実行する手順への追加として、次のオブジェクトに従います。

- `cfgSmartCardLogonEnable`
- `cfgSmartCardCRLEnable`

11

CMC にコマンドラインコンソールの使用を設定する方法

本項では、CMC コマンドラインコンソール（またはシリアル/Telnet/セキュアシェルコンソール）の機能について、およびコンソールからシステム管理操作を実行できるようにシステムを設定する方法について説明します。コマンドラインコンソールを介して CMC で RACADM コマンドを使用する方法については、『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

関連リンク

シリアル、Telnet、または SSH コンソールを使用した CMC へのログイン

CMC コマンドラインコンソールの特徴

CMC は、次のシリアル、Telnet、SSH コンソール機能をサポートしています。

- 単一のシリアルクライアント接続と最大 4 つの Telnet クライアントの同時接続。
- 最大 4 つのセキュアシェル（SSH）クライアント同時接続。
- RACADM コマンドに対応。
- サーバーおよび I/O モジュールのシリアルコンソールに接続するビルトイン connect コマンド。これは racadm onnect としても利用可能です。
- コマンドラインの編集と履歴。
- 全コンソールインタフェースにおけるセッションタイムアウト制御。

CMC コマンドラインのコマンド

CMC コマンドラインに接続すると、次のコマンドを入力できます。

表 27. : CMC コマンドラインのコマンド

コマンド	説明
racadm	RACADM コマンドはキーワード racadm で始まり、サブコマンドが続きます。詳細については、『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。
connect	サーバーまたは I/O モジュールのシリアル コンソールに接続します。詳細は、「接続コマンドでサーバーまたは I/O モジュールに接続する」を参照してください。 **メモ:** また、racadm connect コマンドも使用できます。
exit、logout、quit	これらのコマンドはすべて同じ処置を実行します。現在のセッションを終了してログインプロンプトに戻ります。

CMC での Telnet コンソールの使用

CMC では、Telnet セッションを 4 つまで同時に行うことができます。

管理ステーションで Microsoft Windows XP または Windows 2003 を実行している場合は、CMC の telnet セッションで文字の不具合が発生する可能性があります。この問題は、リターンキーが応答しない、およびパスワードプロンプトが表示されないログインのフリーズといった形で発生する可能性があります。

この問題を修正するには、**support.microsoft.com** からホットフィックス 824810 をダウンロードします。詳細について Microsoft Knowledge Base の記事 824810 を参照することもできます。

CMC での SSH の使用

SSH は Telnet セッションと同じ機能を備えたコマンドラインセッションですが、セッションのネゴシエーションと暗号化によってセキュリティが強化されています。CMC は、パスワード認証付きの SSH バージョン 2 をサポートしています。CMC ではデフォルトで SSH が有効になっています。

メモ: CMC は SSH バージョン 1 をサポートしていません。

CMC ログイン中にエラーが発生した場合は、SSH クライアントがエラーメッセージを発行します。メッセージのテキストはクライアントによって異なり、CMC では制御されません。エラーの原因を特定するには、RACLog メッセージを確認してください。

メモ: `OpenSSH` は Windows の VT100 または ANSI ターミナルエミュレータから実行する必要があります。また、**Putty.exe** を使用して `OpenSSH` を実行できます。Windows のコマンドプロンプトで `OpenSSH` を実行すると、完全には機能しません（一部のキーが応答せず、グラフィックが表示されません）。Linux を実行しているシステムの場合は、SSH クライアントサービスを実行して、いずれかのシェルで CMC に接続します。

SSH は一度に 4 セッションがサポートされます。セッションタイムアウトは、`cfgSsnMgtSshIdleTimeout` プロパティによって制御されます。詳細については、『iDRAC6 および CMC 向け RACADM コマンドラインリファレンスガイド』のデータベースプロパティの章、ウェブインタフェースの **サービス管理** ページ、または「サービスの設定」を参照してください。

CMC では、SSH 経由の公開キー認証（PKA）もサポートされています。この認証方法は、ユーザー ID/ パスワードの組み込みや入力を排除することで SSH スクリプトの自動化を改善します。詳細については、「SSH 経由の公開キー認証の設定」を参照してください。

SSH はデフォルトで有効になっています。SSH が無効になっている場合は、サポートされている他のインタフェースを使用して有効にできます。

SSH を設定するには、サービスの設定 を参照してください。

関連リンク

サービスの設定

サポート対象の SSH 暗号スキーム

SSH プロトコルを使用して CMC と通信するため、次の表に示す複数の暗号化スキームがサポートされています。

表 28. : 暗号スキーム

スキームの種類	スキーム
非対称暗号化	Diffie-Hellman DSA/DSS 512–1024（ランダム）ビット（NIST 仕様に準拠）
対称暗号	• AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
メッセージの整合性	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
認証	パスワード

SSH 経由の公開キー認証の設定

SSH インタフェース経由のサービスユーザー名には、最大 6 つの公開キーを設定できます。公開キーを追加または削除する前に、キーが誤って上書きされたり削除されたりしないように、view コマンドを使って設定済みのキーを確認するようにしてください。サービスユーザー名は、SSH 経由で CMC にアクセスする場合に使用できる特殊なユーザーアカウントです。SSH 経由の PKA が正しく設定されると、CMC にログインするためにユーザー名やパスワードを入力する必要がなくなります。この機能は、各種機能を実行するための自動化されたスクリプトを設定するときに大変便利です。

メモ: この機能を管理するための GUI サポートは用意されていません。使用できるのは RACADM のみです。

新しい公開キーを追加する場合は、追加時に既存のキーがインデックスにないことを確認します。CMC では、新しいキーを追加する前に、前のキーが削除されているかどうかの確認作業は行われません。新しいキーを追加すると、SSH インタフェースが有効な間、自動的に有効になります。

公開キーの公開キーコメントセクションを使用する場合は、CMC で使用するのは最初の 16 文字のみであることに注意してください。 すべての PKA ユーザーはサービスユーザー名を使用してログインします。そのため、RACADM `getssninfo` コマンドを使用する場合は、SSH ユーザーを識別できるように公開キーコメントが使用されます。

たとえば、コメント PC1 およびコメント PC2 を持つ 2 つの公開キーが設定されている場合は、次のようになります。

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

`sshpkauth` の詳細については、『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

関連リンク

Windows を実行するシステム用の公開キーの生成
Linux を実行するシステム用の公開キーの生成

Windows を実行するシステム用の公開キーの生成

アカウントを追加する前に、SSH 経由で CMC にアクセスするシステムからの公開キーが必要になります。公開 / 秘密キーペアを生成する方法には、Windows を実行しているクライアントの PuTTY キー生成アプリケーションを使用する方法と Linux を実行しているクライアントの ssh-keygen を使用する方法の 2 通りあります。

本項では、両方のアプリケーションで使用する公開 / 秘密キーペアを生成する簡単な手順について説明します。これらのツールの使用法の詳細については、アプリケーションヘルプを参照してください。

PuTTY Key Generator を使用して、Windows クライアントを実行しているシステム用の基本キーを作成するには、次の手順を実行します。

1. アプリケーションを起動し、生成するキーの種類として、SSH-2 RSA または SSH-2 DSA を選択します（SSH-1 はサポートされていません）。
2. キーのビット数を入力します。数字は 788～4096 の間で指定します。

   メモ: 768 未満、または 4096 を超えるキーを追加しても CMC から何のメッセージも表示されない場合がありますが、ログインしようとするとこれらのキーは失敗します。
3. **生成** をクリックし、指示に従ってマウスポインタをウィンドウ内で移動させます。

   キーを作成したら、キーコメントフィールドを変更できます。

   パスフレーズを入力すると、キーをセキュリティ保護することもできます。秘密キーを保存したことを確認します。
4. 公開キーの使用方法には 2 つのオプションがあります。
   - 公開キーをファイルに保存し後でアップロードします。
   - テキストオプションを使用してアカウントを追加する場合に、**公開キーの貼り付け** ウィンドウからテキストをコピーして貼り付けます。

Linux を実行するシステム用の公開キーの生成

Linux クライアント用の ssh-keygen アプリケーションは、グラフィカルユーザーインタフェースのないコマンドラインツールです。ターミナルウィンドウを開き、シェルプロンプトで次を入力します。

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

ここで、

-t は、dsa または rsa である必要があります。

-b は 768～4096 で、ビット暗号化サイズを指定します。

-c を使用すると、公開キーコメントを変更できます。これはオプションです。

<passphrase> はオプションです。コマンドを完了したら、パブリックファイルを使用してファイルをアップロードするために RACADM に渡します。

CMC の RACADM 構文メモ

racadm sshpkauth コマンドを使用する場合、次を確認します。

- -i オプションを使用する場合は、パラメータが svcacct である必要があります。CMC では、-i へのそれ以外のパラメータの使用は失敗します。svcacct は、CMC で SSH 経由の公開キー認証を行うための特殊なアカウントです。
- CMC にログインするには、ユーザーはサービスである必要があります。他のカテゴリのユーザーは、sshpkauth コマンドを使用して入力した公開キーにアクセスできません。

公開キーの表示

CMC に追加した公開キーを表示するには、次を入力します。

```
racadm sshpkauth -i svcacct -k all -v
```

キーを一度に 1 つずつ表示するには、`all` を数字の 1～6 に置き換えます。例えば、キー 2 を表示するには、次を入力します。

```
racadm sshpkauth -i svcacct -k 2 -v
```

公開キーの追加

ファイルのアップロード `-f` オプションを使用して公開キーを CMC に追加するには、次のように入力します。

```
racadm sshpkauth -i svcacct -k 1 -p 0xfff -f <公開キーファイル>
```

メモ: ファイルのアップロードオプションは、リモート RACADM でのみ使用できます。詳細については、『iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド』を参照してください。

テキストのアップロードオプションを使用して公開キーを追加するには、次を入力します。

```
racadm sshpkauth -i svcacct -k 1 -p 0xfff -t "<公開キーテキスト>"
```

公開キーの削除

公開キーを削除するには、次を入力します。

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

公開キーをすべて削除するには、次を入力します。

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

前面パネルからの iKVM への接続の有効化

iKVM 前面パネルポートの使用に関する情報および手順は、「前面パネルからの iKVM へのアクセスの有効化と無効化」を参照してください。

ターミナルエミュレーションソフトウェアの設定

CMC は、次の種類のターミナルエミュレーションソフトウェアを実行している管理ステーションからシリアルテキストコンソールをサポートしています。

- Linux Minicom。
- Hilgraeve の HyperTerminal Private Edition（バージョン 6.3）。

必要なタイプのターミナルソフトウェアを設定するには、次の副項の手順に従ってください。

Linux Minicom の設定

Minicom は Linux 用のシリアルポートアクセスユーティリティです。次の手順は Minicom バージョン 2.0 の設定に有効な手順です。他の Minicom バージョンは多少異なる場合がありますが、同じ基本設定が必要です。他の Minicom バージョンを設定するには、「必要な Minicom 設定」の項にある情報を参照してください。

Minicom バージョン 2.0 の設定

メモ: 最適な結果を得るには、**cfgSerialConsoleColumns** プロパティをコンソールの列数に一致するように設定します。プロンプトには 2 列分が使用されることに注意してください。たとえば、80 列のターミナルウィンドウでは、次のように設定します。

```
racadm config -g cfgSerial -o cfgSerialConsoleColumns 80
```

1. Minicom の設定ファイルがない場合には、次の手順に進んでください。Minicom 設定ファイルがある場合は、`minicom<Minicom config file name>` と入力し、 手順 12 に進みます。
2. Linux コマンドプロンプトで、`minicom -s` と入力します。
3. **シリアルポートセットアップ** を選択し、<Enter> を押します。
4. <a> を押して、適切なシリアルデバイスを選択します（例：`/dev/ttyS0`）。
5. <e> を押して、**速度 / パリティ / ビット** のオプションを **115200 8N1** に設定します。
6. <f> を押して、**ハードウェアフロー制御** を **はい** に、**ソフトウェアフロー制御** を **いいえ** に設定します。**シリアルポートセットアップ** メニューを終了するには、<Enter> を押します。
7. **モデムとダイヤル** を選択して、<Enter> を押します。
8. **モデムダイヤルとパラメータセットアップ** メニューで、<Backspace> を押して **init**、**reset**、**connect** および **hangup** 設定をクリアして空白にし、次に <Enter> をクリックして各空白値を保存します。
9. 指定のフィールドがすべてクリアされたら、<Enter> を押して **モデムダイヤルとパラメータセットアップ** メニューを終了します。
10. **Minicom を終了** を選択して、<Enter> を押します。
11. コマンドシェルプロンプトで、`minicom <Minicom config file name>` と入力します。
12. <Ctrl><a>、<x> 、または <Enter> を押して Minicom を終了します。

    Minicom ウィンドウにログインプロンプトが表示されていることを確認します。ログインプロンプトが表示されたら、接続が正常に行われています。これで CMC コマンドラインインタフェースにログインし、アクセスする準備が完了しました。

必要な Minicom 設定

Minicom を設定するには、どのバージョンでも表を参照してください。

表 29. : Minicom 設定

設定の説明	必要な設定
速度 / パリティ / ビット	115200 8N1
ハードウェアフロー制御	あり
ソフトウェアフロー制御	なし
ターミナルエミュレーション	ANSI
モデムダイヤルとパラメータ設定	**初期化**、**リセット**、**接続**、**切断** 設定をクリアして空白にします。

接続コマンドを使用したサーバーまたは I/O モジュールの接続

CMC は、サーバーのシリアルコンソールまたは I/O モジュールをリダイレクトするための接続を確立することができます。

サーバーでは、次を使用してシリアルコンソールリダイレクトを実行できます。

- `racadm connect` コマンド。詳細については、**dell.com/support/manuals** にある『iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド』を参照してください。

- iDRAC ウェブインタフェースのシリアルコンソールリダイレクト機能。
- iDRAC Serial Over LAN（SOL）機能。

シリアル、Telnet、SSH コンソールでは、CMC はサーバーまたは IOM モジュールへのシリアル接続の確立に connect コマンドをサポートします。サーバーシリアルコンソールには、BIOS 起動とセットアップ画面の両方と、オペレーティングシステムシリアルコンソールが備わっています。I/O モジュールには、スイッチシリアルコンソールが利用できます。

注意: CMC シリアルコンソールからの実行時は、CMC がリセットするまで connect -b オプションが接続されたままとなります。この接続はセキュリティリスクとなる可能性があります。

メモ: connect コマンドは、-b（バイナリ）オプションを提供します。-b オプションはバイナリのローデータを渡し、cfgSerialConsoleQuitKey は使用されません。さらに、CMC シリアルコンソールを使用したサーバーへの接続時に、DTR 信号の遷移（例えば、デバッガを接続するためにシリアルケーブルが取り外された場合）でログアウトされることはありません。

メモ: IOM がコンソールリダイレクトをサポートしない場合、connect コマンドは空のコンソールを表示します。この場合に CMC コンソールに戻るには、エスケープシーケンスを入力します。コンソールのデフォルトエスケープシーケンスは <Ctrl><\> です。

管理システムには最大 6 つの IOM があります。IOM に接続するには、以下を実行します。

```
connect switch-n
```

ここで n は IOM ラベル A1、A2、B1、B2、C1 および C2 です。

（シャーシにおける IOM の配置の図解については、 図 13-1 を参照してください。）connect コマンドで IOM を参照する際は、次の表で示されるように、IOM はスイッチにマップされています。

表 30. I/O モジュールからスイッチへのマッピング

I/O モジュールのラベル	スイッチ
A1	switch-a1 または switch- 1
A2	switch-a2 または switch- 2
B1	switch-b1 または switch-3
B2	switch-b2 または switch-4
C1	switch-c1 または switch-5
C2	switch-c2 または switch-6

メモ: IOM 接続は、各シャーシで一度に 1 接続のみが可能です。

メモ: シリアル コンソールからパススルーに接続することはできません。

管理下サーバーシリアルコンソールに接続するには、connect server-<*n*><*x*> コマンドを使用します。ここで *n* は 1〜8、 *x* は a、b、c、または d になります。racadm connect server-n コマンドを使用することもできます。-b オプションを使用してサーバーに接続すると、バイナリ通信が想定され、エスケープシーケンスは無効化されます。iDRAC を使用できない場合は、No route to host エラーメッセージが表示されます。

connect server-n コマンドでは、ユーザーによるサーバーのシリアルポートへのアクセスが可能になります。この接続が確立されると、ユーザーは CMC のシリアルポート経由でサーバーのコンソールリダイレクトを表示できます。これには、BIOS シリアルコンソールとオペレーティングシステムシリアルコンソールが含まれます。

メモ: BIOS 起動画面を表示するには、サーバーの BIOS セットアップでシリアルリダイレクトが有効化される必要があります。また、サーマルエミュレータウィンドウを 80x25 に設定する必要もあります。これを設定しないと、画面が文字化けします。

メモ: BIOS セットアップ画面では一部のキーが使用できないため、**CTRL+ALT+DEL** 用に適切なエスケープシーケンス、およびその他エスケープシーケンスを提供する必要があります。最初のリダイレクト画面に、必要なエスケープシーケンスが表示されます。

関連リンク

シリアルコンソールリダイレクト用に管理されたサーバー BIOS の設定
シリアルコンソールリダイレクトのための Windows の設定
起動中における Linux のシリアルコンソールリダイレクトのための設定
起動後のサーバーシリアルコンソールリダイレクトのための Linux の設定

シリアルコンソールリダイレクト用に管理されたサーバー BIOS の設定

KVM を使用して管理下サーバーに接続（「iKVM でのサーバー管理」を参照）、または iDRAC7 ウェブインタフェースからリモートコンソールセッションを確立する必要があります（**dell.com/support/manuals** の『*iDRAC7 ユーザーズガイド*』を参照）。

BIOS のシリアル通信はデフォルトでオフになっています。ホストテキストコンソールデータをシリアルオーバー LAN にリダイレクトするには、COM1 経由でコンソールリダイレクトを有効化する必要があります。BIOS 設定を変更するには、次の手順を実行します。

1. 管理下サーバーを起動します。
2. POST 中に <F2> キーを押して BIOS セットアップユーティリティを起動します。
3. **シリアル通信** にスクロールダウンし、<Enter> を押します。ポップアップダイアログボックスで、シリアル通信リストが次のオプションを表示します。
   - オフ
   - コンソールリダイレクトなしでオン
   - COM1 経由のコンソールリダイレクトでオン

   矢印キーを使用して、オプション間を移動します。
4. **COM1 経由のコンソールリダイレクトでオン** が有効になっていることを確認します。
5. **起動後のリダイレクト** を有効化します（デフォルトは **無効**）。このオプションは次回再起動時に BIOS コンソールリダイレクトを有効化します。
6. 変更を保存して終了します。
   管理下サーバーが再起動します。

シリアルコンソールリダイレクトのための Windows の設定

Windows Server 2003 以降の Microsoft Windows Server バージョンを実行しているサーバーには設定は必要ありません。Windows は BIOS から情報を受け取り、COM 1 の Special Administration Console（SAC）コンソールを有効化します。

起動中における Linux のシリアルコンソールリダイレクトのための設定

次の手順は Linux GRand Unified Bootloader（GRUB）に固有の手順です。異なるブートローダーを使用する場合は、類似した変更が必要です。

メモ: クライアント VT100 エミュレーションウィンドウの設定時、リダイレクトされたコンソールを表示するウィンドウまたはアプリケーションを 25 行 x 80 列に設定し、テキストが正しく表示されるようにしてください。この設定を行わないと、一部のテキスト画面が文字化けすることがあります。

/etc/grub.conf ファイルを次のように編集します。

1. ファイルの一般設定セクションを見つけ、次の 2 行を新たに追加します。
   ```
   serial --unit=1 --speed=57600 terminal --timeout=10 serial
   ```
2. カーネル行に次の 2 つにオプションを追加します。
   ```
   kernel console=ttyS1,57600
   ```
3. **/etc/grub.conf** に splashimage ディレクティブがある場合は、コメントアウトします。
   次の例は、この手順で説明した変更を示しています。
   ```
   # grub.conf generated by anaconda # # Note that you do not have to rerun
   grub after making changes # to this file # NOTICE: You do not have a /boot
   partition. This means that # all kernel and initrd paths are relative to /,
   e.g. # root (hd0,0) # kernel /boot/vmlinuz-version ro root= /dev/sda1 #
   initrd /boot/initrd-version.img # #boot=/dev/sda default=0 timeout=10
   #splashimage=(hd0,2)/grub/splash.xpm.gz serial --unit=1 --speed=57600 terminal --timeout=10
   serial title Red Hat Linux Advanced Server (2.4.9-e.3smp) root (hd0,0) kernel /
   boot/vmlinuz-2.4.9-e.3smp ro root= /dev/sda1 hda=ide-scsi console=ttyS0
   console= ttyS1,57600 initrd /boot/initrd-2.4.9-e.3smp.img title Red Hat
   Linux Advanced Server-up (2.4.9-e.3) root (hd0,00) kernel /boot/
   vmlinuz-2.4.9-e.3 ro root=/dev/sda1 initrd /boot/initrd-2.4.9-e.3.img
   ```

   /etc/grub.conf ファイルを編集するときは、次のガイドラインに従ってください。

   - GRUB のグラフィカルインタフェースを無効にし、テキストベースのインタフェースを使用します。テキストベースのインタフェースを使用しないと、GRUB 画面が RAC 仮想コンソールで表示されません。グラフィカルインタフェースを無効にするには、splashimage で始まる行をコメントアウトします。
   - 複数の GRUB オプションを開始してシリアル接続経由でコンソールセッションを起動するには、すべてのオプションに次の行を追加します。
     ```
     console=ttyS1,57600
     ```
     この例は、最初のオプションだけに console=ttyS1,57600 が追加されたことを示します。

起動後のサーバーシリアルコンソールリダイレクトのための Linux の設定

/etc/inittab ファイルを次のように編集します。

COM2 シリアルポートに agetty を設定するための新しい行を追加します。

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

次の例は、新しい行が追加されたファイルを示しています。

```
# # 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
```

/etc/securetty ファイルを次のように編集します。

COM2 のシリアル tty の名前を使用して次の新しい行を追加します。

```
ttyS1
```

次の例は、新しい行が追加されたサンプルファイルを示しています。

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

12

FlexAdress および FlexAddress Plus カードの使用

本項には、FlexAddress と FlexAddress Plus カードについて、およびこれらのカードの設定と使用方法についての情報が記載されています。

関連リンク

FlexAddress について
FlexAddress Plus について
FlexAddress および FlexAddress Plus の比較

FlexAddress について

FlexAddress 機能は、オプションのアップグレードです。この機能により、工場出荷時にサーバーモジュールに割り当てられたワールドワイドネームおよびメディアアクセスコントロール（WWN/MAC）のネットワーク ID を、シャーシによって提供される WWN/MAC ID に置き換えることが可能となります。

すべてのサーバーモジュールには製造プロセスの一環として固有の WWN および / または MAC ID が割り当てられます。FlexAddress の導入前は、サーバーモジュールを他のモジュールと交換する必要がある場合に WWN/MAC ID が変更され、新規サーバーモジュールを識別するためにはイーサネット管理ツールおよび SAN リソースを再設定する必要がありました。

FlexAddress は、CMC が WWN/MAC ID を特定のスロットに割り当て、工場出荷時の ID を上書きすることが可能になります。従って、サーバーモジュールが交換されてもスロットベースの WWN/MAC ID は変わりません。この機能によって、新規サーバーモジュールのためにイーサネットネットワーク管理ツールと SAN リソースを再設定する必要がなくなりました。

さらに、*上書き* 処置は、FlexAddress が有効になったシャーシにサーバーモジュールを挿入した場合にのみ行われるため、サーバーモジュールに恒久的な変更は行われません。サーバーモジュールを FlexAddress 非対応のシャーシに移動した場合は、工場出荷時に割り当てられた WWN/MAC ID が使用されます。

FlexAddress 機能カードには、広範囲の MAC アドレスが含まれています。FlexAddress をインストールする前に、, you can determine the range of MAC addresses contained on a feature card by inserting the USB メモリカードリーダーに SD カードを挿入し、**pwwn_mac.xml** ファイルを表示することにより、FlexAddress 機能カードに含まれる MAC アドレスの範囲を判断することができます。これにより、この一意の MAC アドレス範囲のために使用される 16 進数の MAC 開始アドレスである XML タグ *mac_start* が含まれる SD カード上の XML テキストファイルがクリアされます。*mac_count* タグは SD カードが割り当てる MAC アドレスの総数です。割り当てられた MAC 範囲の合計は次の式で求めることができます。

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

ここで、208 は *mac_count* を表し、次の式で求めることができます。

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

たとえば、次のとおりです。

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

メモ: USB メモリカードリーダーに SD カードを挿入する際、SD カードの内容が誤って変更されないように事前にロックしてください。CMC に挿入する前に SD カードのロックを*解除する必要*があります。

FlexAddress Plus について

FlexAddress Plus は、カードバージョン 2.0 に追加された新機能であり、FlexAddress カードバージョン 1.0 のアップグレード版です。FlexAddress Plus には、FlexAddress よりも多くの MAC アドレスが含まれています。どちらの機能も、シャーシによるファイバチャネルおよびイーサネットデバイスへのワールドワイドネーム / メディアアクセスコントロール（WWN/MAC）アドレスの割り当てを可能にします。シャーシによって割り当てられた WWN/MAC アドレスはグローバルレベルで一意であり、サーバースロット固有です。

FlexAddress および FlexAddress Plus の比較

FlexAddress は、208 個のアドレスを 16 のサーバースロットに分けます。つまり、各スロットには、13 個の MAC アドレスが割り当てられます。

FlexAddress Plus は、2928 個のアドレスを 16 のサーバースロットに分けます。つまり、各スロットには、183 個の MAC アドレスが割り当てられます。

次の表では、両方の機能での MAC アドレスの割り当て方法を示しています。

	ファブリック A	ファブリック B	ファブリック C	iDRAC 管理	合計 MAC 数
FlexAddress	4	4	4	1	13
FlexAddress Plus	60	60	60	3	183

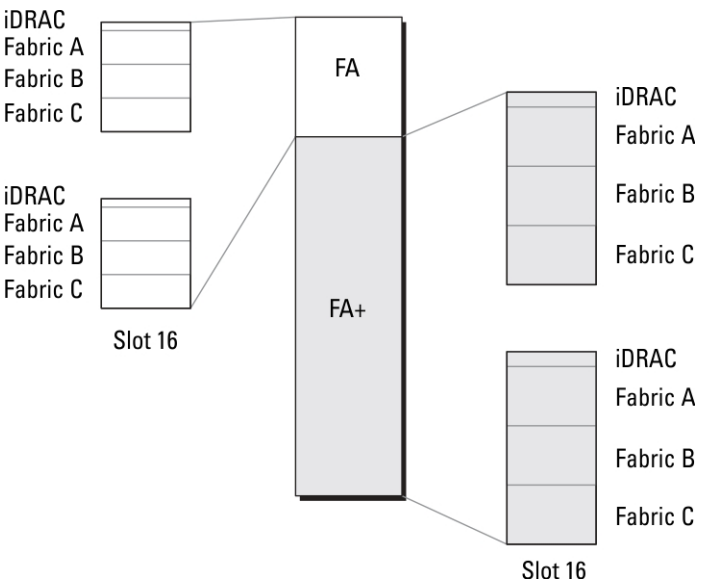


図 3. FlexAdress（FA）と FlexPlusAddress（FA+）の機能

FlexAddress のアクティブ化

FlexAddress はセキュアデジタル（SD）カードに搭載されており、機能をアクティブ化するには SD カードを CMC に挿入する必要があります。FlexAddress 機能をアクティブ化するには、ソフトウェアのアップデートが必要な場合があります。FlexAddress をアクティブ化場合は、これらのアップデートは不要です。次の表にリストされているアップデートには、サーバーモジュール BIOS、I/O メザニン BIOS またはファームウェア、および CMC ファームウェアが含まれます。これらのアップデートは FlexAddress を有効化する前に適用する必

要があります。これらのアップデートが適用されていないと FlexAddress が正しく機能しない場合があります。

コンポーネント	必要最低限のバージョン
Ethernet メザニン カード - Broadcom M5708t、5709、5710	• ブートコードファームウェア 4.4.1 以降 • iSCSI ブートファームウェア 2.7.11 以降 • PXE ファームウェア 4.4.3 以降
FC メザニン カード - QLogic QME2472、FC8	BIOS 2.04 以降
FC メザニン カード - Emulex LPe1105-M4、FC8	BIOS 3.03a3 とファームウェア 2.72A2 以降
サーバーモジュール BIOS	• PowerEdge™ M600 – BIOS 2.02 以降 • PowerEdge™ M605 – BIOS 2.03 以降 • PowerEdge M805 • PowerEdge M905 • PowerEdge M610 • PowerEdge M710 • PowerEdge M710hd
PowerEdgeM600/M605 LAN on motherboard（LOM）	• ブートコードファームウェア 4.4.1 以降 • iSCSI ブートファームウェア 2.7.11 以降
iDRAC	• PowerEdge xx0x システムのバージョン 1.50 以降 • PowerEdge xx1x システムのバージョン 2.10 以降
CMC	バージョン 1.10 以降

メモ: 2008 年 6 月以降にご注文いただいたシステムには、すべて正しいバージョンのファームウェアが搭載されています。

FlexAddress 機能の正しい導入を確実にするため、BIOS とファームウェアを次の順序でアップデートしてください。

1. メザニンカードのファームウェアと BIOS をすべてアップデートします。
2. サーバーモジュールの BIOS をアップデートします。
3. サーバーモジュールの iDRAC ファームウェアをアップデートします。
4. シャーシ内の CMC ファームウェアをすべてアップデートします。冗長 CMC がある場合は、両方をアップデートするようにしてください。
5. 冗長 CMC モジュールシステムではパッシブモジュールに、冗長なしのシステムでは CMC モジュール 1 つに SD カードを挿入します。

   メモ: FlexAddress をサポートする CMC ファームウェア（バージョン 1.10 以降）がインストールされていない場合、FlexAddress の機能はアクティブ化されません。

   SD カードの取り付け手順については、『*Chassis Management Controller （CMC）セキュアデジタル（SD）カード技術仕様*』文書を参照してください。

   メモ: SD カードには FlexAddress 機能が搭載されており、SD カードに格納されているデータは暗号化されています。システム機能を妨げ、システムの誤作動を招く可能性があることから、いかなる複製や改変も行わないでください。

メモ: SD カードの使用は、1 台のシャーシのみに限定されています。シャーシが複数台ある場合は、必要な台数分の SD カードを別途購入してください。

FlexAddress 機能のアクティブ化は、SD 機能カードが取り付けられている CMC を再起動時に自動的に行われます。これにより、この機能が現在のシャーシにバインドされます。SD カードを冗長 CMC システムに取り付けた場合は、冗長 CMC がアクティブになるまで FlexAddress 機能もアクティブ化されません。冗長 CMC のアクティブ化方法については、『*Chassis Management Controller (CMC) セキュアデジタル (SD) カード技術仕様*』文書を参照してください。

CMC の再起動時に、アクティブ化プロセスを検証してください。詳細については、「FlexAddress アクティブ化の検証」を参照してください。

FlexAddress Plus のアクティブ化

FlexAddress Plus は、FlexAddress 機能と共に FlexAddress Plus SD カードで提供されます。

メモ: FlexAddress のラベルの付いた SD カードには FlexAddress のみが含まれ、 FlexAddress Plus のラベルの付いたカードには FlexAddress と FlexAddress Plus が含まれます。機能をアクティブ化するには、カードを CMC に挿入する必要があります。

PowerEdge M710HD などの一部のサーバーでは、それらの設定方法に応じて、FA が CMC に提供できる数より多くの MAC アドレスを必要とする場合があります。これらのサーバーでは、FA+ へのアップグレードにより WWN/MAC 設定の完全な最適化が可能になります。FlexAddress Plus 機能のサポートを受けるには、デルにお問い合わせください。

FlexAddress Plus 機能をアクティブ化するには、サーバー BIOS、サーバー iDRAC、および CMC ファームウェアのソフトウェアアップデートが必要です。これらのアップデートが適用されていない場合は、FlexAddress 機能しか使用できません。これらのコンポーネントの最低必要バージョンについての情報は、**dell.com/support/manuals** で『*Readme*』を参照してください。

FlexAddress 有効化の検証

SD 機能カードとその状態を検証するには、次の RACADM コマンドを使用します。

```
racadm featurecard -s
```

表 31. featurecard -s コマンドによって返される状態メッセージ

状態メッセージ	処置
機能カードが挿入されていません。	CMC をチェックして、SD カードが正しく挿入されていることを確認します。冗長 CMC 構成では、SD 機能カードが取り付けられている CMC がスタンバイ CMC ではなく、アクティブな CMC であることを確認してください。
挿入されている機能カードが有効で、次の FlexAddress 機能が含まれています。機能カードはこのシャーシにバインドされています。	処置の必要はありません。
挿入されている機能カードが有効で、次の FlexAddress 機能が含まれています。この機能カードは別のシャーシ（svctag = ABC1234、SD card SN = 01122334455）にバインドされています。	SD カードを取り外し、現在のシャーシ用の SD カードを取り付けます。

状態メッセージ	処置
挿入されている機能カードは有効で、次の FlexAddress 機能が含まれています。この機能カードはどのシャーシにもバインドされていません。	機能カードは、別のシャーシに移動したり、現在のシャーシで再有効化することができます。現在のシャーシで再有効化するには、機能カードが取り付けられている CMC モジュールがアクティブになるまで racadm racreset を入力し続けます。

シャーシ上でアクティブ化された全機能を表示するには、次の RACADM コマンドを使用します。

```
racadm feature -s
```

このコマンドを実行すると、次の状態メッセージが返されます。

```
機能 = FlexAddress アクティブ化日 = 2008 年 4 月 8 日 - 10:39:40 SD カード SN = 01122334455 からインストールされた機能
```

シャーシ上にアクティブな機能が存在しない場合は、コマンドは次のメッセージを返します。

```
racadm feature -s このシャーシでアクティブな機能はありません
```

Dell 機能カードには複数の機能が含まれている場合があります。シャーシ上で Dell 機能カードに含まれている機能のいずれかがアクティブ化されると、その Dell 機能カードに含まれているその他の機能は異なるシャーシでアクティブ化できなくなります。この場合、racadm feature -s コマンドは対象機能に関して次のメッセージを表示します。

```
エラー：SD カード上の 1 つ、または複数の機能が別のアクティブです。
```

feature および **featurecard** コマンドについての詳細は、『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

FlexAddress の非アクティブ化

RACADM コマンドを使用して、FlexAddress または機能 を非アクティブ化し、SD カードを取り付け前の状態に戻すことができます。ウェブインタフェースには、非アクティブ化機能はありません。非アクティブ化すると、SD カードは別のシャーシ上に装着し、アクティブ化することが可能な元の状態に戻ります。この文脈では、用語 FlexAddress は FlexAddress と FlexAddressPlus の両方を意味します。

メモ: SD カードは、物理的に CMC に取り付ける必要があります。また、非アクティブ化コマンドを実行する前には、シャーシの電源を切る必要があります。

カードが装着されていない状態、または異なるシャーシのカードを装着した状態で非アクティブ化コマンドを実行した場合、機能は非アクティブ化されますが、カードに変更は加えられません。

FlexAddress 機能を非アクティブ化し、SD カードを復元するには、次の RACADM コマンドを使用します。

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

正常に非アクティブ化されると、コマンドが次の状態メッセージを返します。

```
シャーシ上の FlexAddress 機能の非アクティブ化に成功しました。
```

コマンド実行前にシャーシの電源を切らなかった場合、コマンドは失敗し、次のエラーメッセージが表示されます。

```
エラー： シャーシの電源がオンのため、機能を非アクティブ化できません。
```

コマンドの詳細については、『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』の **feature** コマンドの項を参照してください。

FlexAddress 情報の表示

シャーシ全体または個々のサーバーの状態情報を表示することができます。表示される情報には、次が含まれます。

- ファブリック設定。
- FlexAddress のアクティブ / 非アクティブ状況。
- スロットの番号および名前。
- シャーシに割り当てられたアドレスとサーバーに割り当てられたアドレス。
- 使用中のアドレス。

関連リンク

シャーシの FlexAddress 情報の表示
全サーバーの FlexAddress 情報の表示
個別サーバーの FlexAddress 情報の表示

シャーシの FlexAddress 情報の表示

全シャーシの FlexAddress 状態情報を表示することができます。状態情報には、機能がアクティブかどうか、および各サーバーの FlexAddress 状態の概要が含まれます。

CMC ウェブインタフェースを使用してシャーシ FlexAddress 状態を表示するには、**シャーシ概要 → セットアップ → 一般** をクリックします。

シャーシの一般設定 ページが表示されます。

FlexAddress には **アクティブ** または **非アクティブ** の値があります。**アクティブ** という値は、機能がシャーシにインストール済みであることを示し、**非アクティブ** は機能がシャーシにインストールされておらず、使用されていないことを示します。

シャーシ全体の FlexAddress 状態を表示するには、次の RACADM コマンドを使用します。

```
racadm getflexaddr
```

特定のスロットの FlexAddrss 状態を表示するには、次のコマンドを使用します。

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

ここで *<スロット番号>* は 1〜16 の値です。

getflexaddr コマンドに関する詳細については、**dell.com/support/manuals** の『iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド』を参照してください。

全サーバーの FlexAddress 情報の表示

CMC ウェブインタフェースを使用して全サーバーの FlexAddress 状態を表示するには、システムツリーで **サーバー概要 → プロパティ → WWN/MAC** と進みます。

シャーシ内のすべてのスロットに対する次の情報を提供する、**WWN/MAC 概要** ページが表示されます。

ファブリックの設定	ファブリック A、ファブリック B およびファブリック C は、取り付けられている I/O ファブリックの種類を表示します。 iDRAC には、サーバー管理 MAC アドレスが表示されます。

メモ: ファブリック A を有効にすると、未使用スロットがファブリック A のシャーシ割り当て MAC アドレスを表示し、ファブリック B および C（これらが使用中スロットによって使用されている場合）には MAC または WWN を表示します。

WWN/MAC アドレス

シャーシ内の各スロットの FlexAddress 設定を表示します。表示される情報は次のとおりです。

- スロット番号および位置。
- FlexAddress のアクティブ / 非アクティブ状況。
- ファブリックタイプ。
- 使用中のサーバー割り当て、およびシャーシ割り当ての WWN/MAC アドレス。

緑色のチェックマークは、アクティブなアドレスタイプ（サーバー割り当てまたはシャーシ割り当てのいずれか）を示します。

メモ: iDRAC 管理コントローラはファブリックではありませんが、その FlexAddress はファブリックのように処理されます。

メモ: EqualLogic PS-M4110 ブレードアレイでは、FlexAddress はサポートされていません。

各種フィールドについての情報は、『*CMC オンラインヘルプ*』を参照してください。

個別サーバーの FlexAddress 情報の表示

CMC ウェブインタフェースを使用して特定のサーバーの FlexAddress 情報を表示するには、次の手順を実行します。

1. システムツリーで、**サーバーの概要** を展開します。
   展開された **サーバー** リストにすべてのサーバー（1～16）が表示されます。
2. 表示するサーバーをクリックします。
   サーバー状態 ページが表示されます。
3. **セットアップ** タブをクリックし、次に **FlexAddress** サブタブをクリックします。
   選択したサーバーの WWN 設定と MAC アドレスが記載された **FlexAddress** ページが表示されます。詳細については、『*CMC オンラインヘルプ*』を参照してください。

FlexAddress の設定

FlexAddress はオプションのアップグレードで、工場出荷時にサーバーモジュールに割り当てられた WWN/MAC ID を、シャーシ提供の WWN/MAC ID に置き換えることを可能にします。

メモ: 本項では、FlexAddress という用語は FlexAddress Plus も意味します。

FlexAddress を設定するには、FlexAddress アップグレードを購入してインストールする必要があります。アップグレードを購入およびインストールしていない場合は、次のテキストがウェブインタフェースに表示されます。
オプション機能はインストールされていません。シャーシベースの WWN および MAC アドレス管理機能についての情報は、『Dell Chassis Management Controller ユーザーズガイド』を参照してください。本機能を購入するには、デル（www.dell.com）にお問い合わせください。

シャーシと共に FlexAddress を購入された場合、システムへの電源投入時には FlexAddress がインストール済みでアクティブです。FlexAddress を別途購入された場合は、**dell.com/support/manuals** の『*Chassis Management Controller（CMC）セキュアデジタル（SD）カード技術仕様*』マニュアルにある手順で SD 機能カードをインストールする必要があります。
設定を始める前に、サーバーの電源を切る必要があります。FlexAddress はファブリック単位で有効化または無効化できます。さらに、この機能はスロット単位でも有効化または無効化が可能です。ファブリック単位

で機能を有効化した後、有効化するスロットを選択できます。例えば、ファブリック A が有効化されていると、有効化されたスロットではいずれもファブリック A でのみ FlexAddress が有効になります。その他すべてのファブリックは、サーバーで工場出荷時割り当ての WWN/MAC を使用します。

選択されたスロットには、有効化されたファブリックすべてのために FlexAddress が有効化されます。例えば、ファブリック A および B を有効化してから、スロット 1 をファブリック A で FlexAddress 有効化して、ファブリック B では有効化しないことは不可能です。

メモ: ファブリックレベル（A、B、C、または DRAC）FlexAddress を変更する前に、ブレードサーバーの電源がオフになっていることを確認してください。

関連リンク

FlexAddress を利用した Wake-On-LAN の使用
シャーシレベルのファブリックおよびスロット用 FlexAddress の設定
サーバーレベルスロット用 FlexAddress の設定
Linux 向け FlexAddress の追加設定

FlexAddress を利用した Wake-On-LAN の使用

FlexAddress 機能が特定のサーバーモジュール上に初めて導入されたときは、FlexAddress を有効にするために電源切断および投入シーケンスが必要です。イーサネットデバイスの FlexAddress はサーバーモジュール BIOS によってプログラムされます。サーバーモジュール BIOS がアドレスをプログラムするには、サーバーモジュール BIOS が動作可能である必要があり、これにはサーバーモジュールに電源投入する必要があります。電源切断および投入シーケンスが完了すると、シャーシ割り当ての MAC ID が Wake-On-LAN（WOL）機能用に使用できるようになります。

シャーシレベルのファブリックおよびスロット用 FlexAddress の設定

FlexAddress 機能は、ファブリックおよびスロット用にシャーシレベルで有効化または無効化することができます。FlexAddress は、ファブリックごとに有効化され、次に機能に参加させるスロットが選択されます。FlexAddress を正常に設定するには、ファブリックおよびスロットの両方が有効化されている必要があります。

CMC ウェブインタフェースを使用したシャーシレベルファブリックおよびスロット用 FlexAddress の設定

CMC ウェブインタフェースを使用して、ファブリックおよびスロットによる FlexAddress 機能の使用を有効化または無効化するには、次の手順を実行します。

1. システムツリーで **サーバー概要** に進み、次に **セットアップ → FlexAddress** とクリックします。
   FlexAddress の展開 ページが表示されます。
2. **シャーシ割り当ての WWN/MACs セクション用のファブリックの選択** で、FlexAddress を有効化するファブリックタイプを選択します。無効化するには、オプションをクリアします。

   メモ: ファブリックが選択されていない場合は、FlexAddress は選択されたスロットに対して有効になりません。

   シャーシ割り当ての WWN/MACs セクション用のスロットの選択 ページが表示されます。
3. FlexAddress を有効化するスロットに **有効化** オプションを選択します。無効化するには、オプションをクリアします。

   メモ: スロットにサーバーがある場合は、そのスロットで FlexAddress 機能を有効化する前にサーバーの電源を切ってください。

   メモ: スロットが一つも選択されていない場合、FlexAddress は選択されたファブリックに対して有効になりません。

4. **適用** をクリックして変更を保存します。
   詳細については、『*CMC オンラインヘルプ*』を参照してください。

RACADM を使用したシャーシレベルファブリックおよびスロット用 FlexAddress の設定

ファブリックを有効化または無効化するには、次の RACADM コマンドを使用します。

```
racadm setflexaddr [-f <fabricName> <state>]
```

ここで、*<fabricName>* = A, B, C, or iDRAC、および *<state>* = 0 or 1 です。

0 は無効、1 は有効を示します。

スロットを有効化または無効化するには、次の RACADM コマンドを使用します。

```
racadm setflexaddr [-i <slot#> <state>]
```

ここで、 *<slot#>* = 1or 16、および *<state>* = 0 or 1 です。

0 は無効、1 は有効を示します。

setflexaddr コマンドの詳細に関しては、**dell.com/support/manuals** にある『iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド』を参照してください。

サーバーレベルスロット用 FlexAddress の設定

サーバーレベルで、個々のスロットのために FlexAddress 機能を有効化または無効化することができます。

CMC ウェブインタフェースを使用したサーバーレベルスロット用 FlexAddress の設定

CMC ウェブインタフェースを使用して、個々のスロットによる FlexAddress 機能の使用を有効化または無効化するには、次の手順を実行します。

1. システムツリーで、**サーバーの概要** を展開します。
   展開された **サーバー** リストにすべてのサーバー（1〜16）が表示されます。
2. 表示するサーバーをクリックします。
   サーバー状態 ページが表示されます。
3. **セットアップ** タブ、**FlexAddress** サブタブを順にクリックします。
   FlexAddress ページが表示されます。
4. **FlexAddress 有効** ドロップダウンメニューから、**はい** を選択して FlexAddress を有効化するか、**いいえ** を選択して無効化します。
5. **適用** をクリックして変更を保存します。
   詳細については、『*CMC オンラインヘルプ*』を参照してください。

RACADM を使用したサーバーレベルスロット用 FlexAddress の設定

RACADM を使用してサーバーレベルスロット用 FlexAddress を設定するには、次を入力します。

```
racadm setflexaddr [-i <スロット番号> <状況>] [-f <ファブリック名> <状況>]
```

ここで、<スロット番号> = 1〜16

<ファブリック名> = A、B、C

<状況> = 0 または 1

0 は無効、1 は有効を示します。

Linux 向け FlexAddress の追加設定

Linux ベースのオペレーティングシステム上で、サーバー指定の MAC ID からシャーシ指定の MAC ID に変更する場合、追加の設定手順が必要となる場合があります。

- SUSE Linux Enterprise Server 9 および 10: Linux システム上で Yet another Setup Tool（YAST）を実行してネットワークデバイスの設定を行ってから、ネットワークサービスを再起動する必要がある場合があります。
- Red Hat Enterprise Linux 4 および Red Hat Enterprise Linux 5： システム上の新規または交換されたハードウェアを検出し、設定するためのユーティリティである Kudzu を実行します。Kudzu はハードウェア検出メニューを表示します。 これは、ハードウェアが取り外され、新しいハードウェアが追加されると、MAC アドレスの変更を検出します。

ワールドワイド名 / メディアアクセスコントロール（WWN/MAC）ID の表示

WWN/MAC サマリ ページでは、シャーシ内のスロットの WWN 設定および MAC アドレスを表示することができます。

ファブリックの設定

ファブリック設定 セクションには、ファブリック A、ファブリック B、およびファブリック C のために取り付けられた入力 / 出力ファブリックのタイプが表示されます。緑色のチェックマークはファブリックで FlexAddress が有効化されていることを示します。FlexAddress 機能は、シャーシ内の様々なファブリックおよびスロットに対して、シャーシ割り当てかつスロット固定の WWN/MAC アドレスを展開するために使用されます。この機能は、ファブリックごとおよびスロットごとに有効になります。

メモ: FlexAddress 機能の詳細については、「CMCNoble_FlexAddress について」を参照してください。

WWN/MAC アドレス

WWN/MAC アドレス セクションは、サーバー スロットが空の場合を含めて、全サーバーに割当てられた WWN/MAC の情報を表示します。

- **場所** は、入力 / 出力モジュールが占有するスロットの場所を表示します。6 個のスロットは、グループ名（A、B、または C）およびスロット番号（1〜2）を組み合わせたスロット名 A1、A2、B1、B2、C1、または C2 で識別されます。iDRAC はサーバーの統合管理コントローラです。
- **ファブリック** は、I/O ファブリックのタイプを表示します。
- **サーバー割り当て** は、コントローラのハードウェアに組み込まれたサーバー割り当ての WWN/MAC アドレスを表示します。
- **シャーシ割り当て** は、特定のスロットで使用されるシャーシ割り当ての WWN/MAC アドレスを表示します。

サーバー割り当て または **シャーシ割り当て** 列の緑色のチェックマークは、アクティブなアドレスのタイプを示します。シャーシ割り当てのアドレスは、シャーシで FlexAddress がアクティブ化されると割り当てられ、 スロット固定のアドレスを表します。シャーシ割り当てアドレスにチェックマークが付くと、ひとつのサーバーが別のサーバーに取り替えられた場合でも、これらのアドレスが使用されます。

コマンドメッセージ

次の表に、RACADM コマンドと、一般的な FlexAddress 状況における出力をリストします。

表 32. FlexAddress コマンドと出力

状況	コマンド	出力
アクティブ CMC モジュールの SD カードが他のサービスタグにバインドされている。	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)`

状況	コマンド	出力
		FlexAddress: The feature card is bound to another chassis, svctag = <Service tag Number> SD card SN = <Valid flex address serial number>
同じサービスタグにバインドされている アクティブ CMC モジュールの SD カード。	$racadm featurecard -s	The feature card inserted is valid and contains the following feature(s) FlexAddress: The feature card is bound to this chassis
どのサービスタグにもバインドされていない アクティブ CMC モジュールの SD カード。	$racadm featurecard -s	The feature card inserted is valid and contains the following feature(s) FlexAddress: The feature card is not bound to any chassis
何らかの理由（SD カードが挿入されていない、破損した SD カード、機能の非アクティブ化後、SD カードが異なるシャーシにバインドされている）で FlexAddress 機能がシャーシ上でアクティブではない。	$racadm setflexaddr [-f *<fabricName> <slotState>*] $racadm setflexaddr [-i *<slot#> <slotstate>*]	ERROR: Flexaddress feature is not active on the chassis
ゲストユーザーによるスロットまたはファブリックへの FlexAddress の設定試行。	$racadm setflexaddr [-f *<fabricName> <slotState>*] $racadm setflexaddr [-i *<slot#> <slotstate>*]	ERROR: Insufficient user privileges to perform operation
シャーシの電源がオンの状態での FlexAddress 機能の無効化。	racadm feature -d -c flexaddress	ERROR: Unable to deactivate the feature because the chassis is powered ON
ゲストユーザーがシャーシ上の機能の無効化を試みる。	racadm feature -d -c flexaddress	ERROR: Insufficient user privileges to perform operation
サーバーモジュールの電源がオンの状態で、スロット / ファブリックの FlexAddress 設定を変更する。	$racadm setflexaddr -i 1 1	ERROR: Unable to perform the set operation because it affects a powered ON server

FlexAddress DELL ソフトウェア製品ライセンス契約

これは、ユーザーであるお客様と Dell Products L.P または Dell Global B.V.（「Dell」）との法的な契約書です。本契約書は 、Dell 製品に同梱されているすべてのソフトウェアに適用されます。お客様と製造者または本ソフトウェア所有者（以下、総称として「ソフトウェア」とします）間で個別にライセンス契約を締結することはありません。本契約書は、ソフトウェアまたはその他知的財産権の販売のためのものではありません。ソフトウェアに対するおよびソフトウェアに含まれる、すべての所有権と知的財産権は、ソフトウェアの製造者または所有者が有します。本契約書において明確に付与されていない権利は、すべてソフトウェアの製造者または所有者によって保留されます。本ソフトウェアのパッケージを開梱または開封、本ソフトウェアをインストールまたはダウンロード、お使いの製品にあらかじめロードされているまたは組み込まれている本ソフトウェアを使用したりすると、本契約書の条項に同意したとみなされます。これらの条件に同意しない場合は、すべてのソフトウェア（ディスク、印刷物、およびパッケージ）をすみやかに返却し、一切の事前ロードまたは組込みのソフトウェアを削除してください。

本ソフトウェアは、1 度につき 1 部を 1 台のコンピュータにのみインストールして使用することができます。本ソフトウェアのライセンスを複数所有されている場合はいつでも、ライセンスの数だけ本ソフトウェアを使用できます。コンピュータの一時メモリまたは永久ストレージに本ソフトウェアをロードする場合を「使用」とします。本ソフトウェアを配布する各コンピュータに個別のライセンスがある場合に限り、他のコンピュータへの配布を唯一の目的として、ネットワークサーバーにインストールすることは「使用」ではありません。お客様は、ネットワークサーバーにインストールされたソフトウェアを使用する人数が、お持ちのライセンス数を超えないことを確認する必要があります。 ネットワークサーバーにインストールされた本ソフトウェアを使用するユーザー数がライセンス数を超える場合は、追加ユーザーに本ソフトウェアの使用を許可する前に、ライセンス数とユーザー数が同じになるように追加ライセンスを購入する必要があります。お客様が Dell または Dell 関連会社の法人顧客である場合、お客様は、Dell または Dell により選出された代理人に対して、通常の営業時間内に本ソフトウェア使用に関する監査を行う権利をここに付与します。お客様は、このような監査において Dell に協力することに同意し、かつ、本ソフトウェア使用に合理的に関連するすべての記録を Dell に提供することに同意するものとします。監査は、お客様による本契約諸条件の順守の確認に限定されます。

本ソフトウェアはアメリカ合衆国の著作権法および国際条約によって保護されています。本ソフトウェアは、バックアップまたはアーカイブの目的でのみ、複製を一部作成できます。また、オリジナルのソフトウェアをバックアップまたはアーカイブの目的でのみ保存することを条件として、一台のハードディスクに本ソフトウェアをインストールできます。客様は、FlexAddress および FlexAdress Plus カードを使用するソフトウェア 240 を賃貸またはリースしたり、本ソフトウェアに同梱の印刷物を複製することはできません。ただし、お客様が複製を保持せず、被譲渡者が本条項に同意した場合は、ソフトウェアおよびすべての同梱物を Dell 製品の販売または譲渡の一部として永久的に譲渡することができます。譲渡する場合は、必ず最新のアップデートとすべての旧バージョンが含まれていなければなりません。本ソフトウェアのリバースエンジニアリング、逆コンパイル、または逆アセンブリを行わないでください。製品に同梱のパッケージには、コンパクトディスク、3.5 インチおよび / または 5.25 インチディスクが入っており、お使いのコンピュータに適したディスクのみを使用することができます。他のコンピュータまたはネットワークでそれらのディスクを使用したり、本契約書で許可される以外の他のユーザーに、貸与、賃貸、リース、または譲渡することはできません。

限定保証

Dell では、お客様が本ソフトウェアディスクを受領した日から 90 日間、通常の使用において材質または製作上の欠陥を生じないことを保証します。本保証は、お客様のみに限定され、譲渡することはできません。すべての黙示的保証は、お客様が本ソフトウェアを受領した日から 90 日間に制限されます。国や地域によっては黙示的保証期間が制限されることがないため、この限定はお客様に適用されない場合があります。Dell および Dell のサプライヤーの法的義務全域、およびお客様の排他的な救済は、本ソフトウェアに支払われた代金の返却、または（b）お客様の費用負担および自己責任において、Dell の返品確認番号と共に返却された本保証の要件を満たさないすべてのディスクの交換、のいずれかとなるものとします。事故、誤用、乱用、または Dell 以外による修正が原因でディスクが損傷した場合は、本限定保証は無効となります。交換されたディスクの保証期間については、オリジナルのディスクの残余保証期間、または 30 日間のいずれか長い方が適用されます。

Dell および Dell のサプライヤーは、本ソフトウェアの機能がお客様の要求に合うこと、または本ソフトウェアの動作が妨げられない、またはエラーが無いことは保証しません。 お客様が期待する成果を得るための本ソフトウェアの選択、および本ソフトウェアの使用と使用結果につきましては、お客様の責任とさせていただきます。

Dell は、Dell およびそのサプライヤーを代表して、本ソフトウェアおよびそれに付属する印刷物に対し、明示的であるかまたは黙示的であるかにかかわらず、商品性、特定目的への適合性、または権利や非侵害に対するいかなる保証を含む（ただしこれに限定されません）、その他のあらゆる保証を否認します。本限定保証は、特定の法的権利をお客様に付与するものです。お客様は、管轄区域ごとに異なる権利を有することもあります。

ソフトウェアの使用、または使用できなかった場合に起きる利益の損失、ビジネスの中断、ビジネス情報の消失、または金銭的喪失などを含む（ただしこれに限定されません）あらゆる損害に対し、Dell またはそのサプライヤーは、そのような可能性が事前に何らかの形で指摘されていたとしても、責任は負いません。一部の地域では、付随的または偶発的な損害に対する除外または制限が許可されないため、上記制限はお客様に適用されない場合があります。

オープンソースソフトウェア

本 CD にはオープンソースソフトウェアが含まれている場合があります。オープンソースソフトウェアは、そのソフトウェアの配布に関する特定のライセンスの条項および条件に基づいてご使用いただけます。

このオープンソースソフトウェアは、有益であることを意図して配布されていますが、明示的であるかまたは黙示的であるかにかかわらず、商品性、特定目的への適合性を含む（ただしこれに限定されません）、あらゆる保証なくして「現状のまま」で提供されています。いかなる事態が発生しようとも、著作権保有者である DELL または寄与メンバーは、直接的、間接的、偶発的、特殊的、典型的、必然的な損傷（代替商品やサービスの調達、利用機会、データ、収益の損失、ビジネスの中断を含みますが、これらに限りません）に対する責任を負わないものとします。いかなる原因で発生した場合でも、法的責任の有無、契約上での示唆、強制法規上にかかわらず、または不法行為（過失やその他を含む）であったとしても、このオープンソースソフトウェアの使用から発生したいかなることに対しても責任を負いません。また、そのような可能性が事前に何らかの形で指摘されていたとしても同様です。

米国政府の限定的権利

本ソフトウェアおよび付属マニュアルは、48 C.F.R.2.101 で定義されている「商用品目」であり、48 C.F.R.12.212 で用いられているように「商用コンピュータソフトウェア」および「商用コンピュータソフトウェアマニュアル」で構成されています。8 C.F.R.12.212 および 48 C.F.R. 227.7202-1 から 227.7202-4 の規定に準拠し、すべての米国政府エンドユーザーは、本契約にて規定された権利のみを伴うソフトウェアおよび付属マニュアルを取得します。

契約者 / 製造者は Dell Products, L.P. であり、その所在地は One Dell Way, Round Rock, TX 78682 です。

一般条項

本ライセンスは解約されない限り有効です。上記に定められている条件により、または、お客様が本契約条項のいずれかに違反した場合に本契約は解約されます。解約にあたり、お客様はソフトウェア、それに伴う同梱物、およびすべての複製を破棄するものとします。本契約は、テキサス州の法律に基づいて解釈されるものとします。本契約書の各条項は分離可能です。施行できない条項があることが判明しても、本契約書の他の条項、条件、または要件の施行には影響しません。本契約書は、受領者および譲渡者を拘束します。Dell およびお客様は、本ソフトウェアまたは本契約書に関して、陪審による裁判を受ける権利を法律で認められた範囲内で放棄することに合意します。一部の地域では本権利放棄は効力を有さないため、お客様には適用されない場合があります。お客様は、本契約書をお読みになり、理解し、また条件に同意して、本契約書が本ソフトウェアに関するお客様と Dell との完全かつ排他的な契約書であることを承認するものとします。

13

I/O ファブリックの管理

シャーシには最大 6 個の I/O モジュール（IOM）を取り付ける事が可能で、各 IOM はパススルーまたはスイッチモジュールです。IOM は A、B、および C の 3 つのグループに分類されます。各グループには 2 つのスロット（スロット 1 およびスロット 2）があります。

これらのスロットは、A1 | B1 | C1 | C2 | B2 | A2 という具合に、シャーシ背面の左から右の順に文字で指定されます。各サーバーには IOM に接続するための 2 個のメザニンカード（MC）用スロットがあります。MC およびそれに対応する IOM は同じファブリックを持つ必要があります。

シャーシ IO は、A、B および C の 3 つの離散データパスに分離されます。これらのパスはファブリックと呼ばれ、イーサネット、ファイバチャネル、または InfiniBand をサポートします。これらの離散ファブリックパスは、バンク 1 およびバンク 2 の 2 つの IO バンクに分割されます。各サーバー IO アダプタ（メザニンカードまたは LOM）は、機能に応じて 2 つまたは 4 つのポート持つことができます。これらのポートは、冗長性を確保するために、IOM バンク 1 と 2 に均等に分配されます。イーサネット、iSCSI、またはファイバチャネルネットワークを展開するときは、最大可用性のため、それらの冗長リンクをバンク 1 と 2 全体にスパンしてください。外付け IOM はファブリック識別子およびバンク番号で識別されます。

例：A1 はバンク 1 のファブリック A を表し、C2 はバンク 2 のファブリック C を表します。

シャーシは 3 つのファブリックまたはプロトコルタイプをサポートします。グループ内の IOM および メザニンカードは、同じ、または互換性のあるファブリックタイプを持つ必要があります。

- グループ A IOMS は常にサーバーのオンボードイーサネットアダプタに接続されています。グループ A のファブリックタイプは常にイーサネットです。
- グループ B については、IOM スロットは各サーバーモジュールの 1 番目の MC スロットに永続的に接続されています。
- グループ C では、IOM スロットは永続的に 2 番目の DC スロットに接続されています。

メモ: CMC CLI では、IOM は A1=スイッチ-1、A2=スイッチ-2、B1=スイッチ-3、B2=スイッチ-4、C1=スイッチ-5 および C2=スイッチ-6 のように スイッチ-n の規則で命名されます。

関連リンク

ファブリック管理の概要
無効な構成
初回電源投入シナリオ
IOM 正常性の監視
IOM 用ネットワークの設定
IOM 用 VLAN の管理
IOM の電源制御操作の管理
IOM のための LED 点滅の有効化または無効化
工場出荷時のデフォルト設定への IMO のリセット

ファブリック管理の概要

ファブリック管理は、シャーシで確立されたファブリックタイプとの互換性がないファブリックタイプを持つ IOM または MC の取り付けによる電気、構成、接続関連の問題を避けるために役立ちます。無効なハードウェア構成は、シャーシまたはそのコンポーネントに電気または機能的な問題を生じる可能性があります。ファブリック管理は、無効な構成に電源が投入されることを防ぎます。

次の図はシャーシ内の IOM の位置を表しています。各 IOM の位置はグループ番号（A、B、または C）で示されます。これらの離散ファブリックパスはバンク 1 および 2 の 2 つの IO バンクに分割されます。シャーシでは、IOM スロット名は A1、A2、B1、B2、C1、および C2 とマーク付けされます。

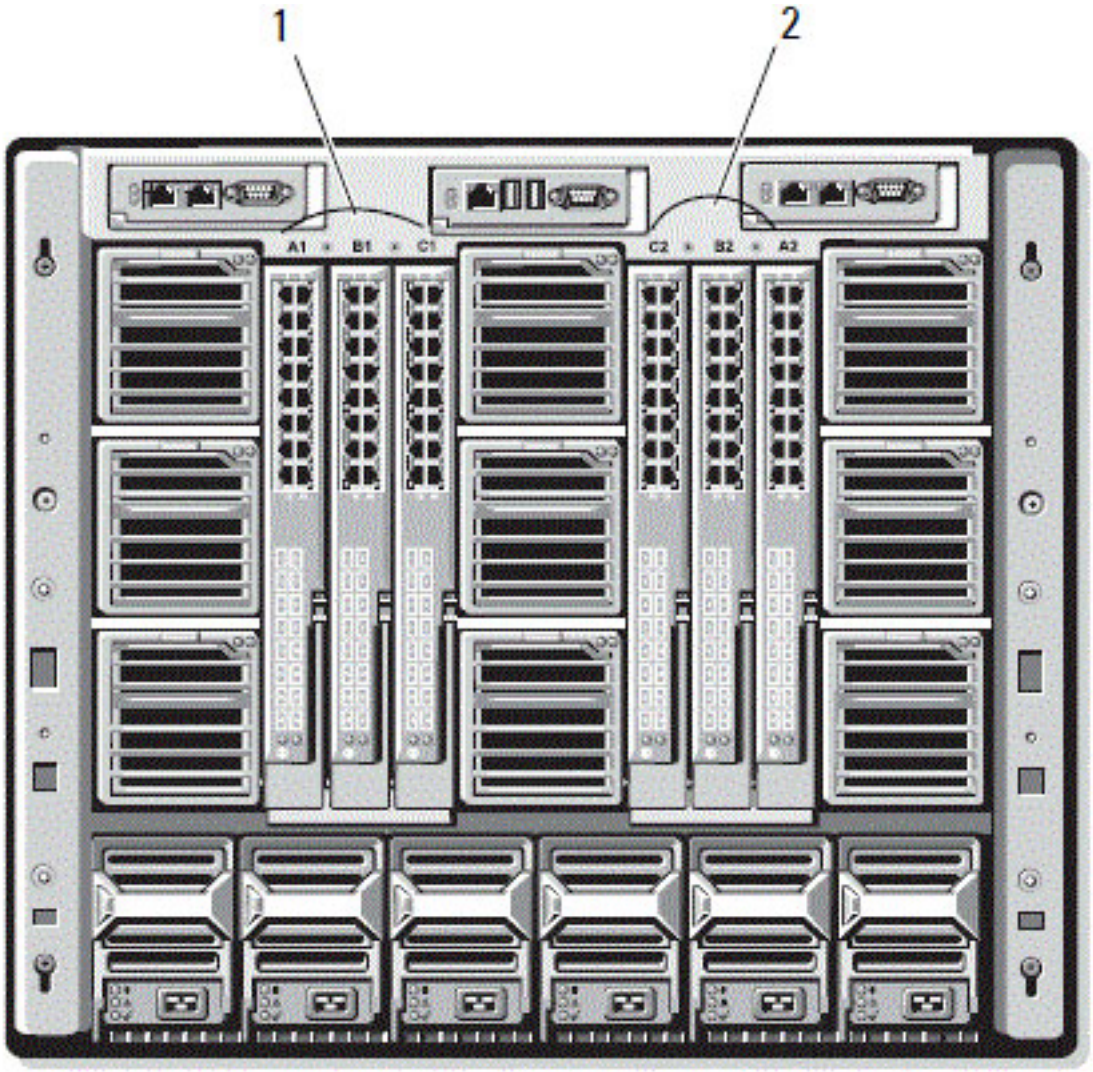


図 4. IOM の位置を示すシャーシの背面図

1　　バンク 1（スロット A1、B1、C1）　　2　　バンク 2（スロット A2、B2、C2）

CMC は、無効なハードウェア構成に関するエントリをハードウェアログと CMC ログの両方に作成します。たとえば、次のとおりです。

- ファイバチャネル IOM に接続されているイーサネット MC は無効な構成です。ただし、同じ IOM グループに取り付けられているイーサネットスイッチとイーサネットパススルー IOM の両方に接続されたイーサネット MC は有効な接続です。
- スロット B1 および B2 のファイバチャネルパススルー IOM とファイバチャネルスイッチは、全サーバーの最初の MC が同じくファイバチャネルである場合は有効な構成です。この場合、CMC が IOM とサーバーに電源投入します。ただし、特定のファイバチャネル冗長性ソフトウェアはこの構成をサポートしない場合があります。すべての有効構成が対応構成であるとは限りません。

  サーバー IOM と MC のファブリック検証は、シャーシに電源投入されているときにのみ実行されます。シャーシがスタンバイ電源を使用している場合、サーバーモジュールの iDRAC の電源は切れたま

まとなるため、サーバーの MC ファブリックタイプを報告できません。MC ファブリックタイプは、サーバーの iDRAC に電源投入されるまで CMC ユーザーインタフェースに報告されない場合があります。さらに、シャーシに電源投入されている場合、サーバーまたは IOM の挿入時にファブリック検証が行われます（オプション）。ファブリックの不一致が検出された場合、サーバーまたは IOM の電源はオンになりますが、状態 LED が橙色に点滅します。

無効な構成

無効な構成には、次の 3 タイプがあります。

- 無効な MC または LOM 構成では、サーバーの新しく取り付けられたファブリックタイプが既存の IOM ファブリックと異なる、つまり、単一のサーバーの LOM または MC がそれに対応する IOM によってサポートされていません。この場合、シャーシ内の他のサーバーはすべて稼働していますが、不一致 MC カードがあるサーバーの電源はオンにできません。サーバーの電源ボタンが橙色に点滅してファブリックの不一致を警告します。
- 無効な IOM-MC 構成では、IOM モジュールの新しく取り付けられたファブリックタイプと常駐する MC のファブリックタイプが一致しない、またはそれらに互換性がありません。一致しない IOM は電源が切れた状況に維持されます。CMC は無効な構成が記され、IOM 名が指定されているエントリを CMC およびハードウェアログに追加します。CMC は不一致のファブリックタイプを持つ IOM のエラー LED を点滅させます。アラートを送信するように CMC が設定されている場合は、CMC はこのイベントの E-メールおよび SNMP アラートを送信します。
- 無効な IOM-IOM 構成では、新しく取り付けられた IOM に、グループ内にすでに取り付けられている IMO と異なる、または互換性のないファブリックタイプが存在します。CMC は新しく取り付けられた IOM を電源が切れた状況に維持し、IOM のエラー LED を点滅させ、CMC およびハードウェアログ不一致についてのエントリをログします。

初回電源投入シナリオ

シャーシが電源に接続され、電源投入されると、サーバーよりも I/O モジュールが優先されます。各グループの最初の IOM が一番最初に電源投入されます。この時、ファブリックタイプの検証は行われません。グループの最初のスロットに IOM がない場合、そのグループの 2 番目のスロットにあるモジュールに電源投入されます。両方のスロットに IOM がある場合は、整合性について 2 番目のスロットにあるモジュールが最初のスロットにあるモジュールと比較されます。

IOM に電源が投入された後、サーバーに電源が投入され、CMC はサーバーのファブリックタイプの整合性を検証します。

パススルーモジュールとスイッチは、ファブリックが同じである場合、同じグループに属することが可能です。スイッチとパススルーモジュールは、異なるベンダーによって製造されたものである場合でも、同じグループに存在できます。

IOM 正常性の監視

IOM 正常性の監視についての情報は、「全 IOM の情報と正常性状態の表示」および「個々の IOM の情報と正常性状態の表示」を参照してください。

ウェブインタフェースを使用した I/O モジュールのアップリンクおよびダウンリンク状態の表示

CMC ウェブインタフェースを使用して、Dell PowerEdge M I/O アグリゲータのアップリンクおよびダウンリンク状態情報を表示することができます。

1. **シャーシ概要** へ進み、システムツリーで **I/O モジュール概要** を展開します。

展開されたリストに、すべての IOM（1〜6）が表示されます。

2. 表示する IOM（スロット）をクリックします。
   その IOM スロットに固有の **I/O モジュール状態** ページが表示されます。**I/O モジュールアップリンク状態** および **I/O モジュールダウンロード状態** 表が表示されます。これらの表には、ダウンリンクポート（1〜32）およびアップリンクポート（33〜56）に関する情報が表示されます。詳細に関しては、『CMC オンラインヘルプ』を参照してください。

   メモ: ポートリンク状態がアップになるように、I/O アグリゲータに有効な設定があることを確認してください。このページは I/O アグリゲータの状態を表示します。状態がダウンの場合は、I/O アグリゲータのサーバーポートが無効な設定のためにダウンしている可能性があることを示します。

ウェブインタフェースを使用した I/O モジュール FCoE セッション情報の表示

CMC ウェブインタフェースを使用して Dell PowerEdge M I/O アグリゲータの FCoE セッション情報を表示することができます。

1. システムツリーで **シャーシ概要** に進み、**I/O モジュール概要** を展開します。
   展開されたリストに、すべての IOM（1〜6）が表示されます。

2. 表示する IOM（スロット）をクリックして、**プロパティ → FCoE** をクリックします。
   その IOM スロットに固有の **FCoE I/O モジュール** ページが表示されます。

3. **ポートの選択** ドロップダウンメニューで、選択された IOM に必要なポート番号を選択し、**セッションの表示** をクリックします。
   FCoE セッション情報 セクションに、スイッチの FCoE セッション情報が表示されます。

   メモ: このセクションでは、I/O アグリゲータでアクティブな FCoE 情報が実行されている場合のみ、FCoE 情報が表示されます。

Dell PowerEdge M I/O アグリゲータのスタッキング情報の表示

racadm getioinfo コマンドを使用して、以下の Dell PowerEdge M I/O アグリゲータのスタッキング情報を表示することができます。

- スタック ID — スタックマスターの MAC アドレスで、このモジュールに関連するスタックを特定します。
- スタックユニット — スタック内の I/O アグリゲータの位置を特定する整数です。
- シャーシ ID — この ID はスタックの物理的なトポロジを示すために役立ち、特定のスイッチの場所を特定します。
- スタック役割 — スタック内におけるこのモジュールの機能を特定します。有効な値は、マスター、メンバー、スタンバイです。

-s オプションを付けた **racadm getioinfo** コマンドは、シャーシ内にあるスイッチに対する I/O アグリゲータ関連のスタッキング情報、およびそれらのローカルシャーシと外部シャーシ両方のスタックユニットの表示を可能にします。

ローカルシャーシ内のスイッチのみに対するスタッキング情報を表示するには、次のコマンドを使用します。

```
racadm getioinfo -s
```

ローカルスタックユニットに加え、外部シャーシのユニットのスタッキング情報も表示するには、次のコマンドを使用します。

```
racadm getniccfg [-m <module>]
```

『iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド』にある **racadm getioinfo** コマンドの項を参照してください。

IOM 用ネットワークの設定

IOM を管理するために使用されるインタフェースのネットワーク設定を指定することができます。イーサネットスイッチには帯域外管理ポート（IP アドレス）が設定されます。帯域内管理ポート（つまり VLAN1）の設定にはこのインタフェースは使用されません。

IOM のネットワーク設定を行う前に、IOM に電源が入っている事を確認してください。

ネットワーク設定を行うには、次が必要です。

- グループ A の IOM を設定するためのファブリック A に対する管理者権限。
- グループ B の IOM を設定するためのファブリック B に対する管理者権限。
- グループ C の IOM を設定するためのファブリック C に対する管理者権限。

メモ: イーサネットスイッチの場合、帯域内（VLAN1）および帯域外管理 IP アドレスを同じする、または同じネットワークに設定することはできません。これを行うと、帯域外 IP アドレスが設定されません。デフォルトの帯域内管理 IP アドレスについては、IOM マニュアルを参照してください。

メモ: イーサネットパススルースイッチまたは Infiniband スイッチ用に I/O モジュールのネットワーク設定を行わないでください。

CMC ウェブインタフェースを使用した IOM 用ネットワークの設定

メモ: 本機能は PowerEdge M I/O Aggregator IOM でのみサポートされています。MXL 10/40GbE を含むその他の IOM はサポートされていません。

CMC ウェブインタフェースを使用して IOM 用ネットワーク設定を行うには、次の手順を実行します。

1. システムツリーで **I/O モジュールの概要** に進んで **セットアップ** をクリックするか、**I/O モジュールの概要** を展開して IOM を選択し、**セットアップ** をクリックします。
   I/O モジュールの展開 ページに、電源投入された IOM が表示されます。
2. 必要な IOM のために、DHCP を有効化し、IP アドレス、サブネットマスク、ゲートウェアアドレスを入力します。
3. 管理可能な IOM には、ルートパスワード、SNMP RO コミュニティ文字列、および Syslog サーバー IP アドレスを入力します。各種フィールドについての情報は、『*CMC オンラインヘルプ*』を参照してください。

   メモ: CMC から IOM に設定された IP アドレスは、スイッチの恒久的な起動設定には保存されません。IP アドレスを恒久的に保存するには、`connect switch-n` コマンド、または `racadm connect switch -n` RACADM コマンドを入力するか、IOM GUI へのダイレクトインタフェースを使用して、起動設定ファイルにアドレスを保存する必要があります。
4. **適用** をクリックします。
   ネットワーク設定が IOM 用に設定されました。

   メモ: 管理可能な IOM には、VLAN、ネットワークプロパティ、および IO ポートをデフォルト設定にリセットすることができます。

RACADM を使用した IOM 用ネットワークの設定

RACADM を使用して IOM 用のネットワーク設定を行うには、日付と時刻を設定します。『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』の **deploy** コマンドの項を参照してください。

RACADM **deploy** コマンドを使用して、IOM のユーザー名、パスワード、および SNMP 文字列を設定することができます。

```
racadm deploy -m switch-<n> -u root -p <password>
```

```
racadm deploy -m switch-<n> -v SNMPv2 <snmpCommunityString> ro
```

```
racadm deploy -a [server|switch] -u root -p <password>
```

工場出荷時のデフォルト設定への IMO のリセット

IOM は、**I/O モジュールの展開** ページを使用して工場出荷時のデフォルト設定にリセットすることができます。

メモ: 本機能は PowerEdge M I/O Aggregator IOM でのみサポートされています。MXL 10/40GbE を含むその他の IOM はサポートされていません。

CMC ウェブインタフェースを使用して、選択した IOM を工場出荷時のデフォルト設定にリセットするには、次の手順を実行します。

1. システムツリーで **I/O モジュールの概要** に進んで **セットアップ** をクリックするか、システムツリーで **I/O モジュールの概要** を展開して IOM を選択し、**セットアップ** をクリックします。
   I/O モジュールの展開 ページに、電源投入された IOM が表示されます。
2. 必要な IOM で **リセット** をクリックします。
   警告メッセージが表示されます。
3. **OK** をクリックして続行します。

関連リンク

ファブリック管理の概要
無効な構成
初回電源投入シナリオ
IOM 正常性の監視
IOM 用ネットワークの設定
IOM 用 VLAN の管理
IOM の電源制御操作の管理
IOM のための LED 点滅の有効化または無効化

CMC ウェブインタフェースを使用した IOM ソフトウェアのアップデート

IOM ソフトウェアは、指定された場所から必要なソフトウェアイメージを選択することでアップデートできます。また、以前のソフトウェアバージョンにロールバックすることもできます。

メモ: 本機能は PowerEdge M I/O Aggregator IOM でのみサポートされています。MXL 10/40GbE を含むその他の IOM はサポートされていません。

CMC ウェブインタフェースから IOM インフラストラクチャデバイスソフトウェアをアップデートするには、次の手順を実行します。

1. **シャーシ概要 → I/O モジュール概要 → アップデート** と移動します。
   IOM ファームウェアとソフトウェア ページが表示されます。
   または、次のいずれかのページに移動します。
   - **シャーシの概要 → アップデート**

- **シャーシの概要** → **シャーシコントローラ** → **アップデート**
- **シャーシの概要** → **iKVM** → **アップデート**

IOM ファームウェアとソフトウェア ページへのリンクが記載された**ファームウェアアップデート** ページが表示されます。

2. **IOM ファームウェアとソフトウェア** ページの **IOM ソフトウェア** セクションで、ソフトウェアをアップデートする IOM の **アップデート** 列のチェックボックスを選択して、**ソフトウェアアップデートの適用** をクリックします。
   または、以前のバージョンのソフトウェアにロールバックするには、**ロールバック** 列のチェックボックスを選択します。
3. **参照** オプションを使用してソフトウェアアップデート用のソフトウェアイメージを選択します。ソフトウェアイメージの名前が **IOM ソフトウェアの場所** フィールドに表示されます。
   アップデート状態 セクションでは、ソフトウェアアップデートまたはロールバックの状態情報を提供します。イメージファイルがアップロードされる間、ページにステータスインジケータが表示されます。ファイルの転送時間は、接続速度によって異なります。内部アップデート処理が始まると、ページは自動的に更新され、ファームウェアアップデートのタイマーが表示されます。

   メモ: ファイル転送時に、**更新** アイコンをクリックしたり、他のページへ移動しないでください。

   メモ: IOMINF ファームウェアのアップデート時には、ファイル転送タイマーは表示されません。

   アップデートまたはロールバックが完了すると、IOM デバイスがリセットされて新しいファームウェアが **IOM ファームウェアとソフトウェア** ページに表示されるため、IOM デバイスとの接続が一時的に失われます。

IOM 用 VLAN の管理

IOM 用仮想 LAN（VLAN）は、セキュリティとその他の理由のために、ユーザーを個々のネットワークセグメントに分けることを可能にします。VLAN を使用することにより、32 ポートスイッチの個々のユーザーのためにネットワークを隔離することができます。スイッチ上の選択されたポートを選択した VLAN と関連付け、これらのポートを個別のスイッチとして扱うこともできます。

CMC ウェブインタフェースでは、IOM に帯域内管理ポート（VLAN）を設定することが可能になります。

関連リンク

CMC ウェブインタフェースを使用した VLAN の設定
CMC ウェブインタフェースを使用した VLAN の表示
CMC ウェブインタフェースを使用した IOM の現在の VLAN 設定の表示
CMC ウェブインタフェースを使用した IOM 用のタグ付き VLAN の追加
CMC ウェブインタフェースを使用した IOM 用 VLAN の削除
CMC ウェブインタフェースを使用した IOM 用のタグ無し VLAN のアップデート
CMC ウェブインタフェースを使用した IOM 用 VLAN のリセット

ウェブインタフェースを使用した IOM 上での管理 VLAN の設定

VLAN を I/O アグリゲータの帯域内管理を行うことができます。この VLAN は、使用前に導入されている必要があります。CMC では帯域内管理 VLAN 導入が可能です。スイッチの帯域内管理 VLAN は、次の基本設定が適用されることを必要とします。

- 有効
- VLAN ID
- 優先順位

メモ:

Vlan 設定 ページでの管理 VLAN の設定には、**シャーシ設定** 権限が必要です。この権限は、特定のファブリック A、B、または C に対する **管理者** 権限に加え、IOM VLAN 設定にも必要です。

CMC ウェブインタフェースを使用して IOM の管理 VLAN を設定するには、次の手順を実行します。

1. システムツリーで **シャーシ概要** へ移動し、**ネットワーク → VLAN** をクリックします。
   VLAN タグ設定 ページが表示されます。
2. **I/O モジュール** セクションで、IOM 用の VLAN を有効化し、優先順位を設定して ID を入力します。フィールドについての詳細は、『CMC オンラインヘルプ』を参照してください。
3. 設定を保存するには、**適用** をクリックします。

RACADM を使用した IOM 上での管理 VLAN の設定

RACADM を使用して IOM 上で管理 VLAN を設定するには、`racadm setniccfg –m switch-n -v` コマンドを使用します。

- 次のコマンドで、特定の IOM の VLAN ID と優先順位を指定します。
  `racadm setniccfg -m switch -<n> -v <VLAN id> <VLAN priority>`

  `<n>` の有効値は 1～6 です。

  `<VLAN>` に指定できる値は 1～4000、および 4021～4094 の範囲の数値です。デフォルトは 1 です。

  `<VLAN priority>` の有効値は 0～7 です。デフォルトは 0 です。

  たとえば、次のとおりです。
  `racadm setniccfg -m switch -1 -v 1 7`

  たとえば、次のとおりです。
- IOM VLAN を削除するには、指定した IOM のネットワークの VLAN 機能を無効化します。
  `racadm setniccfg -m switch-<n> -v`

  `<n>` の有効値は 1～6 です。

  たとえば、次のとおりです。
  `cadm setniccfg -m switch-1 -v`

CMC ウェブインタフェースを使用した VLAN の設定

メモ: VLAN 設定は、PowerEdge M I/O アグリゲータ IOM でのみ設定可能です。MXL 10/40GbE を含むその他の IOM はサポートされません。

CMC ウェブインタフェースを使用して VLAN 設定を行うには、次の手順を実行します。

1. システムツリーで **I/O モジュール概要** に進み、**セットアップ → VLAN Manager** とクリックします。
   VLAN Manager ページに、電源投入された IOM と利用可能なポートが表示されます。
2. **手順 1：I/O モジュールの選択** セクションで、ドロップダウンリストから設定タイプを選択し、次に必要な IOM を選択します。
   このフィールドについての詳細は、『*CMC オンラインヘルプ*』を参照してください。
3. **手順 2: ポート範囲の指定** セクションで、選択した IOM に割り当てられるファブリックポートの範囲を選択します。
   このフィールドについての詳細は、『*CMC オンラインヘルプ*』を参照してください。
4. **選択** または **すべて選択解除** オプションを選択して、すべての IOM に変更を適用、またはどの IOM にも変更を適用しません。

または

特定のスロットに対するチェックボックスを選択し、必要な IOM を選択します。

5. **手順 3：VLAN の編集** セクションで、IOM の VLAN ID を入力します。VLAN ID は 1～4094 の範囲内であり、範囲として、またはカンマで区切って入力できます（例：1,5,10,100-200）。
6. ドロップダウンメニューから、必要に応じて次のオプションのいずれかを選択します。
   - タグ付き VLAN の追加
   - VLAN の削除
   - タグ無し VLAN のアップデート
   - 全 VLAN のリセット
   - VLAN の表示
7. **保存** をクリックして **VLAN Manager** ページで行った新規設定を保存します。
   このフィールドについての詳細は、『*CMC オンラインヘルプ*』を参照してください。

   メモ: 全ポートの VLAN の概要セクションには、シャーシに存在する IOM と割り当て済み VLAN についての情報が表示されます。現在の VLAN 設定サマリの csv ファイルを保存するには、保存 をクリックします。

   メモ: CMC 管理下 VLAN セクションに、IOM に割り当てられた全 VLAN のサマリが表示されます。
8. **適用** をクリックします。
   ネットワーク設定が IOM 用に設定されました。

CMC ウェブインタフェースを使用した VLAN の表示

CMC ウェブインタフェースを使用して VLAN を表示するには、次の手順を実行します。

1. システムツリーで **I/O モジュール概要** に進み、**セットアップ → VLAN Manager** とクリックします。
   VLAN Manager ページが表示されます。
   全ポートの VLAN のサマリ セクションに、IOM のための現在の VLAN 設定についての情報が表示されます。
2. **保存**をクリックして、VLAN 設定をファイルに保存します。

CMC ウェブインタフェースを使用した IOM の現在の VLAN 設定の表示

CMC ウェブインタフェースを使用して IOM の現在の VLAN 設定を表示するには、次の手順を実行します。

1. システムツリーで **I/O モジュールの概要** に移動し、**セットアップ → VLAN Manager** とクリックします。
   VLAN Manager ページが表示されます。
2. **VLAN の編集** セクションで、ドロップダウンリストから **VLAN の表示** を選択し、**適用** をクリックします。
   操作成功メッセージが表示されます。IOM に割り当てられた現在の VLAN 設定が VLAN 割り当てサマリフィールドに表示されます。

CMC ウェブインタフェースを使用した IOM 用のタグ付き VLAN の追加

CMC ウェブインタフェースを使用して IOM 用のタグ付き VLAN を追加するには、次の手順を実行します。

1. システムツリーで **I/O モジュール概要** に進み、**セットアップ → VLAN Manager** とクリックします。
   VLAN Manager ページが表示されます。
2. **手順 1：I/O モジュールの選択** セクションで、必要な IOM を選択します。
3. **手順 2: ポート範囲の指定** セクションで、選択した IOM に割り当てられるファブリックポートの範囲を選択します。

フィールドについての情報は、『*CMC オンラインヘルプ*』を参照してください。

4. **選択** または **すべて選択解除** オプションを選択して、すべての IOM に変更を適用、またはどの IOM にも変更を適用しません。
   または
   特定のスロットに対するチェックボックスを選択し、必要な IOM を選択します。
5. **手順 3 : VLAN の編集** セクションで、ドロップダウンリストから **タグ付き VLAN の追加** を選択し、**適用** をクリックします。
   タグ付き VLAN が選択した IOM に割り当てられます。
   操作成功メッセージが表示されます。IOM に割り当てられた現在の VLAN 設定が **VLAN 割り当て概要フィールド** に表示されます。

CMC ウェブインタフェースを使用した IOM 用 VLAN の削除

CMC ウェブインタフェースを使用して IOM から VLAN を削除するには、次の手順を実行します。

1. システムツリーで **I/O モジュール概要** に進み、**セットアップ → VLAN Manager** とクリックします。
   VLAN Manager ページが表示されます。
2. **手順 1 : I/O モジュールの選択** セクションで、必要な IOM を選択します。
3. **手順 3 : VLAN の編集** セクションで、ドロップダウンリストから **VLAN の削除** を選択し、**適用** をクリックします。
   選択した IOM に割り当てられた VLAN が削除されます。
   操作成功メッセージが表示されます。IOM に割り当てられた現在の VLAN 設定が **VLAN 割り当て概要** フィールドに表示されます。

CMC ウェブインタフェースを使用した IOM 用のタグ無し VLAN のアップデート

CMC ウェブインタフェースを使用して IOM 用のタグ無し VLAN をアップデートするには、次の手順を実行します。

1. システムツリーで **I/O モジュール概要** に進み、**セットアップ → VLAN Manager** とクリックします。
   VLAN Manager ページが表示されます。
2. **手順 1: I/O モジュールの選択** セクションで、必要な IOM を選択します。
3. **手順 2: ポート範囲の指定** セクションで、選択した IOM に割り当てられるファブリックポートの範囲を選択します。
   フィールドについての情報は、『*CMC オンラインヘルプ*』を参照してください。
4. **選択 / すべてを選択解除** オプションを選択して、すべての IOM に変更を適用、またはどの IOM にも変更を適用しません。
   または
   特定のスロットに対するチェックボックスを選択し、必要な IOM を選択します。
5. **手順 3: VLAN の編集** セクションで、ドロップダウンリストから **タグ無し VLAN のアップデート** を選択し、**適用** をクリックします。
   既存のタグ無し VLAN の設定が、新しく割り当てられたタグ無し VLAN の設定で上書きされるという警告メッセージが表示されます。
6. **OK** をクリックして確定します。
   タグ無し VLAN が、新しく割り当てられたタグ無し VLAN の設定でアップデートされます。
   操作成功メッセージが表示されます。IOM に割り当てられた現在の VLAN 設定が VLAN 割り当て概要フィールドに表示されます。

CMC ウェブインタフェースを使用した IOM 用 VLAN のリセット

CMC ウェブインタフェースを使用して IOM 用 VLAN をデフォルト設定にリセットするには、次の手順を実行します。

1. システムツリーで **I/O モジュール概要** に進み、**セットアップ → VLAN Manager** とクリックします。
   VLAN Manager ページが表示されます。
2. **手順 1 : I/O モジュールの選択** セクションで、必要な IOM を選択します。
3. **手順 3 : VLAN の編集** セクションで、ドロップダウンリストから **VLAN のリセット** を選択し、**適用** をクリックします。
   既存 VLAN の設定がデフォルト設定で上書きされることを示す警告メッセージが表示されます。
4. **OK** をクリックして確定します。
   デフォルト設定に従って VLAN が選択した IOM に割り当てられます。
   操作成功メッセージが表示されます。IOM に割り当てられた現在の VLAN 設定が VLAN 割り当てサマリフィールドに表示されます。

IOM の電源制御操作の管理

IOM 用に電源制御操作を設定するための情報は、「IOM での電源制御操作の実行」を参照してください。

IOM のための LED 点滅の有効化または無効化

IOM のための LED 点滅の有効化についての情報は、「シャーシ上のコンポーネントを識別するための LED の設定」を参照してください。

14

iKVM の設定と使用

Dell M1000e サーバーシャーシ用のローカルアクセス KVM モジュールは、Avocent Integrated KVM スイッチモジュール、または iKVM と呼ばれます。iKVM はシャーシに差し込むアナログキーボード、ビデオ、およびマウススイッチです。これはオプションのシャーシへのホットプラグが可能なモジュールで、ローカルキーボード、マウス、およびビデオにシャーシ内のサーバー、およびアクティブな CMC のコマンドラインへのアクセスを提供します。

関連リンク

iKVM ユーザーインタフェース
iKVM 主要機能
物理的な接続インタフェース

iKVM ユーザーインタフェース

iKVM は、ホットキーでアクティブ化される On Screen Configuration and Reporting（OSCAR）グラフィカルユーザーインタフェースを使用します。OSCAR では、ローカルキーボード、ディスプレイ、およびマウスでアクセスしたいサーバーのひとつ、または Dell CMC コマンドラインを選択することができます。シャーシ 1 台につき、1 つの iKVM セッションのみが許可されます。

関連リンク

OSCAR の使用

iKVM 主要機能

- セキュリティ — スクリーンセーバーパスワードでシステムを保護します。ユーザー定義の時間経過後、スクリーンセーバーモードが実行され、OSCAR を再アクティブ化するための正しいパスワードが入力されるまで、アクセスは拒否されます。
- スキャニング — サーバーのリストを選択できます。このサーバーリストは OSCAR がスキャンモードの間に選択された順序で表示されます。
- サーバー識別 — CMC はシャーシ内のすべてのサーバーに固有のスロット名を割り当てます。階層型接続から OSCAR インタフェースを使用してサーバーに名前を割り当てる事もできますが、CMC 割り当ての名前が優先され、OSCAR を使用してサーバーに割り当てた新しい名前はいずれも上書きされます。

  CMC ウェブインタフェースを使用してスロット名を変更するには、「スロット名の設定」を参照してください。RACADM を使用してスロット名を変更するには、『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』の **setslotname** の項 を参照してください。
- ビデオ — iKVM ビデオ接続では、640 x 480（60Hz）から最大 1280 x 1024（60Hz）までのビデオ画面解像度がサポートされています。
- プラグアンドプレイ — iKVM はデータ表示チャネル（DDC）プラグアンドプレイをサポートしています。DDC はビデオモニタの設定を自動化するもので、VESA DDC2B 規格に準拠しています。
- フラッシュアップグレード可能 — CMC ウェブインタフェースまたは RACADM `fwupdate` コマンドを使用して iKVM ファームウェアをアップデートできます。

関連リンク

OSCAR の使用
iKVM によるサーバーの管理
CMC からの iKVM の管理

iKVM ファームウェアのアップデート

物理的な接続インタフェース

シャーシの前面パネル、アナログコンソールインタフェース（ACI）、およびシャーシの背面パネルから、iKVM を介してサーバーまたは CMC CLI コンソールに接続できます。

メモ: シャーシ前面にあるコントロールパネルのポートは、オプションの iKVM 専用に設計されています。iKVM モジュールをお持ちでない場合は、前面のコントロールパネルポートを使用することはできません。

iKVM の 接続手順

接続は一度に 1 接続のみが可能です。iKVM は接続の各タイプに優先順位を割り当てることから、複数の接続がある場合は 1 つの接続のみが利用可能となり、他の接続は無効化されます。

iKVM 接続の優先順位は次のとおりです。

1. 前面パネル
2. ACI
3. 背面ペイン

例えば、前面パネルと ACI に iKVM 接続がある場合、前面パネル接続はアクティブのままですが、ACI 接続は無効化されます。ACI および背面接続がある場合は、ACI 接続が優先されます。

ACI 接続を介した階層化

iKVM では、サーバーおよび iKVM の CMC コマンドラインコンソールとの階層型接続が可能になります。この接続は、Remote Console Switch ポートを介してローカルに、または Dell RCS ソフトウェアを介してリモートで行います。iKVM は次の製品からの ACI 接続をサポートします。

- 180AS、2160AS、2161DS、2161DS-2、または 4161DS Dell Remote Console Switches
- Avocent AutoView スイッチシステム
- Avocent DSR スイッチシステム
- Avocent AMX スイッチシステム

メモ: 2161DS は Dell CMC コンソール接続はサポートしていません。

メモ: iKVM は Dell 180ES および 2160ES への ACI 接続もサポートしますが、階層化はシームレスではありません。この接続には USB から PS2 の SIP が必要です。

OSCAR の使用

本項では、OSCAR インタフェースを起動、設定、および使用するための情報を提供します。

関連リンク

OSCAR の起動
ナビゲーションの基本
OSCAR の設定

OSCAR の起動

Oscar を起動するには、次の手順を実行します。

1. <Print Screen> を押します。
   メインダイアログボックスが表示されます。
   パスワードが割り当てられている場合、<Print Screen> をクリックした後で **パスワード** ダイアログボックスが表示されます。
2. パスワードを入力して、**OK** をクリックします。
   メインダイアログボックスが表示されます。

   メモ: OSCAR の呼び出しオプションは 4 つあります。メインダイアログボックスの OSCAR の呼び出しセクションにあるボックスを選択することによって、1 つ、複数、またはすべてのキーシーケンスを有効化できます。

関連リンク

コンソールセキュリティの設定
ナビゲーションの基本

ナビゲーションの基本

表 33. : OSCAR キーボードとマウスの操作

キーまたはキーシーケンス	結果
• <Print Screen>-<Print Screen> • <Shift>-<Shift> • <Alt>-<Alt> • <Ctrl>-<Ctrl>	**OSCAR の呼び出し** 設定に応じて、これらのどのキーシーケンスでも OSCAR が開きます。**メイン** ダイアログボックスの **OSCAR の呼び出し** セクションのボックスを選択して **OK** をクリックすることによって、これらのキーシーケンスの 2 つ、3 つ、またはすべてを有効化できます。
<F1>	現在のダイアログボックスの **ヘルプ** 画面を開きます。
<Esc>	変更を保存せずに現在のダイアログボックスを閉じて、前のダイアログボックスに戻ります。 **メイン** ダイアログボックスでは、<Esc> で OSCAR インタフェースを終了して、選択したサーバーに戻ります。 メッセージボックスでは、ポップアップボックスを閉じて現在のダイアログボックスに戻ります。
<Alt>	下線付きの英字やその他の指定した文字と組み合わせて使用し、ダイアログボックスを開いたり、オプションを選択（チェックボックスをオンに）したり、処置を実行したりします。
<Alt>+<X>	現在のダイアログボックスを閉じて、前のダイアログボックスに戻ります。
<Alt>+<O>	**OK** を選択して前のダイアログボックスに戻ります。
<Enter>	**メイン** ダイアログボックスでスイッチ操作を完了し、OSCAR を終了します。
シングルクリック、<Enter>	テキストボックスで編集するテキストを選択し、左および右矢印キーを有効化してカーソルを動かします。<Enter> を再度押して編集モードを終了します。
<Print Screen>、<Backspace>	他のキー入力がない場合は、前の選択項目に切り替えます。

キーまたはキーシーケンス	結果
<Print Screen>、<Alt>+<0>	サーバーからユーザーをただちに切断します。サーバーは選択されていません。状態フラッグがフリーを表示します。（この処置はキーパッドではなくキーボードの =<0> のみに適用されます。）
<Print Screen>、<Pause>	スクリーンセーバーモードを即座にオンにし、パスワード保護されている場合は、そのコンソールへのアクセスを防ぎます。
上 / 下矢印キー	リストの行から行へとカーソルを移動します。
左 / 右矢印キー	テキストボックスの編集時に列内でカーソルを移動します。
<Home>/<End>	カーソルをリストの先頭（Home）または一番下（End）に移動します。
<Delete>	テキストボックスの文字を削除します。
数字キー	キーボードまたはキーパッドから入力します。
<Caps Lock>	無効化されています。大文字と小文字を切り替えるには、<Shift> キーを使用します。

OSCAR の設定

OSCAR 設定は、**セットアップ** ダイアログボックスを使用して設定できます。

セットアップダイアログボックスへのアクセス

セットアップ ダイアログボックスにアクセスするには、次の手順を実行します。

1. <Print Screen> を押して OSCAR インタフェースを起動します。
   メイン ダイアログボックスが表示されます。
2. **セットアップ** をクリックします。
   カスタムセットアップ ダイアログボックスが表示されます。

機能	目的
メニュー	サーバーのリスト表示をスロットの番号順と、名前のアルファベット順の間で切り替えます。
セキュリティ	– パスワードを設定してサーバーへのアクセスを制限します。 – スクリーンセーバーを有効にし、スクリーンセーバーが表示されるまでのアイドル時間を設定して、スクリーンサーバーモードを設定します。
フラグ	状態フラグの表示、タイミング、色、配置を変更します。
言語	OSCAR の全画面の言語を変更します。
ブロードキャスト	キーボードとマウスの操作で複数のサーバーを同時に制御するように設定します。
スキャン	最大 16 台のサーバーのカスタムスキャンパターンを設定します。

関連リンク

表示動作の変更
OSCAR 用キーシーケンスの割り当て
OSCAR の画面表示待ち時間の設定
状態フラグ表示の設定

表示動作の変更

サーバーの表示順序を変更し、OSCAR の画面遅延時間を設定するには、**メニュー** ダイアログボックスを使用します。

表示動作を変更するには、次の手順を実行します。

1. <Print Screen> を押して OSCAR を起動します。
   メイン ダイアログボックスが表示されます。
2. **セットアップ**、**メニュー** の順にクリックします。
   メニュー ダイアログボックスが表示されます。
3. サーバーのデフォルト表示順序を選択するには、次のいずれかを実行します。
   - **名前** を選択して、サーバーを名前に基づいてアルファベット順に表示します。
   - **スロット** を選択して、サーバーをスロット番号順に表示します。
4. **OK** をクリックします。

OSCAR 用キーシーケンスの割り当て

OSCAR のアクティブ化のために 1 つ、または複数のキーシーケンスを割り当てるには、**OSCAR の呼び出し** メニューからキーシーケンスを選択し、**OK** をクリックします。OSCAR を呼び出すためのデフォルトキーは <Print Screen> です。

OSCAR の画面表示待ち時間の設定

OSCAR のために画面表示待ち時間を設定するには、<Print Screen> を押した後、OSCAR 表示を遅らせる秒数（0～9）を入力し、**OK** をクリックします。

<0> と入力すると、遅延なしで OSCAR が起動します。

OSCAR の表示を遅延させる時間を設定すると、ソフトスイッチの完了が可能になります。

関連リンク

ソフトスイッチ

状態フラグ表示の設定

状態フラグはお使いのデスクトップに表示され、選択したサーバーの名前、または選択したスロットの状態を示します。フラグダイアログボックスを使用して、サーバー別の表示フラグの設定、またはフラグの色、不透明度、表示時間、およびデスクトップ上の位置の変更を行います。

フラグ	説明
	名前別のフラグタイプです。
	ユーザーがすべてのシステムから切断されたことを示すフラグです。
	ブロードキャストモードが有効であることを示すフラグです。

状態フラグの表示を設定するには、次の手順を実行します。

1. <Print Screen> を押して OSCAR を起動します。

メイン ダイアログボックスが表示されます。

2. **セットアップ**、**フラグ** の順にクリックします。
   フラグ ダイアログボックスが表示されます。
3. フラグを常に表示するには **表示** を選択し、切り替え後 5 秒間だけフラグを表示するには **表示** および **時間指定** を選択します。

   メモ: 時間指定 だけを選択すると、フラグは表示されません。
4. **表示色** セクションで、フラグの色を選択します。オプションは、黒、赤、青、および紫です。
5. **表示モード** で、無地のカラーフラグには**不透明** を選択し、フラグからデスクトップが透けて見えるようにするには **透明** を選択します。
6. デスクトップ上での状態フラッグの位置を設定するには、**位置の設定** をクリックします。
   位置の設定 フラグが表示されます。
7. 表題バーを左クリックし、デスクトップの希望の位置までドラッグした後、右クリックして **フラグ** ダイアログボックスに戻ります。
8. **OK** をクリックし、再度 **OK** をクリックして設定を保存します。

   変更を保存せずに終了するには、 。

iKVM によるサーバーの管理

iKVM は、最大 16 台のサーバーをサポートするアナログスイッチマトリックスです。iKVM スイッチは、サーバーの選択と設定のために OSCAR ユーザーインタフェースを使用します。さらに、iKVM には、CMC への CMC コマンドラインコンソール接続を確立するためのシステム入力も含まれています。

アクティブなコンソールリダイレクトセッションが存在し、低解像度のモニタが iKVM に接続されている場合、ローカルコンソールでサーバーが選択されると、サーバーコンソールの解像度がリセットされる場合があります。システムが Linux オペレーティングシステムを実行している場合、ローカルモニターで X11 コンソールを表示できないことがあります。iDRAC7 仮想コンソールで <Ctrl><Alt><F1> を押して、Linux をテキストコンソールに切り換えます。

関連リンク

周辺機器の互換性とサポート
サーバーの表示と選択

周辺機器の互換性とサポート

iKVM は次の周辺機器と互換性があります。

- QWERTY、QWERTZ、AZERTY、および日本語 109 配列の標準 PC USB キーボード。
- DDC をサポートしている VGA モニタ。
- 標準 USB ポインティングデバイス。
- iKVM のローカル USB ポートに接続されているセルフパワー USB 1.1 ハブ。
- Dell M1000e シャーシの前面パネルコンソールに接続されているパワー USB 2.0 ハブ。

メモ: iKVM ローカル USB ポートでは、複数のキーボードとマウスを使用することができます。iKVM は入力信号を集約します。複数の USB キーボードやマウスからの同時の入力信号がある場合、予期しない結果が生じる場合があります。

メモ: USB 接続は対応キーボード、マウス、および USB ハブに限定されます。iKVM はその他の USB 周辺機器から送信されるデータはサポートしません。

サーバーの表示と選択

OSCAR を起動すると **メイン** ダイアログボックスが表示されます。**メイン** ダイアログボックスを使用して、iKVM 経由でサーバーを表示、設定、および管理します。サーバーは名前ごとまたはスロットごとに表示できます。スロット番号は、サーバーが使用するシャーシスロット番号です。**スロット** 列はサーバーが取り付けられているスロット番号を示します。

メモ: Dell CMC コマンドラインはスロットを占有します。このスロットを選択すると、RACADM コマンドを実行したり、サーバーのシリアルコンソールまたは I/O モジュールに接続することができる CMC コマンドラインが表示されます。

メモ: サーバー名とスロット番号は CMC によって割り当てられます。

関連リンク

ソフトスイッチ
サーバー状態の表示
サーバーの選択

サーバー状態の表示

メイン ダイアログボックスの右列は、シャーシ内のサーバー状態を示します。次の表は状態記号を説明しています。

表 34. OSCAR インタフェースのステータス記号

記号	説明
	サーバーがオンラインです。
	サーバーがオフライン、またはシャーシに存在しません。
	サーバーは使用できません。
	サーバーは次の文字によって示されるユーザーチャネルによってアクセスされています。 • A= 背面パネル • B= 前面パネル

サーバーの選択

メイン ダイアログボックスを使用してサーバーを選択します。サーバーを選択するとき、iKVM はキーボードとマウスをそのサーバーに適した設定に再設定します。

- サーバーを選択するには、次のいずれかを行います。
  - サーバー名かスロット番号をダブルクリックします。
  - サーバーのリストがスロット順に表示されている場合は（スロット ボタンが押された状態）、スロット番号を入力して <Enter> を押します。
  - サーバーのリストが名前順に表示されている場合は（名前 ボタンが押された状態）、固有のサーバー名として確立するまで、最初の文字をいくつか入力して <Enter> を 2 回押します。
- 以前のサーバーを選択するには、<Print Screen> を押し、次に <Backspace> を押します。このキーの組み合わせは、以前の接続と現在の接続を切り替えます。
- サーバーからユーザーを切断するには、次のいずれかを行います。
  - <Print Screen> を押して OSCAR にアクセスしてから切断をクリックします。

– <Print Screen> を押してから <Alt> <0> を押します。これによって、サーバーが選択されていないフリー状況になります。お使いのデスクトップ上の状態フラグ（アクティブな場合）がフリーを表示します。「**状態フラグ表示の設定**」を参照してください。

ソフトスイッチ

ソフトスイッチとは、ホットキーシーケンスを利用したサーバー間の切り替えです。<Print Screen> を押してサーバーにソフトスイッチし、その名前の最初数個の文字、または番号を入力します。遅延時間（<Print Screen> を押した後に **メイン** ダイアログボックスが表示されるまでの秒数）を以前に設定しており、その時間が経過する前にキーシーケンスを押した場合、OSCAR インタフェースは表示されません。

関連リンク

ソフトスイッチの設定
サーバーへのソフトスイッチ

ソフトスイッチの設定

OSCAR にソフトスイッチを設定するには、次の手順を実行します。

1. <Print Screen> を押して OSCAR インタフェースを起動します。
   メイン ダイアログボックスが表示されます。
2. **セットアップ**、**メニュー** の順にクリックします。
   メニュー ダイアログボックスが表示されます。
3. 表示 / 並べ替えキーの **名前** または **スロット** を選択します。
4. **画面遅延時間** フィールドに遅延時間を秒で入力します。
5. **OK** をクリックします。

サーバーへのソフトスイッチ

サーバーにソフトスイッチするには、次の手順を実行します。

- サーバーを選択するには <Print Screen> を押します。お使いのサーバーリストの表示順序が選択に従ってスロット順になっている場合は（つまり、スロットボタンが押された状態になっている）、スロット番号を入力して <Enter> を押します。
  または
  お使いのサーバーリストの表示順序が選択に従って名前順になっている場合は（つまり、名前 ボタンが押された状態になっている）、固有のサーバー名として確立するまで、最初の文字をいくつか入力して <Enter> を 2 回押します。
- 前のサーバーに戻るには、<Print Screen> を押してから <Backspace> を押します。

ビデオ接続

iKVM には、シャーシの前面および背面パネルにビデオ接続があります。前面パネル接続の信号は、背面パネルの信号よりも優先されます。前面パネルにモニタが接続されているときは、ビデオ接続は背面パネルに渡されず、背面パネルの KVM および ACI 接続が無効化されたことを示す OSCAR メッセージが表示されます。モニタが無効化されると（つまり、前面パネルから取り外されるか、CMC コマンドによって無効化される）、ACI 接続はアクティブ化されますが、背面パネル KVM は引き続き無効化されたままとなります。

関連リンク

iKVM の 接続手順
前面パネルからの iKVM へのアクセスの有効化または無効化

割り込み警告

通常、iKVM からサーバーコンソールに接続しているユーザーと、iDRAC ウェブインタフェースコンソールリダイレクト機能を使用して同じサーバーコンソールに接続している別のユーザーは、両者とも同時にコンソールにアクセスして入力することができます。

このシナリオを回避するため、リモートユーザーは iDRAC ウェブインタフェースコンソールリダイレクトを開始する前に iDRAC ウェブインタフェースでローカルコンソールを無効化することができます。ローカル iKVM ユーザーには、指定された時間中、接続が占有されるという OSCAR メッセージが表示されます。ローカルユーザーは、サーバーへの iKVM 接続が切断される前にコンソールの使用を終えるようにしてください。

iKVM ユーザーが使用できる割り込み機能はありません。

メモ: リモート iDRAC ユーザーが特定のサーバーのためのローカルビデオを無効化した場合、そのサーバーのビデオ、キーボード、およびマウスが iKVM に対して使用不可になります。OSCAR メニューではサーバー状況が黄色の丸でマークされ、サーバーがロックされており、ローカルでの使用が不可であることを示します。「サーバー状態の表示」を参照してください。

関連リンク

サーバー状態の表示

コンソールセキュリティの設定

OSCAR では、iKVM コンソールでセキュリティ設定を行うことが可能になります。指定された遅延時間の間コンソールが不使用のままであった後で実行されるスクリーンセーバーモードをセットアップすることができます。このモードが実行されると、任意のキーを押したり、マウスを動かすまでコンソールのロック状態が維持されます。スクリーンセーバーパスワードを入力して続行します。

セキュリティ ダイアログボックスを使用して、パスワードでのコンソールのロック、パスワードの設定または変更、スクリーンセーバーの有効化を行います。

メモ: iKVM のパスワードを失った、または忘れた場合は、CMC ウェブインタフェースまたは RACADM を使用して iKVM を工場出荷時のデフォルトにリセットできます。

関連リンク

セキュリティダイアログボックスへのアクセス
パスワードの設定
コンソールのパスワード保護
自動ログアウトの設定
コンソールからのパスワード保護の削除
パスワード保護なしのスクリーンセーバーモードの有効化
スクリーンセーバーモードの終了
失った、または忘れたパスワードのクリア

セキュリティダイアログボックスへのアクセス

セキュリティダイアログボックスにアクセスするには、次の手順を実行します。

1. <Print Screen> を押します。
   メイン ダイアログボックスが表示されます。
2. **セットアップ**、**セキュリティ** の順にクリックします。
   セキュリティ ダイアログボックスが表示されます。

パスワードの設定

パスワードを設定するには、次の手順を実行してください。

1. **新規** フィールドでシングルクリックして <Enter> を押すか、ダブルクリックします。
2. 新規パスワードを入力して、<Enter> を押します。パスワードは大文字と小文字を区別し、5～12 文字が必要です。これには、最低 1 つの文字と 1 つの数字が含まれている必要があります。適合文字は A～Z、a～z、0～9、スペース、およびハイフンです。
3. **再入力** フィールドにパスワードをもう一度入力して <Enter> を押します。
4. **OK** をクリックして、ダイアログボックスを閉じます。

コンソールのパスワード保護

コンソールにパスワードを設定するには、次の手順を実行します。

1. 「パスワードの設定」の説明どおり、パスワードを設定します。
2. **スクリーンセーバーを有効にする** チェックボックスをオンにします。
3. パスワード保護とスクリーンセーバーのアクティブ化を遅らせる **アイドル時間**（1～99）を分単位で入力します。
4. **モード**：モニタが ENERGY STAR® 準拠の場合は、**Energy**、それ以外の場合は **画面** を選択します。
   - モードが **Energy** に設定されている場合、アプライアンスはモニタをスリープモードにします。これは通常、モニタの電源が切れ、電源 LED が緑色から橙色に変わることで示されます。
   - モードが **画面** に設定されている場合、テスト期間中、OSCAR フラグが画面全体を飛び回ります。テスト開始前に、警告ポップアップボックスが次のメッセージを表示します。「Energy モードは ENERGY STAR 非準拠のモニタを損傷する可能性があります。ただし、テストの開始後は、マウスまたはキーボードの連携でテストを即時に終了することができます。」

   注意: Energy Star 準拠ではないモニタで Energy モードを使用すると、モニタが損傷する原因となる場合があります。
5. オプション：スクリーンセーバーテストをアクティブ化するには、**テスト** をクリックします。**スクリーンセーバーテスト** ダイアログボックスが表示されます。 **OK** をクリックしてテストを開始します。

   テストには 10 秒かかります。完了後、**セキュリティ** ダイアログボックスに戻ります。

自動ログアウトの設定

一定のアイドル時間が経過すると自動的にログアウトするように OSCAR を設定できます。

1. **メイン** ダイアログボックスで **セットアップ**、**セキュリティ** の順にクリックします。
2. **アイドル時間** フィールドに、自動的に切断されるまで接続したままでいる時間を入力します。
3. **OK** をクリックします。

コンソールからのパスワード保護の削除

コンソールのパスワード保護を解除するには、次の手順を実行してください。

1. **メイン** ダイアログボックスで **セットアップ**、**セキュリティ** の順にクリックします。
2. **セキュリティ** ダイアログボックスで、**新規** フィールドをシングルクリックして <Enter> を押すか、ダブルクリックします。
3. **新規** フィールドを空にしたまま <Enter> を押します。
4. **再入力** フィールドをシングルクリックして <Enter> を押すか、ダブルクリックします。
5. **繰り返し** フィールドを空にしたまま <Enter> を押します。
6. **OK** をクリックします。

パスワード保護なしのスクリーンセーバーモードの有効化

メモ: お使いのコンソールがパスワード保護されている場合、パスワード保護を削除する必要があります。パスワード保護なしのスクリーンセーバーモードを有効化する前にパスワードを削除します。

パスワード保護なしのスクリーンセーバーモードを有効化するには、次の手順を実行します。

1. **スクリーンセーバーの有効化** を選択します。
2. スクリーンセーバーの起動を遅らせる時間 （1～99）を分で入力します。
3. モニタが ENERGY STAR 準拠の場合は、**Energy**、それ以外の場合は **画面** を選択します。

   注意: Energy Star 準拠ではないモニタで Energy モードを使用すると、モニタが損傷する原因となる場合があります。
4. オプション： スクリーンセーバーテストをアクティブ化するには、**テスト** をクリックします。**スクリーンセーバーテスト** ダイアログボックスが表示されます。 **OK** をクリックしてテストを開始します。

   テストには 10 秒かかります。完了後、**セキュリティ** ダイアログボックスが表示されます。

   メモ: スクリーンセーバー モードを有効化すると、ユーザーがサーバーから切断されます。これは、サーバーが選択されていないことを意味します。状態フラグが **フリー** を表示します。

スクリーンセーバーモードの終了

スクリーンセーバーモードを終了して **メイン** ダイアログボックスに戻るには、どれかキーを押すか、マウスを動かします。

スクリーンセーバーをオフにするには、**セキュリティ** ダイアログボックスで、**スクリーンセーバーの有効化** ボックスをクリアし、**OK** をクリックします。

スクリーンセーバーを即座にオンにするには、<Print Screen> を押してから <Pause> を押します。

失った、または忘れたパスワードのクリア

iKVM パスワードを失ったり忘れたりした場合は、それを iKVM の工場出荷時デフォルトにリセットしてから、そのパスワードを変更することができます。パスワードは CMC ウェブインタフェースまたは RACADM のいずれかを使用してリセットできます。

CMC ウェブインタフェースを使用して、失った、または忘れた iKVM パスワードをリセットするには、システムツリーで **シャーシ概要 → iKVM** と移動し、**セットアップ** タブをクリックしてから **デフォルト値の復元** をクリックします。

OSCAR を使用してパスワードをデフォルトから変更することができます。詳細については、「パスワードの設定」を参照してください。

RACADM を使用して、失った、または忘れたパスワードをリセットするには、CMC へのシリアル /Telnet/SSH テキストコンソールを開いてログインし、次を入力します。

```
racadm racresetcfg -m kvm
```

メモ: 前面トパネル有効と Dell CMC コンソール有効の設定がデフォルト値と異なる場合、`racresetcfg` コマンドを使用すると、それらがリセットされます。

`racresetcfg` サブコマンドの詳細については、『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

言語の変更

言語 ダイアログボックスを使用して、表示する OSCAR テキストを任意の対応言語に変更します。テキストは、すべての OSCAR 画面で選択した言語にただちに変更されます。

OSCAR の言語を変更するには、次の手順を実行します。

1. <Print Screen> を押します。
   メイン ダイアログボックスが表示されます。
2. **セットアップ**、**言語** の順にクリックします。
   言語 ダイアログボックスが表示されます。
3. 必要な言語を選択し、**OK** をクリックします。

バージョン情報の表示

iKVM ファームウェアとハードウェアのバージョンを表示し、言語とキーボードの設定を確認するには、**バージョン** ダイアログボックスを使用します。

バージョン情報を表示するには、次の手順を実行します。

1. <Print Screen> を押します。
   メイン ダイアログボックスが表示されます。
2. **コマンド**、**バージョンの表示** の順にクリックします。
   バージョン ダイアログボックスが表示されます。**バージョン** ダイアログボックスの上半分にサブシステムバージョンがリストされます。
3.  <Esc> を押して **バージョン** ダイアログボックスを閉じます。

システムのスキャン

スキャンモードでは、iKVM はスロットからスロット（サーバーからサーバー）へのスキャンを自動で行います。スキャンするサーバーと、各サーバーが表示される秒数を指定することによって、最大 16 台のサーバーをスキャンできます。

関連リンク

スキャンリストへのサーバーの追加
スキャンリストからのサーバーの削除
スキャンモードの開始
スキャンモードのキャンセル

スキャンリストへのサーバーの追加

スキャンリストにサーバーを追加するには、次の手順を実行します。

1. <Print Screen> を押します。
   メイン ダイアログボックスが表示されます。
2. **セットアップ**、**スキャン** の順にクリックします。
   シャーシ内の全サーバーがリストされた **スキャン** ダイアログボックスが表示されます。
3. 次の機能いずれかを実行します。
   - スキャンするサーバーを選択。
   - サーバー名またはスロットをダブルクリック。
   - <Alt> とスキャンするサーバーの番号を押す。最大 16 台のサーバーを選択できます。
4. **時間** フィールドに、スキャンがリストの次のサーバーに移動するまで iKVM が待つ時間（3～99）を秒で入力します。
5. **追加 / 削除** をクリックし、次に **OK** をクリックします。

スキャンリストからのサーバーの削除

サーバーをスキャンリストから削除するには、次の手順を実行します。

1. **スキャン** ダイアログボックスで、次のいずれかを行います。
   - 削除するサーバーを選択。
   - サーバー名かスロットをダブルクリック。
   - **クリア** をクリックして、すべてのサーバーを **スキャン** リストから削除。
2. **追加 / 削除** をクリックし、次に **OK** をクリックします。

スキャンモードの開始

スキャンモードを開始するには、次の手順を実行します。

1. <Print Screen> を押します。
   メイン ダイアログボックスが表示されます。
2. **コマンド** をクリックします。
   コマンド ダイアログボックスが表示されます。
3. **スキャン有効** オプションを選択します。
4. **OK** をクリックします。
   マウスとキーボードがリセットされたというメッセージが表示されます。
5.  をクリックしてメッセージボックスを閉じます。

スキャンモードのキャンセル

スキャンモードをキャンセルするには、次の手順を実行します。

1. OSCAR が開いており、**メイン** ダイアログボックスが表示されている場合は、リストからサーバーを選択します。
   または
   OSCAR が開いていない場合は、マウスを動かすか、キーボードで任意のキーを押します。
   メイン ダイアログボックスが表示されます。リスト内のサーバーを選択します。
2. **コマンド** をクリックします。
   コマンド ダイアログボックスが表示されます。
3. **スキャン有効** オプションをクリアして、**OK** をクリックします。

サーバーへのブロードキャスト

システム内の複数のサーバーを同時に制御して、選択されたすべてのサーバーが同じ入力を受け取ることを確実にすることができます。キー入力および / またはマウスの動作を個別にブロードキャストすることも選択できます。

- キー入力のブロードキャスト：キー入力を使用する場合、キー入力が同じであると解釈されるためには、ブロードキャストを受信するすべてのサーバーでキーボードの状況が同じであることが必要です。つまり、<Caps Lock> と <Num Lock> のモードがすべてのキーボードで同じである必要があります。iKVM は選択したサーバーにキー入力を同時に送信しようとしますが、一部のサーバーの抑制によって伝送が遅延する場合があります。
- マウス動作のブロードキャスト：マウスが正確に機能するには、すべてのサーバーのマウスドライバ、デスクトップ（同じアイコンの配置など）、およびビデオ解像度が同じであることが必要です。また、マウスがすべての画面で同じ場所にある必要もあります。なければなりません。これらの条件を満たすことは難しいため、複数のサーバーにマウスの動作をブロードキャストすると、予測不能な結果が生じることがあります。

メモ: 最大 16 のサーバーに対して同時にブロードキャストすることができます。

サーバーにブロードキャストするには、次の手順を実行します。

1. <Print Screen> を押します。
   メイン ダイアログボックスが表示されます。
2. **セットアップ**、**ブロードキャスト** の順にクリックします。
   ブロードキャスト ダイアログボックスが表示されます。
3. チェックボックスをオンにして、ブロードキャストコマンドを受信するサーバーのマウスやキーボードを有効にします。
   または
   上下の矢印を押して、目的のサーバーまでカーソルを移動します。次に <Alt><K> を押してキーボードのチェックボックスを選択、および / または <Alt><M> を押してマウスのチェックボックスを選択します。
   追加サーバーにこの手順を繰り返します。
4. **OK** を押して設定を保存し、**セットアップ** ダイアログボックスに戻ります。
5.  をクリック、または <Escape> を押して、**メイン** ダイアログボックスに戻ります。
6. **コマンド** をクリックします。
   コマンド ダイアログボックスが表示されます。
7. **ブロードキャスト有効** チェックボックスをオンにしてブロードキャストをアクティブにします。
   ブロードキャスト警告 ダイアログボックスが表示されます。
8. **OK** をクリックしてブロードキャストを有効化します。キャンセルして **コマンド** ダイアログボックスに戻るには、  または <Esc> を押します。
9. ブロードキャストが有効になっている場合は、情報を入力、または / およびブロードキャストするマウスの動作を管理ステーションから実行します。リストのサーバーのみがアクセス可能です。

CMC からの iKVM の管理

次の操作が可能です。

- iKVM のステータスとプロパティの表示
- iKVM ファームウェアのアップデート
- 前面パネルからの iKVM へのアクセスの有効化または無効化
- Dell CMC コンソールからの iKVM へのアクセスの有効化または無効化

関連リンク

iKVM ファームウェアのアップデート
前面パネルからの iKVM へのアクセスの有効化または無効化
iKVM の情報と正常性状態の表示
Dell CMC コンソールからの iKVM へのアクセスの有効化

前面パネルからの iKVM へのアクセスの有効化または無効化

CMC ウェブインタフェースまたは RACADM を使用して、前面パネルからの iKVM へのアクセスを有効化または無効化できます。

ウェブインタフェースを使用した前面パネルから iKVM へのアクセスの有効化または無効化

CMC ウェブインタフェースを使用して前面パネルからの iKVM へのアクセスを有効化または無効化するには、次の手順を実行します。

1. システムツリーで **シャーシ概要 → iKVM** と進み、**セットアップ** タブをクリックします。
   iKVM 設定 ページが表示されます。
2. 有効化するには、**前面パネル USB/ ビデオ有効** オプションを選択します。無効化するには、**前面パネル USB/ ビデオ有効** オプションをクリアします。
3. **適用** をクリックして設定を保存します。

RACADM を使用した前面パネルから iKVM へのアクセスの有効化または無効化

RACADM を使用した前面パネルから iKVM へのアクセスを有効または無効にするには、CMC へのシリアル / Telnet/SSH テキストコンソールを開いて CMC へ進み、ログイン後、次を入力します。

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

ここで <値> は 1（有効）または 0（無効）になります。

```
config
```

サブコマンドについての詳細は、『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

Dell CMC コンソールからの iKVM へのアクセスの有効化

CMC ウェブインタフェースを使用して、iKVM から CMC CLI へのアクセスを有効化するには、システムツリーで **シャーシ概要 → iKVM** と進み、**セットアップ** タブをクリックします。**iKVM から CMC CLI へのアクセスを許可する** オプションを選択し、**適用** をクリックして設定を保存します。

RACADM を使用して iKVM から CMC CLI へのアクセスを有効化するには、CMC へのシリアル /Telnet/SSH テキスト コンソールを開いて ログインし、次を入力します。

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

関連リンク

シリアル、Telnet、または SSH コンソールを使用した CMC へのログイン

15

電力の管理と監視

Dell PowerEdge M1000e サーバーエンクロージャは、電力効率が最も優れたモジュラーサーバーエンクロージャです。高効率の電源装置とファンを装備するように設計されており、システム内の通気がより良く行われるように最適化されたレイアウトと、電力最適化されたコンポーネントをエンクロージャ全体に備えています。最適化されたハードウェア設計と、Chassis Management Controller（CMC）、電源装置、および iDRAC 内蔵の高性能電源管理機能が一体となり、電力効率をさらに強化して、電力環境を完全に制御することが可能になります。

M1000e の電源管理機能は、システム管理者が電力消費を削減し、環境固有の必要に合わせて電力を調整するためにエンクロージャの設定を行う際に役立ちます。

PowerEdge M1000e モジュラーエンクロージャは電力を利用し、その負荷をアクティブな内部電源装置ユニット（PSU）すべてに振り分けます。このシステムは、サーバーモジュールおよび関連エンクロージャインフラストラクチャに割り当てられた最大 16685 ワットの入力電力を供給することが可能です。

PowerEdge M1000e エンクロージャは、PSU の動作に影響を与え、システム管理者に対するシャーシ冗長性状況の報告方法を決定する 3 つの冗長性ポリシーのいずれかに設定することできます。

電源管理は **Power Measure, Mitigate, and Manage Console（PM3）** を介して制御することもできます。PM3 が外部から電源を制御するとき、CMC は引き続き次を維持します。

- 冗長性ポリシー
- リモート電力ログ
- 電源冗長性よりサーバーパフォーマンスを優先する
- 動的電源供給（DPSE）
- 110 VAC 動作 — これは AC PSU のみにサポートされています。

PM3 は次を管理します。

- サーバー電源
- サーバーの優先順位
- システム入力電力容量
- 最大節電モード

メモ: 実際の電源供給は、設定と作業負荷に応じて異なります。

CMC における次の電源制御の管理と設定には、CMC ウェブインタフェースまたは RACADM を使用できます。

- シャーシ、サーバーおよび PSU への電力割り当て、消費量および状態の表示。
- シャーシの電力バジェットおよび冗長性の設定。
- シャーシの電源制御操作（電源投入、電源切断、システムリセット、パワーサイクル）の実行。

関連リンク

冗長性ポリシー
動的電源供給
デフォルトの冗長性設定
ハードウェアモジュールの電力バジェット
電力消費量状態の表示
電力バジェット状態の表示

冗長性状態と全体的な電源正常性
電力バジェットと冗長性の設定
電源制御操作の実行

シャーシ、サーバー、および IOM のために次の電源制御操作を実行できます。

冗長性ポリシー

冗長性ポリシーとは、CMC がシャーシへの電力をどのように管理するかを決定する、設定可能なプロパティの一式です。次の冗長性ポリシーは動的な PSU 電源供給の有無に関わらず、設定可能です。

- グリッド冗長性
- 電源装置冗長性
- 冗長性なし

グリッド冗長性ポリシー

グリッド冗長性ポリシーの目的は、モジュラーエンクロージャシステムを電源障害に耐えるモードで動作できるようにすることです。これらの障害は、入力電力グリッド、ケーブル配線と電源供給、または PSU 自体に由来することが考えられます。

グリッド冗長性のためにシステムを構成する場合、スロット 1、2 および 3 にある PSU は第 1 グリッド、スロット 4、5 および 6 にある PSU は第 2 グリッドに振り分けられます。CMC は、グリッドのいずれかが故障した場合、システムが劣化することなく動作を継続するよう電力を管理します。AC 冗長性は個々の PSU の故障にも耐えます。

メモ: グリッド冗長性は、電力グリッド全体の障害にもかかわらずシームレスなサーバー動作を提供します。したがって、2 つのグリッドの容量がほぼ同等の場合、グリッド冗長性を維持するための最大電力が確保できます。

メモ: グリッド冗長性は、負荷要件が最も弱い電源グリッドの容量を超えない場合のみ実現されます。

グリッド冗長性レベル

グリッド冗長性を設定するには、各グリッドにつき最低 1 台の PSU が必要です。追加の構成は、各グリッドに少なくとも 1 台の PSU があるすべての組み合わせで行うことができます。ただし、最大電力を使用できるようにするには、各グリッドの PSU の電力合計ができるだけ同じに近くなるようにしてください。グリッド冗長性を維持する間の電力上限は、2 つのグリッドのうち弱い方で使用可能な電力となります。次の図では、グリッドごとに 2 台の PSU があり、グリッド 1 での電源障害が生じていることを示しています。

CMC がグリッド冗長性を維持することができない場合、**冗長性の損失** イベントのアラート用に設定されていれば、E-メールまたは SNMP アラートが管理者に送信されます。

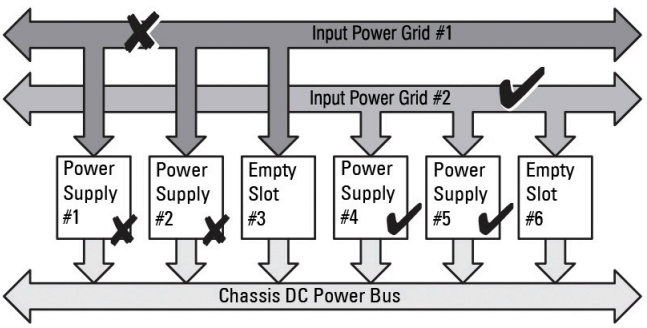


図 5. グリッドにつき PSU が 2 台、グリッド 1 で電源障害

この構成で単一の PSU が故障した場合、失敗状態のグリッド内にある残りの PSU がオンラインとしてマーク付けされます。この状況では、残りのどの PSU での故障もシステムの動作を中断することなく許容されま

す。PSU が故障すると、シャーシ正常性が非重要としてマーク付けされます。小さい方のグリッドがシャーシ電力割り当ての合計量をサポートできない場合は、グリッド冗長性ステータスが **冗長性なし** と報告され、シャーシ正常性が **重要** と表示されます。

電源装置の冗長性ポリシー

電源装置の冗長性ポリシーは、冗長電源グリッドが使用できない場合に便利ですが、モジュラーエンクロージャ内のサーバーをダウンさせる単一 PSU 障害からの保護も推奨されます。この目的のため、最大容量 PSU がオンライン予約に維持されます。これにより、電源装置冗長プールが形成されます。下図は、電源装置の冗長性モードを図解しています。

電力と冗長性のために必要な分を超えた PSU を利用することも可能で、これらは障害時に備えて冗長性プールに追加されます。

AC 冗長性とは異なり、電源冗長性が選択されると、CMC では PSU ユニットを特定の PSU スロットの位置に設置する必要がありません。

メモ: 動的電源供給（DPSE）では、PSU をスタンバイにすることが可能になります。スタンバイ状況とは、PSU から電力が供給されない物理的状況を示します。DPSE を有効化すると、効率性を向上させ、電力を節約するために、追加の PSU がスタンバイモードに設定される場合があります。

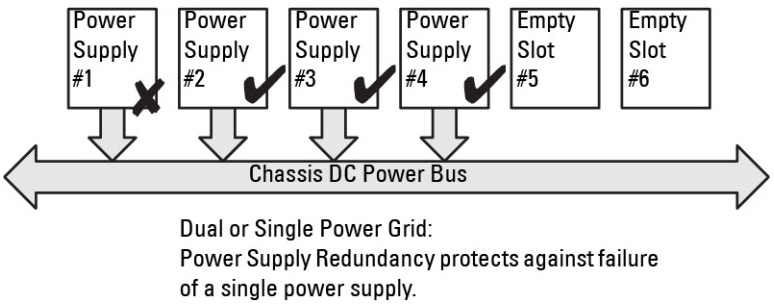


図 6. 電源装置の冗長性：合計 4 台の PSU があり、そのうち 1 台が故障。

冗長性なしポリシー

冗長性なしモードは、PSU 3 台構成のための工場出荷時デフォルト設定で、シャーシに電源冗長性が全く設定されていないことを示します。この構成では、シャーシの全体的な冗長性状態が常に冗長性なしを示します。下図は、PSU 3 台構成用の工場出荷時デフォルト設定である冗長性なしモードを図解します。

冗長性なし が設定されている場合、CMC では、PSU ユニットを特定の PSU スロット位置に設置する必要はありません。

メモ: 冗長性なし モードであるときに DPSE が無効化されていると、シャーシ内の全 PSU が **オンライン** になります。DPSE が有効化されると、シャーシ内のアクティブ PSU のすべてが **オンライン** としてリストされ、システムの電力効率を向上させるために、追加の PSU が **スタンバイ** に設定される場合があります。

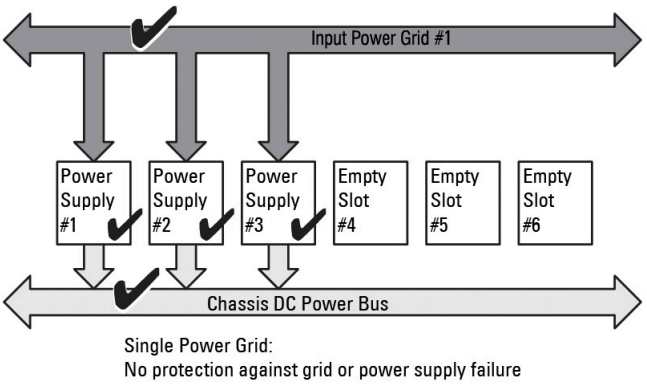


図 7.3 台の PSU を備えたシャーシでの冗長性なし

PSU 障害が発生すると、シャーシの電力割り当てをサポートするために、他の PSU が必要に応じてスタンバイモードから切り替えられます。4 台の PSU があり、3 台だけが必要である場合、1 台の PSU が故障すると、4 台目の PSU がオンラインになります。シャーシでは、6 台の PSU すべてをオンラインにすることができます。

DPSE を有効化すると、システムの電力効率を向上させ、電力を節約するために、追加の PSU がスタンバイモードに設定される場合があります。詳細については、「デフォルトの冗長性設定」を参照してください。

動的電源供給

動的電源供給（DPSE）モードはデフォルトで無効化されています。DPSE はシャーシに電力を供給する PSU の電力効率性を最適化することによって節電します。これにより、PSU の寿命を延ばし、熱発生を削減することにもなります。

CMC は、エンクロージャ全体の電力割り当てを監視し、PSU をスタンバイ状態にします。PSU をスタンバイ状態にすると、次が行われます。

- シャーシの電力割り当てのすべてを少数の PSU で供給。
- 高利用率での稼働によるオンライン PSU の効率性の向上。
- スタンバイ PSU の効率性および耐久性の向上。

残りの PSU を最大の効率性で動作させるには、次の手順を実行します。

- DPSE を使用した **冗長性なし** モードは、最適な PSU 台数がオンラインになっており、電力効率性が非常に高くなります。必要でない PSU はスタンバイモードになります。
- DPSE を使用した **PSU 冗長性** モードも、電力効率性を提供します。少なくとも 2 台の PSU がオンラインであり、そのうち 1 台の PSU が構成への電力供給を行い、もう 1 台は PSU 障害時のための冗長性を提供します。PSU 冗長性モードは、1 台の PSU 障害に対する保護を提供しますが、AC グリッド喪失発生時での保護は提供しません。
- 少なくとも 2 台の PSU（各電力グリッドに 1 台ずつ）がアクティブになっている DPSE での **グリッド冗長性** モードは、部分負荷を受けるモジュラーエンクロージャ構成における効率性と最大可用性の優れたバランスを提供します。
- DPSE を無効化すると、6 台 の PSU すべてがアクティブで負荷を共有しするため、電力効率が最も低くなります。これにより、各電源装置の活用率も低下します。

DPSE は、3 つのすべての電源装置冗長性設定（**冗長性なし**、**電源装置冗長性**、**AC 冗長性**）のために有効化することが可能です。

- DPSE を使用した **冗長性なし** 設定では、M1000e で最大 5 台の電源装置ユニットを **スタンバイ** 状況にすることができます。PSU 6 台構成では、一部の PSU ユニットが **スタンバイ** に設定され、電力効率向上のために未使用状態にされます。この構成でオンライン PSU が取り外されたり、故障したりすると、**スタンバイ** 状況の PSU が **オンライン** になります。ただし、スタンバイ PSU がアクティブになる

には最大 2 秒かかるため、**冗長性なし** 設定で移行中、一部のサーバーモジュールで電力喪失が発生する場合があります。

メモ: PSU 3 台構成では、サーバー負荷によって PSU が スタンバイ に移行できないことがあります。

- **電源装置冗長性** 設定では、エンクロージャは、エンクロージャへの電力供給に必要な PSU に加え、もう 1 台の PSU の電源を常にオンにして **オンライン** に設定しておきます。電力使用率を監視し、システム全体の負荷に応じて、最大 4 台の PSU をスタンバイ状態にすることができます。PSU 6 台の構成では、常に最低 2 台の電源装置の電源がオンになってます。

  電源装置冗長性 設定のエンクロージャでは追加の PSU が常に起動状態であるため、エンクロージャはオンライン PSU 1 台の損失に耐えることが可能です。また、取り付けられているサーバーモジュールに対して十分な電力供給を維持することもできます。オンライン PSU が失われると、スタンバイ PSU がオンラインになります。複数の PSU に障害が同時に発生すると、スタンバイ PSU がオンになるまでの間、一部のサーバーモジュールに対して電力が失われる可能性があります。
- **グリッド冗長性** 設定では、シャーシに電源が投入されると、すべての電源装置が起動されます。電力使用率が監視され、システム構成と電力使用率に応じて許容される場合は、PSU が **スタンバイ** 状況になります。グリッド内の PSU の **オンライン** 状態は他方のグリッドの状態をミラーするため、エンクロージャは、エンクロージャへの電力を中断することなく、グリッド全体への電力喪失に耐えることができます。

  グリッド冗長性 設定における電力需要の上昇により、**スタンバイ** 状況の PSU が起動されます。これにより、デュアルグリッド冗長性に必要なミラー設定が維持されます。

  メモ: DPSE を有効にすると、3 つの電源冗長ポリシーモードすべてにおいて電力需要が上昇した場合、電力を回収するためにスタンバイ PSU が **オンライン** になります。

デフォルトの冗長性設定

シャーシのデフォルト冗長性設定は、次の表に示されるとおり、シャーシに取り付けられた PSU の台数に応じて異なります。

表 35. デフォルトの冗長性設定

PSU 構成	デフォルトの冗長性ポリシー	デフォルトの動的 PSU 電源供給設定
PSU 6 台	グリッド冗長性	無効
PSU 3 台	冗長性なし	無効

グリッド冗長性

6 台の PSU を備えたグリッド冗長性モードでは、6 台の PSU すべてがアクティブです。 左側の PSU 3 台は 1 つの入力電源グリッドに、右側の 3 台は別の電源グリッドに接続する必要があります。

注意: システムエラーを回避し、グリッド冗長性を効率的に機能させるには、PSU 一式がバランス良く個別のグリッドに適切に接続される必要があります。

一方のグリッドが故障した場合、まだ機能しているグリッドに接続されている 3 台の PSU でサーバーやインフラストラクチャに支障なく引き続き電力を供給します。

注意: グリッド冗長性モードでは、バランスのとれた台数の PSU セットが必要です（各グリッドに少なくとも 1 台の PSU が必要）。この条件を満たさない場合、グリッド冗長性を実現できない可能性があります。

電源装置の冗長性

電源装置の冗長性が有効化されると、シャーシ内の 1 台の PSU がスペアとして維持され、PSU のうちいずれかの故障がサーバーまたはシャーシの電源切断を引き起こさないことを確実にします。電源装置の冗長性モードには、最大 4 台の PSU が必要です。追加の PSU が存在する場合、これらは DPSE 有効時の電力効率性向

上のために活用されます。 冗長性喪失後の障害は、シャーシ内のサーバーの電源切断の原因になる場合があります。

冗長性なし

障害発生時においても、シャーシへの電力供給に必要な量を越える電力が、シャーシへの電力供給を継続するために利用可能です。

注意: シャーシ要件のために DPSE が有効になると、冗長性なしモードは最適に PSU を使用します。このモードで単一の PSU に障害が発生すると、サーバーが電力とデータを失う原因となる場合があります。

ハードウェアモジュールの電力バジェット

CMC は、シャーシの電力バジェット、冗長、動的電源機能を設定する電力バジェットサービスを提供します。

電源管理サービスは、電力消費量の最適化、および必要に応じて異なるモジュールに電力を再割り当てする機能を持ちます。

次の図は、PSU 6 台構成のシャーシを示しています。PSU は、エンクロージャの左側から 1〜6 番になります。

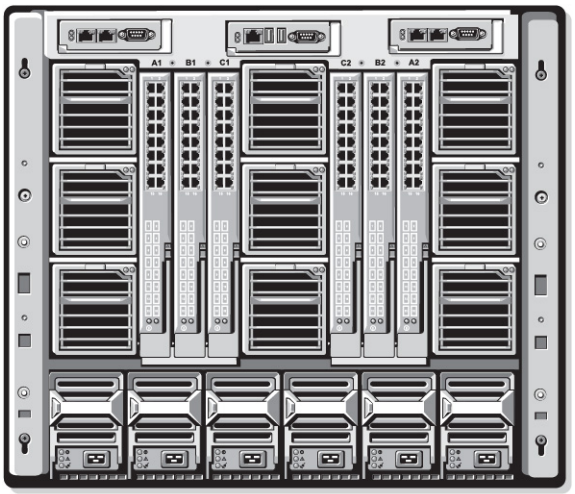


図 8. PSU 6 台構成のシャーシ

CMC は、取り付けられているすべてのサーバーとコンポーネントに必要なワット数を蓄える、エンクロージャ用の電力バジェットを維持します。

CMC はシャーシ内の CMC インフラストラクチャおよびサーバーに電力を割り当てます。CMC インフラストラクチャは、ファン、I/O モジュール、および iKVM（存在する場合）などのシャーシ内のコンポーネントで構成されます。シャーシには、iDRAC を介してシャーシと通信するサーバーを最大 16 台装備できます。詳細については、**support.dell.com/manuals** で『*iDRAC7 ユーザーズガイド*』を参照してください。

iDRAC は、サーバーへの電源投入前に CMC にパワーエンベロープ要件を提示します。パワーエンベロープには、サーバーの動作を維持するために必要な最大および最低電力要件が含まれています。iDRAC の初期推定値は、サーバー内のコンポーネントについての当初の理解に基づいています。動作が開始され、コンポーネントがさらに検出されると、iDRAC は初期電力要件を増加または削減する場合があります。

エンクロージャでサーバーが起動されると、iDRAC ソフトウェアは電力要件を推定し直して、パワーエンベロープの次回変更を要求します。

CMC は要求された電力をサーバーに対して提供し、割り当てられたワット数は利用可能バジェットから差し引かれます。サーバーの電力要求が認められると、サーバーの iDRAC ソフトウェアが実際の電力消費を継続

的に監視します。実際の電力要件に応じて、iDRAC パワーエンベロープは時間の経過と共に変化する場合があります。iDRAC は、割り当てられた電力をサーバーが完全に消費している場合にのみ、電力増加を要求します。

高負荷下では、電力消費がユーザー設定の *システム入力電力上限*未満に留まることを確実にするため、サーバーのプロセッサのパフォーマンスが劣化する場合があります。

PowerEdge M1000e エンクロージャは、ほとんどのサーバー構成のピークパフォーマンスに十分な電力を供給できますが、使用できる多くのサーバー構成では、エンクロージャが供給できる最大電力を消費しません。データセンターでのエンクロージャ用電力のプロビジョニングに役立てるため、M1000e では、シャーシ全体の AC 電力利用が特定のしきい値未満に保たれることを確実にする *システム入力電力上限* を指定することができます。CMC はまず、ファン、IO モジュール、iKVM（存在する場合）、および CMC そのものを動作させるために十分な電力を確保します。この電力割り当ては*シャーシインフラストラクチャに割り当てられた入力電力*と呼ばれます。シャーシインフラストラクチャの次に、エンクロージャ内のサーバーに電源が投入されます。実際の消費量より低い *システム入力電力上限*の設定試行は失敗します。

総電力バジェットを *システム入力電力上限*以下に保つために必要な場合、CMC はサーバーに対して要求された最大電力よりも少ない値を割り当てます。サーバーには *サーバー優先順位*設定に基づいて電力が割り当てられるので、優先順位の高いサーバーには最大電力が提供され、優先度 2 のサーバーは、優先度 1 のサーバーの後に電力が割り当てられることになります。優先順位の低いサーバーは、*システム入力最大電力容量*とユーザー設定の *システム入力電力上限*設定に基づいて優先度 1 のサーバーより少ない電力が提供される場合があります。

シャーシへの追加サーバーなどの構成の変化には、*システム入力電力上限*の引き上げが必要な場合があります。温度状態が変化して、ファンをより高速に稼働させる必要がある時にも、追加電力を消費する原因となることから、モジュラーエンクロージャでの電力需要が増加します。I/O モジュールと iKVM の挿入も、モジュラーエンクロージャの電力需要を増加させます。管理コントローラを起動させておくためにサーバーの電源が切られる時でさえも、サーバーによってごく少量の電力が消費されます。

追加サーバーは、十分な電力が使用可能である場合にのみ、モジュラーエンクロージャ内での電源投入が可能です。*システム入力電力上限*は、追加サーバーへの電源投入を行うため、最大値の 16685 ワットまで常時増加させることができます。

電力割り当てを削減するモジュラーエンクロージャの変化には、次が含まれます。

- サーバーの電源オフ
- サーバー
- I/O モジュール
- iKVM の取り外し
- シャーシの電源オフ状態への移行

*システム入力電力上限*は、シャーシがオンであるかオフであるかに関わらず、再設定することができます。

サーバースロットの電力優先順位の設定

CMC では、エンクロージャ内の 16 個のサーバースロットのそれぞれに電力優先順位を設定することができます。優先順位設定は、1（最高）から 9（最低）になります。これらの設定はシャーシ内のスロットに割り当てられ、スロットの優先順位はそのスロットに挿入されるサーバーすべてによって引き継がれます。CMC はスロットの優先順位を使用して、エンクロージャ内で優先順位が最も高いサーバーに優先的に電力をバジェットします。

デフォルトのサーバースロット優先順位設定では、電力はすべてのスロットに均等に分配されます。スロットの優先順位を変更することによって、システム管理者は電力割り当ての優先権が与えられたサーバーを優先することができます。より重要なサーバーモジュールをデフォルトのスロット優先順位 1 のままにすると、重要度の低いサーバーモジュールは低い優先値 2 以降に変更され、優先順位 1 サーバーが最初に電源投入されます。これらの優先順位の高いサーバーには最大の電力割り当てが提供されますが、優先順位の低いサーバーには、システム入力電力上限とサーバー電力要件がどれだけ低いかによって最大パフォーマンスで稼働するために十分な電力が割り当てられなかったり、電源投入されない場合もあります。

システム管理者が優先順位の高いサーバーモジュールより先に優先順位の低いサーバーモジュールを手動で起動すると、その優先順位の低いサーバーモジュールが、優先順位の高いサーバーに対応するために最小値まで電力割り当てが削減される最初のモジュールになります。従って、使用できる割り当て電力の全てが消費されると、CMC が優先順位が低い、または同じサーバーから、それらの最低電力レベルに達するまで電力を回収します。

メモ: I/O モジュール、ファン、および iKVM（存在する場合）には、最高の優先順位が提供されます。CMC が優先順位順位の高いモジュールまたはサーバーの電力需要を満たすために電力を回収するのは、優先順位の低いデバイスからのみです。

サーバーへの優先順位の割り当て

サーバーの優先順位は、追加電力が必要なときに CMC がどのサーバーの電力を使用するかを決定します。

メモ: サーバーに割り当てる優先順位は、サーバーそのものではなくサーバーのスロットにリンクされます。サーバーを新しいスロットに移動させる場合は、新しいスロットの場所に優先順位を再設定する必要があります。

メモ: 電力管理処置を行うには、**シャーシ設定システム管理者** 特権が必要です。

CMC ウェブインタフェースを使用したサーバーへの優先度レベルの割り当て

CMC ウェブインタフェースを使用して優先度レベルを割り当てるには、次の手順を実行します。

1. システムツリーで **サーバー概要** に移動し、**電力 → 優先順位** とクリックします。
   サーバー優先順位 ページに、シャーシ内のすべてのサーバーがリストされます。
2. 1 台、複数台、またはすべてのサーバーのために優先度レベル（1～9、ここでは 1 が最優先）を選択します。デフォルトの値は 1 です。同じ優先度レベルを複数のサーバーに割り当てることができます。
3. **適用** をクリックして変更を保存します。

RACADM を使用したサーバーへの優先度レベルの割り当て

CMC へのシリアル /Telnet/SSH テキストコンソールを開いてログインし、次を入力します。

```
racadm config -g cfgServerInfo -o cfgServerPriority -i <スロット番号> <優先度レベル>
```

ここで、<*スロット番号*>（1～16）はサーバーの位置を表し、<*優先度レベル*> は 1～9 の数値になります。
例えば、スロット 5 のサーバーに優先度レベル 1 を設定するには、次のコマンドを入力します。

```
racadm config -g cfgServerInfo -o cfgServer Priority -i 5 1
```

電力消費量状態の表示

CMC は、システム全体の実際の入力電力消費量を提供します。

CMC ウェブインタフェースを使用した電力消費状態の表示

CMC ウェブインタフェースを使用して電力消費状態を表示するには、**シャーシ概要** に移動し、**電力 → 電源監視** とクリックします。電源監視ページには、電源正常性、システム電源状態、リアルタイム電力統計、およびリアルタイムエネルギー統計が表示されます。詳細については、『CMC オンラインヘルプ』を参照してください。

メモ: システムツリー → ステータスタブ の電源装置で電源冗長性状態を表示することもできます。

RACADM を使用した電力消費状態の表示

RACADM を使用して電力消費状態を表示するには、次の手順を実行します。

シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインした後、次を入力します。

```
racadm getpminfo
```

電力バジェット状態の表示

電力バジェット状態は、CMC ウェブインタフェースまたは RACADM を使用して表示できます。

CMC ウェブインタフェースを使用した電力バジェット状態の表示

CMC ウェブインタフェースを使用して電力バジェットを表示するには、システムツリーで **シャーシ概要** に進み、**電力 → バジェット状態** とクリックします。**電力バジェット状態** ページに、システムの電源ポリシー設定、電力バジェット詳細、サーバーモジュールに割り当てられたバジェット、およびシャーシ電源装置詳細が表示されます。詳細については、『*CMC オンラインヘルプ*』を参照してください。

RACADM を使用した電力バジェット状態の表示

シリアル /Telnet/SSH テキストコンソールを開いてログインし、次を入力します。

```
racadm getpbinfo
```

出力詳細を含む **getpbinfo** の詳細については、『*iDRAC6 および CMC 向け RACADM コマンドラインリファレンスガイド*』の **getpbinfo** コマンドの項を参照してください

冗長性状態と全体的な電源正常性

冗長性状態は全体的な電源正常性を決定する要因です。たとえば、電源冗長性ポリシーがグリッド冗長性に設定され、冗長性状態がシステムが稼動していることを示す場合、全体的な電源状態は通常 **OK** になります。ただし、グリッド冗長性がある状態で稼動するための条件を満たすことができない場合は、冗長性状態は **いいえ** になり、全体的な電源正常性は **重要** になります。これは、システムが設定されている冗長性ポリシーに従って稼働できないためです。

メモ: CMC では、冗長性ポリシーをグリッド冗長性に変更、またはグリッド冗長性から他の設定に変更するときに、これらの条件の事前チェックを行いません。そのため、冗長性ポリシーの設定が、即時に冗長性喪失または冗長性回復をもたらす可能性があります。

関連リンク

劣化または非冗長性ポリシーでの PSU 障害
冗長性ポリシーが劣化またはない状態の PSU の取り外し
新規サーバーの電源供給ポリシー
システムイベントログにおける電源装置および冗長性ポリシーの変更

劣化または非冗長性ポリシーでの PSU 障害

PSU 障害などの電力不足イベントが発生した場合、CMC はサーバーへの電力を削減します。サーバーへの電力を削減した後、CMC はシャーシの電力必要量を再計算します。引き続き電力要件が満たされない場合、CMC は優先順位の低いサーバーの電源をオフにします。
電力必要量が電力バジェット内にとどまると同時に、優先順位の高いサーバーへの電力供給が徐々に回復されていきます。冗長性ポリシーを設定するには、「電力バジェットと冗長性の設定」を参照してください。

冗長性ポリシーが劣化またはない状態の PSU の取り外し

CMC は、PSU または PSU AC ケーブルを取り外すと、電力の節約を開始する場合があります。CMC は、電力割り当てがシャーシ内の残りの PSU によってサポートされるまで、優先順位の低いサーバーへの電力を削減します。複数の PSU の取り外す場合、CMC は 2 番目の PSU が取り外された時に電力要件を再評価して、ファ

ームウェアの対応を見極めます。電力要件が引き続き満たされない場合は、CMC は優先順位の低いサーバーの電源を切る場合があります。

制限

- CMC は、優先順位の高いサーバーに電源投入するために優先順位の低いサーバーの電源を *自動的に* 切ることはありませんが、ユーザーが電源を切ることはできます。
- PSU 冗長性ポリシーの変更は、シャーシ内の PSU の数によって制限されます。PSU 冗長性設定は、「デフォルト冗長性設定」にリストされている 3 つの設定から、任意のものを選択できます。

新規サーバーの電源供給ポリシー

電源が投入された新しいサーバーに必要な電力がシャーシに供給される電力を超える場合、CMC が優先度の低いサーバーに対する電力を削減することがあります。これにより、新しいサーバーにより多くの電力を供給することができます。この状態は、以下の場合に生じます。

- 管理者が、サーバーに対するフル電力割り当てに必要な電力を下回る電力制限をシャーシに設定した。
- シャーシ内の全サーバーのワーストケース電力要件に対して使用可能な電力が不十分である。

優先度の低いサーバーに割り当てられた電力を低減させることによって十分な電力が解放されないと、新しいサーバーへの電源投入が行えない場合があります。

シャーシと新しいサーバーを含むすべてのサーバーをフル電力で稼動させるために必要な持続電力の最大量がワーストケース電力要件です。この電力量が利用可能な場合、ワーストケース電力要件より低い電力がサーバーに割り当てられることはなく、新しいサーバーへの電源投入も可能になります。

次の表は、前述したシナリオで新しいサーバーに電源が投入されたときに CMC が行う処置を説明しています。

表 36. サーバーへの電源投入試行時の CMC の対応

ワーストケース電力が使用可能	CMC の対応	サーバーへの電源投入
はい	節電は不要	許可
いいえ	節電を実施： • 新しいサーバーに必要な電力が使用可能 • 新しいサーバーに必要な電力が使用不可	許可 不許可

PSU に障害が発生すると、非重要な正常性状況が生じ、PSU 障害イベントが生成されます。PSU を取り外すと、PSU 取り外しイベントが生成されます。

どちらか一方のイベントによって冗長性が損失された場合は、電力割り当てに基づいて、*冗長性の喪失* イベントが生成されます。

その後の電力容量またはユーザーの電力容量がサーバーの割り当てよりも大きい場合、サーバーのパフォーマンスを劣化させる、またはワーストケースの場合には、サーバーの電源がオフになる可能性があります。これらの状態はどちらも優先順位の逆順に行われます。つまり、優先順位の低いサーバーから電源がオフになります。

次の表では、さまざまな PSU 冗長構成における PSU の電源切断または PSU の取り外しに対するファームウェアの対応を示します。

表 37. PSU 障害または取り外しによるシャーシへの影響

PSU 構成	動的 PSU 電源供給	ファームウェアの対応
グリッド冗長性	無効	CMC はユーザーにグリッド冗長性の喪失を警告します。
電源装置冗長性	無効	CMC はユーザーに電源装置冗長性の喪失を警告します。

PSU 構成	動的 PSU 電源供給	ファームウェアの対応
冗長性なし	無効	必要に応じて、優先順位の低いサーバーへの電力を低減します。
グリッド冗長性	有効	CMC はユーザーにグリッド冗長性の喪失を警告します。PSU 障害または取り外しによって失われた電力バジェットを補うため、スタンバイモードの PSU（存在する場合）の電源がオンになります。
電源装置冗長性	有効	CMC はユーザーに電源装置冗長性の喪失を警告します。PSU 障害または取り外しによって失われた電力バジェットを補うため、スタンバイモードの PSU（存在する場合）の電源がオンになります。
冗長性なし	有効	必要に応じて、優先順位の低いサーバーへの電力を低減します。

システムイベントログにおける電源装置および冗長性ポリシーの変更

電源装置状況および電源冗長性ポリシーの変更はイベントとして記録されます。システムイベントログ（SEL）にエントリを記録する電源装置関連のイベントは、電源装置の挿入と取り外し、電源装置入力ケーブルの挿入と取り外し、および電源装置の出力アサートとアサート停止です。

次の表には、電源装置の変更に関連する SEL エントリがリストされています。

表 38. 電源装置の変更に対する SEL イベント

電源装置イベント	システムイベントログ（SEL）エントリ
挿入	電源装置<*番号*> が存在します。
取り外し	電源装置 <*番号*> は存在しません。
グリッドまたは電源装置の冗長性喪失	電源装置の冗長性が失われました。
グリッドまたは電源装置の冗長性回復	電源装置は冗長です。
入力電力受電	電源装置 <*番号*> への入力電力が回復しました。
入力電力喪失	電源装置 <*番号*> への入力電力が失われました。
DC 出力生成	電源装置 <*番号*> は正常に動作しています。
DC 出力喪失	電源装置 <*番号*> が故障しました。
入力過電圧	電源装置 <*番号*> で過電圧障害が検知されました。
入力電圧不足	電源装置 <*番号*> で電圧不足障害が検知されました。
入力過電流	電源装置 <*番号*> で過電流障害が検知されました。
入力電流不足	電源装置 <*番号*> で電流不足障害が検知されました。
DC 出力電圧不足	電源装置 <*番号*> で出力電圧不足障害が検知されました。
DC 出力過電流	電源装置 <*番号*> で出力過電流障害が検知されました。
DC 出力電流不足	電源装置 <*番号*> で出力電流不足障害が検知されました。
通信障害	電源装置 <*番号*> と通信できません。
通信回復	電源装置 <*番号*> への通信が回復しました。
状態データの通信障害	電源装置 <*番号*> から状態情報を取得できません。
状態データの通信回復	電源装置 <番号> 状態情報が正しく取得されました。

過度の高 / 低温	電源装置 <*番号*> の温度が範囲外です。
ファンまたは通気エラー / 警告	電源装置 <*番号*> でファンの障害が検知されました。
ファン速度上書き	電源装置 <*番号*> でファンの障害が検知されました。
製造障害	電源装置 <*番号*> が故障しました。
マイクロプロセッサービジー	電源装置 <*番号*> が故障しました。
FRU エラー	電源装置 <*番号*> が故障しました。
非承認の 110V 動作の検出	電源装置の低入力電圧（110）がアサートされました。
110V 動作の確認	電源装置の低入力電圧（110）がアサート停止されました。

SEL にエントリを記録する電源冗長性状態の変更に関連するイベントは、**グリッド冗長性** 電源ポリシーまたは **電源装置冗長性** 電源ポリシーのいずれかに設定されたモジュラーエンクロージャにおける冗長性の喪失と回復です。次の表には、電源冗長性ポリシーの変更に関連する SEL エントリがリストされています。

表 39. 電源冗長性ポリシー変更に対する SEL イベント

電源ポリシーイベント	システムイベントログ（SEL）エントリ
冗長性喪失	冗長性喪失がアサートされました
冗長性回復	冗長性喪失がアサート停止されました

電力バジェットと冗長性の設定

電力バジェット、冗長性、および 6 台の電源装置ユニット（PSU）を使用するシャーシ全体（シャーシ、サーバー、I/O モジュール、iKVM、CMC、電源装置）の動的電力を設定できます。電源管理サービスは電力消費を最適化し、要件に基づいてさまざまなモジュールに電力を割り当て直します。

次を設定することができます。

- システム入力電力の上限
- 冗長性ポリシー
- 電源冗長性よりサーバーパフォーマンスを優先
- 電源装置の動的連動の有効化
- シャーシ電源ボタンの無効化
- 110 VAC 操作の許可
- 最大電力節減モード
- リモート電力ログ
- リモート電力ログの間隔
- サーバーベースの電源管理

関連リンク

節電と電力バジェット
最大節電モード
電源バジェットを維持するためのサーバー電力の低減
110V PSU AC 動作
電源冗長性よりサーバーパフォーマンスを優先する
リモートロギング
外部電源管理
CMC ウェブインタフェースを使用した電力バジェットと冗長性の設定

RACADM を使用した電力バジェットと冗長性の設定

節電と電力バジェット

CMC は、ユーザー設定の電力最大制限に到達すると、節電を実行します。電力に対する需要がユーザー設定のシステム入力電力上限を越えると、CMC は、優先順位の低いサーバー順にサーバーへの電力を削減します。これにより、優先順位の高いサーバーおよびシャーシ内のその他モジュールに電力を確保できます。

シャーシ内のすべて、または複数のスロットが同じ優先度レベルに設定されている場合、CMC はスロット番号の低い順にサーバーの電力を削減します。例えば、スロット 1 と 2 のサーバーの優先順位が同じである場合、スロット 1 のサーバーの電力が先に削減され、次にスロット 2 のサーバーの電力が削減されます。

メモ: シャーシ内の各サーバーに 1 から 9 の番号を割り当てることによって、それぞれの優先度レベルを割り当てることができます。すべてのサーバーのデフォルト優先度レベルは 1 です。番号が低くなるほど、優先度レベルは高くなります。

電力バジェットは、3 台の PSU セットのうち最も弱い PSU の最大値に制限されます。*システム入力電力上限*値を越える AC 電力バジェット値を設定しようとすると、CMC がエラーメッセージを表示します。電力バジェットは 16685 ワットに制限されます。

最大節電モード

CMC は、次の場合に最大節電モードを実行します。

- 最大節電モードが有効化されている。
- UPS デバイスにより発行された自動コマンドラインスクリプトが、最大節電モードを有効化する。

最大節電モードでは、すべてのサーバーが最低限の電力レベルで動作し始め、その後のサーバー電力割り当て要求はすべて拒否されます。このモードでは、電源投入されたサーバーのパフォーマンスが劣化する可能性があります。追加サーバーには、その優先順位にかかわらず、電源を投入することはできません。

最大節電モードがクリアされると、システムがフルパフォーマンス状態に戻ります。

電源バジェットを維持するためのサーバー電力の低減

システムの消費電力量をユーザー設定の*システム入力電力制限*の範囲内に保つためにさらに電力が必要な場合、CMC は優先順位の低いサーバーへの電力割り当てを削減します。たとえば、新しいサーバーの追加時における電力 297 の管理と監視のため、CMC は優先順位が低いサーバーへの電力を削減し、新しいサーバーに供給する電力を増量することがあります。優先順位の低いサーバーへの電力割り当てを削減した後も電力量が不十分である場合は、CMC は新しいサーバーへの電力投入に十分な電力が解放されるまで、サーバーの性能を低下させます。

CMC は次の 2 つの場合にサーバーの電力割り当てを削減します。

- 合計消費電力量が設定可能な*システム入力電力制限*を超える場合。
- 非冗長構成で電力障害が発生した場合。

110V PSU AC 動作

一部の PSU は 110V AC 入力での動作をサポートします。この入力は、分岐回路の許容制限を越える可能性があります。110V AC に接続された PSU がある場合、ユーザーは、このエンクロージャの通常動作用に CMC を設定する必要があります。設定が行われておらず、110V PSU が検出されると、その後のサーバー電力割り当て要求はすべて拒否されます。この場合、追加サーバーには、その優先順位にかかわらず、電源を投入することはできません。CMC は、ウェブインタフェースまたは RACADM を使用して 110 V PSU を使用するように設定することができます。

次の場合、電源装置エントリが SEL ログにログされます。

- 110V 電源装置が検出された、または取り外されたとき。
- 110V AC 入力動作が有効化または無効化されたとき。

シャーシが 110V モードで動作しており、ユーザーが 110V 動作をまだ有効化していな場合、全体的な電源正常性は少なくとも非重要状況になります。非重要状況時には、「警告」アイコンがウェブインタフェースのメインページに表示されます。

110V と 220V が混在した動作はサポートされません。両方の電圧が使用されていることを CMC が検出すると、一方の電圧が選択され、もう一方の電圧に接続されている電源装置の電源が切断されて、障害とマーク付けされます。

電源冗長性よりサーバーパフォーマンスを優先する

このオプションを有効化すると、電源冗長性の維持よりもサーバーパフォーマンスおよびサーバー起動が優先されます。無効化されると、システムはサーバーパフォーマンスよりも電源冗長性を優先します。無効化した時に、シャーシ内の 298 管理および監視電源装置が供給する電力が冗長性とフルパフォーマンスの両方に十分な電力を提供しない場合、冗長性を保つために一部のサーバーで次が行われない場合があります。

- フルパフォーマンスで稼働するために十分な電力の提供
- 電源投入

リモートロギング

電力消費のレポートを、リモートのシステムログサーバーに報告することができます。収集期間中のシャーシの電力消費の合計量、最大値、最小値、および平均値をログすることができます。この機能の有効化、および収集 / ログ間隔の設定に関する詳細については、「電源制御操作の実行」の項を参照してください。

外部電源管理

CMC 電源管理は、オプションで Power Measure, Mitigate, and Manage Console（PM3）によって制御されます。詳細については、『*PM3 ユーザーズガイド*』を参照してください。

外部電源管理を有効にすると、PM3 は次を管理します。

- 第 12 世代サーバーのサーバー電力
- 第 12 世代サーバーのサーバー優先順位
- システム入力電力容量
- 最大節電モード

CMC は次の維持または管理を継続します。

- 冗長性ポリシー
- リモート電力ログ
- 電源冗長性よりサーバーパフォーマンスを優先
- 電源装置の動的制御
- 第 11 世代以前のサーバーのサーバー電力

PM3 は次に、シャーシインフラストラクチャと前世代のブレードサーバーへの電力の割り当て後に使用できるバジェットから、第 12 世代ブレードサーバーの優先順位付けと電力を管理します。リモート電力ログは、外部電源管理には影響を受けません。

サーバーベースの電源管理モードが有効化された後、シャーシが PM3 管理用に準備されます。すべての第 12 世代サーバーの優先順位は 1（高）に設定されています。PM3 はサーバー電力および優先順位を直接管理し

ます。PM3 は互換性のあるサーバー電力割り当てを制御するので、CMC は最大節電モードを制御しなくなります。従って、この選択は無効化されます。

最大節電モードが有効化されると、CMC はシステム入力電力容量を、シャーシが対応できる最大量に設定します。CMC は電力の最大容量の超過を許容しませんが、PM3 は他の電力容量制限のすべてに対応します。

電力の PM3 管理が無効化されると、CMC は外部管理が有効になる前のサーバー優先度設定に戻ります。

メモ: PM3 管理が無効化されても、CMC は最大シャーシ電力の以前の設定には戻りません。設定値を手動で回復するには、以前の設定の **CMC ログ** を参照してください。

CMC ウェブインタフェースを使用した電力バジェットと冗長性の設定

メモ: 電力管理処置を行うには、**シャーシ設定システム管理者** 特権が必要です。

ウェブインタフェースを使用して電力バジェットを設定するには、次の手順を実行します。

1. システムツリーで **シャーシ概要** に移動し、**電力 → 設定** とクリックします。
   バジェット / 冗長性設定 ページが表示されます。
2. 必要に応じて、次から任意のプロパティ、またはすべてのプロパティを選択します。各フィールドについての情報は、『*CMC オンラインヘルプ*』を参照してください。
   - サーバーベースの電源管理の有効化
   - システム入力電力の上限
   - 冗長性ポリシー
   - 電源の冗長性を超えたサーバーパフォーマンス
   - 電源装置の動的制御を有効にする
   - シャーシ電源ボタンの無効化
   - 110 VAC 操作の許可
   - 最大電力節減モード
   - リモート電力ログを有効にする
   - リモート電力ログの間隔
3. **適用** をクリックして変更を保存します。

RACADM を使用した電力バジェットと冗長性の設定

メモ: 電力管理処置を行うには、**シャーシ設定システム管理者** 特権が必要です。

冗長性を有効にして冗長性ポリシーを設定するには、次の手順を実行します。

1. シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインします。
2. 必要に応じてプロパティを設定します。
   - 冗長性ポリシーを選択するには、次を入力します。
     ```
     racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy <value>
     ```
     ここで <*値*> は 0（冗長性なし）、1（グリッド冗長性）、2（電源装置冗長性）です。デフォルトは 0 です。

     例えば、次のコマンドは冗長性ポリシーを 1 に設定します。
     ```
     racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy 1
     ```
   - 電力バジェット値を設定するには、次を入力します。
     ```
     racadm config -g cfgChassisPower -o cfgChassisPowerCap <value>
     ```
     ここで、<*値*> は 2715～16685 の範囲の数値で、電力の上限値をワット数で表します。デフォルトは 16685 です。

例えば、次のコマンドは最大電力バジェットを 5400 ワットに設定します。

```
racadm config -g cfgChassisPower -o cfgChassisPowerCap 5400
```

– PSU の動的電源供給を有効または無効にするには、次を入力します。

```
racadm config -g cfgChassisPower -o
cfgChassisDynamicPSUEngagementEnable <value>
```

ここで <*値*> は 0（無効）、1（有効）です。デフォルトは 0 です。

例えば、次のコマンドは動的 PSU 電源供給を無効化します。

```
racadm config -g cfgChassisPower -o
cfgChassisDynamicPSUEngagementEnable 0
```

– 最大節電モードを有効にするには、次を入力します。

```
racadm config -g cfgChassisPower -o cfgChassisMaxPowerConservationMode
1
```

– 通常の動作を復元するには、次を入力します。

```
racadm config -g cfgChassisPower -o cfgChassisMaxPowerConservationMode
0
```

– 110 VAC PSU を有効にするには、次を入力します。

```
racadm config -g cfgChassisPower -o cfgChassisAllow110VACOperation 1
```

– 電源冗長性よりサーバーパフォーマンスを優先するオプションを有効化するには、次を入力します。

```
racadm config -g cfgChassisPower -o
cfgChassisPerformanceOverRedundancy 1
```

– 電源冗長性よりサーバーパフォーマンスを優先するオプションを無効化するには、次を入力します。

```
racadm config -g cfgChassisPower -o
cfgChassisPerformanceOverRedundancy 0
```

– 電力リモートログ機能を有効にするには、次のコマンドを入力します。

```
racadm config -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingEnabled 1
```

– 電力リモートログの間隔を指定するには、次のコマンドを入力します。

```
racadm config -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingInterval
n
```

ここで n は 1～1440 分になります。

– 電力リモートログ機能が有効かどうかを判定するには、次のコマンドを入力します。

```
racadm getconfig -g cfgRemoteHosts -o
cfgRhostsSyslogPowerLoggingEnabled
```

– 電力リモートログ機能を有効にするには、次のコマンドを入力します。

```
racadm getconfig -g cfgRemoteHosts -o
cfgRhostsSyslogPowerLoggingInterval
```

電力リモートログ機能は、事前に設定されたリモート Syslog ホストに依存します。1 つ、または複数のリモート Syslog ホストへのログを有効化する必要があり、しなかった場合は電力消費がログされます。これは、ウェブ GUI または RACADM CLI のいずれかを使用して実行できます。詳細は、**dell.com/support/manuals** で、『iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド』の **リモート syslog 設定** の説明を参照してください。

– 電力測定、緩和、制御コンソール（PM3）を使用してリモート電力管理を有効にするには、以下を入力します。

```
racadm config -g cfgChassisPower -o cfgChassisServerBasedPowerMgmtMode
1
```

– CMC 電力管理を復元するには、次入力します。

```
racadm config -g cfgChassisPower -o cfgChassisServerBasedPowerMgmtMode
0
```

シャーシ電力の RACADM コマンドの詳細については、『*iDRAC7 および CMC 向け RACADM コマンドライン リファレンスガイド*』の **config**、**getconfig**、**getpbinfo**、および **cfgChassisPower** の項を参照してください。

電源制御操作の実行

シャーシ、サーバー、および IOM のために次の電源制御操作を実行できます。

メモ: 電源制御操作はシャーシ全体に影響します。

関連リンク

シャーシに対する電源制御操作の実行
サーバーに対する電源制御操作の実行
IOM での電源制御操作の実行

シャーシに対する電源制御操作の実行

CMC は、手順に従ったシャットダウンなど、ユーザーがシャーシ全体（シャーシ、サーバー、IOM、iKVM、PSU）におけるいくつかの電源管理操作をリモートで実行することを可能にします。

メモ: 電源管理処置を行うには、**シャーシ設定システム管理者** 特権が必要です。

ウェブインタフェースを使用したシャーシでの電源制御操作の実行

CMC ウェブインタフェースを使用してシャーシの電源制御操作を行うには、次の手順を実行します。

1. システムツリーで **シャーシ概要** に移動し、**電力 → 制御** とクリックします。
   シャーシーの電源制御 ページが表示されます。
2. 次の電源制御操作のいずれかを選択します。
   - システムの電源を入れる
   - システムの電源を切る
   - システムのパワーサイクル（コールドブート）
   - CMC のリセット（ウォームブート）
   - 非正常なシャットダウン

   各オプションの詳細については、『*CMC オンラインヘルプ*』を参照してください。
3. **適用** をクリックします。
   確認を求めるダイアログボックスが表示されます。
4. **OK** をクリックして、電源管理処置（例えば、システムをリセットするなど）を行います。

RACADM を使用したシャーシでの電源制御操作の実行

シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインした後、次を入力します。

```
racadm chassisaction -m chassis <action>
```

ここでの <*action*> は、`powerup`、`powerdown`、`powercycle`、`nongraceshutdown`、または `reset` になります。

サーバーに対する電源制御操作の実行

複数のサーバーに対して一度に、またはシャーシ内の個々のサーバーに対して電源管理処置をリモートで行うことができます。

メモ: 電源管理処置を行うには、**シャーシ設定システム管理者** 特権が必要です。

CMC ウェブインタフェースを使用した複数サーバーの電源制御操作

CMC ウェブインタフェースを使用して複数サーバーの電源制御操作を行うには、次の手順を実行します。

1. システムツリーで **サーバー概要** に移動し、**電力 → 制御** とクリックします。
   電源制御 ページが表示されます。
2. **操作** 列のドロップダウンメニューから、必要サーバーのために次の電源制御操作の 1 つを選択します。
   - 操作なし
   - サーバーの電源を入れる
   - サーバーの電源を切る
   - 正常なシャットダウン
   - サーバーのリセット（ウォームブート）
   - サーバーの電源を入れなおす（コールドブート）

   オプションの詳細については、『*CMC オンラインヘルプ*』を参照してください。
3. **適用** をクリックします。
   確認を求めるダイアログボックスが表示されます。
4. **OK** をクリックして、電源管理処置（例えば、サーバーリセットの実行など）を行います。

CMC ウェブインタフェースを使用したサーバーでの電源制御操作の実行

CMC ウェブインタフェースを使用して個々のサーバーの電源制御操作を行うには、次の手順を実行します。

1. システムツリーで **シャーシ概要** に移動し、**サーバー概要** をクリックします。
2. 電源制御操作を行うサーバーをクリックし、**電源** タブをクリックします。
   サーバーの電源管理 ページが表示されます。
3. 次の電源制御操作のいずれかを選択します。
   - サーバーの電源を入れる
   - サーバーの電源を切る
   - サーバーをリセットする（ウォームブート）
   - サーバーの電源を入れなおす（コールドブート）

   オプションの詳細については、『*CMC オンラインヘルプ*』を参照してください。
4. **適用** をクリックします。
   確認を求めるダイアログボックスが表示されます。
5. **OK** をクリックして、電源管理処置（例えば、サーバーをリセットするなど）を行います。

RACADM を使用したサーバーでの電源制御操作の実行

サーバーで、RACADM を使用した電源制御操作を実行するには、シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインして次を入力します。

```
racadm serveraction -m <module> <action>
```

ここで、<*モジュール*> はシャーシ内のスロット番号（サーバー 1～16）でサーバーを指定し、<*処置*> は実行する操作（powerup、powerdown、powercycle、graceshutdown、hardreset）です。

IOM での電源制御操作の実行

個々の IOM におけるリセットまたはパワーサイクルをリモートで実行することができます。

メモ: 電源管理処置を行うには、**シャーシ設定システム管理者** 特権が必要です。

CMC ウェブインタフェースを使用した IOM での電源制御操作の実行

CMC ウェブインタフェースを使用して IOM の電源制御操作を行うには、次の手順を実行します。

1. システムツリーで **シャーシ概要** → **I/O モジュール概要** と進み、**電源** をクリックします。
   電源制御 ページが表示されます。
2. リスト内の IOM のために、ドロップダウンメニューから実行する操作を選択します（リセットまたはパワーサイクル）。
3. **適用** をクリックします。
   確認を求めるダイアログボックスが表示されます。
4. **OK** をクリックして、電源管理処置（例えば、IOM のパワーサイクルを行うなど）を行います。

RACADM を使用した IOM での電源制御操作の実行

IOM で、RACADM を使用した電源制御操作を実行するには、シリアル /Telnet/SSH テキストコンソールを開いて CMC に進み、ログインして次を入力します。

```
racadm chassisaction -m switch-<n> <処置>
```

ここで <*n*> は、1～6 の番号で IOM（A1、A2、B1、B2、C1、C2）を指定し、<処置> は、実行する操作（powercycle または reset）を示します。

16

トラブルシューティングとリカバリ

本項では、CMC ウェブインタフェースを使用したリカバリおよびリモートシステム上の問題のトラブルシューティングに関連したタスクの実行方法について説明します。

- シャーシ情報の表示。
- イベントログの表示。
- 設定情報、エラーステータス、エラーログの収集。
- 診断コンソールの使用。
- リモートシステムの電源管理。
- リモートシステムの Lifecycle Controller ジョブの管理。
- コンポーネントのリセット。
- ネットワークタイムプロトコル（NTP）問題に関するトラブルシューティング。
- ネットワーク問題に関するトラブルシューティング。
- アラート問題に関するトラブルシューティング。
- システム管理者パスワードを忘れた場合のリセット。
- シャーシ構成設定および証明書の保存と復元。
- エラーコードおよびログの表示。

RACDUMP を使用した設定情報、シャーシ状態、およびログの収集

racdump サブコマンドは、包括的なシャーシ状態、設定状況情報、イベントログの履歴を収集するための単一のコマンドを提供します。

racdump サブコマンドは、次の情報を表示します。

- 一般的なシステム /RAC 情報
- CMC 情報
- シャーシ情報
- セッション情報
- センサー情報
- ファームウェアビルド情報

対応インタフェース

- CLI RACADM
- リモート RACADM
- Telnet RACADM

Racdump には次のサブシステムが含まれており、次の RACADM コマンドを集約します。racdump の詳細については、『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

サブシステム	RACADM コマンド
システム / RAC の一般情報	getsysinfo
セッション情報	getssinfo
センサー情報	getsensorinfo
スイッチ情報（IO モジュール）	getioinfo
メザニンカード情報（ドーターカード）	getdcinfo
全モジュールの情報	getmodinfo
電力バジェット情報	getpbinfo
KVM 情報	getkvminfo
NIC 情報（CMC モジュール）	getniccfg
冗長性情報	getredundancymode
トレースログ情報	gettracelog
RAC イベントログ	gettraclog
システムイベントログ	getsel

SNMP Management Information Base（MIB）ファイルのダウンロード

CMC SNMP MIB ファイルは、シャーシタイプ、イベント、およびインジケータを定義します。CMC は、ウェブインタフェースを使用した MIB ファイルのダウンロードを可能にします。

CMC ウェブインタフェースを使用して CMC の SNMP Management Information Base（MIB）ファイルをダウンロードするには、次の手順を実行します。

1. システムツリーで **シャーシ概要** に進み、**ネットワーク → サービス → SNMP** とクリックします。
   SNMP 設定 セクションが表示されます。
2. **保存** をクリックして CMC **MIB** ファイルをローカルシステムにダウンロードします。
   SNMP **MIB** ファイルの詳細については、**dell.com/support/manuals** にある『*Dell OpenManage Server Administrator SNMP リファレンスガイド*』を参照してください。

リモートシステムをトラブルシューティングするための最初の手順

次の質問は、管理下システムで発生する複雑な問題をトラブルシューティングするためによく使用されるものです。

- システムの電源はオンになっていますか、オフになっていますか?
- 電源がオンの場合は、オペレーティングシステムが正しく機能していますか、それともクラッシュまたはフリーズしていますか?
- 電源がオフの場合は、電源は突然切れましたか?

電源のトラブルシューティング

次の情報は、電源装置および電源関連問題のトラブルシューティングに役立ちます。

- **問題：電源の冗長性ポリシー** を **AC 冗長性** に設定すると、電源装置の冗長性喪失イベントが生じた。

- **解決策 A**： この設定には、モジュラーエンクロージャのサイド 1（左側 3 つのスロット）に少なくとも 1 台の電源装置、およびサイド 2（右側 3 つのスロット）に 1 台の電源装置が存在し、動作可能であることが必要です。さらに、各サイドの容量は、シャーシが **AC 冗長性** を維持するための総電力割り当てをサポートするために十分である必要があります。（完全な AC 冗長性動作のため、6 台の電源装置が装備された完全な PSU 構成が利用可能であるようにしてください。）
- **解決策 B**：すべての電源装置が 2 つの AC グリッドに正しく接続されていることを確認します。サイド 1 の電源装置は一方の AC グリッドに、サイド 2 の電源装置は他方の AC グリッドに接続され、両方の AC グリッドが機能していることが必要です。このうちひとつの AC グリッドが機能していないと、**AC 冗長性** は失われます。

- **問題：** AC ケーブルが接続されていて、電力配分装置も良好な AC 出力を行っているにも関わらず、PSU に **障害（AC なし）** と表示されます。
  - **解決策 A：** AC ケーブルをチェックして交換します。電源装置に電力を供給している電力配分装置が期待通りに動作していることをチェックして確かめます。引き続き問題が解決しない場合は、電源装置の交換のため、Dell カスタマーサービスにお電話ください。
  - **解決策 B：** その PSU が他の PSU と同じ電圧に接続されていることをチェックします。ひとつの PSU が異なる電圧で動作していることを CMC が検知した場合、その PSU の電源が切られ、障害とマーク付けされます。
- **問題：** 動的電源供給が有効化されているのに、どの電源装置も **スタンドバイ** 状況として表示されない。
  - **解決策 A：** 余剰電力が十分ではありません。1 つまたは複数の電源装置がスタンバイ状況に移行するのは、エンクロージャで利用できる余剰電力が、少なくとも 1 つの電源装置の容量を超えた場合に限られます。
  - **解決策 B：** 動的電源供給が、エンクロージャ内に存在する電源装置ユニットで完全にサポートできません。これが原因であるかをチェックするには、ウェブインタフェースを使用して **動的電源供給** をオフにしてから、再度オンにします。動的電源供給を完全にサポートできない場合は、メッセージが表示されます。
- **問題**：新しいサーバーを十分な電源装置があるエンクロージャに取り付けましたが、サーバーの電源がオンになりません。
  - **解決策 A:** システム入力電力上限設定が追加サーバーに電源を供給するには低すぎる設定になっていないことを確認します。
  - **解決策 B：** 110V の動作をチェックします。電源装置のいずれかが 110V の分岐回路に接続されている場合、サーバーの電源をオンにする前に、その構成が有効であることを確認する必要があります。詳細については、電源設定を参照してください。
  - **解決策 C：** 最大節電設定をチェックしてください。これが設定されていると、サーバーへの電源投入が可能です。詳細については、電源設定を参照してください。
  - **解決策 D:** 新しく取り付けたサーバーに関連付けられているスロットのサーバースロット電力優先順位が他のサーバースロットの電力優先順位より低く設定されていないことを確認してください。
- **問題：** モジュラーエンクロージャ構成を変更していないのに、利用可能な電力の表示が頻繁に変わる。
  - **解決策：** CMC 1.2 以降のバージョンには、エンクロージャがユーザー設定の電力上限のピーク近くで動作している場合にサーバーへの電力割り当てを一時的に減少させる動的ファン電源管理機能が搭載されています。これによって、電力利用が **システム入力電力上限** を超えないようにするため、サーバーのパフォーマンスを低減することによってファンに電力が割り当てられます。これは通常の動作です。

- **問題：** **ピークパフォーマンス時の余剰電力** が 2000 W と報告される。
  - **解決策：** 現行の構成では、エンクロージャに 2000 W の使用可能な余剰電力があり、**システム入力電力上限** は、サーバーのパフォーマンスに影響を与えることなく、この報告された量まで安全に引き下げることができます。

- **不具合**：シャーシが 6 台の電源装置での **AC 冗長性**構成で稼働していたにも関わらず、AC グリッドに障害が発生した後、サーバーのサブセットが電力を失った。

  - **解決策：** この問題は、AC グリッド障害が発生した時に、電源装置が冗長 AC グリッドに正しく接続されていなかった場合に発生します。**AC 冗長性** ポリシーでは、左側 3 台の電源装置がひとつの AC グリッドに接続され、右側 3 台の電源装置がもう一方の AC グリッドに接続されている必要があります。2 台の PSU が正しく接続されていない場合（例えば、PSU3 と PSU4 が誤った AC グリッドに接続されているなど）、AC グリッド障害は優先順位の最も低いサーバーの電力喪失の原因になります。

- **問題：** PSU に障害が発生した後、優先順位の最も低いサーバーが電力を失った。

  - **解決策：** これは、エンクロージャの電源ポリシーが **冗長性なし** に設定されている場合に予期される動作です。サーバーの電源が切れる原因となる今後の電源装置障害を避けるため、シャーシには少なくとも 4 台の電源装置が装備され、PUS 障害によるサーバー動作への影響を避けるため、サーバーに **電源装置冗長性** ポリシーが設定されているようにしてください。

- **問題：** データセンターの周囲温度が上がるとサーバー全体のパフォーマンスが低下する。

  - **解決策：** この問題は、ファンの電力需要の増加がサーバーへの電力割り当てを削減することによって埋め合わされる結果となる値に **システム入力電力上限** が設定されている場合に発生します。サーバーパフォーマンスに影響することなくファンに追加電力を割り当てる事を可能にするため、ユーザーは **システム入力電力上限** をより大きい値に増やすことができます。

アラートのトラブルシューティング

CMC アラートのトラブルシューティングには、CMC ログとトレースログを使用します。各 E-メール、および / または SNMP トラップの送信試行の成功と失敗は CMC ログに、特定のエラーを説明する追加情報はトレースログにログされます。ただし、SNMP はトラップの送信を確認しないので、ネットワークアナライザ、または Microsoft の snmputil などのツールを使用して、管理下システムのパケットをトレースしてください。

関連リンク

アラートを送信するための CMC の設定

イベントログの表示

管理下システムで発生したシステムにとって重要なイベントについての情報のため、ハードウェアおよび CMC ログを表示することができます。

関連リンク

ハードウェアログの表示
CMC ログの表示

ハードウェアログの表示

CMC はシャーシで発生したイベントのハードウェアログを生成します。ハードウェアログは、ウェブインタフェースおよびリモート RACADM を使用して表示できます。

メモ: ハードウェアログをクリアするには、**ログのクリアシステム管理者** 特権が必要です。

メモ: 特定のイベント発生時に E-メールまたは SNMP トラップを送信するように CMC を設定することができます。アラートを送信するための CMC の設定についての情報は、「アラートを送信するための CMC の設定」を参照してください。

ハードウェアログエントリの例

```
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
```

関連リンク

イベントログの表示

CMC ウェブインタフェースを使用したハードウェアログの表示

ハードウェアログは表示、保存、およびクリアすることが可能です。ログは、列の見出しをクリックすることにより、重大度、日付 / 時刻、または説明を基準に並べ替えすることができます。列の見出しを再度クリックして、並び順を逆にします。

CMC ウェブインタフェースを使用してハードウェアログを表示するには、システムツリーで **シャーシ概要** に進み、**ログ → ハードウェアログ** とクリックします。**ハードウェアログ** ページが表示されます。管理下ステーションまたはネットワークにハードウェアログのコピーを保存するには、**ログの保存** をクリックしてから、ログのテキストファイルの場所を指定します。

メモ: ログはテキストファイルとして保存されるため、ユーザーインタフェースで重大度を示すために使用されるグラフィックイメージは表示されません。テキストファイルでは、重大度は OK、情報、不明、警告、重大という言葉で示されます。日付 / 時刻のエントリは昇順で表示されます。<システム起動> が **日付 / 時刻** 列に表示される場合は、日時を記録できないモジュールのシャットダウンまたはスタートアップ中にイベントが発生したことを意味します。

ハードウェアログをクリアするには、**ログのクリア** をクリックします。

メモ: CMC はログがクリアされたことを示す新しいログエントリを作成します。

RACADM を使用したハードウェアログの表示

RACADM を使用してハードウェアログを表示にするには、CMC へのシリアル /Telnet/SSH テキスト コンソールを開いて CMC へ進み、ログイン後、次を入力します。

```
racadm getsel
```

ハードウェアログをクリアするには、次を入力します。

```
racadm clrsel
```

CMC ログの表示

CMC は、シャーシ関連のイベントのログを生成します。

メモ: CMC ログをクリアするには、**ログのクリアシステム管理者** 特権が必要です。

関連リンク

イベントログの表示

ウェブインタフェースを使用した CMC ログの表示

CMC ログは表示、保存、およびクリアすることが可能です。ログは、列の見出しをクリックすることにより、ソース、日付 / 時刻、または説明を基準に並べ替えすることができます。列の見出しを再度クリックして、並び順を逆にします。

CMC ウェブインタフェースを使用して CMC ログを表示するには、システムツリーで **シャーシ概要** に移動し、**ログ → CMC ログ** とクリックします。**CMC ログ** ページが表示されます。

お使いの管理下ステーションまたはネットワークに CMC ログのコピーを保存するには、**ログの保存** をクリックして、ログファイルを保存する場所を指定します。

RACADM を使用した CMC ログの表示

RACADM を使用して CMC ログ情報を表示するには、CMC へのシリアル /Telnet/SSH テキストコンソールを開いてログインし、次を入力します。

```
racadm getraclog
```

ハードウェアログをクリアするには、次を入力します。

```
racadm clrraclog
```

診断コンソールの使用

高度な技術を持つ CMC ユーザーである、またはテクニカルサポートの指示に従っている場合、CLI コマンドを使用してシャーシハードウェア関連の問題を診断することができます。

メモ: これらの設定を変更するには、**デバッグコマンドシステム管理者** 特権が必要です。

CMC ウェブインタフェースを使用して診断コンソールにアクセスするには、次の手順を実行します。

1. システムツリーで **シャーシ概要** に進み、**トラブルシューティング → 診断** とクリックします。
   診断コンソール ページが表示されます。
2. **コマンド** テキストボックスにコマンドを入力し、**送信** をクリックします。
   コマンドの詳細については、『*CMC オンラインヘルプ*』を参照してください。
   診断結果ページが表示されます。

コンポーネントのリセット

アクティブな CMC のリセット、オペレーティングシステムの再起動なしでの iDRAC のリセット、または取り外されて再挿入されたかのようにサーバーを動作させるためのサーバーの仮想的な再装着を行うことができます。シャーシにスタンバイ CMC がある場合は、アクティブな CMC のリセットはフェイルオーバーを生じ、スタンバイ CMC がアクティブになります。

メモ: コンポーネントをリセットするには、**デバッグ コマンド管理者** 特権が必要です。

CMC ウェブインタフェースを使用してコンポーネントをリセットするには、次の手順を実行します。

1. システムツリーで **シャーシ概要** に進み、**トラブルシューティング → コンポーネントのリセット** とクリックします。
   コンポーネントのリセット ページが表示されます。
2. アクティブな CMC をリセットするには、**CMC 状態** セクションで **CMC のリセット / フェイルオーバー** をクリックします。スタンバイ CMC が存在し、シャーシに完全な冗長性がある場合は、フェイルオーバーが生じ、スタンバイ CMC がアクティブになります。
3. オペレーティングシステムを再起動せずに iDRAC のみをリセットするには、**サーバーのリセット** セクションで、iDRAC をリセットするサーバーの **リセット** ドロップダウンメニューから **iDRAC リセット** をクリックして、**選択の適用** をクリックします。これで、オペレーティングシステムを再起動せずにサーバーの iDRAC がリセットされます。
   詳細については、『*CMC オンラインヘルプ*』を参照してください。
   RACADM を使用して、オペレーティングシステムを再起動せずに iDRAC のみをリセットするには、『*iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド*』を参照してください。

   メモ: iDRAC がリセットされると、サーバーのファンが 100% に設定されます。

   メモ: サーバーの仮想的な再装着を試行する前に、iDRAC のリセットを試行することが推奨されます。
4. サーバーを仮想的に再装着するには、**サーバーのリセット** セクションで、再装着するサーバーの **リセット** ドロップダウンボックスの **仮想的再装着** をクリックし、**選択の適用** をクリックします。
   詳細については、『*CMC オンラインヘルプ*』を参照してください。
   この操作を行うと、サーバーを取り外されて再挿入されたかのように動作させることができます。

シャーシ設定の保存と復元

システムツリーの CMC ウェブインタフェースを使用してシャーシ設定のバックアップの保存または復元を行うには、**シャーシ概要** へ移動し、**セットアップ → シャーシバックアップ** をクリックします。

シャーシバックアップ ページが表示されます。

シャーシ設定を保存するには、**保存** をクリックします。デフォルトのファイルパスを上書きし（オプション）、**OK** をクリックしてファイルを保存します。

メモ: デフォルトのバックアップファイル名にはシャーシのサービスタグが含まれています。このバックアップファイルは、このシャーシの設定と証明書を復元するために限り、後から使用することができます。

シャーシ設定を復元するには、**ファイルの選択** をクリックし、バックアップファイルを指定して **復元** をクリックします。

メモ: CMC 自体は設定の復元時にリセットされることはありませんが、CMC サービスに新しい、または変更された設定内容が事実上反映されるまで、しばらく時間がかかる場合があります。反映が正常に完了した後、現行のセッションがすべて閉じられます。

ネットワークタイムプロトコル（NTP）エラーのトラブルシューティング

ネットワーク上のリモートタイムサーバーの時刻と同期化するように CMC のクロックを設定した後は、日付と時刻が変更されるまで数分かかる場合があります。数分後も変更されない場合は、問題をトラブルシュートする必要がある場合があります。CMC は、次の理由でクロックを同期化できない可能性があります。

- NTP サーバー 1、NTP サーバー 2、および NTP サーバー 3 設定の問題。
- 無効なホスト名または IP アドレスが誤って入力された可能性がある。
- CMC と設定済みの NTP サーバーとの通信を妨げるネットワーク接続問題がある。
- NTP サーバーホスト名が解決されるのを妨げる DNS 問題がある。

これらの NTP 関連問題のトラブルシューティングを行うには、CMC トレースログをチェックしてください。このログには NTP 関連障害のエラーメッセージが含まれています。CMC がどの設定済みリモート NTP サーバーとも同期化できない場合は、CMC 時刻はローカルシステムのクロックと同期化され、トレースログには次のメッセージに似たエントリが記録されます。

```
Jan 8 20:02:40 cmc ntpd[1423]: synchronized to LOCAL(0), stratum 10
```

次の racadm コマンドを入力することで、ntpd 状態を確認することもできます。

```
racadm getractime -n
```

「*」が設定済みサーバーのいずれかに表示されない場合、設定が正しく行われていない可能性があります。このコマンドの出力には、問題のデバッグに役立つ可能性のある詳しい NTP 統計が含まれています。

Windows ベースの NTP サーバーの設定を試行する場合、ntpd の MaxDist パラメータの増加が役立つ場合があります。デフォルト設定は大部分の NTP サーバーと連動するために十分な大きさが必要であることから、このパラメータを変更する前に、変更による影響すべてについて理解しておいてください。

パラメータを変更するには、次のコマンドを入力します。

```
racadm config -g cfgRemoteHosts -o cfgRhostsNtpMaxDist 32
```

変更後 NTP を無効化し、5〜10 秒間待ってから再度 NTP を有効化します。

メモ: NTP は、再同期化のためにさらに 3 分時間を費やす場合があります。

NTP を無効化するには、次を入力します。

```
racadm config -g cfgRemoteHosts -o cfgRhostsNtpEnable 0
```

NTP を有効化するには、次を入力します。

```
racadm config -g cfgRemoteHosts -o cfgRhostsNtpEnable 1
```

NTP サーバーが正しく設定されているにもかかわらず、このエントリがトレースログに存在する場合は、CMC が設定された NTP サーバーのいずれとも同期できないことが確実になります。

NTP サーバーの IP アドレスが設定されていない場合、次に似たトレースログエントリが記録される場合があります。

```
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
```

NTP サーバーが無効なホスト名で設定されていると、次のようなトレースログエントリが記録される場合があります。

```
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
```

CMC ウェブインタフェースを使用してトレースログを確認するための gettracelog コマンドを入力する方法についての情報は、「診断コンソールの使用」を参照してください。

LED の色と点滅パターンの解釈

シャーシ上の LED は、以下のコンポーネント状態を示します。

- 緑色 LED の点灯は、コンポーネントに電力投入されていることを示します。緑色 LED の点滅は、ファームウェアアップロードなど、重要ではあっても慣例的なイベントを示します。 この間、ユニットは操作できなくなりますが、障害を示すものではありません。
- モジュール上の橙色 LED の点滅は、モジュール上の不具合を示します。
- 青色 LED の点滅は、ユーザー設定が可能で、識別に使用されます（「SNMP Management Information Base（MIB）ファイルのダウンロード」を参照してください）。

表 40. LED の色と点滅パターン

コンポーネント	LED の色、点滅パターン	状態
CMC	緑色、点灯	電源オン
	緑色、点滅	ファームウェアのアップロード中
	緑色、消灯	電源オフ
	青色、点灯	アクティブ
	青色、点滅	ユーザーによって有効化されたモジュール識別
	橙色、点灯	不使用
	橙色、点滅	障害
	青色、消灯	スタンバイ
iKVM	緑色、点灯	電源オン
	緑色、点滅	ファームウェアのアップロード中
	緑色、消灯	電源オフ
	橙色、点灯	不使用

コンポーネント	LED の色、点滅パターン	状態
	橙色、点滅	障害
	橙色、消灯	障害なし
サーバー	緑色、点灯	電源オン
	緑色、点滅	ファームウェアのアップロード中
	緑色、消灯	電源オフ
	青色、点灯	正常
	青色、点滅	ユーザーによって有効化されたモジュール識別
	橙色、点灯	不使用
	橙色、点滅	障害
	青色、消灯	障害なし
IOM（共通）	緑色、点灯	電源オン
	緑色、点滅	ファームウェアのアップロード中
	緑色、消灯	電源オフ
	青色、点灯	正常 / スタックマスター
	青色、点滅	ユーザーによって有効化されたモジュール識別
	橙色、点灯	不使用
	橙色、点滅	障害
	青色、消灯	障害なし / スタックスレーブ
IOM（パススルー）	緑色、点灯	電源オン
	緑色、点滅	不使用
	緑色、消灯	電源オフ
	青色、点灯	正常
	青色、点滅	ユーザーによって有効化されたモジュール識別
	橙色、点灯	不使用
	橙色、点滅	障害
	青色、消灯	障害なし
ファン	緑色、点灯	ファン作動中
	緑色、点滅	不使用
	緑色、消灯	電源オフ
	橙色、点灯	ファンタイプを認識できない、CMC ファームウェアのアップデート
	橙色、点滅	ファン障害。タコメーターが範囲外
	橙色、消灯	不使用

コンポーネント	LED の色、点滅パターン	状態
PSU	（楕円）緑色、点灯	AC OK
	（楕円）緑色、点滅	不使用
	（楕円）緑色、消灯	AC OK 外
	橙色、点灯	不使用
	橙色、点滅	障害
	橙色、消灯	障害なし
	（円）緑色、点灯	DC OK
	（円）緑色、無灯	DC OK 外

無応答 CMC のトラブルシューティング

いずれのインタフェース（ウェブインタフェース、Telnet、SSH、リモート RACADM、シリアルなど）を使用しても CMC にログインできない場合は、CMC 上の LED の観察、DB-9 シリアルポートを使用したリカバリ情報の取得、または CMC ファームウェアイメージのリカバリなどを行うことにより、CMC が機能しているかどうかを確認できます。

メモ: シリアルコンソールを使ってスタンバイ CMC にログインすることはできません。

問題特定のための LED の観察

シャーシに取り付けられている CMC の前面を見ると、カードの左側に LED が 2 つあります。

- 上部 LED — 上部の緑色の LED は電力を示します。これが点灯していない場合は、次を確認してください。
  - 少なくとも 1 台の電源装置に AC 電源がある。
  - CMC カードが正しく装着されている。取り出しハンドルを解放、または引いて CMC を取り外し、基板が完全に挿入され、ラッチが正しく閉じることを確認しながら CMC を再度挿入します。
- 下部 LED — 下部 LED には複数の色があります。CMC がアクティブかつ実行中で、問題がない場合は下部 LED が青色になります。橙色になっている場合は、障害が検出されています。障害は次の 3 つのイベントのいずれかによって発生する可能性があります。
  - コアの障害。この場合、CMC 基板を交換する必要があります。
  - セルフテストの失敗。この場合、CMC 基板を交換する必要があります。
  - イメージの破損。この場合、CMC ファームウェアイメージをアップロードして、CMC を回復します。

  メモ: 通常の CMC 起動またはリセットは、そのオペレーティングシステムを完全に起動し、ログインできるようになるまでに 1 分以上かかります。青色の LED がアクティブ CMC で点灯します。冗長の 2 つの CMC 構成の場合は、スタンバイ CMC で緑色の上部 LED だけが点灯されます。

DB-9 シリアルポートからのリカバリ情報の入手

下部の LED が橙色の場合、CMC の前面にある DB-9 シリアル ポートからリカバリ情報を取得できます。

リカバリ情報を取得するには、次の手順を実行します。

1. CMC とクライアントコンピュータの間に NULL モデムケーブルを取り付けます。
2. 任意のターミナルエミュレータ（HyperTerminal または Minicom など）を開き、セットアップを 8 ビット、パリティ無し、フロー制御無し、ボーレート 115200 にします。

   5 秒おきにコアメモリ障害がエラーメッセージを表示します。
3. <Enter>を押します。

   リカバリプロンプトが表示されたら、追加情報を使用できます。プロンプトには、CMC スロット番号と障害タイプが示されます。

   障害の理由と、いくつかのコマンドの構文を表示するには、`recover` と入力し、<Enter> を押します。

   プロンプト例：

   ```
   recover1[self test] CMC 1 self test failure

   recover2[Bad FW images] CMC2 has corrupted images
   ```

   - プロンプトがセルフテストの失敗を示している場合、CMC にはサービス可能なコンポーネントはありません。CMC が不良であることから、Dell に返品する必要があります。
   - プロンプトが **FW イメージ不良** を示している場合は、「ファームウェアイメージのリカバリ」の手順に従って問題を解決してください。

ファームウェアイメージのリカバリ

正常な CMC OS の起動が不可能な場合、CMC はリカバリモードになります。リカバリモードでは、ファームウェアアップデートファイル **firmimg.cmc** をアップロードすることによってフラッシュデバイスを再プログラムできる、少数のコマンドのサブセットを使用することができます。このファームウェアイメージファイルは、正常のファームウェアアップデートで使用されるものと同じファイルです。リカバリプロセスは現在のアクティビティを表示し、完了時に CMC OS を起動します。

リカバリ プロンプトで recover と入力して <Enter> を押すと、回復理由と使用可能なサブコマンドが表示されます。リカバリシーケンス例は次のとおりです。

```
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
```

メモ: ネットワークケーブルを左端の RJ45 に接続します。

メモ: リカバリモードでは、アクティブなネットワークスタックがないため、通常の方法で CMC を ping することはできません。`recover ping <TFTP サーバー IP>` コマンドを使うことで、TFTP サーバーを ping して LAN 接続を確認できます。一部のシステムでは、`setniccfg` コマンド後に `recover reset` コマンドを使用する必要がある場合があります。

ネットワーク問題のトラブルシューティング

内部 CMC トレースログでは、CMC アラートとネットワークのデバッグを行うことが可能です。トレースログには CMC ウェブインタフェースまたは RACADM を使ってアクセスできます。『*iDRAC7 および CMC 向けコマンドラインリファレンスガイド*』の `gettracelog` の項を参照してください。

トレースログは次の情報を追跡します。

- DHCP — DHCP サーバーから送受信されたパケットをトレースします。
- DDNS — 動的 DNS アップデート要求と応答をトレースします。
- ネットワークインタフェースへの設定変更。

トレースログには、管理下システムのオペレーティングシステムではなく、CMC の内部ファームウェアに関連する CMC ファームウェア固有のエラーコードが含まれている場合もあります。

システム管理者パスワードのリセット

注意: 修理作業の多くは、認定されたサービス技術者のみが行うことができます。製品マニュアルで許可されている範囲に限り、またはオンラインサービスもしくは電話サービスとサポートチームの指示によってのみ、トラブルシューティングと簡単な修理を行うようにしてください。デルで認められていない修理（内部作業）による損傷は、保証の対象となりません。製品に付属しているマニュアルの「安全にお使いいただくために」をお読みになり、指示に従ってください。

管理処置を行うには、**システム管理者** 特権を持つユーザーが必要です。CMC ソフトウェアには、システム管理者アカウントパスワードを忘れた場合に無効化できるユーザーアカウントパスワード保護セキュリティ機能があります。システム管理者アカウントパスワードを忘れた場合は、CMC 基板の PASSWORD_RSET ジャンパを使用して回復できます。

CMC 基板には、次の図に示されるように、2 ピンのパスワードリセットコネクタがあります。リセットコネクタにジャンパが取り付けられると、デフォルトのシステム管理者アカウントとパスワードが有効化され、デフォルト値 ユーザー名： root および パスワード： calvin に設定されます。システム管理者アカウントは、アカウントが削除された、またはパスワードが変更されたかどうかにかかわらず、リセットされます。

メモ: 作業を開始する前に、CMC モジュールがパッシブ状態にあることを確認してください。

管理処置を実行するには、**システム管理者** 特権を持つユーザーが必要です。システム管理者アカウントパスワードを忘れた場合は、CMC 基板の PASSWORD_RST ジャンパを使用してリセットできます。

PASSWORD_RST ジャンパは、次の図で示されるように 2 ピンコネクタを使用します。

PASSWORD_RST ジャンパが取り付けられている場合、デフォルトのシステム管理者アカウントとパスワードが有効化され、次のデフォルト値に設定されます。

ユーザー名： root

パスワード： calvin

システム管理者アカウントは、アカウントが削除された、またはパスワードが変更されたかどうかにかかわらず、一時的にリセットされます。

メモ: PASSWORD_RST ジャンパが取り付けられると、次のようにデフォルトのシリアルコンソール設定（設定プロパティ値ではなく）が使用されます。

```
cfgSerialBaudRate=115200
cfgSerialConsoleEnable=1
cfgSerialConsoleQuitKey=^\
cfgSerialConsoleIdleTimeout=0
cfgSerialConsoleNoAuth=0
cfgSerialConsoleCommand=""
cfgSerialConsoleColumns=0
```

1. ハンドルの CMC リリースラッチを押し、ハンドルをモジュールの前面パネルから離します。CMC モジュールをエンクロージャから引き出します。

   メモ: 静電気放電（ESD）イベントは、CMC を損傷する可能性があります。特定の状況下では、ESD が体内またはオブジェクト上に蓄積され、CMC に放電される場合があります。ESD 損傷を防ぐには、シャーシ外で CMC を扱う、および CMC にアクセスする間は、体内から静電気を放電するための措置を行う必要があります。

2. パスワードリセットコネクタからジャンパプラグを取り外し、2 ピンジャンパを挿入してデフォルトのシステム管理者アカウントを有効化します。CMC 基板のパスワードジャンパの位置を確認するには、次の図を参照してください。

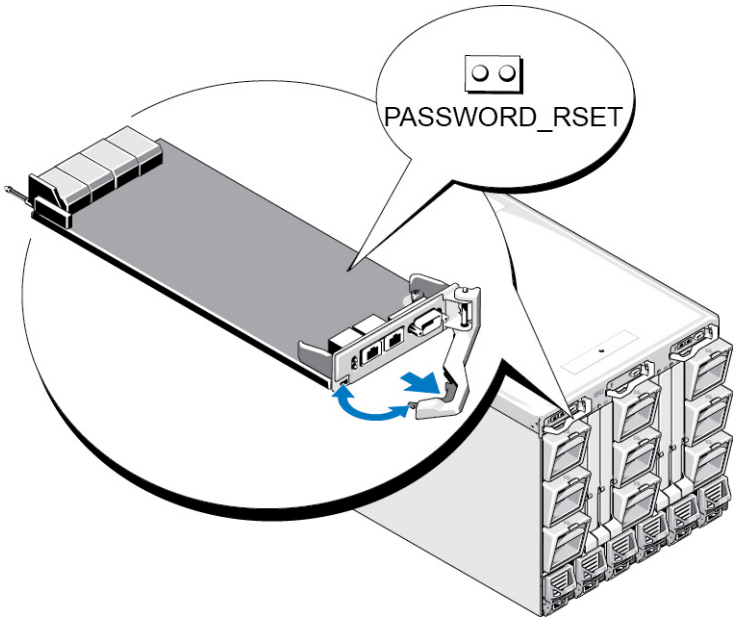


図 9. パスワードリセットジャンパの位置

表 41. CMC パスワードジャンパの設定

PASSWORD_RSET	（デフォルト）	パスワードリセット機能は無効です。
		パスワードリセット機能は有効です。

3. CMC モジュールをエンクロージャ内に差し込みます。取り外したケーブルをすべて再度接続します。

   メモ: CMC モジュールがアクティブ CMC になり、残りの手順が終了するまでアクティブ CMC のままであるようにします。

4. ジャンパを取り付けた CMC モジュールが唯一の CMC である場合は、それが再起動するのを待ちます。シャーシ内に冗長 CMC がある場合は、ジャンパを取り付けた CMC モジュールをアクティブにするための切り替えを開始します。ウェブインタフェースのシステムツリーで **シャーシ概要** に進み、**電源 → 制御** とクリックし、**CMC のリセット（ウォームブート）** を選択して **適用** をクリックします。

   CMC が自動的に冗長モジュールにフェールオーバーし、そのモジュールがアクティブになります。

5. デフォルトのシステム管理者ユーザー名： root とパスワード： calvin を使用してアクティブ CMC にログインし、必要なユーザーアカウント設定を復元します。既存のアカウントとパスワードは無効化されておらず、アクティブなままです。
6. 新規システム管理者パスワードの作成を含む、必要な管理アクションを実行します。
7. 2 ピン PASSWORD_RST ジャンパを取り外し、ジャンパプラグを元に戻します。
   a) ハンドルの CMC リリースラッチを押し、ハンドルをモジュールの前面パネルから離します。CMC モジュールをエンクロージャから引き出します。
   b) 2 ピンジャンパを取り外し、ジャンパプラグを元に戻します。
   c) CMC モジュールをエンクロージャ内に差し込みます。取り外したケーブルをすべて再度接続します。手順 4 を繰り返して、ジャンパを取り外した CMC モジュールをアクティブ CMC にします。

17

LCD パネルインタフェースの使用

LCD パネルを使用して設定と診断を実行したり、シャーシやそのコンテンツの状態情報を取得することができます。

次の図は、LCD パネルの図解です。LCD 画面には、メニュー、アイコン、画像、およびメッセージが表示されます。

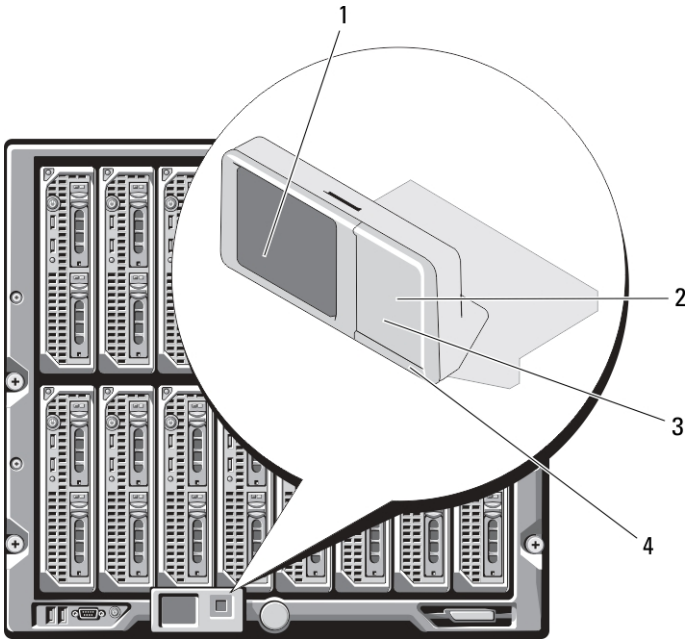


図 10. LCD ディスプレイ

1	LCD 画面	2	選択（「チェック」）ボタン
3	スクロールボタン（4）	4	状態インジケータ LED

関連リンク

LCD のナビゲーション
診断
LCD ハードウェアのトラブルシューティング
前面パネル LCD メッセージ
LCD エラーメッセージ
LCD モジュールとサーバー状態情報

LCD のナビゲーション

LCD パネルの右側には 5 つのボタン（4 つの矢印ボタン（上下左右）と中央ボタン）があります。

- *画面間を移動するには、右（次へ）および左（前へ）矢印ボタンを使用します。パネルの使用中はいつでも前の画面に戻ることができます。*
- *画面上のオプション間を移動するには、上下の矢印ボタンを使用します。*
- *画面上の項目を選択して保存し、次の画面へ移動するには、中央ボタンを使用します。*

上、下、左、および右矢印ボタンは、画面上で選択されているメニュー項目またはアイコンを変更します。選択された項目は水色の背景、または枠付きで表示されます。

LCD 画面に表示されたメッセージが画面の幅よりも長い場合は、左右の矢印ボタンを使ってテキストを左と右にスクロールします。

次の表で説明するアイコンは、LCD 画面間の移動に使用されます。

表 42. LCD パネルのナビゲーション用アイコン

標準アイコン	ハイライト表示アイコン	アイコン名および説明
		**戻る** — 前の画面に戻るには、中央ボタンをハイライトして押します。
		**確定 / はい** — 変更を確定して前の画面に戻るには、中央ボタンをハイライトして押します。
		**スキップ / 次へ** — 変更をスキップして次の画面に進むには、中央ボタンをハイライトして押します。
		**いいえ** — 質問に「いいえ」と答え、次の画面に進むには、中央ボタンをハイライトして押します。
		**交替** — シャーシの前面および背面グラフィカルビュー間を切り替えるには、中央ボタンをハイライトして押します。 **メモ:** 橙色の背景は、反対側のビューにエラーがあることを示します。
		**コンポーネント識別** — コンポーネントの青色 LED を点滅させます。 **メモ:** コンポーネント識別 が有効になると、このアイコンを囲む青い長方形が点滅します。

LCD パネル上の状態インジケータ LED は、シャーシとそのコンポーネントの全体的な正常性目安を提供します。

- 青色の点灯は、正常性が良好であることを示します。

- 橙色の点滅は、少なくとも 1 つのコンポーネントに障害があることを示します。
- 青色の点滅は、シャーシグループ内の 1 つのシャーシを識別するために使用される ID 信号です。

関連リンク

メインメニュー
LCD セットアップメニュー
言語セットアップ画面
デフォルト画面
グラフィカルサーバー状態画面
グラフィカルモジュール状態画面
エンクロージャメニュー画面
モジュール状態画面
エンクロージャ状態画面
IP サマリ画面

メインメニュー

メイン メニューから次のいずれかの画面に移動できます。

- **LCD セットアップメニュー** — 使用する言語と、LCD を使用していないときに表示する LCD 画面を選択します。
- **サーバー** — サーバーの状態情報を表示します。
- **エンクロージャ** — シャーシの状態情報を表示します。

上下矢印ボタンを使ってアイテムをハイライト表示します。
中央ボタンを押して選択アイテムをアクティブ化します。

LCD セットアップメニュー

LCD セットアップ メニューには、設定可能アイテムのメニューが表示されます。

- **言語セットアップ** — LCD 画面のテキストとメッセージに使用する言語を選択します。
- **デフォルト画面** — LCD パネルにアクティビティがないときに表示される画面を選択します。

上下矢印ボタンを使ってメニュー内のアイテムをハイライト表示するか、**メイン** メニューに戻る場合は **戻る** アイコンをハイライト表示します。
中央ボタンを押して選択アイテムをアクティブにします。

言語セットアップ画面

言語セットアップ 画面では、LCD パネルメッセージに使用する言語を選択することができます。現在アクティブな言語が、水色背景でハイライト表示されます。

1. 上下左右の矢印ボタンを使って任意の言語をハイライト表示します。
2. 中央のボタンを押します。
   承認 アイコンが表示されてハイライトされます。
3. 中央のボタンを押して変更を確認します。
   LCD セットアップ メニューが表示されます。

デフォルト画面

デフォルト画面 では、LCD パネルでアクティビティがないときにパネルが表示する画面を変更することができます。工場出荷時のデフォルト画面は **メインメニュー** です。表示する画面は次から選択できます。

- **メインメニュー**
- **サーバー状態**（シャーシの前面図）
- **モジュール状態**（シャーシの背面図）
- **カスタム**（シャーシ名を伴う Dell のロゴ）

現在アクティブなデフォルト画面は青でハイライト表示されます。

1. 上下矢印ボタンを使って、デフォルトに設定する画面をハイライト表示します。
2. 中央のボタンを押します。
   承認 アイコンがハイライト表示されます。
3. 中央のボタンを再度押して変更を確認します。
   デフォルト画面 が表示されます。

グラフィカルサーバー状態画面

グラフィカルサーバー状態 画面には、シャーシに取り付けられている各サーバーのアイコンが表示され、それぞれの全般的な正常性状態が示されます。サーバー正常性は、サーバーアイコンの色によって示されます。

- 灰色 — サーバーがオフで障害なし
- 緑色 — サーバーがオンで障害なし
- 黄色 — サーバーに 1 つまたは複数の重要ではないエラーがある
- 赤色 — サーバーに 1 つまたは複数の重要なエラーがある
- 黒色 — サーバーが存在しない

サーバーアイコンを囲んで点滅する水色の長方形は、そのモジュールがハイライト表示されていることを示します。

グラフィカルモジュール状態 画面を表示するには、交替アイコンをハイライト表示し、中央ボタンを押します。

サーバーの状態画面を表示するには、矢印ボタンを使用して希望のサーバーをハイライト表示し、中央ボタンを押します。**サーバー状態** 画面が表示されます。

メインメニュー に戻るには、矢印ボタンを使用して **戻る** アイコンをハイライト表示し、中央ボタンを押します。

グラフィカルモジュール状態画面

グラフィカルモジュール状態 画面には、シャーシの後部に取り付けられているモジュールのすべてが表示され、各モジュールの正常性のサマリ情報が提供されます。モジュールの正常性は、次のように各モジュールアイコンの色で示されます。

- 灰色 — モジュールがオフ、またはスタンバイでエラーなし
- 緑色 — モジュールがオンでエラーなし
- 黄色 — モジュールに 1 つまたは複数の重要ではないエラーがある
- 赤色 — サーバーに 1 つまたは複数の重要なエラーがある
- 黒色 — モジュールが存在しない

モジュールアイコンを囲んで点滅する水色の長方形は、そのモジュールがハイライト表示されていることを示します。

グラフィカルサーバー状態 画面を表示するには、交替アイコンをハイライト表示し、中央ボタンを押します。

モジュールの状態画面を表示するには、上、下、左、および右矢印ボタンを使用して希望のモジュールをハイライト表示し、中央ボタンを押します。**モジュール状態** 画面が表示されます。

メインメニュー に戻るには、矢印ボタンを使用して戻るアイコンをハイライト表示し、中央ボタンを押します。**メインメニュー** が表示されます。

エンクロージャメニュー画面

この画面から、次の画面に移動できます。

- **モジュール状態画面**
- **エンクロージャ状態画面**
- **IP サマリ 画面**
- **メインメニュー**

ナビゲーションボタンを使用して希望のアイテムをハイライト表示し（**メインメニュー** に戻るには **戻る** アイコンをハイライト表示）、中央ボタンを押します。選択した画面が表示されます。

モジュール状態画面

モジュール状態 画面には、モジュールに関する情報とエラーメッセージが表示されます。この画面に表示される可能性のあるメッセージついては、「LCD モジュールとサーバー状態情報」および「LCD エラーメッセージ」を参照してください。

メッセージ間を移動するには、上および下矢印キーを使用してください。左および右矢印キーは、画面に収まりきらないメッセージをスクロールするために使用します。

グラフィカルモジュール状態 画面に戻るには、**戻る** アイコンをハイライト表示し、中央のボタンを押します。

エンクロージャ状態画面

エンクロージャ状態 画面には、エンクロージャについての情報およびエラーメッセージが表示されます。この画面に表示される可能性のあるメッセージについては、「LCD エラーメッセージ」を参照してください。上下矢印キーを使用して、メッセージ間を移動します。

画面に収まらないメッセージは、左右矢印キーを使ってスクロールします。

エンクロージャ状態 画面に戻るには、**戻る** アイコンをハイライト表示し、中央ボタンを押します。

IP サマリ画面

IP サマリ 画面には、取り付けられている各サーバーの CMC と iDRAC の IP 情報が表示されます。

上下矢印ボタンを使ってリスト内をスクロールします。画面に収まりきらない長さの選択済みメッセージをスクロールするには、左右矢印ボタンを使用します。

エンクロージャ メニューに戻るには、上下矢印ボタンを使って **戻る** アイコンを選択し、中央のボタンを押します。

診断

LCD パネルはシャーシ内の任意のサーバーまたはモジュールの問題の診断に役立ちます。シャーシ、またはシャーシ内のサーバーやその他モジュールに問題または障害がある場合、LCD パネルの状態インジケータが

橙色に点滅します。メインメニューで、不良サーバーやモジュールの原因となるメニューアイテム（サーバーまたはエンクロージャ）の横に橙色背景のアイコンが表示されます。

LCD メニューシステムで橙色のアイコンをたどっていくことにより、問題のあるアイテムの状態画面とエラーメッセージを表示できます。

LCD パネルのエラーメッセージは、問題の原因となっているモジュールやサーバーの取り外し、またはモジュールやサーバーのハードウェアログのクリアによって削除できます。サーバーエラーでは、iDRAC ウェブインタフェースまたはコマンドラインインタフェースを使用して、サーバーのシステムイベントログ（SEL）をクリアします。シャーシエラーでは、CMC ウェブインタフェースまたはコマンドラインインタフェースを使用して、ハードウェアログをクリアします。

LCD ハードウェアのトラブルシューティング

CMC の使用に関して LCD で何らかの問題に遭遇した場合は、次のハードウェアのトラブルシューティング項目を使用して、LCD ハードウェアまたは接続に問題がないか調べます。

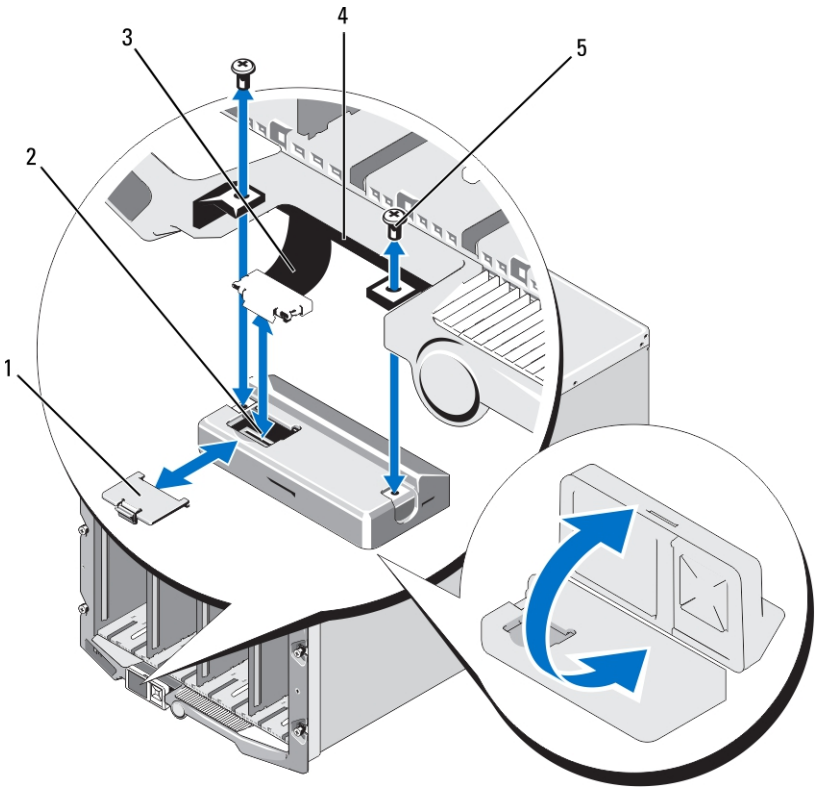


図 11. LCD モジュールの取り外しと取り付け

1	ケーブルカバー	2	LCD モジュール
3	リボンケーブル	4	ヒンジ（2）
5	ネジ（2）		

表 43. LCD ハードウェアのトラブルシューティング項目

現象	問題	回復処置
アラート画面に CMC が応答しません のメッセージが表示され、LED が橙色に点滅する。	CMC から LCD 前面パネルへの通信の損失です。	CMC が起動していることを確認した上で、GUI または RACADM コマンドを使用して CMC をリセットします。
アラート画面に CMC が応答しません のメッセージが表示され、LED が橙色に点灯、または消灯する。	CMC のフェールオーバーまたは再起動中に、LCD モジュールの通信が停止しました。	GUI または RACADM コマンドを使用してハードウェアログを確認します。LCD コントローラと通信できません と提示するメッセージを探してください。 LCD モジュールのリボンケーブルを抜き差しします。
画面のテキストが文字化けしている。	欠陥のある LCD 画面です。	LCD コントローラモジュールを交換してください。
LED が消灯しており、LCD がオフになっている。	LCD ケーブルが正しく接続されていないかケーブルに欠陥がある、または LCD モジュールに欠陥があります。	GUI または RACADM コマンドを使用してハードウェアログを確認します。次を提示するメッセージを探してください。 • LCD モジュールケーブルが接続されていないか、または正しく接続されていません。 • コントロールパネルケーブルが接続されていないか、または正しく接続されていません。 ケーブルを接続し直します。
LCD 画面に CMC が見つかりません のメッセージが表示される。	シャーシに CMC が存在しません。	シャーシに CMC を挿入します。CMC が存在する場合は、既存の CMC を装着しなおします。

前面パネル LCD メッセージ

このセクションには 2 つのサブセクションがあり、前面パネル LCD に表示されるエラーと状態情報をリストにします。

LCD の *エラーメッセージ*の形式は、CLI またはウェブインタフェースで表示されるシステムイベントログ（SEL）に似ています。

エラーセクションの表は、各種 LCD 画面に表示されるエラーおよび警告メッセージと、考えられるメッセージの原因をリストします。山括弧（< >）で囲まれたテキストは、そのテキストが様々であることを示します。

LCD の *状態情報*には、シャーシ内のモジュールについての記述的情報が含まれます。このセクションの表には、各コンポーネントに対して表示される情報が説明されています。

LCD エラーメッセージ

表 44. CMC 状態画面

重大度	メッセージ	原因
重要	CMC <番号> バッテリが故障しました。	CMC CMOS バッテリが存在しないか、電圧がありません。
重要	CMC <番号> LAN のハートビートが失われました。	CMC の NIC の接続が取り外されたか、または接続されていません。
警告	スロット <番号> の iDRAC と CMC 間にファームウェアまたはソフトウェアの非互換性が検知されました。	1 つまたは複数の機能をサポートするためのファームウェアが、2 つのデバイス間で一致しません。
警告	スロット <番号> の iDRAC と CMC 間にファームウェアまたはソフトウェアの非互換性が検知されました。	1 つまたは複数の機能をサポートするためのファームウェアが、2 つのデバイス間で一致しません。
警告	CMC 1 と CMC 2 との間でファームウェアまたはソフトウェアの非互換性が検出されました。	1 つまたは複数の機能をサポートするためのファームウェアが、2 つのデバイス間で一致しません。

表 45. エンクロージャ / シャーシ状態画面

重大度	メッセージ	原因
重要	ファン <番号> が取り外されました。	このファンはエンクロージャ / シャーシを正しく冷却するために必要です。
警告	電源装置の冗長性が劣化しています。	1 台または複数の PSU が故障したか、取り外されたため、システムが完全な PSU 冗長性をサポートできなくなりました。
重要	電源装置の冗長性が失われました。	1 台または複数の PSU が故障したか、取り外されたため、システムの冗長性がなくなりました。
重要	電源装置が非冗長です。正常な動作を維持するためのリソースが不足しています。	1 台または複数の PSU が故障したか、取り外されたため、システムに正常な動作を維持するための電力が不足しています。これにより、サーバーの電源が切れる可能性があります。
警告	コントロールパネルの周辺温度が、警告しきい値の上限を超えています。	シャーシ / エンクロージャの吸気温度が警告しきい値を超えました。
重要	コントロールパネルの周辺温度が、警告しきい値の上限を超えています。	シャーシ / エンクロージャの吸気温度が警告しきい値を超えました。
重要	CMC の冗長性が失われました。	CMC は冗長ではなくなりました。これは、スタンバイ CMC が削除された場合に発生します。
重要	すべてのイベントのログが無効化されています。	シャーシ / エンクロージャはこのログにイベントを保存できなくなりました。これは通常、コントロールパネルまたはコントロールパネルケーブルの問題を示します。

重大度	メッセージ	原因
警告	ログが満杯です。	あと 1 つエントリを追加すると CEL（ハードウェアログ）が満杯になることを、シャーシが検出しました。
警告	ログがほとんど満杯です。	シャーシイベントログは 75% 満杯です。

表 46. ファン状態画面

重大度	メッセージ	原因
重要	ファン <番号> の RPM が、重要なしきい値の下限を下回って稼働しています。	指定したファンの速度は、システムに十分な冷却を提供できません。
重要	ファン <番号> の RPM が、重要なしきい値の上限を上回って稼働しています。	指定されたファンの速度が早すぎます。これは通常、ファンのブレードが損傷したことが原因です。

表 47. IOM 状態画面

重大度	メッセージ	原因
警告	I/O モジュール <番号> でのファブリックの不一致が検出されました。	この IO モジュールのファブリックが、サーバーまたは冗長 I/O モジュールのファブリックと一致しません。
警告	I/O モジュール <番号> でリンクチューニング障害が検出されました。	この IO モジュールを、1 つまたは複数のサーバーの NIC を正しく使用するように設定することができませんでした。
重要	I/O モジュール <番号> で障害が検出されました。	I/O モジュールには不具合が発生しています。I/O モジュールがサーマルトリップしている場合でも同じエラーが生成されます。

表 48. iKVM 状態画面

重大度	メッセージ	原因
警告	ローカル KVM 用にコンソールが使用できません。	ファームウェアの破損などの軽度のエラーです。
重要	ローカル KVM がどのホストにも見つかりません。	USB ホスト列挙エラーです。
重要	OSCAR（オンスクリーン表示）がローカル KVM で機能しません。	OSCAR の障害です。
回復不能	ローカル KVM が機能せず、電源がオフになっています。	シリアル RIP 障害または USB ホストチップ障害です。

表 49. PSU 状態画面

重大度	メッセージ	原因
重要	電源装置 <番号> に障害が発生しました。	PSU に障害が発生しました。
重要	電源装置 <番号> の電源入力が失われました。	AC 電源が失われたか、AC コードが抜かれています。
警告	電源装置 <番号> が 110 ボルトで動作しており、ブレーカーの故障を引き起こす可能性があります。	電源装置が 110 ボルトの電源に接続されています。

表 50. サーバー状態画面

重大度	メッセージ	原因
警告	システムボードの周辺温度が、警告しきい値の下限を下回っています。	サーバー温度が低下しています。
重要	システム基板の周辺温度が、重要なしきい値の下限を下回っています。	サーバー温度が低下しています。
警告	システム基板の周辺温度が、警告しきい値の上限を超えています。	サーバー温度が上昇しています。
重要	システム基板の周辺温度が、重要なしきい値の上限を超えています。	サーバー温度が熱くなりすぎています。
重要	システム基板の電流ラッチ電流が許容範囲外です。	電流がエラーしきい値を超えました。
重要	システム基板バッテリが故障しました。	CMOS バッテリが不在、または電圧がありません。
警告	ストレージバッテリの残量が低下しています。	ROMB バッテリの残量が低下しています。
重要	ストレージバッテリが故障しました。	CMOS バッテリが不在、または電圧がありません。
重要	CPU <番号> <電圧センサー名> 電圧が許容範囲外です。	
重要	システム基板 <電圧センサー名> 電圧が許容範囲外です。	
重要	メザニンカード <番号> <電圧センサー名> 電圧が許容範囲外です。	
重要	ストレージ <電圧センサー名> 電圧が許容範囲外です。	
重要	CPU <番号> に内部エラー（IERR）があります。	CPU 障害です。
重要	CPU <番号> にサーマルトリップ（過熱）イベントが発生しています。	CPU が過熱状態です。
重要	CPU <番号> 構成がサポートされていません。	誤ったプロセッサタイプ、または搭載場所が間違っています。
重要	CPU <番号> がありません。	必要な CPU が見つからないか、不在です。
重要	メザニン B <スロット番号> 状態： メザニン B <スロット番号> のアドインカードセンサー、取り付けエラーがアサートされました。	IO ファブリックに間違ったメザニンカードが取り付けられています。
重要	メザニン C <スロット番号> 状態： メザニン C <スロット番号> のアドインカードセンサー、取り付けエラーがアサートされました。	IO ファブリックに間違ったメザニンカードが取り付けられています。
重要	ドライブ <番号> が取り外されました。	ストレージドライブが取り外されました。

重大度	メッセージ	原因
重要	ドライブ <番号> で障害が検知されました。	ストレージドライブが故障しました。
重要	システム基板のフェールセーフ電圧が許容範囲外です。	システム基板の電圧が正常レベルではない場合に、このイベントが生成されます。
重要	ウォッチドッグタイマーが切れました。	iDRAC ウォッチドッグタイマーが切れましたが、処置が設定されていません。
重要	ウォッチドッグタイマーによってシステムがリセットされました。	iDRAC ウォッチドッグは、システムがクラッシュしたことを検知しました (タイマーはホストからの応答がないために切れました)。処置は再起動に設定されています。
重要	ウォッチドッグタイマーによってシステムの電源がオフになりました。	iDRAC ウォッチドッグは、システムがクラッシュしたことを検知しました (タイマーはホストからの応答がないために切れました)。処置は電源オフに設定されています。
重要	ウォッチドッグタイマーによってシステムのパワーサイクルが行われました。	iDRAC ウォッチドッグは、システムがクラッシュしたことを検知しました (タイマーはホストからの応答がないために切れました)。処置はパワーサイクルに設定されています。
重要	ログが満杯です。	SEL デバイスは、SEL が満杯になる前に追加できるエントリが 1 つしかないことを検出しました。
警告	<場所> のメモリデバイスで、訂正可能な永続的エラーが検出されました。	
警告	<場所> のメモリデバイスで、訂正可能な永続的エラーの発生率が増加しました。	修正可能な ECC エラーが重要な発生率に到達しました。
重要	<場所> のメモリデバイスで、マルチビットメモリエラーが検出されました。	訂正不能 ECC エラーが検知されました。
重要	バス <番号> デバイス <番号> 機能 <番号> のコンポーネントで、I/O チャネルチェック NMI が検出されました。	I/O チャネルに重要な割り込みが生成されました。
重要	スロット <番号> のコンポーネントで、I/O チャネルチェック NMI が検出されました。	I/O チャネルに重要な割り込みが生成されました。
重要	バス <番号> デバイス <番号> 機能 <番号> のコンポーネントで、PCI パリティエラーが検出されました。	PCI バスにパリティエラーが検出されました。
重要	スロット <番号> のコンポーネントで、PCI パリティエラーが検出されました。	PCI バスにパリティエラーが検出されました。
重要	バス <番号> デバイス <番号> 機能 <番号> のコンポーネントで、PCI システムエラーが検出されました。	デバイスによって PCI エラーが検出されました。
重要	スロット <番号> のコンポーネントで、PCI システムエラーが検出されました。	デバイスによって PCI エラーが検出されました。

重大度	メッセージ	原因
重要	<場所> のメモリデバイスで、訂正可能な永続的エラーのログが無効化されました。	メモリデバイスに過剰なシングルビットエラーがログされると、シングルビットエラーのログが無効になります。
重要	すべてのイベントのログが無効化されています。	
回復不能	CPU プロトコルエラーが検出されました。	プロセッサプロトコルが回復不能状況になりました。
回復不能	CPU バスパリティエラーが検知されました。	プロセッサバス PERR が回復不能状況になりました。
回復不能	CPU 初期化エラーが検出されました。	プロセッサ初期化が回復不能状況になりました。
回復不能	CPU マシンチェックが検出されました。	プロセッサマシンチェックが回復不能状況になりました。
重要	メモリ冗長性が失われました。	
重要	バス <番号> デバイス <番号> 機能 <番号> のコンポーネントで、バスの致命的なエラーが検出されました。	PCIe バスに致命的なエラーが検知されました。
重要	バス <番号> デバイス <番号> 機能 <番号> のコンポーネントで、ソフトウェア NMI が検出されました。	チップエラーが検出されました。
重要	バス <番号> デバイス <番号> 機能 <番号> のコンポーネントで、仮想 MAC アドレスのプログラムに失敗しました。	このデバイスには FlexAddress をプログラムできます。
重要	メザニンカード <番号> のデバイスオプション ROM が、リンクチューニングまたは FlexAddress のサポートに失敗しました。	オプション ROM が FlexAddress またはリンクチューニングをサポートしていません。
重要	iDRAC からのリンクチューニングまたは FlexAddress データの取得に失敗しました。	

メモ: その他のサーバー関連の LCD メッセージについての情報は、『サーバーユーザーガイド』を参照してください。

LCD モジュールとサーバー状態情報

本項の表では、シャーシ内のコンポーネントタイプごとに前面パネル LCD に表示される状態項目について説明します。

表 51. CMC の状態

項目	説明
例： CMC1、CMC2	名前または場所。
エラーなし	エラーがない場合はメッセージ「エラーなし」が表示されますが、それ以外の場合はエラーメッセージが重要エラー、警告の順で表示されます。

ファームウェアバージョン	アクティブな CMC についてのみ表示されます。スタンバイ CMC にはスタンバイと表示されます。
IP4 <有効、無効>	アクティブな CMC についてのみ、現在の IPv4 有効化状況を表示します。
IP4 アドレス： <アドレス、取得中>	アクティブな CMC についてのみ、IPv4 が有効化されているかどうかだけを表示します。
IP6 <有効、無効>	アクティブな CMC についてのみ、現在の IPv6 有効化状況を表示します。
IP6 ローカルアドレス： <アドレス>	アクティブな CMC についてのみ、IPv6 が有効化されているかどうかだけを表示します。
IP6 グローバルアドレス： <アドレス>	アクティブな CMC についてのみ、IPv6 が有効化されているかどうかだけを表示します。

表 52. シャーシまたはエンクロージャ状態

項目	説明
ユーザー定義名	例：「Dell ラックシステム」。このオプションは、CMC コマンドラインインタフェース（CLI）またはウェブインタフェースで設定できます
エラーメッセージ	エラーがない場合はメッセージ「エラーなし」が表示されますが、それ以外の場合はエラーメッセージが重要エラー、警告の順で表示されます。
モデル番号	例：「PowerEdgeM1000e」。
電力消費量	現在のワット単位での電力消費量です。
ピーク電力	ワット単位のピーク電力消費量です。
最小電力	ワット単位の最小電力消費量です。
周囲温度	現在の摂氏での周辺温度です。
サービスタグ	工場出荷時に割り当てられたサービスタグです。
CMC 冗長性モード	非冗長または冗長になります。
PSU 冗長性モード	非冗長、AC 冗長、または DC 冗長になります。

表 53. ファン状態

項目	説明
名前 / 場所	例：ファン 1、ファン 2 など。
エラーメッセージ	エラーがない場合は、「エラーなし」表示されます。それ以外の場合は、エラーメッセージが重要エラー、警告の順で表示されます。
RPM	現在のファン速度（RPM）です。

表 54. PSU 状態

項目	説明
名前 / 場所	例：PSU1、PSU2 など。
エラーメッセージ	エラーがない場合はメッセージ「エラーなし」が表示されますが、それ以外の場合はエラーメッセージが重要エラー、警告の順で表示されます。
状態	オフライン、オンライン、またはスタンバイになります。
最大ワット数	PSU がシステムに供給できる最大ワット数です。

表 55. IOM 状態

項目	説明
名前 / 場所	例：IOM A1、IOM B1 など。
エラーメッセージ	エラーがない場合はメッセージ「エラーなし」が表示されますが、それ以外の場合はエラーメッセージが重要エラー、警告の順で表示されます。詳細については『LCD エラーメッセージ』を参照してください。
状態	オフまたはオンになります。
モデル	IOM のモデルです。
ファブリックタイプ	ネットワークタイプです。
IP アドレス	IOM がオンの場合にのみ表示されます。パススルータイプ IOM の値はゼロです。
サービスタグ	工場出荷時に割り当てられたサービスタグです。

表 56. iKVM の状態

項目	説明
名前	iKVM。
エラーなし	エラーがない場合はメッセージ「エラーなし」が表示されますが、それ以外の場合はエラーメッセージが重要エラー、警告の順で表示されます。詳細については『LCD エラーメッセージ』を参照してください。
状態	オフまたはオンになります。
モデル / メーカー	iKVM モデルの説明です。
サービスタグ	工場出荷時に割り当てられたサービスタグです。
パーツ番号	メーカーのパーツ番号です。
ファームウェアバージョン	iKVM ファームウェアバージョンです。
ハードウェアバージョン	iKVM ハードウェアバージョンです。

メモ: この情報は動的にアップデートされます。

表 57. サーバー状態

項目	説明
例： サーバー 1、サーバー 2、など。	名前 / 場所。
エラーなし	エラーがない場合はメッセージ「エラーなし」が表示されますが、それ以外の場合はエラーメッセージが重要エラー、警告の順で表示されます。詳細については『LCD エラーメッセージ』を参照してください。
スロット名	シャーシスロット名です。例えば SLOT-01 です。 **メモ:** この表は、CMC CLI またはウェブインタフェースを使用して設定できます。
名前	ユーザーが Dell OpenManage を使用して設定することができるサーバーの名前です。この名前は、iDRAC の起動が完了し、サーバーがこの機能をサポートする場合のみ表示されます。そうでない場合は、iDRAC の起動メッセージが表示されます。
モデル番号	iDRAC の起動が完了すると表示されます。
サービスタグ	iDRAC の起動が完了すると表示されます。
BIOS バージョン	サーバー BIOS ファームウェアのバージョンです。
最終の POST コード	最終のサーバー BIOS POST コードメッセージ文字列を表示します。
iDRAC ファームウェアバージョン	iDRAC の起動が完了すると表示されます。 **メモ:** iDRAC バージョン 1.01 は 1.1 と表示されます。iDRAC バージョンに 1.10 はありません。
IP4 <有効、無効>	現在の IPv4 の有効化状況を表示します。
IP4 アドレス： <アドレス、取得中>	IPv4 が有効な場合にのみ表示されます。
IP6 <有効、無効>	iDRAC が IPv6 をサポートする場合にのみ表示されます。現在の IPv6 有効化状況を表示します。
IP6 ローカルアドレス： <アドレス>	iDRAC が IPv6 をサポートし、かつ IPv6 が有効な場合にのみ表示されます。
IP6 グローバルアドレス： <アドレス>	iDRAC が IPv6 をサポートし、かつ IPv6 が有効な場合にのみ表示されます。
ファブリック上で有効化された FlexAddress	機能がインストールされている場合にのみ表示されます。このサーバー用に有効化されたファブリックをリストします（つまり、A、B、C）。

表の情報は動的にアップデートされます。サーバーがこの機能をサポートしていない場合は、次の情報は表示されません。サポートしている場合は、サーバー管理者のオプションは次のとおりです。

- オプション「なし」= LCD には一切の文字列を表示しない。
- オプション「デフォルト」= 影響なし。
- オプション「カスタム」= サーバー名の文字列が入力可能。

この情報は、iDRAC の起動が完了している場合にのみ表示されます。この機能の詳細については、**dell.com/support/manuals** で、『iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド』を参照してください。

18

よくあるお問い合わせ

本項では、次に関するよくあるお問い合わせをリストします。

RACADM

CMC リセットの実行後（RACADM racreset サブコマンドを使用）、コマンドを入力すると、次のメッセージが表示されます。

```
racadm <subcommand> Transport: ERROR: (RC=-1)
```

このメッセージは、別のコマンドの発行は CMC がリセットを完了した後に行う必要があることを示しています。

RACADM サブコマンドを使用すると、次のエラーの 1 つ、または複数が表示されることがあります。

- ローカルエラーメッセージ — 構文、入力ミス、名前の誤りなどの問題。例：`ERROR: <message>`

RACADM `help` サブコマンドを使って、正しい構文と使用方法を表示します。

CMC 関連のエラーメッセージ — CMC が処置を実行できないった問題。「racadm コマンドが失敗しました。」と表示される場合もあります。

デバッグ情報を取得するには、`racadm gettracelog` と入力します。

リモート RACADM の使用中、プロンプトが「>」に変わり、「$」プロンプトが表示されなくなります。

コマンド内で一致しない二重引用符（"）または一致しない引用符（'）が使用されると、CLI が「>」プロンプトに変わり、すべてのコマンドが待ち状態になります。

$ プロンプトに戻すには、<Ctrl>–d を入力します。

`$ logout` および `$ quit` コマンドの使用中、「見つかりません」というエラーメッセージが表示されます。

logout および quit コマンドは、CMC RACADM インタフェースでサポートされていません。

リモートシステムの管理と復元

CMC ウェブインタフェースへのアクセス中に、SSL 証明書のホスト名と CMC のホスト名が一致しないというセキュリティ警告が表示されます。

CMC には、ウェブインタフェースとリモート RACADM 機能のネットワークセキュリティを確保するため、デフォルトの CMC サーバー証明書が備わっています。この証明書が使用される時、CMC のホスト名（例えば IP アドレス）に一致しないデフォルト証明書が CMC デフォルト証明書に発行されるため、ウェブブラウザがセキュリティ警告を表示します。

このセキュリティ問題に対処するには、CMC の IP アドレスに発行された CMC サーバー証明書をアップロードします。証明書の発行のために使用される証明書署名要求（CSR）を生成するときは、CSR のコモンネーム

（CN）が CMC の IP アドレス（例えば 192.168.0.120）または登録済み DNS CMC 名に一致することを確認してください。

CSR を登録済み DNS CMC 名と一致させるには、次の手順を実行します。

1. CMC ウェブインタフェースでシステムツリーに移動し、**シャーシ概要** をクリックします。
2. **ネットワーク** タブをクリックしてから **ネットワーク** をクリックします。
   ネットワーク設定 ページが表示されます。
3. **DNS** オプションで **CMC の登録** を選択します。
4. **DNS CMC 名** フィールドに CMC 名を入力します。
5. **変更の適用** をクリックします。
   CSR の生成と証明書の発行についての詳細は、「証明書の取得」を参照してください。

プロパティを変更すると、リモート RACADM とウェブベースのサービスを使用できなくなるのはなぜですか?

CMC ウェブサーバーをリセットすると、リモート RACADM サービスとウエブインタフェースに再度アクセスできるようになるまでしばらく時間がかかることがあります。CMC ウェブサーバーは、以下の発生後にリセットされます。

- CMC ウェブインタフェースを使用してネットワーク設定やネットワークセキュリティのプロパティを変更する。
- **cfgRacTuneHttpsPort** プロパティが変更された（`config -f <config file>` コマンドが変更する場合も含む）。
- `racresetcfg` が使用されたか、またはシャーシ構成のバックアップが回復された。
- CMC がリセットされた。
- 新しい SSL サーバー証明書がアップロードされた。

DNS サーバーは、マイ CMC を登録しません。

一部の DNS サーバーは、最大 31 文字までの名前のみを登録します。

CMC ウェブインタフェースにアクセスする時、SSL 証明書が信頼されていない認証局（CA）によって発行されたというセキュリティ警告が表示されます。

CMC には、ウェブインタフェースとリモート RACADM 機能のネットワークセキュリティを確保するためのデフォルトの CMC サーバー証明書が備わっています。この証明書は信頼できる認証局（CA）によって発行されたものではありません。このセキュリティ問題に対処するには、信頼できる認証局（Thawte または Verisign など）によって発行された CMC サーバー証明書をアップロードしてください。証明書についての詳細は、「証明書の取得」を参照してください。

次のメッセージが原因不明の理由で表示されるのはなぜですか?

Remote Access: SNMP Authentication Failure

IT Assistant は、検出の一環として、デバイスの **get** コミュニティ名および **set** コミュニティの検証を試行します。IT Assistant では、**get community name = public** であり、**set community name = private** です。デフォルトでは、CMC エージェントのコミュニティ名は public です。IT Assistant が set 要求を送信すると、CMC エージェントは SNMP 認証エラーを生成します。これは、CMC エージェントが **community = public** の要求のみを受け入れるからです。

RACADM を使用して CMC コミュニティ名を変更してください。CMC コミュニティ名を表示するには、次のコマンドを使用します。

```
racadm getconfig -g cfgOobSnmp
```

CMC コミュニティ名を設定するには、次のコマンドを使用します。

```
racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <community name>
```

SNMP 認証トラップが生成されないようにするには、 エージェントによって受け入れられるコミュニティ名を入力してください。CMC では 1 つのコミュニティ名のみが許可されているため、IT Assistant 検出セットアップには同じ get コミュニティ名と set コミュニティ名を入力します。

Active Directory

Active Directory は複数ツリー全体での CMC ログインをサポートしますか?

はい。CMC の Active Directory クエリアルゴリズムは、1 つのフォレストで複数のツリーをサポートします。

混在モード（つまりフォレストのドメインコントローラが Microsoft Windows NT 2000 や Windows Server 2003 などの異なるオペレーティングシステムを実行）での Active Directory を使った CMC へのログインは可能ですか?

はい。混在モードでは、CMC クエリプロセスで使用されるすべてのオブジェクト（ユーザー、RAC デバイスオブジェクト、関連オブジェクトなど）は同じドメインにある必要があります。

デル拡張 Active Directory ユーザーとコンピュータスナップインはモードをチェックし、混合モードであれば、ドメイン間でオブジェクトを作成するためにユーザーを制限します。

CMC と Active Directory の併用は、複数のドメイン環境をサポートしますか?

はい。ドメインフォレスト機能レベルはネイティブモードまたは Windows 2003 モードである必要があります。さらに、関連オブジェクト、RAC ユーザーオブジェクト、および RAC デバイスオブジェクト（関連オブジェクトを含む）間のグループは、ユニバーサルグループである必要があります。

これらの Dell 拡張オブジェクト（Dell 関連オブジェクト、Dell RAC デバイス、および Dell 権限オブジェクト）をいくつかのドメインに分散できますか?

関連オブジェクトと特権オブジェクトは、同じドメインにある必要があります。Dell 拡張 Active Directory ユーザーとコンピュータスナップインは、これらの 2 つのオブジェクトを同じドメインでのみ作成することができます。その他のオブジェクトは異なるドメイン内に置くことができます。

ドメインコントローラの SSL 設定に何か制限はありますか？

はい。CMC では、信頼できる認証局の署名付き SSL 証明書を 1 つしかアップロードできないため、フォレスト内の Active Directory サーバーの SSL 証明書はすべて同じルート認証局によって署名される必要があります。

新規 RAC 証明書が作成されてアップロードされた後、ウェブインタフェースが起動しません。

RAC 証明書の生成に Microsoft 証明書サービス使用された場合、証明書作成時にウェブ証明書ではなくユーザー証明書オプションが使用された可能性があります。

これを修正するには、CSR を生成して、Microsoft 証明書サービスから新しいウェブ証明書を作成し、次の RACADM コマンドを使用してアップロードします。

```
racadm sslcsrgen [-g] [-f {filename}]
racadm sslcertupload -t 1 -f {web_sslcert}
```

FlexAddress と FlexAddressPlus

機能カードが取り外されるとどうなりますか？

機能カードが取り外されても、特に変化はありません。 機能カードは取り外して保管、またはそのままにしておくことができます。

あるシャーシで使用していた機能カードを取り外し、別のシャーシに取り付けるとどうなりますか？

ウェブインタフェースが次のエラーメッセージを表示します。

```
This feature card was activated with a different chassis. It must be removed
before accessing the FlexAddress feature.
Current Chassis Service Tag = XXXXXXXX
```

```
Feature Card Chassis Service Tag = YYYYYYYY
```

```
An entry is added to the CMC log that states:
```

```
cmc <date timestamp> : feature 'FlexAddress@YYYYYYYY' not activated; chassis
ID='XXXXXXXX'
```

機能カードが取り外され、非 FlexAddress カードが取り付けられるとどうなりますか？

カードのアクティブ化や変更はいずれも行われません。カードは CMC によって無視されます。この場合、**$racadm featurecard -s** コマンドが次のメッセージを返します。

```
No feature card inserted
```

```
ERROR: can't open file
```

シャーシのサービスタグが再プログラムされた場合、そのシャーシにバインドされている機能カードはどうなりますか？

- そのシャーシ、または他のシャーシのアクティブな CMC に元の機能カードが存在する場合、ウェブインタフェースが次のエラーメッセージを表示します。

  ```
  This feature card was activated with a different chassis. It must be
  removed before accessing the FlexAddress feature.
  ```

  ```
  Current Chassis Service Tag = XXXXXXXX
  ```

  ```
  Feature Card Chassis Service Tag = YYYYYYYY
  ```

  デルサービスが元のシャーシサービスタグの再プログラムを行ってシャーシに戻し、そのシャーシで元の機能カードを持つ CMC がアクティブ化されない限り、元の機能カードはそのシャーシ、または他のどのシャーシでも非アクティブ化の対象にはならなくなります。
- FlexAddress 機能は本来バインドされていたシャーシでアクティブ状態が維持されます。そのシャーシ機能の*バインディング*は、新規サービスタグを反映するようにアップデートされます。

2 つの機能カードが冗長 CMC システムに取り付けられた場合、エラーメッセージが表示されますか?

いいえ、エラーメッセージは表示されません。アクティブ CMC の機能カードがアクティブで、シャーシに取り付けられます。2 番目のカードは CMC によって無視されます。

SD カードには、書き込み防止ロック機能はありますか？

はい、あります。SD カードを CMC モジュールにインストールする前に、書き込み防止ラッチがアンロックの位置にあることを確認してください。SD カードが書き込み防止されていると、FlexAddress 機能をアクティブ化することはできません。この場合、**$racadm feature -s** コマンドが次のメッセージを返します。

```
No features active on the chassis. ERROR: read only file system
```

アクティブな CMC モジュールに SD カードが存在しなければ、どうなりますか？

$racadm featurecard -s コマンドを実行すると、次のメッセージが返されます。

```
No feature card inserted.
```

サーバー BIOS のバージョンがバージョン 1.xx から 2.xx にアップデートされると FlexAddress 機能はどうなりますか？

サーバーモジュールは、FlexAddress と併用する前に電源を切る必要があります。サーバー BIOS アップデートの完了後、サーバーモジュールはサーバーがパワーサイクルされるまでシャーシ割り当てのアドレスを取得しません。

単一の CMC を持つシャーシが、バージョン 1.10 以前のファームウェアにダウングレードされるとどうなりますか？

- FlexAddress 機能と設定は、シャーシから削除されます。
- シャーシでこの機能をアクティブ化するために使用された機能カードは変更されず、シャーシにバインドされたままになります。このシャーシの CMC ファームウェアがこの後 1.10 以降にアップグレードされると、元の機能カードの再挿入（必要な場合）、CMC のリセット（ファームウェアアップグレード完了後に機能カードが挿入された場合）、および機能の再設定を行うことによって FlexAddress 機能が再アクティブ化されます。

冗長 CMC を持つシャーシで、1 つの CMC ユニットを 1.10 以前のファームウェアを持つ CMC に交換するとどうなりますか?

冗長 CMC を持つシャーシで、CMC がバージョン 1.10 以前のファームウェアを持つ CMC に交換された場合は、次の手順に従って、現在の FlexAddress 機能と設定が削除されないようにする必要があります。

- アクティブな CMC ファームウェアのバージョンは、常に 1.10 以降であるようにしてください。
- スタンバイ CMC を取り外し、その代わりに新しい CMC を取り付けます。
- アクティブ CMC から、スタンバイ CMC のファームウェアをバージョン 1.10 以降にアップグレードします。

メモ: スタンバイ CMC ファームウェアが 1.10 以降にアップデートされず、フェイルオーバーが発生すると、FlexAddress 機能は設定されません。この機能は再アクティブ化して、再設定する必要があります。

FlexAddress で deactivation コマンドが実行されたときにシャーシに SD カードがなかった場合、どのように SD カードを回復できますか?

問題は、FlexAddress が無効化されたときに SD カードが CMC になかった場合、別のシャーシに FlexAddress をインストールするためにそのカードを使用できないということです。カードを使用できるように回復するには、バインドされているシャーシの CMC にそのカードを挿入し直し、FlexAddress を再インストールして、その後 FlexAddress を再度非アクティブ化します。

SD カードが正しく取り付けられ、ファームウェアまたはソフトウェアのアップデートもすべてインストール済みです。FlexAddress がアクティブですが、サーバー導入画面に導入オプションが表示されません。何が間違っていますか?

これは、ブラウザのキャッシュの問題です。ブラウザを一度閉じてから、再度開いてください。

RACADM コマンド racresetcfg を使用してシャーシ設定をリセットする必要がある場合、FlexAddress はどうなりますか?

FlexAddress 機能は引き続きアクティブ状態で使用可能です。すべてのファブリックとスロットがデフォルトとして選択されています。

メモ: RACADM コマンド `racresetcfg` を発行する前に、シャーシの電源を切ることを強くお勧めします。

FlexAddressPlus 機能のみを無効にした後（FlexAddress はアクティブのまま）、まだアクティブな CMC 上で racadm setflexaddr コマンドが失敗するのはなぜですか?

FlexAddressPlus 機能カードがカードスロットに入ったままで、後から CMC がアクティブ化されると、FlexAddressPlus 機能が再アクティブ化され、スロットまたはファブリックの FlexAddress 設定の変更を再開できます。

iKVM

前面パネルに接続されているモニタに「CMC コントロールによってユーザーが無効化されました」というメッセージが表示されます。なぜですか?

前面パネル接続が CMC によって無効化されています。CMC ウェブインタフェースまたは RACADM のいずれかを使用して前面パネルを有効化します。

CMC ウェブインタフェースを使用して前面パネルを有効化するには、**iKVM → セットアップ** タブと進み、**前面パネル USB/ ビデオ有効** オプションを選択して、**適用** をクリックして設定を保存します。

RACADM を使用して前面パネルを有効化するには、CMC へのシリアル /Telnet/SSH テキストコンソールを開き、ログインして次を入力します。

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

背面パネルアクセスが機能しません。なぜですか?

前面パネルの設定が CMC によって有効になり、現在前面パネルにモニタが接続されています。

接続は一度に 1 接続のみが可能です。ACI および背面パネルよりも前面パネル接続が優先されます。接続の優先順位についての詳細は、「iKVM 接続優先順位」を参照してください。

背面パネルに接続されているモニタに、「現在別のアプライアンスが階層化されているため、ユーザーが無効になりました」というメッセージが表示されます。

ネットワークケーブルが iKVM の ACI ポートコネクタとセカンダリ KVM アプライアンスに接続しています。

接続は一度に 1 接続のみが可能です。背面パネルモニタ接続よりも ACI 階層型接続が優先されます。優先順位は、前面パネル、ACI、次に背面パネルとなります。

iKVM の橙色の LED が点滅しています。なぜですか?

次の 3 つの原因が考えられます。

- iKVM の再プログラムが必要な **iKVM の問題がある。** この問題を修正するには、iKVM ファームウェアのアップデート手順に従ってください。
- **iKVM が CMC コンソールインタフェースを再プログラムしている。** この場合、CMC コンソールは一時的に使用できなくなり、OSCAR インタフェースで黄色の丸で示されます。この処理には最大 15 分かかります。
- **iKVM ファームウェアがハードウェアエラーを検出した。** 詳細については、iKVM 状態を表示してください。

使用している iKVM は ACI ポートから外部 KVM スイッチまで階層化されていますが、ACI 接続のすべてのエントリが使用不可です。

OSCAR インタフェースで状態のすべてに黄色のドットが表示されます。

前面パネル接続が有効化され、モニタが接続されています。その他すべての iKVM 接続よりも前面パネルが優先されるため、ACI および背面パネル接続は無効化されます。

ACI ポート接続を有効にするには、まず最初に前面パネルアクセスを無効化するか、前面パネルに接続されているモニタを取り外します。外部 KVM スイッチの OSCAR エントリがアクティブおよびアクセス可能になります。

ウェブインタフェースを使用して前面パネルを無効化するには、**iKVM → セットアップ** タブに進み、**前面パネル USB/ ビデオ有効** オプションをクリアして適用をクリックします。

RACADM を使用して前面パネルを無効化するには、CMC へのシリアル /Telnet/SSH テキストコンソールを開き、ログインして次を入力します。

racadm config -g cfgKVMInfo -o cfgKVMFrontPanelEnable 0

OSCAR メニューで、Dell CMC 接続に赤い X が表示され、CMC に接続できません。なぜですか?

次の 2 つの原因が考えられます。

- **Dell CMC コンソールが無効化されている。** この場合、CMC ウェブインタフェースまたは RACADM のいずれかを使用して有効化します。
- **初期化中、スタンバイ CMC への切り替え中、または再プログラム中であるため CMC が使用不可。** この場合は、CMC の初期化が終了するまで待機してください。

サーバーのスロット名が OSCAR で「初期化中」と表示され、選択できません。なぜですか?

サーバーが初期化中か、そのサーバーの iDRAC が初期化に失敗したかのどちらかです。

まず、60 秒間待ってください。サーバーが引き続き初期化中の場合は、初期化完了直後にスロット名が表示され、サーバーも選択可能になります。

60 秒後、OSCAR にスロットが初期化中であることが引き続き表示される場合は、シャーシ内のサーバーを取り外して再び挿入します。この処置により、iDRAC が初期化されます。

IOM

設定変更後、CMC に IP アドレスが 0.0.0.0 と表示されることがあります。

更新 アイコンをクリックして、IP アドレスがスイッチで正しく設定されているかどうかを確認します。IP/ マスク / ゲートウェイの設定でエラーがあった場合、スイッチは IP アドレスを設定せず、すべてのフィールドで 0.0.0.0 を返します。

一般的なエラーには、次が含まれます。

- 帯域外 IP アドレスを帯域内管理 IP アドレスと同じ IP アドレス、または同じネットワーク上のアドレスに設定。
- 無効なサブネットマスクを入力。
- デフォルトゲートウェイ を、スイッチに直接接続されているネットワークにないアドレスに設定。

IOM ネットワーク設定の詳細については、**dell.com/support/manuals** で、『*Dell PowerConnect M6220 スイッチ重要情報*』マニュアル、および『*Dell PowerConnect 6220 シリーズポートアグリゲータホワイトペーパー*』を参照してください。

シングルサインオン

CMC のセットアップはシングルサインオン（SSO）を許可しますが、ブラウザには空白ページが表示されます。

現時点では、SSO には Mozilla Firefox および Internet Explorer ブラウザのみがサポートされています。正しいセットアップになっているようにブラウザ設定をチェックしてください。詳細は、「SSO ログインのためのブラウザの設定」の項を参照してください。

ブラウザが正しく設定されている場合は、両方のブラウザで、名前およびパスワードを入力しなくてもログインすることができます。CMC には完全修飾ドメイン名（FQDN）を使用してください。たとえば、ブラウザのアドレスバーに **myCMC.Domain.ext/** と入力します。ブラウザは、**https**（セキュアモード）にリダイレクトし、CMC にログインすることを可能にします。ブラウザでは **http** および **https** の両方が有効です。URL をブックマークとして保存すれば、例にあるフォワードスラッシュ以降は何も入力する必要がありません。引き続き SSO を使ってログインできない場合は、「Active Directory ユーザーに対する CMC SSO またはスマートカードログインの設定」の項を参照してください。

19

使用事例シナリオ

本項は、本ガイドの特定の項に移動して、典型的な使用事例のシナリオを実行するために役立ちます。

シャーシの基本設定とファームウェアアップデート

このシナリオは、以下のタスクを実行するガイドとなります。

- 基本設定でのシャーシの起動。
- CMC によってハードウェアがエラーを伴わずに検出されていることの検証。
- CMC、IOM、およびサーバーコンポーネントのファームウェアのアップデート。

1. CMC はシャーシに事前に取り付けられているため、取り付けは必要ありません。2 台目の CMC を取り付けて、アクティブ CMC のスタンバイとして使用できます。
   2 台目の CMC の取り付けに関する情報は、「冗長 CMC 環境について」の項を参照してください。
2. 「シャーシセットアップのチェックリスト」で説明されている手順を使用したシャーシのセットアップ。
3. LCD パネルまたは Dell CMC シリアルコンソールを使用した CMC 管理 IP アドレスおよび CMC ネットワークの設定。
   この情報については、「初期 CMC ネットワークの設定」の項を参照してください。
4. ログ作成のためのログとアラートの設定、および管理下システムで発生する特定のイベントのためのアラートの設定。
   この情報については、「アラートを送信するための CMC の設定」の項を参照してください。
5. CMC ウェブインタフェースを使用したサーバーの IP アドレスおよびネットワークの設定。
   この情報については、「サーバーの設定」を参照してください。
6. CMC ウェブインタフェースを使用した IOM の IP アドレスおよびネットワークの設定。
   詳細については、「IOM 用ネットワークの設定」の項を参照してください。
7. サーバーへの電源投入。
8. 無効なハードウェア設定のためのハードウェアログ、CMC ログ、E-メールまたは SNMP トラップアラートのチェック。
   詳細については、「イベントログの表示」の項を参照してください。
9. ハードウェア関連の問題を診断するには、**診断コンソール** を使用します。
   診断コンソール の使用に関する詳細については、「診断コンソールの使用」の項を参照してください。
10. ハードウェア設定問題におけるエラーについての情報は、**dell.com/support/manuals** にある『Dell イベントメッセージリファレンスガイド』または『Server Administrator メッセージリファレンスガイド』を参照してください。
11. CMC、IOM、およびサーバーコンポーネントのファームウェアのアップデート。
    この情報については、「ファームウェアのアップデート」の項を参照してください。

CMC 設定およびサーバー設定のバックアップ

1. シャーシ設定をバックアップするには、「シャーシ設定の保存または復元」の項を参照してください。
2. サーバーの設定を保存するには、CMC の **サーバークローニング** 機能を使用します。
   この情報については 「サーバークローンを使用したプロファイル設定の実行」 を参照してください。
3. CMC ウェブインタフェースを使って、サーバーの既存の設定を外部ストレージカードに保存します。
   この情報については 「プロファイルの追加または保存」の項を参照してください。
4. CMC ウェブインタフェースを使用して、外部ストレージカードに保存された設定を必要なサーバーに適用します。
   この情報については 「プロファイルの適用」の項を参照してください。

サーバーのダウンタイムを伴わない管理コンソールのファームウェアのアップデート

CMC、iDRAC、Lifecycle Controller の管理コンソールのファームウェアは、サーバーのダウンタイムを伴わずにアップデートすることができます。

1. プライマリおよびスタンバイ CMC の両方が存在するシナリオでは、サーバーまたは IOM のダウンタイムを伴わずに CMC ファームウェアをアップデートすることができます。
2. プライマリ CMC 上のファームウェアをアップデートするには、「ファームウェアのアップデート」の項を参照してください。
   プライマリ CMC でファームウェアをアップデートする場合、スタンバイ CMC がプライマリ CMC の役割を引き継ぐことから、IOM およびサーバーのダウンタイムが発生しません。

   メモ: ファームウェアアップデートプロセスは、IOM および iDRAC サーバーの管理コンソールのみに影響します。サーバーと IOM 間の外部接続には影響しません。
3. シャーシのダウンタイムを伴わずに iDRAC または Lifecycle Controller のファームウェアをアップデートするには、Lifecycle Controller サービスを使ってアップデートを実行します。Lifecycle Controller を使用したサーバーコンポーネントファームウェアのアップデートに関する詳細については、「サーバーコンポーネントファームウェアのアップグレード」の項を参照してください。

   メモ: メザニンカード、NDC コントローラ、BIOS などのその他のコンポーネントのアップデート中は、サーバーのダウンタイムが発生します。