Dell Chassis Management Controller Version 3.3 for Dell EMC PowerEdge VRTX

ユーザーズガイド

July 2020
Rev. A00

DELL EMC

メモ、注意、警告

メモ: 製品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、その危険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。

目次

1

概要

Dell Chassis Management Controller (CMC) for Dell EMC PowerEdge VRTX は、**PowerEdge VRTX** 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。CMC には独自のマイクロプロセッサとメモリがあり、差し込まれたモジュラーシャーシによって電源供給されます。

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
- シャーシおよびサーバーのリモートでの電源オン / オフ
- サーバーモジュール内のサーバーおよびコンポーネントでのイベントアラートの有効化
- VRTX シャーシ内のストレージコントローラとハードディスクドライブの表示と管理
- VRTX シャーシ内の PCIe サブシステムの管理
- シャーシ内の iDRAC と I/O モジュールに 1 対多の管理インタフェースを提供

PowerEdge VRTX 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。次に示すように、電源および温度の管理は 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 はシステムの電力要件を監視し、オプションの動的電源供給 (DPSE) モードをサポートします。このモードは、サーバーがスタンバイモードである間に電源装置を設定し、負荷および冗長性要件を動的に管理することによって、CMC が電力効率を改善することを可能にします。
  - 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、オプションのエンクロージャ最大電力制限 (システム入力電力上限) をサポートしています。この機能は警告を行い、エンクロージャが定義された最大電力制限値未満を維持するように、サーバーの電力消費量を制限したり、新しいサーバーの電源投入を妨げるなどの処置を実行します。
  - CMC は冷却ファンと送風装置を監視し、それらの動作を実際の周囲温度と内部温度の測定値に基づいて自動的に制御します。
  - 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。
  - Dell PowerEdge VRTX 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 スイッチおよび iDRAC ネットワーク設定。
  - サーバーモジュールにおける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。
  - ストレージコントローラ用のフォールトトレラントモードを含むストレージコンポーネント
  - PCIe スロット。

温度、ハードウェアの誤った構成、停電、ファン速度、送風装置などの警告やエラーについて E-メールアラートや 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。

トピック：

本リリースの新機能

Dell EMC PowerEdge VRTX 向け CMC の本リリースは以下をサポートしています。

- iDRAC ネットワーク パラメーターを設定するシャーシ プロファイルの拡張。
- RACADM インターフェイスを使用したサーバー プロファイルの適用。
- オープンソースのセキュリティ脆弱性への対処。

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。
- ローカルユーザー、Active Directory、および LDAP のログイン管理と設定。
- ECM (拡張冷却モード) やファンオフセットなどの高度な冷却オプションを有効にして冷却効果を高め、パフォーマンスを改善。
- SNMP、ウェブインタフェース、KVM、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シャーシ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、サーバー上の iDRAC、シャーシインフラストラクチャ、およびシャーシストレージのファームウェアアップデートが可能。
- Lifecycle Controller を使用したシャーシ内の複数サーバーにおける、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のファームウェアアップデート。
- Dell OpenManage ソフトウェア統合 — Dell OpenManage Server Administrator または OpenManage Essentials (OME) 1.2 からの CMC ウェブインタフェースの起動が可能。
- CMC アラート — リモート Syslog E-メールメッセージまたは SNMP トラップを使って管理下ノードに関する潜在的な問題を通知。
- リモート電源管理 — 管理コンソールからのシャーシコンポーネントの電源オフやリセットなどのリモート電源管理機能を提供。
- 電源使用率の報告。
- Secure Sockets Layer (SSL) 暗号化 — ウェブインタフェースを介した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する、工場割り当て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) アドレスのシャーシ割り当て WWN/MAC アドレスへの置き換え
- 拡張 WWN/MAC アドレスインベントリに対する iDRAC I/O アイデンティティ機能のサポート。
- 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。
- 最大 8 つまでのシャーシをリードシャーシから監視できるマルチシャーシ管理。
- シャーシ上のストレージコンポーネントの設定。
- サーバーおよびそれらの識別情報への PCIe スロットのマッピング。

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たユーザー ID およびパスワードの設定。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

この図は、CMC コネクタを示しています。

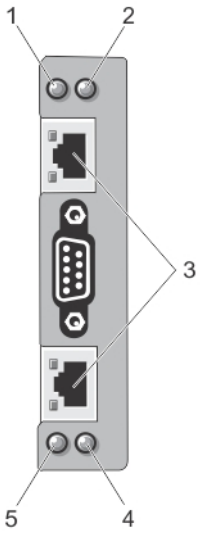


図 1. CMC コネクタおよび LED

表 1. CMC コネクタおよび LED

アイテム	インジケータ、ボタン、またはコネクタ
1	ステータス / 識別インジケータ（CMC 1）
2	電源インジケータ（CMC 1）
3	CMC コネクタポート（2）
4	電源インジケータ（CMC 2）
5	ステータス / 識別インジケータ（CMC 2）

次に、シャーシの背面パネル図と、CMC で利用できる部品およびデバイスを記した表を示します。

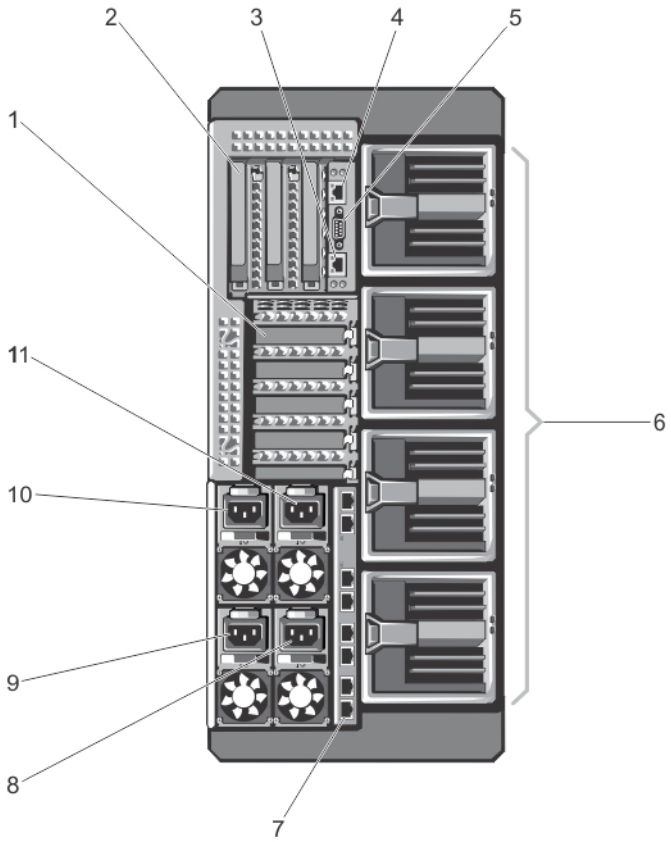


図 2. CMC の背面パネル

表 2. CMC の背面パネル - 部品

アイテム	インジケータ、ボタン、またはコネクタ
1	PCIe 拡張カードスロットロープロファイル（5）
2	PCIe 拡張カードスロットフルハイト（3）
3	CMC GB Ethernet ポート（CMC-2）
4	CMC GB Ethernet ポート（CMC-1）
5	シリアルコネクタ
6	送風機モジュール（4）
7	I/O モジュールポート
8	PSU 4
9	PSU 3
10	PSU 1
11	PSU 2

次に、シャーシの前面パネル図と、CMC で利用できる部品およびデバイスを記した表を示します。

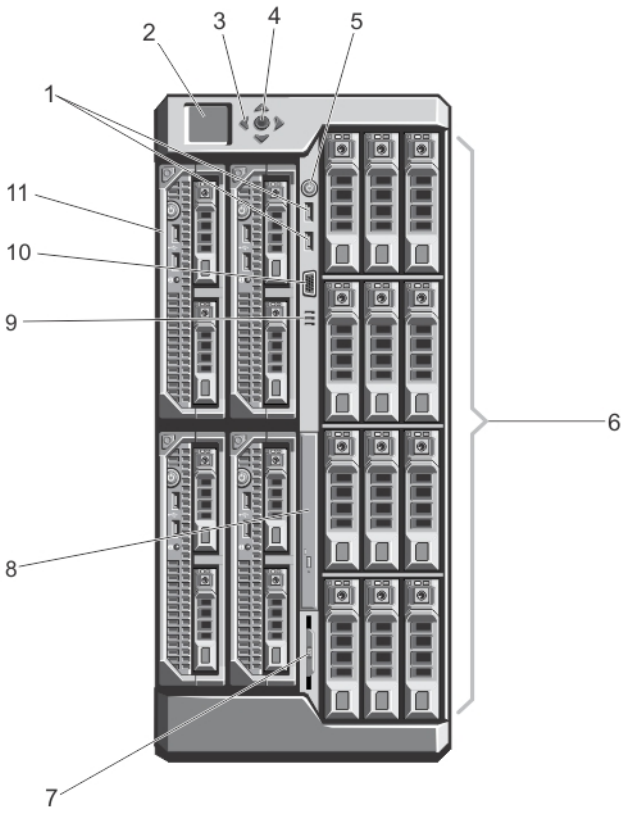


図 3. 前面パネルの機能とインジケータ - 3.5 インチハードディスクドライブシャーシ

表 3. 前面パネル - 機能とインジケータ

アイテム	インジケータ、ボタン、またはコネクタ	説明
1	USB コネクタ (2)	キーボードとマウスをシステムに接続することができます。
2	LCD パネル	システムが正常に動作しているとき、またはシステムに注意が必要なときを示すシステム情報、状態、およびエラーメッセージが表示されます。
3	LCD メニュースクロールボタン (4)	カーソルを 1 段ずつ移動させます。
4	選択 (「チェック」) ボタン	LCD 画面上のアイテムを選択して保存し、次の画面に移動します。
5	エンクロージャ電源インジケータ、電源ボタン	電源オンインジケータは、エンクロージャに電源が入っているときに点灯します。電源ボタンによってシステムへの PSU 出力を制御します。
6	ハードディスクドライブ (HDD)	**2.5 インチハードドライブエンクロージャ** 最大 25 台のホットスワップ対応 2.5 インチハードディスクドライブ。 **3.5 インチハードディスクドライブエンクロージャ** 最大 12 台のホットスワップ対応 3.5 インチハードディスクドライブ。
7	情報タグ	サービスタグ、NIC、MAC アドレス、システムの電力定格、および世界各国の規制機関マークなどのシステム情報を記録することができる、引き出し式のラベルパネル。
8	オプティカルドライブ(オプション)	オプションの SATA DVD-ROM ドライブまたは DVD+/-RW ドライブ 1 台。
9	通気孔	温度センサーの通気孔。 **メモ: 適切な冷却を確保するため、通気孔がふさがれていないことを確認してください。**
10	ビデオコネクタ	モニターをシステムに接続することができます。

表 3. 前面パネル - 機能とインジケータ（続き）

アイテム	インジケータ、ボタン、またはコネクタ	説明
11	サーバーモジュール	エンクロージャ用に設定された、最大 4 台の PowerEdge M520、M620、M630、または M640 サーバーモジュール、または最大 2 台の M820 サーバーモジュール。

CMC の必要最低バージョン

次の表には、リストされたサーバーモジュールを有効に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. サーバーモジュール用 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 M520	CMC 1.36
PowerEdge M620	CMC 1.36
PowerEdge M820	CMC 1.36
PowerEdge M630	CMC 2.00
PowerEdge M830	CMC 2.00
PowerEdge M640	CMC 3.00

次の表には、リストされた I/O モジュールを有効に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 5. I/O モジュール用 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
R1 VRTX 1Gb パススルー	CMC 1.20
R1-2401 VRTX 10GbE スイッチ	CMC 1.20
R1-2210 VRTX 10Gb スイッチ	CMC 2.00

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の専用ネットワークインタフェース。 • 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 I/O モジュール へのバイナリプロトコルによる通信を行うため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。 • アクティブ CMC のみへのアクセスを提供。

対応プラットフォーム

CMC は、PowerEdge VRTX プラットフォーム用に設計されたモジュラー型サーバーをサポートしています。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** にある『*Dell Chassis Management Controller（CMC）for Dell PowerEdge VRTX バージョン 3.3 リリース ノート*』を参照してください。

対応 Web ブラウザー

次の Web ブラウザーが Dell PowerEdge VRTX 用にサポートされています。

- Microsoft Internet Explorer 11
- Microsoft EDGE
- Safari バージョン 10.1.2
- Safari バージョン 11.1.2
- Mozilla Firefox 61
- Mozilla Firefox 62
- Google Chrome 68
- Google Chrome 69

メモ: このリリースでは、デフォルトで TLS 1.1 および TLS 1.2 がサポートされます。ただし、TLS 1.0 を有効にするには、次の racadm コマンドを使用します。

```
$ racadm config -g cfgRacTuning -o cfgRacTuneTLSProtocolVersionEnable TLSv1.0+
```

ライセンスの管理

CMC 機能は、購入したライセンス（CMC Express または CMC Enterprise）に基づいて使用可能になります。CMC を設定または使用できるインタフェースでは、ライセンス許諾された機能のみが使用可能です。たとえば、CMC ウェブインタフェース、RACADM、WS-MAN などです。CMC ライセンス管理およびファームウェアアップデート機能は常に、CMC ウェブインタフェースおよび RACADM を介して使用できます。

ライセンスのタイプ

提供されるライセンスには次のタイプがあります。

- 30 日間の評価および延長 - このライセンスは 30 日後に失効しますが、期限を 30 日間延長することもできます。評価ライセンスは継続時間ベースであり、電力がシステムに供給されているときにタイマーが稼動します。
- 永続 — サービスタグにバインドされたライセンスで、永続的です。

ライセンスの取得

次のいずれかの方法を使用して、ライセンスを取得できます。

- E-メール — テクニカルサポートセンターにライセンスを要求すると、ライセンスが添付された E-メールが送付されます。
- セルフサービスポータル — CMC から、セルフサービスポータルへのリンクを利用できます。このリンクをクリックして、ライセンスを購入できるインターネット上のライセンスセルフサービスポータルを開きます。詳細については、セルフサービスポータルページのオンラインヘルプを参照してください。
- 販売時 — システムの発注時にライセンスを取得します。

ライセンス操作

ライセンス管理の作業を実行する前に、ライセンスを取得しておく必要があります。詳細については、support.dell.com にある『概要および機能ガイド』を参照してください。

一対一のライセンス管理には CMC、RACADM、および WS-MAN を、一対多のライセンス管理には Dell License Manager を使用して、次のライセンス操作を実行できます。

メモ: **すべてのライセンスが事前にインストールされているシステムを購入した場合、ライセンス管理は必要ありません。**

- 表示 — 現在のライセンス情報を表示します。
- インポート — ライセンスの取得後、ライセンスをローカルストレージに保存し、サポートされているいずれかのインタフェースを使用して CMC にインポートします。検証チェックに合格すれば、ライセンスがインポートされます。

  メモ: **一部の機能では、機能の有効化に CMC の再起動が必要になります。**
- エクスポート — バックアップ目的、またはサービス部品交換後の再インストールのために、インストールされているライセンスを外部ストレージデバイスにエクスポートします。エクスポートされたライセンスのファイル名と形式は <EntitlementID>.xml になります。
- 削除 — コンポーネントが欠落している場合に、そのコンポーネントに割り当てられているライセンスを削除します。ライセンスが削除されると、そのライセンスは CMC に保存されず、基本的な製品機能が有効になります。
- 置き換え — 評価ライセンスの有効期限を延長したり、評価ライセンスなどのライセンスタイプを購入ライセンスに変更したり、有効期限の切れたライセンスを延長するために、ライセンスを置換します。
- 評価ライセンスは、アップグレードされた評価ライセンスまたは購入したライセンスと置換できます。
- 購入したライセンスは、アップデートされたライセンス、またはアップグレードされたライセンスと置き換えることができます。ライセンスについての詳細は、デルソフトウェアライセンス管理ポータルをクリックしてください。
- 詳細表示 — インストールされているライセンス、またはサーバーにインストールされているコンポーネントに使用可能なライセンスの詳細を表示します。

  メモ: **詳細オプションが正しいページを表示するため、セキュリティ設定の信頼済みサイトのリストに *.dell.com が追加されているようにしてください。詳細については、Internet Explorer のヘルプマニュアルを参照してください。**

ライセンスコンポーネントの状態または状況と使用可能な操作

次の表は、ライセンスの状態または状況に基づいて使用できるライセンス操作をリストしています。

表 7. 状態および状況に基づいたライセンス操作

ライセンス / コンポーネントの状態または状況	インポート	エクスポート	削除	置き換え	もっと詳しく知る
非システム管理者ログイン	無	有	無	無	有
アクティブなライセンス	有	有	有	有	有
期限切れのライセンス	無	有	有	有	有
ランセンスがインストールされているが、コンポーネントが欠落している	無	有	有	無	有

CMC ウェブインタフェースを使用したライセンスの管理

CMC ウェブインタフェースを使用してライセンスを管理するには、**シャーシ概要** > **セットアップ** > **ライセンス** と移動します。

ライセンスをインポートする前に、ローカルシステムまたは CMC がアクセス可能なネットワーク共有上に有効なライセンスファイルを保存しておくようにしてください。ライセンスは組み込まれているか、**セルフサービスウェブポータル** またはライセンスキー管理ツールからメールで送信されています。

ライセンス ページに、デバイスに関連付けられたライセンス、またはインストールされているもののデバイスがシステムに存在しないライセンスが表示されます。ライセンスのインポート、エクスポート、削除、または交換の詳細については、『オンラインヘルプ』を参照してください。

RACADM を使用したライセンスの管理

RACADM コマンドを使用してライセンスを管理するには、次のライセンス サブコマンドを使用します。

```
racadm license <ライセンスコマンドタイプ>
```

RACADM コマンドの詳細については、dell.com/support/Manuals にある『Chassis Management Controller for PowerEdge VRTX 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 におけるライセンス取得可能な機能

お持ちのライセンスに基づいて有効化されている CMC 機能のリストがこの表に示されます。

表 8. ライセンス取得可能な機能

機能	Express	Enterprise	メモ
CMC ネットワーク	有	有	
CMC シリアル ポート	有	有	
RACADM (SSH、ローカル、および リモート)	有	有	
CMC セットアップのバックアップ	無	有	
CMC セットアップの復元	有	有	
WS-MAN	有	有	
snmp	有	有	
Telnet	有	有	
SSH	有	有	
ウェブベースのインタフェース	有	有	
E-メール アラート	有	有	
LCD 導入	有	有	
拡張 iDRAC 管理	有	有	
リモート Syslog	無	有	
ディレクトリ サービス	なし*	有	*デフォルト以外のディレクトリ サービス設定の場合、Express ライセンスで許可されるのはディレクトリ サービスのリセットのみです。ディレクトリ サービスのリセットは、ディレクトリ サービスを工場出荷時のデフォルトに設定します。
iDRAC シングル サイン オン	無	有	
2 要素認証	無	有	
PK 認証	無	有	
リモート ファイル共有	有	有	

表 8. ライセンス取得可能な機能（続き）

機能	Express	Enterprise	メモ
スロットリソース管理	無	有	
エンクロージャレベルの電力制限	なし*	有	*デフォルト以外の電力制限設定の場合、Express ライセンスで許可されるのは電力制限の復元のみです。電力制限の復元は、電力制限設定を工場出荷時のデフォルトにリセットします。
動的電源供給	なし*	有	*デフォルト以外の DPSE 設定の場合、Express ライセンスで許可されるのは DPSE の復元のみです。DPSE の復元は、DPSE を工場出荷時のデフォルトにリセットします。
Multi-chassis management（マルチシャーシ管理）	無	有	
詳細設定	無	有	
エンクロージャレベルのバックアップ	無	有	
FlexAddress の有効化	なし*	有	*デフォルト以外の FlexAddress 設定の場合、Express ライセンスで許可されるのはデフォルトの復元のみです。デフォルトの復元は、FlexAddress 設定を工場出荷時のデフォルトにリセットします。
PCIe アダプタマッピング	はい*	有	*Express ライセンスでは、サーバー 1 台につき最大 2 台の PCIe アダプタを割り当てることができます。
仮想アダプタからスロットへのマッピング	なし*	有	*デフォルト以外の仮想アダプタマッピングの場合、Express ライセンスで許可されるのはデフォルトマッピングのみです。デフォルトの復元は、仮想アダプタのマッピングを工場出荷時のデフォルトに変更します。
仮想アダプタとスロットのマッピング解除	有	有	
サーバークローニング	無	有	
1 対多のサーバーファームウェアアップデート	無	有	
iDRAC の 1 対多設定	無	有	
起動 ID	無	有	
シャーシプロファイル	無	有	
簡易展開	無	有	

他言語の CMC ウェブインタフェースの表示

他言語の CMC ウェブインタフェースを表示するには、ウェブブラウザのマニュアルをお読みください。

対応管理コンソールアプリケーション

CMC は、Dell OpenManage コンソールとの統合をサポートします。詳細については、**dell.com/support/manuals** にある OpenManage コンソールのマニュアルを参照してください。

本ガイドの使用方法

本ユーザーズガイドの記載内容は、次を使用したタスクの実行を可能にします。

- Web インターフェイス：本書では、タスクに関連した情報のみが提供されます。各種フィールドやオプションの詳細については、Web インターフェイスから開くことができる、*CMC for Dell PowerEdge VRTX のオンライン ヘルプ*を参照してください。
- RACADM コマンド：本書では、使用する必要のある RACADM コマンドまたはオブジェクトが提供されます。RACADM コマンドの詳細については、**dell.com/cmcmanuals** にある『*Chassis Management Controller for PowerEdge VRTX 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。

その他の必要マニュアル

Dell サポート サイトから文書にアクセスするには、次の手順を実行します。このリファレンスガイドと合わせて、**dell.com/support/manuals** で利用できる次のガイドにアクセスすることができます。

- *VRTX CMC のオンライン ヘルプ*で、Web インターフェイスの使用方法について説明しています。オンライン ヘルプにアクセスするには、CMC Web インターフェイスで [**ヘルプ**] をクリックしてください。
- 『*Chassis Management Controller for Dell PowerEdge VRTX RACADM バージョン 3.3 コマンド ライン リファレンス ガイド*』には、VRTX 関連の RACADM 機能の使用に関する情報が記載されています。
- **dell.com/cmcmanuals** の『*Dell Chassis Management Controller (CMC) for Dell PowerEdge VRTX バージョン 3.3 リリース ノート*』には、システムやマニュアルに加えられたアップデートの最新情報、または専門知識をお持ちのユーザーや技術者のための高度な技術情報が記載されています。
- 『*Integrated Dell Remote Access Controller (iDRAC) ユーザーズガイド*』には、管理下システムでの iDRAC の取り付け、設定、および管理に関する情報が記載されています。
- 『*Dell PowerEdge VRTX ストレージサブシステム互換性マトリックス*』には、PowerEdge VRTX ストレージサブシステムのベースラインリリースについての情報が記載されています。このマニュアルは **dell.com/support/manuals** からオンラインで入手できます。
- 『*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 OpenManage SNMP for iDRAC and Chassis Management Controller リファレンスガイド*』は、SNMP MIB についての情報を提供します。
- 『*Dell Update Packages ユーザーズガイド*』には、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が記載されています。
- 『*Dell Shared PowerEdge RAID Controller (PERC) 8 ユーザーズ ガイド*』には、Shared PERC8 カードの導入、およびストレージ サブシステムの管理についての情報が記載されています。この文書は **dell.com/storagecontrollermanuals** からオンラインで入手できます。
- Dell システム管理アプリケーションのマニュアルでは、システム管理ソフトウェアのインストール方法と使い方を説明しています。

また、次のシステムマニュアルは、VRTX CMC がインストールされているシステムに関する追加情報を提供します。

- 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** にある法令遵守に関するホーム 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。
- システムに同梱されている『Dell PowerEdge VRTX はじめに』には、システム機能の概要、システムの設定、および技術仕様が記載されています。
- システムに同梱のセットアッププレースマットには、初期のシステムセットアップおよび設定の情報が記載されています。
- サーバーモジュールの『*オーナーズマニュアル*』には、サーバーモジュールの機能に関する情報が記載されており、サーバーモジュールのトラブルシューティング方法およびサーバーモジュールのコンポーネントの取り付けまたは交換方法が説明されています。このマニュアルは、**dell.com/poweredgemanuals** からオンラインで使用できます。
- ラックソリューションに付属のマニュアルでは、システムをラックに取り付ける方法について説明しています (必要な場合)。
- 本書で使用されている略語や頭字語の正式名については、**dell.com/support/manuals** で『用語集』を参照してください。
- 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。
- システムに付属のメディアには、OS、システム管理ソフトウェア、システムアップデート、およびシステムと同時に購入されたシステムコンポーネントに関するものを含め、システムの設定と管理用のマニュアルとツールが収録されています。システムの詳細については、システム上、およびシステムに同梱のシステム セットアップ プレースマットにあるクイック リソース ロケーター(QRL) をスキャンしてください。お使いのモバイルプラットフォームから QRL アプリケーションをダウンロードして、モバイルデバイス上でアプリケーションを有効化します。

Dell EMC サポートサイトからのドキュメントへのアクセス

必要なドキュメントにアクセスするには、次のいずれかの方法で行います。

- 次のリンクを使用します。
  - Dell EMC エンタープライズ システム管理、Dell EMC リモート エンタープライズ システム管理、および Dell EMC 仮想化ソリューションのマニュアル — https://www.dell.com/esmmanuals
  - Dell EMC OpenManage マニュアル — https://www.dell.com/openmanagemanuals
  - iDRAC マニュアル — https://www.dell.com/idracmanuals
  - Dell EMC OpenManage Connections エンタープライズ システム管理マニュアル — https://www.dell.com/OMConnectionsEnterpriseSystemsManagement
  - Dell EMC Serviceability Tools マニュアル — https://www.dell.com/serviceabilitytools
- Dell EMC サポート サイトからアクセスします。
  1. https://www.dell.com/support にアクセスします。
  2. [**すべての製品の参照**] をクリックします。
  3. [**すべての製品**] ページで [**ソフトウェア**] をクリックして、次の中から必要なリンクをクリックします。
     - **分析**
     - **クライアントシステム管理**
     - **エンタープライズアプリケーション**
     - **エンタープライズシステム管理**
     - **メインフレーム**
     - **オペレーティングシステム**
     - **公共機関向けソリューション**
     - **Serviceability Tools**
     - **サポート**
     - **ユーティリティ**
     - **仮想化ソリューション**
  4. マニュアルを表示するには、該当する製品をクリックして、該当するバージョンをクリックします。
- 検索エンジンを使用します。
  - 検索 ボックスに名前および文書のバージョンを入力します。

2

CMC のインストールと設定

本項では、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。

トピック：

作業を開始する前に

CMC 環境をセットアップする前に、PowerEdge VRTX 用の最新バージョンの CMC ファームウェアを **dell.com/support/** から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。

シャーシ設定のチェックリスト

次のタスクによって、シャーシを正確にセットアップすることが可能になります。

1. ブラウザを使用する CMC および管理ステーションは、管理ネットワークと呼ばれる同一のネットワークにあることが必要です。イーサネットネットワークケーブルを CMC のアクティブポートから管理ネットワークに接続します。
2. シャーシに I/O モジュールを取り付け、ネットワークケーブルをシャーシに接続します。
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 のタスクが完了したら、電源ボタンを押すか、CMC ウェブインタフェースからシャーシの電源をオンにします。

メモ: **サーバーの電源は入れないでください。**

6. LCD パネルを使用して、IP の概要に移動し、チェックボタンをクリックして選択します。管理システムブラウザ (IE、Chrome、Mozilla) で、CMC の IP アドレスを使用します。CMC に DHCP を設定するには、LCD パネルで、**メインメニュー** > **設定** > **ネットワーク設定** をクリックします。
7. ウェブブラウザを使用してデフォルトのユーザー名 (root) とパスワード (calvin) を入力することで、CMC IP アドレスに接続します。
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。この情報は、CMC ウェブインタフェースの サーバの概要 > セットアップ で確認できます。これは高度なライセンスオプションである可能性があります。この場合、各サーバのセットアップ機能を使用する必要があります。**
9. CMC ウェブインタフェースの IO モジュールに IP アドレスを入力します。IP アドレスは、**I/O モジュールの概要** をクリックして、**セットアップ** をクリックすると知ることができます。
10. ウェブブラウザから各 iDRAC に接続し、iDRAC の最終設定を行います。デフォルトのユーザー名は `root` で、パスワードは `calvin` です。
11. ウェブブラウザを使用して 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。

メモ: **コントロールパネルがシャーシに正しく取り付けられていないと、CMC はリスタートします。**

CMC の基本的なネットワーク接続

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。

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 **support.dell.com** 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しません。DVD-ROM を手動でマウントしてから、コマンド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 コマンドについてのヘルプは、前のコマンドを実行した後で `racadm help` と入力します。RACADM の詳細については、『Chassis Management Controller for Dell PowerEdge VRTX 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は、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。例えば、`racadm getconfig -f <file name>` となります。

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てから、`-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、管理することができます。**dell.com/support/manuals** にある『Dell Systems ソフトウェアサポートマトリックス』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、*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が必要です。セキュリティ要件に基づいて、管理ネットワークは隔離された非常に安全性の高い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、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、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。管理ステーションが Windows オペレーティングシステムを実行していると、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。

メモ: セキュリティ問題に対応するため、Microsoft Internet Explorer はクッキー管理における時刻を厳密に監視します。これをサポートするため、Internet Explorer を実行するコンピュータの時刻を CMC の時刻と同期化させる必要があります。

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。
4. **プロキシサーバー** セクションで、**LAN にプロキシサーバーを使用する (これらの設定はダイヤルアップまたは VPN 接続には適用されません)** オプションを選択し、**詳細設定** をクリックします。
5. **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 19.0 で例外リストを編集するには、次の手順を実行します。

1. Mozilla Firefox を起動します。
2. **ツール** > **オプション** をクリックするか (Windows で動作するシステムの場合)、または **編集** > **プリファランス** (Linux で動作するシステムの場合) をクリックします。
3. **詳細設定**、**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。

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お使いの管理システムの Internet Explorer で有効になっており、また CMC にインターネットへのアクセスがない場合、CMC へのアクセスが数秒遅れることがあります。この遅延は、このブラウザ、またはリモート RACADM などの別のインタフェースを使用中に生じる可能性があります。フィッシング詐欺検出機能を無効にするには、次の手順を実行します。

1. Internet Explorer を起動します。
2. **ツール** > **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** オプションを選択し、**OK** をクリックします。

証明書失効リストのフェッチ

CMC がインターネットにアクセスできない場合は、Internet Explorer で証明書失効リスト（CRL）のフェッチ機能を無効にします。この機能は、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した失効している証明書のリストにある証明書を使用す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は、ブラウザを使用して、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から CMC にアクセスするときに、この機能によって数秒の遅延が発生することがあります。

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** オプションをクリアし、**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場合、**暗号化されたページをディスクに保存しない** オプションが有効化されていないときに問題が発生することがあります。

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** > **詳細設定** をクリックします。
3. **セキュリティ** セクションで、**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** > **詳細設定**をクリックします。
3. **マルチメディア** セクションに移動し、**Web ページのアニメーションを再生する** オプションを選択します。

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: PowerEdge VRTX 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、「初期 CMC ネットワークの設定」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、PowerEdge VRTX シャーシ内の共通の内蔵ネットワークに接続されます。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 を介して確立されます。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。

シャーシ管理はデータネットワークから分離することが推奨されます。データネットワーク上における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がサーバー向けのトラフィックによって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。これらの遅延は、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ができます。

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でも後でも行うことができます。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

IP アドレスが与えられた後に 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。

- シリアルコンソール、Telnet、SSH、Dell CMC コンソールなどのコマンドラインインタフェース (CLI)。
- リモート RACADM
- CMC ウェブインタフェース
- LCD パネルインタフェース

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

LCD パネルインタフェースを使用して CMC ネットワークを設定できます。

メモ: 上下ボタンを 2 秒ほど長押しすると、LCD ディスプレイの向きをカスタマイズできます (ラック モードまたはタワー モード)。右左ボタンを使用することもできます。CMC LCD パネルのボタン操作については、「LCD のナビゲーション」を参照してください。

1. CMC 設定を開始するには、次の手順を実行します。
   - まだ設定を行っていないシャーシの場合は、[**LCD 言語**] パネルが表示されます。[**LCD 言語**] パネルで、矢印ボタンを使用して目的の言語に移動します。目的の言語が強調表示されたら、中央のボタンを押して言語を選択します。[**ネットワーク設定**] パネルが表示されます。
   - すでに設定を行ったシャーシの場合は、[**メイン メニュー**] パネルが表示されます。[**メイン メニュー**] で [**設定**]、[**ネットワーク設定**] の順に選択します。
2. [**ネットワーク設定**] パネルで目的のセットアップ モードを選択します。
   - **クイック セットアップ (DHCP)** — このモードを選択すると、DHCP アドレスを使用して CMC を簡単にセットアップできます。このモードで CMC を設定する方法については、「**クイック セットアップを使用した CMC の設定 (DHCP)**」を参照してください。
   - **詳細セットアップ** — このモードを選択すると、CMC の詳細なセットアップを行うことができます。このモードで CMC を設定する方法については、「**詳細セットアップを使用した CMC の設定**」を参照してください。

クイックセットアップを使用した CMC の設定 (DHCP)

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. [**ネットワーク設定**] パネルで [**クイック セットアップ (DHCP)**] を選択します。パネルに次のメッセージが表示されます。

```
About to get DHCP addresses. Ensure CMC network cable is connected.
```

2. 中央のボタンを押して、確定ボタンをハイライト表示します。もう一度、中央のボタンを押して設定を確定します。または戻る矢印に移動して中央のボタンを押し、前に戻って設定を変更します。

詳細セットアップを使用した CMC の設定

1. **ネットワーク設定** パネルで **詳細セットアップ** を選択した場合、CMC を設定することを確認する次のメッセージが表示されます。

```
Configure CMC?
```

2. 詳細セットアッププロパティを使用して CMC を設定するには、中央のボタンをクリックしてチェックアイコンを選択します。

   メモ: CMC の設定を省略するには、「X」アイコンに移動して中央のボタンを押します。

3. 適切なネットワーク速度を選択するかどうかを尋ねられた場合は、適切なボタンを使用して適切なネットワーク速度（**自動（1 Gb）**、**10 Mb**、または **100 Mb**）を選択します。

   効果的なネットワーク スループットを得るには、ネットワーク速度の設定とネットワーク構成が一致していなければなりません。ネットワーク速度をネットワーク構成の速度より遅くすると、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で上記のネットワーク速度に対応しているかどうかを確認し、適切な設定を行ってください。ネットワーク構成がいずれの値にも一致しない場合は、[**自動（1 Gb）**] オプションを選択するか、ネットワーク機器メーカーのユーザー マニュアルを参照してください。

4. 次のタスクのいずれかを実行します。

   - [**自動（1Gb）**] を選択します。中央のボタンを押して、もう一度中央のボタンを押します。[**プロトコル**] パネルが表示されます。手順 6 に進みます。
   - [**10Mb**] または [**100Mb**] を選択します。[**二重モード**] パネル

     が表示されます。手順 5 に進みます。

   それ以外の場合、

5. [**二重モード**] パネルでネットワーク環境に一致する二重モード ([**全二重**] または [**半二重**]) を選択するには、中央のボタンを押し、中央のボタンを再度押します。[**プロトコル**] パネルが表示されます。

   メモ: [オート ネゴシエーション] が [オン] にセットされている、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行えません。オート ネゴシエーションを片方のデバイスで有効にし、別のデバイスではオフにしていると、オート ネゴシエーションを使用するデバイスは他方のデバイスのネットワーク速度を判別することはできますが、二重モードは判別できません。この場合、オート ネゴシエーションでは半二重モードが選択されます。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。

6. **プロトコル** パネルで、CMC に使用するインターネットプロトコル（**IPv4 のみ**、**IPv6 のみ**、または **両方**）を選択し、中央のボタンを押した後、再度中央ボタンを押します。
7. - [**IPv4**] または [**両方**] を選択する場合は、[**DHCP**] または [**静的**] モードを選択します。手順 8 に進みます。
   - これ以外、[**IPv6**] を選択すると、[**iDRAC の設定**] パネルが表示されます。この手順についてはステップ 11 で行います。
8. [**モード**] パネルで、CMC が NIC IP アドレスを取得する際のモードを選択します。DHCP を選択すると、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、ネットワークで割り振られる固有の IP アドレスが割り当てられます。[**DHCP**] を選択した場合は、中央のボタンを押してから、中央のボタンをもう一度押します。[**iDRAC の設定**] パネルが表示されます。この手順についてはステップ 11 で行います。
9. **静的** を選択した場合は、LCD パネルの指示にしたがって IP アドレス、ゲートウェイ、およびサブネットマスクを入力します。

   入力した IP 情報が表示されます。中央のボタンを押してから、中央のボタンをもう一度押します。[**CMC 設定**] 画面に、入力した [**静的 IP アドレス**]、[**サブネット マスク**][**ゲートウェイ**] の設定値が表示されます。設定値に間違いがないか確認してください。設定を修正するには、該当するボタンを押します。中央のボタンを押し、もう一度中央のボタンを押します。[**DNS を登録しますか？**] というパネルが表示されます。
10. 登録する場合は、チェック アイコンを選択して中央のボタンを押します。DNS IP アドレスを設定し、チェック アイコンを選択して中央のボタンを押します。DNS 登録が不要な場合は、「X」アイコンを選択して中央のボタンを押します。
11. iDRAC を設定するかどうかを指定します。

    - **いいえ**：「X」アイコンを選択して中央のボタンを押します。この手順についてはステップ 17 で行います。
    - **はい**：チェックアイコンを選択して中央のボタンを押します。

    また、CMC ウェブインタフェースから iDRAC を設定することもできます。
12. **プロトコル** パネルで、サーバー用に使用する IP タイプを選択します。

    - **IPv4** - **DHCP** または **静的** オプションが表示されます。
    - **両方**

      — **DHCP** または **静的** オプションが表示されます。
    - **IPv6**

      - [**iDRAC の設定**] パネルが表示されます。手順 15 に進みます。
13. **DHCP** または **静的** を選択します。

表 9. ネットワークモード

ネットワークモード	説明
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、ネットワークで割り振られる固有の IP アドレスが割り当てられます。中央のボタンを押します。**IPMI オーバー LAN** パネルが表示されます。

静的	**静的** を選択した場合は、LCD 画面の指示にしたがって IP アドレス、ゲートウェイ、および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、次を行います。
	a. スロット 1 の IP を使用して自動的に増分するかどうかを尋ねる、次のメッセージが表示されます。
	`IPs will auto-increment by slot number.`
	中央のボタンをクリックします。スロット 1 の IP 番号を入力するように求める、次のメッセージが表示されます。
	`Enter slot 1 (starting) IP`
	スロット 1 の IP 番号を入力し、中央のボタンを押します。
	b. 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。
	c. 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。
	d. [**ネットワーク概要**] 画面に、入力した [**静的 IP アドレス**]、[**サブネット マスク**]、[**ゲートウェイ**] の設定値が表示されます。設定値に間違いがないか確認してください。設定を修正するには、該当するボタンを押してから中央のボタンを押します。
	e. 入力した設定が正確であることを確認したら、手順 10 に進みます。
	IPMI オーバー LAN パネルが表示されます。

14. [**IPMI Over LAN**] パネルで [**有効化**] または [**無効化**] を選択して、IPMI Over LAN を有効または無効にします。中央のボタンを押して先に進みます。
15. **iDRAC 設定** パネルに、次のメッセージが表示されます。

    ```
    Apply settings to installed servers?
    ```

    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、チェック アイコンを選択し、中央のボタンを押します。これ以外は、「X」アイコンを選択して中央のボタンを押します。
16. 次の **iDRAC 設定** パネルに、以下のメッセージが表示されます。

    ```
    Auto-Apply settings to newly-inserted servers?
    ```

    新たにインストールし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、チェック アイコンを選択して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、以前に設定されたネットワーク設定ポリシーを使用してサーバーを自動的に導入するかどうかを確認するプロンプトが LCD に表示されます。iDRAC ネットワーク設定を新しくインストールしたサーバーに適用したくない場合は、「X」アイコンを選択して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 ネットワークの設定値は設定されません。
17. **iDRAC 設定** パネルに、次のメッセージが表示されます。

    ```
    Apply All Enclosure Settings?
    ```

    すべてのエンクロージャ設定を適用するには、チェック アイコンを選択して中央のボタンを押します。これ以外は、「X」アイコンを選択して中央のボタンを押します。
18. [**IP サマリー**] パネルの 30 秒お待ちくださいパネルの後、入力した IP アドレスを確認して、アドレスに間違いがないことを確認します。設定を修正するには、左矢印アイコンを押し、中央のキーを押して、その設定の画面に戻ります。IP アドレスを修正したら、中央のボタンを押します。

    入力した設定が正確であることを確認したら、中央のボタンを押し、もう一度中央のボタンを押します。[**メイン メニュー**] パネル ID 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。

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 ネットワーク設定項目を設定すると、さまざまなインタフェースから CMC にリモートアクセスすることができます。次の表は、CMC へのリモートアクセスに使用できるインタフェースを示しています。

メモ: Telnet は他のインタフェースのようには安全ではないため、デフォルトでは無効になっています。Telnet は、ウェブ、SSH、リモート RACADM から有効にしてください。

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 10. 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で CMC にリモートアクセスします。ウェブインタフェースは CMC のファームウェア内蔵で、管理ステーションにある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『Dell システムソフトウェアサポートマトリックス』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 で CMC にログインしてアクセスします。ファームウェア RACADM コマンドは、CMC の IP、ユーザー名、パスワードを指定しなくても実行できます。RACADM プロンプトに入ると、racadm プレフィックスなしでコマンドを直接実行できます。
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。 ・ アラートと CMC IP の表示 ・ DHCP の設定 ・ CMC 静的 IP の設定 ・ アクティブ CMC の CMC MAC アドレスの表示 ・ CMC IP の末尾に付加された CMC VLAN ID を表示（VLAN 設定済みの場合）
Telnet	ネットワーク経由でコマンドラインにより、CMC にアクセスします。RACADM コマンドラインインタフェースと、サーバまたは 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。
WSMan	WSMan サービスは、Web Services for Management（WSMan）プロトコルをベースにしており、1 対多のシステム管理タスクを実行します。CMC サービス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 WSMan 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、WSMan 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。 WSMan は、システム管理に使用される Simple Object Access Protocol（SOAP）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、管理対象システムで変更可能なセマンティクスと情報タイプを定義します。

表 10. CMC インタフェース（続き）

インタフェース	説明
	CMC WSMan はトランスポートセキュリティにポート 443 で SSL を使用して実装され、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/** · WSMan リリースノートファイル。 · **www.wbemsolutions.com/ws_management.html** · DMTF WSManagement 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。 WinRM ツールは、送信するすべての WSMan コマンドのデフォルトの応答タイムアウトを 60 秒に設定します。WinRM では、このタイムアウト間隔を変更することはできません。 WinRM ツールのバグのため、"winrm set winrm/config @{MaxTimeoutms="80000"}" を使用しても、タイムアウトは変更されません。したがって、実行を完了するために 1 分以上かかるコマンドには WinRM を使用しないことを推奨します。 SOAP-XML パケットを作成するライブラリを使用することを推奨します。ユーザーはこれらのライブラリを使用してタイムアウト時間を設定できます。 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 のユーザー名とパスワードのデフォルト値は、`root` と `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

CMC は、Dell Server Administrator または Dell OpenManage Essentials を使って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で、**システム** > **メインシステムシャーシ** > **リ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.com/support/manuals** にある『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

ネットワーク上の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な場所とシャーシ名の設定

CMC ウェブインタフェースを使用してシャーシの場所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. 左ペインで [**シャーシ概要**] に移動し、**[セットアップ]** をクリックします。

2. [**一般シャーシ設定**] ページで、位置のプロパティとシャーシ名を入力します。シャーシのプロパティを設定する方法については、*CMC のオンライン ヘルプ*を参照してください。

   SSH で CMC にログインする場合にシャーシ名を表示するには、[**SSH プロンプトにシャーシ名を表示する**] を選択します。デフォルトでは、[**SSH プロンプトにシャーシ名を表示する**] オプションは選択されていません。

   メモ: [シャーシの位置] フィールドはオプションです。シャーシの物理的な位置を示すには、[データ センター]、[通路]、[ラック]、[ラック スロット] フィールドを使用します。

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用してシャーシ名、場所、日付、および時刻を設定するには、**setsysinfo** コマンドおよび **setchassisname** コマンドを参照してください。詳細については、『Chassis Management Controller for PowerEdge VRTX 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ます。また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 で日付と時刻を設定するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** > **セットアップ** > **日付 / 時刻** をクリックします。
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、**日付 / 時刻** ページで **NTP を有効にする** を選択し、最大 3 台の NTP サーバーを指定します。日付と時刻を手動で設定するには、**NTP を有効にする** オプションの選択を解除して、**日付** フィールドと **時刻** フィールドを編集します。
3. ドロップダウンメニューから **タイムゾーン** を選択し、**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用して日付と時刻を設定するには、**dell.com/support/manuals** にある『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』で、**config** コマンドおよび `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

シャーシ上のコンポーネントを識別できるようにするために、コンポーネント (シャーシ、サーバー、物理ディスクドライブ、仮想ディスク、および I/O モジュール) の LED の点灯を有効化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 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

1 つ、複数、またはすべてのコンポーネント LED を点滅させるには、次の手順を実行します。

- 左ペインで、次のいずれかのページに移動します。
  - **シャーシ概要** > **トラブルシューティング**。
  - **シャーシ概要** > **シャーシコントローラ** > **トラブルシューティング**。
  - **シャーシ概要** > **サーバー概要** > **トラブルシューティング**。

メモ: このページではサーバーのみを選択できます。

- シャーシ概要 > I/O モジュール概要 > トラブルシューティング。
- ストレージ > トラブルシューティング > 識別。

メモ: エンクロージャごとの物理ディスク、エンクロージャごとの仮想ディスク、外付けストレージコンポーネント LED はこのページで選択できます。

コンポーネント LED を点滅させるには、物理ディスクドライブまたは仮想ディスクまたはエンクロージャに対応する **すべて選択 / 選択解除** オプションを選択し、**点滅** をクリックします。コンポーネント LED の点滅を無効にするには、その LED に対応する **すべて選択 / 選択解除** オプションをクリアして、**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 <module> [-l <ledState>]`。ここで *<module>* には、設定する LED が存在するモジュールを指定します。設定オプションは次のとおりです。

- `server-n` (ここで *n* は 1~4)
- `switch-1`
- `cmc-active`

および *<ledState>* は LED を点滅させるかどうかを指定します。設定オプションは次のとおりです。

- 0 — 点滅なし (デフォルト)
- 1 — 点滅

`racadm raid <operation> <component FQDD>`。ここで *動作* 値は `blink` または `unblink` であり、FQDD はコンポーネントの物理ディスクドライブ、仮想ディスクおよびエンクロージャのものです。

CMC プロパティの設定

ウェブインタフェースまたは RACADM コマンドを使って、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. 左側のペインで、**シャーシ概要** > **セットアップ** 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、**dell.com/support/manuals** の *Chassis Management Controller PowerEdge VRTX 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: 次のタスクを行うには、シャーシ設定管理者 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. 左側のペインで **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、左側のペインで **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ついては、**dell.com/support/manuals** にある『Chassis Management Controller for PowerEdge VRTX 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 の機能が停止した場合にそれを引き継ぐスタンバイ CMC をインストールできます。冗長 CMC は事前にインストールされている場合がありますが、あとからインストールすることもできます。完全な冗長性または最良のパフォーマンスを得るには、CMC ネットワークが適切にケーブル配線されていることが重要です。

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。dell.com/support/manuals にある『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』で `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。dell.com/support/manuals にある『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』で、`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からアクティブ CMC をリセット。「電力制御操作の実行」で説明されている **電力制御操作** の `Reset CMC` オプションを参照してください。
- 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 フェー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 セッションがログオフされます。セッションからログオフしたユーザーは、新しいアクティブ CMC に再接続する必要があります。

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。両方の CMC のファームウェアリビジョンは同じである必要がありますが、スタンバイ CMC に設定を全く同じにする必要はありません。

メモ: CMC の取り付けについては、『VRTX 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 への CMC ファームウェアのインストール手順については、「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

PowerEdge VRTX エンクロージャは、サーバーと I/O モジュールを機能停止から保護するためにフェイルセーフモードを有効化します。フェイルセーフモードは、CMC がシャーシを制御していないときに有効になります。CMC フェイルオーバー期間、または単一 CMC 管理機能喪失中は、次の状態になります。

- 新しく取り付けたサーバーに電源投入できない。
- 既存のサーバーにリモートでアクセスできない。
- CMC の管理が復旧するまで、電力消費制限のためにサーバーのパフォーマンスが低下する。

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、単一、または冗長 CMC で構成することができます。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 がシャーシ管理をそれを引き継ぎます。

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、スロットは優先順位を示しているわけではなく、最初に取り付けた、または起動した CMC がアクティブ CMC の役割を担います。CMC が 2 つ取り付けられている状態で AC 電源を入れると、CMC シャーシスロット 1 に取り付けられている CMC が通常アクティブ CMC の役割を担います。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 を挿入する場合、自動アクティブまたはスタンバイネゴシエーションに最大 2 分間かかることがあります。通常のシャーシの動作は、ネゴシエーション完了時に再開されます。

冗長 CMC の正常性状態の取得

ウェブインタフェースでスタンバイ CMC の正常性状態を表示できます。ウェブインタフェースでの CMC の正常性状態へのアクセスについての詳細は、「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」を参照してください。

前面パネルの設定

次を設定することができます。

- 電源ボタン
- LCD
- DVD ドライブ

電源ボタンの設定

シャーシの電源ボタンを設定するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** > **前面パネル** > **セットアップ** をクリックします。
2. **フロントパネル設定** ページの **電源ボタン設定** セクションで、**シャーシ電源ボタンの無効化** オプションを選択してから **適用** をクリックします。
   シャーシ電源ボタンが無効になります。

LCD の設定

1. 左ペインで、**シャーシ概要** > **前面パネル** > **セットアップ** をクリックします。
2. **設定** ページの **LCD 設定** セクションで、次を実行します。
   - **コントロールパネル LCD のロック** オプションを選択して、LCD インタフェースを使用して実行できる設定をすべて無効にします。
   - **LCD 言語** ドロップダウンメニューから、必要な言語を選択します。
   - **LCD の向き** ドロップダウンメニューから必要なモード（**タワーモード** または **ラックモード**）を選択します。

   メモ: LCD ウィザードを使用してシャーシを設定するときに、新しく挿入されたサーバーに設定を自動適用 オプションを選択した場合、Basic ライセンスでは 新しく挿入されたサーバーに設定を自動適用 機能を無効にすることはできません。機能を有効にしない場合は、LCD に表示されるメッセージを無視するか（自動的に消えます）、LCD の 許可しない ボタンを押してから、中央のボタンを押します。

3. **適用** をクリックします。

KVM を使用したサーバーへのアクセス

サーバーを KVM にマップし、KVM インタフェースを介したサーバーリモートコンソールへのアクセスを有効化するには、CMC ウェブインタフェース、RACADM、または LCD インタフェースを使用できます。

CMC ウェブインタフェースを使用したサーバーの KVM へのマッピング

KVM コンソールがシャーシに接続されていることを確認してください。

KVM にサーバーをマップするには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** > **前面パネル** > **セットアップ** をクリックします。
2. **フロントパネル設定** ページの **KVM 設定** セクションにある **KVM マッピング** リストから、KVM にマップする必要のあるスロットを選択し、**適用** をクリックします。

メモ: KVM では、すべてのサーバースロットへのマッピングが可能です。フルハイトサーバーの挿入、またはハーフハイトサーバーのフルハイトサーバーとの交換は、マッピング動作を変更しませんが、KVM が下部スロットにマップされていて、そのスロットにフルハイトサーバーがある場合は、KVM は上部スロット経由でしか使用できません。KVM を上部スロットに再マップする必要があります。

LCD を使用した KVM へのサーバーのマッピング

KVM コンソールがシャーシに接続されていることを確認してください。

LCD を使用した KVM へのサーバーのマッピング — LCD の **メインメニュー** 画面から、**KVM マッピング** に移動し、マップされる必要のあるサーバーを選択し、OK を押します。

DVD ドライブへのサーバーのマッピング

シャーシ DVD ドライブにサーバーをマップするには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** > **前面パネル** > **セットアップ** をクリックします。
2. **前面パネル設定** ページの **DVD ドライブの設定** セクションで、次を行います。

   DVD マップ済み ドロップダウンメニューから、サーバーのひとつを選択します。シャーシ DVD ドライブアクセスを必要とするサーバーを選択します。
3. **適用** をクリックします。

DVD では、すべてのサーバースロットへのマッピングが可能です。フルハイトサーバーの挿入、またはハーフハイトサーバーのフルハイトサーバーとの交換は、マッピング動作を変更しませんが、DVD が下部スロットにマップされていて、そのスロットにフルハイトサーバーがある場合は、DVD は上部スロット経由でしか使用できません。DVD を上部スロットに再マップする必要があります。

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。

メモ: CMC は、シャーシプロファイルからの XML を使用したユーザー名またはパスワードに、次の特殊文字をサポートしていません。

"、!、#、$、%、^、&、*、(,)、-、_、+、=、?、{,}、+、&、>、|、.、'、[

トピック：

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: Microsoft Internet Explorer を使用しており、プロキシで接続して、エラーメッセージ `The XML page cannot be displayed` が表示された場合、続行するために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、次の手順を実行します。

1. システムでサポートされるウェブブラウザを開きます。

   対応ウェブブラウザの最新情報については、**dell.com/support/manuals** にある『Dell Systems ソフトウェアサポートマトリックス』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 address>`

     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 address>:<port number>`
   - IPv6 アドレスを使用して CMC にアクセスするには：`https://[<CMC IP address>]`

     デフォルトの HTTPS ポート番号 (ポート 443) が変更された場合、`https://[<CMC IP address>]:<port number>` を入力します。ここで、*<CMC IP address>* は CMC の IP アドレスであり、*<port number>* は HTTPS ポート番号です。

     CMC の ログイン ページが表示されます。

   メモ: IPv6 の使用中は、CMC の IP アドレスを角かっこ ([ ]) で囲む必要があります。

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 と共に出荷されるデフォルトの管理者アカウントです。

メモ:

- **セキュリティ強化のために、初期設定時に、ルート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推奨します。**
- **証明書検証が有効になっているときは、システムの FQDN を指定する必要があります。証明書検証が有効で、ドメインコントローラに IP アドレスが指定されていると、ログインに失敗します。**

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。

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。
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: Active Directory ユーザーの場合、ユーザー名 フィールドでは大文字と小文字が区別されます。
3. **ドメイン** フィールドのドロップダウンメニューから、必要なドメインを選択します。
4. 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。デフォルト値は、**ウェブサービスアイドルタイムアウト** です。
5. **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。

   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。

メモ: LDAP 認証が有効で、ローカルの資格情報を使用して CMC にログインしようとすると、その資格情報は最初に LDAP サーバーでチェックされてから、CMC でチェックされます。

スマートカードを使用した CMC へのログイン

この機能を使用するには、Enterprise ライセンスが必要です。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: スマートカードログインでは、IP アドレスを使用して 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>`

   スマートカードの挿入を求める **CMC ログイン** ページが表示されます。

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 ダイアログボックスが表示されます。
3. PIN を入力し、**送信** をクリックします。

   メモ: このスマートカードユーザーが Active Directory 内に存在する場合、Active Directory パスワードは必要ありません。存在しない場合は、適切なユーザー名とパスワードを使用してログインする必要があります。

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

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) が有効になっている場合は、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しないで CMC にログインできます。この機能を使用するには、Enterprise ライセンスが必要です。

メモ: IP アドレスを使って SSO 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。

SSO を使用して CMC にログインする前に、次の点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。

SSO 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。
   例えば、`cmc-6G2WXF1.cmcad.lab`, です。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、<cmcname.domain-name>:<port number> を使用して CMC ウェブインタフェースにアクセスします。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。

   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ておらず、Internet Explorer 以外のブラウザを使用している場合、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。

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 接続を介して 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、次のタスクを実行して 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 にログインされました。

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、KVM 上での 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。

- 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。

メモ: リモート **RACADM** は、『**Dell Systems Management Tools and Documentation 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。

- ファームウェア RACADM - Telnet、SSH、またはシリアル接続を使って CMC にログインすることを可能にします。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 実装を実行できます。

リモート RACADM コマンドをスクリプトで使用して、複数の CMC を設定できます。CMC ではサポートされていないため、これらのスクリプトを CMC ウェブインタフェース上で直接実行することはできません。

RACADM の詳細については、『Chassis Management Controller for PowerEdge VRTX 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 CMC 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 CMC 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ます。この機能を使用するには、Enterprise ライセンスが必要です。

たとえば、次のとおりです。

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

サービスアカウントを使用してログインする際、公開キーまたは秘密キーのペアを作成するときにパスフレーズを設定した場合には、そのパスフレーズの再入力を求められる可能性があります。パスフレーズがキーと共に使用される場合は、Windows および Linux を実行しているクライアントシステムによって、その方法を自動化するメソッドが提供されます。Windows を実行するクライアントシステムでは、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 を実行するクライアントシステムでは、ssh エージェントを使用できます。これらのいずれかのアプリケーションをセットアップおよび使用するには、それらの製品マニュアルを参照してください。

複数の CMC セッション

各種のインタフェースを使用することで可能な複数の CMC セッションのリストが、ここに表示されます。

表 11. 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。**

Web インターフェイスを使用したデフォルト ログイン パスワードの変更

CMC Web インターフェイ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。この操作を行うには、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：+、&、?、>、-、}、|、.、!、(、'、,、_、[、"、@、#、)、*、;、$、]、/、§、%、=、<、:、{、l、\

   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。これらの文字を使用して値を設定すると、予期しない作動が発生します。
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 にログインします。

   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、*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。

詳細については、**dell.com/support/manuals** にある『Chassis Management Controller for PowerEdge VRTX 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** の権限が必要です。

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、『*Chassis Management Controller for PowerEdge VRTX 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。

Web インターフェイスを使用した強制パスワード変更

初めて CMC インターフェイスにアクセスしたとき、デフォルトのパスワードを変更できます。この機能は、ネットワークにアクセス可能で、ユーザー名とパスワードの認証を必要とする環境に適用されます。**強制パスワード変更**機能は、いつでも設定およびリセットすることができます。CMC Web インターフェイスにログインしてアクセスするには、パスワードの変更が必須です。デフォルトのユーザー名は「root」です。

1. **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：+、&、?、>、-、}、|、.、!、(、'、,、_、[、"、@、#、)、*、:、$、]、/、§、%、=、<、;、{、l、~、^ および \

   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。これらの文字を使用して値を設定すると、予期しない作動が発生します。

2. [**パスワードの確認**] テキスト ボックスに新しいパスワードを再度入力します。
3. [**続行**] をクリックして、CMC Web インターフェイスにログインするための新規パスワードを送信します。

使用事例シナリオ

本項では、Dell PowerEdge VRTX の Chassis Management Controller バージョン 3.3 を使って実行できる典型的な使用事例とタスクについて説明します。

ウェブインタフェースを使った外付け共有 PERC 8 カード高可用性から非高可用性モードへの変換

Dell PowerEdge VRTX シャーシには、HA モードで PCI スロット 5 および PCI スロット 6 に 2 つの共有 PERC 8 カードが必要です。

ワークフロー

1. シャーシの電源を切ります。外付け共有 PERC 8 カードから MD 12x0 エンクロージャに接続されているすべての SAS ケーブルを外します。
2. シャーシに電源投入します。
3. CMC ウェブインタフェースへログインし、**ストレージ → コントローラ → トラブルシューティング** の順に移動し、スロット 5 の外付け共有 PERC 8 カードのドロップダウンメニューから**フォールトトレランス** を無効にし、**適用**をクリックしてからスロット 6 を無効にするを選択し、**適用**をクリックします。
4. 両方の PERC をリセットしてから非 HA モードに反映されるまでには、2 分かかる場合があります。
5. シャーシの電源を切り、非 HA モードでエンクロージャに接続します。
6. シャーシに電源投入します。
7. 外付け共有 PERC 8 カードが高可用性モードでない場合、**ストレージ →トラブルシューティング→ セットアップのトラブルシューティング** の順に移動して、非 HA ステータスを表示します。

ウェブインタフェースを使った外付け共有 PERC 8 カード非高可用性から高可用性モードへの変換

Dell PowerEdge VRTX シャーシには、PCI スロット 5 および PCI スロット 6 に 2 つの共有 PERC 8 カードが必要です。

ワークフロー

1. シャーシの電源を切ります。外付け共有 PERC 8 カードから MD 12x0 エンクロージャに接続されているすべての SAS ケーブルを外します。
2. シャーシに電源投入します。
3. CMC ウェブインタフェースへログインし、**ストレージ → コントローラ → トラブルシューティング** の順に移動し、スロット 5 の外付け共有 PERC 8 カードのドロップダウンメニューから**フォールトトレランス** を有効にし、**適用**をクリックしてからスロット 6 を無効にするを選択し、**適用**をクリックします。
4. 両方の PERC をリセットしてから HA モードに反映されるまでには、2 分かかる場合があります。
5. シャーシの電源を切り、HA モードでエンクロージャに接続します。
6. シャーシに電源投入します。
7. 外付け共有 PERC 8 カードが高可用性モードの場合、**ストレージ →トラブルシューティング→ セットアップのトラブルシューティング** の順に移動して、HA ステータスを表示します。

RACADM を使った外付け共有 PERC 8 カード高可用性から非高可用性モードへの変換

Dell PowerEdge VRTX シャーシには、PCI スロット 5 および PCI スロット 6 に 2 つの共有 PERC 8 カードが必要で、HA モードでなければなりません。

ワークフロー

1. シャーシの電源を切ります。外付け共有 PERC 8 カードから MD 12x0 エンクロージャに接続されているすべての SAS ケーブルを外します。
2. シャーシに電源投入します。
3. サーバーの電源が切れた状態で、CMC RECADM にログインし、次のコマンドを実行します。

```
racadm  raid set controllers:RAID.ChassisSlot.5-1 -p HighAvailabilityMode None
```

4. コマンド `racadm raid set controllers:RAID.ChassisSlot.6-1 -p HighAvailabilityMode None` を、外付け共有 PERC 8 カードで実行します。
5. 両方の PERC をリセットしてから HA モードに反映されるまでには、2 分かかる場合があります。
6. シャーシの電源を切り、非 HA モードでエンクロージャに接続します。
7. シャーシに電源投入します。
8. 外付け共有 PERC 8 カードが高可用性モードでない場合、次のコマンドを使ってステータスを表示します。

```
racadm raid get controllers -o -p HighAvailabilityMode
```

RACADM を使った外付け共有 PERC 8 カード非高可用性から高可用性モードへの変換

Dell PowerEdge VRTX シャーシには、PCI スロット 5 および PCI スロット 6 に共有 PERC 8 カードが必要です。

ワークフロー

1. シャーシの電源を切ります。外付け共有 PERC 8 カードから MD 12x0 エンクロージャに接続されているすべての SAS ケーブルを外します。
2. シャーシに電源投入します。
3. サーバーの電源が切れた状態で、CMC RECADM にログインし、次のコマンドを実行します。

```
racadm raid set controllers:RAID.ChassisSlot.5-1 -p HighAvailabilityMode ha
```

4. コマンド `racadm raid set controllers:RAID.ChassisSlot.6-1 -p HighAvailabilityMode ha` を、外付け共有 PERC 8 カードで実行します。

5. 両方の PERC をリセットしてから HA モードに反映されるまでには、2 分かかる場合があります。
6. シャーシの電源を切り、HA モードでエンクロージャに接続します。
7. シャーシに電源投入します。
8. 外付け共有 PERC 8 カードは高可用性モードであれば、次のコマンドを使って HA ステータスを表示できます。

```
racadm raid get controllers -o -p HighAvailabilityMode
```

。

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
- シャーシインフラストラクチャ
- 内蔵または外付けエンクロージャの VRTX エキスパンダまたはストレージバックプレーンエキスパンダファームウェア
- エンクロージャごとの物理ディスク (HDD)

  メモ: HDD ファームウェアは、必要な場合のみアップデートすることができます。

次の I/O およびサーバーコンポーネントに対してファームウェアをアップデートできます。

- I/O モジュール
- BIOS
- iDRAC
- Lifecycle Controller
- 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
- サーバーモジュール上の RAID コントローラ

メモ: ファームウェアのアップデートには完了まで数分かかる場合があります。

トピック：

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。

VRTX シャーシファームウェアのアップデート中は、次の順序でシャーシコンポーネントのファームウェアバージョンをアップデートすることをお勧めします。

1. ブレードコンポーネントファームウェア
2. CMC ファームウェア
3. シャーシインフラストラクチャファームウェア
4. 共有 PERC8 ファームウェア (内蔵および外付け)
5. 内部ストレージバックプレーンファームウェアおよび外部エンクロージャエキスパンダ
6. HDD ファームウェア (外付けおよび内蔵エンクロージャ)

VRTX シャーシのアップデート順序の詳細については、**dell.com/cmcmanuals** にある『*CMC ファームウェア 3.3 リリース ノート*』を参照してください。

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** > **サーバー概要** > **サーバーコンポーネントアップデート**
- **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** > **ストレージ** > **ストレージコンポーネントアップデート**

ファームウェアアップデート ページに、リスト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することを可能にします。

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 **ファームウェアアップデート** ページにリストされます。

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 iDRAC と CMC の IP 情報、および CMC サービスタグまたは資産タグを表示するには、`racadm getsysinfo` サブコマンドを実行します。その他の RACADM コマンドの詳細については、『Chassis Management Controller for PowerEdge VRTX 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

Web インターフェイスまたは RACADM を使って CMC ファームウェアをアップデートできます。デフォルトでは、ファームウェアのアップデート後も現在の CMC 設定を保持します。アップデート処理中、CMC の設定を工場出荷時のデフォルト設定にリセットできます。

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権限が必要です。

システム コンポーネント ファームウェアのアップデートに Web ユーザー インターフェイスのセッションを利用する場合、ファイル転送時間を許容できるように [**アイドル タイムアウト (0、60 ~ 10800)**] を高めに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は、最大 30 分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における、シャーシ内の冷却ファンの一部または全部の 100% 速度での回転は、通常の動作です。

シャーシに冗長 CMC を取り付けた場合、両方の CMC を一度の操作で同時に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っている場合にフェールオーバーが発生すると、不測の結果が生じることがあります。

メモ:

- **1600W 電源装置搭載のシャーシでは、CMC ファームウェアを 2.0 を除く以前のバージョンにアップデートすることはできません。**

- **CMC ファームウェアのアップデートまたはロールバックは、ファームウェアバージョン 1.2、1.25、1.3、1.31、1.35、1.36、2.0、2.01、および 2.04 以降でのみサポートされます。これらのバージョン以外を使用している場合は、まずこれらのバージョンのいずれかにアップデートし、次に必要なバージョンにアップデートします。**

ファームウェアが正常にアップロードされた後、アクティブ CMC がリセットされ、一時的に使用できなくなります。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。アップデートをアクティブ CMC にのみ適用した場合、リセット完了後、アクティブ CMC はアップデートされたイメージを実行せず、スタンバイ CMC だけがそのイメージを持つことになります。一般に、アクティブ CMC とスタンバイ CMC のファームウェアバージョンを同一に保つことを強くお勧めします。

スタンバイ CMC をアップデートしたら、新たにアップデートされた CMC がアクティブ CMC になり、以前のファームウェアの CMC がスタンバイになるように、CMC の役割を交換します。役割の交換の詳細については、『Chassis Management Controller for PowerEdge VRTX 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。このコマンドを実行すると、2 番目の CMC のファームウェアをアップデートする前に、アップデートが成功し、新しいファームウェアが正常に動作していることを確認するのに役立ちます。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 ファームウェア リビジョン 2.x は、`cmcchangeover` コマンドを実行せずに、プライマリー CMC と冗長 CMC の両方をアップデートします。

CMC では、ファームウェアアップデート処理の最終フェーズ中、CMC がネットワークに接続されていないために、ブラウザセッションと CMC との接続が一時的に失われます。CMC は、この一時的なネットワーク喪失により、シャーシの全体的な正常性が危険な状態であると報告します。数分後、CMC が再起動したら、CMC にログインします。CMC は、シャーシの全体的な正常性に異常はなく、CMC ネットワークリンクがアップ状態であると報告します。CMC のリセット後、新しいファームウェアバージョンが **ファームウェアアップデート** ページに表示されます。

リセット中に他のユーザーからの接続が切断されるのを避けるため、CMC にログイン可能な、許可されているユーザーに通知して、[**セッション**] ページでアクティブなセッションをチェックしてください。[**セッション**] ページを開くには、左ペインで [**シャーシ概要**] をクリックし、[**ネットワーク**] をクリックして、[**セッション**] をクリックします。

CMC との間でファイルを転送しているときには、ファイル転送アイコンが回転します。アイコンが回転しない場合は、アニメーションを許可するようにブラウザが設定されていることを確認しします。ブラウザでのアニメーションの詳細については、「Internet Explorer でアニメーションの再生」を参照してください。

メモ: 現在のバージョンの CMC でスロット名の長さを 15 文字を超えて設定している場合、CMC ファームウェアをダウングレードするとスロット名の長さが 15 文字に切り捨てられます。

署名済み CMC ファームウェアイメージ

VRTX CMC 2.0 以降では、ファームウェアに署名が含まれています。CMC ファームウェアは、アップロードされたファームウェアの信ぴょう性を確実にするため、その署名を検証します。ファームウェアアップデートプロセスは、ファームウェアイメージがサービスプロバイダからの有効なイメージで、かつ改ざんされていないことを CMC が証明した場合にのみ、正常に行われます。ファームウェアのアップデートプロセスは、アップロードされたファームウェアイメージの署名を CMC が検証できない場合は停止されます。その後、警告イベントがログに記録され、該当するエラーメッセージが表示されます。

署名検証は、VRTX ファームウェアバージョン 1.2、またはそれ以降で実行可能です。1.2 より前の VRTX バージョンへのファームウェアダウングレードには、まず最初にファームウェアを 2.0 より前の 1.2 以降の VRTX CMC バージョンにアップデートします。このアップデートの実行後、以前の署名されていない VRTX バージョンへのファームウェアダウングレードを実行することができます。

CMC およびメインファームウェアのアップデート

CMC とメインボードファームウェアの両方が更新されるまで、外付け共有 PERC 8 カードの共有機能は使用できません。

メモ:

- **MD 12x0 のケーブル接続図を表示するには、dell.com/support/manuals で *『共有ストレージ拡張するための PoweEdge RVTX のアップグレードユーザーズガイド』* または *『Dell PowerEdge VRTX システムのための Dell PowerEdge RAID コントローラ (PERC) 8 カードユーザーズガイド』* を参照してください。**
- **外部共有ストレージアダプタの場合、外付け共有 PERC 8 カードをサポートするには、CMC v2.20 以降およびメインボード v2.21 以降を更新する必要があります。**
- **外付け共有アダプタがついた 2.2 より前の CM ファームウェアはダウングレードできません。**

CMC とメインボードファームウェア をアップデートするには、次の手順を実行します。

1. CMC ファームウェアのアップデート。
2. メインボードファームウェアをアップデートします。
3. シャーシの電源をオフにし、PCIe スロット 5 およびスロット 6 に共有ストレージアダプタをインストールします。

4. シャーシの電源をオンにします。
5. シャーシの電源をオンにしたら、外付け共有ストレージアダプタを更新します。

メモ: デフォルトでは、外付け共有 PERC 8 カードは非フォールトトレラントモードです。このカードは正しく配線した後に、フォールトトレラントモードに変更する必要があります。詳細については、「共有ストレージ拡張するための PowerEdge VRTX のアップグレード」を参照してください。

イベントで、CMC または MPC/メインボードファームウェアまたは CMC および MPC ファームウェアバージョンをロールバックするには、次のタスクを実行します。

CMC とメインボードファームウェアをロールバックするには、次の手順を実行します。

1. シャーシの電源をオフにします。
2. PCI スロットからすべての外付けストレージアダプタを取り外します。
3. シャーシの電源を入れます。
4. CMC および/またはメインボードファームウェアをロールバックします。

外部共有ストレージアダプタが検出された場合、CMC をダウングレードすることはできません。

プロセスに適切に従わないと、システム動作がランダムになり、システムの一部が不安定になる恐れがあります。CMC がログを記録するのは、IOV または RAID コントローラメッセージのみです。CMC の旧バージョンに表示されるのは、PERC 1 および PERC 2 用の共有ストレージ VA マッピングのみです。すべての外付け共有ストレージ VA マッピングは、旧バージョンの CMC には存在しません。外付け共有 PERC 8 カードが、ロールバック後に挿入された場合、CMC はそれを非共有アダプタとして扱います。HOST PERC ドライバによって、外付け共有 PERC 8 カードがサポートされない場合もあります。

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

メモ:

- **CMC のアップデートを適用する前に、シャーシの電源が入っていることを確認してください。ブレードの電源が入っていても、CMC のアップデートのためにブレードの電源を切る必要はありません。**
- **外付け共有アダプタで 2.1 以前の CMC ファームウェアにダウングレードする操作はブロックされています。**

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. 左ペインで、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**
   - **シャーシの概要** > **シャーシコントローラ** > **アップデート**
2. **ファームウェアアップデート** ページの **CMC ファームウェア** セクションで、アップデートする CMC(スタンバイ CMC が存在する場合は複数になります) の **ターゲットのアップデート** 列で必要なコンポーネントを選択します。その後、**CMC アップデートを適用** をクリックします。
3. **ファームウェアイメージ** フィールドで、**参照** (Internet Explorer または Firefox) または **ファイルの選択** (Google Chrome) をクリックして、ファイルの場所を参照します。CMC ファームウェアイメージファイルのデフォルトの名前は `vrtx_cmc.bin` です。
4. **ファームウェアのアップデートを開始** をクリックします。**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。イメージファイルのアップロード中、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. 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、ファームウェアアップデートプロセスの最終フェーズで、ブラウザセッションと CMC との接続が一時的に失われます。アクティブ CMC がネットワークに接続されなくなるためです。数分後、アクティブ CMC が再起動してからログインする必要があります。CMC のリセット後、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: ファームウェアの更新後、ウェブブラウザのキャッシュからファイルを削除してください。ブラウザキャッシュのクリアの手順については、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。

補足的指示：

- ファイル転送中は、**更新** アイコンをクリックしたり、別のページに移動しないでください。
- 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** オプションを選択します。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 のアップデートプロセスには数分かかる場合があります。

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。RACADM コマンドの詳細については、『Chassis Management Controller for PowerEdge VRTX RACADM コントローラ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: 1 つのリモート racadm セッションに対してのみ 1 回だけ、ファームウェアのアップデートコマンドを実行します。

シャーシインフラストラクチャファームウェアのアップデート

シャーシインフラストラクチャアップデート操作は、メイン基板および PCIe サブシステム管理ファームウェアなどのコンポーネントをアップデートします。

メモ: シャーシインフラストラクチャファームウェアをアップデートする場合は、シャーシの電源がオンで、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。

メモ: メインボードが以降のバージョンにアップグレードされるときは、シャーシとシャーシ管理コントローラが再起動される場合があります。

CMC ウェブインタフェースを使用したシャーシインフラストラクチャファームウェアのアップデート

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**。
2. **ファームウェアアップデート** ページの **シャーシインフラストラクチャファームウェア** セクションにある **ターゲットのアップデート** 列でオプションを選択し、**シャーシインフラストラクチャファームウェアの適用** をクリックします。
3. **ファームウェアアップデート** ページで **参照** をクリックし、適切なシャーシインフラストラクチャファームウェアを選択します。
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 セクションに、ファームウェアアップデートの状態情報が表示されます。状態インジケータは、イメージファイルのアップロード中表示されます。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、ページが自動的に更新され、ファームウェアアップデートタイマーが表示されます。

追加手順：

- ファイル転送中は **更新** アイコンをクリックしたり、別のページに移動しないでください。
- **アップデート状況** フィールドにはファームウェアのアップデート状態が表示されます。

アップデートが完了すると、メイン基板がリセットされて新しいファームウェアが **ファームウェアアップデート** ページに表示されるため、メイン基板との接続が一時的に失われます。

RACADM を使用したシャーシインフラストラクチャファームウェアのアップデート

RACADM を使用してシャーシインフラストラクチャをアップデートするには、`fwupdate` サブコマンドを使用します。RACADM コマンドの使用方法の詳細については、『Chassis Management Controller for PowerEdge VRTX 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

iDRAC のファームウェアは、CMC ウェブインタフェース、または RACADM を使用してアップデートできます。この機能を使用するには、Enterprise ライセンスが必要です。

iDRAC 搭載のサーバーの場合、iDRAC ファームウェアバージョンは 1.40.40 以降であることが必要です。

ファームウェアアップデート後は、iDRAC（サーバー上）がリセットされ、一時的に使用不可になります。

メモ: Chassis Management Controller を使用して iDRAC ファームウェアをアップデートするには、シャーシ内で SD カードが使用可能である必要があります。ただし、iDRAC ウェブインタフェースを介して iDRAC ファームウェアをアップデートする場合は、CMC 内に SD カードは必要ありません。CMC からの iDRAC ウェブインタフェースの起動に関する詳細については、「サーバー状態ページからの iDRAC の起動」を参照してください。

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

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。
   - **シャーシ概要** > **アップデート**。
   - **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**。

   ファームウェアのアップデート ページが表示されます。

   メモ:

   サーバー iDRAC ファームウェアは、シャーシ概要 > サーバー概要 > アップデート を使用してアップデートすることもできます。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デート」を参照してください。
2. iDRAC7 または iDRAC8 ファームウェアをアップデートするには、それぞれ **iDRAC7 ファームウェア** または **iDRAC8 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」を参照してください。
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 iDRAC ファームウェアイメージ名は `firming.imc` 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** をクリックします。
   ァームウェアアップデートの進行状況 セクションに、ファームウェアアップデートの状態情報が表示されます。進捗バーがアップロードプロセス状態を示します。ファイル転送時間は、接続速度に応じて変化します。内部アップデート処理が始まると、ページが自動的に更新され、ファームウェアアップデートタイマーが表示されます。

   メモ: 追加手順：

   - **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。**

   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。

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 の 1 対多のアップデート機能を使用すれば、複数のサーバのサーバコンポーネントファームウェアをアップデートできます。サーバコンポーネントファームウェアは、ローカルシステムまたはネットワーク共有上の Dell Update Package（DUP）を使用してアップデートします。この操作は、サーバーの Lifecycle Controller 機能を使用しています。

Lifecycle Controller サービスは、iDRAC を利用したサーバ単位で使用可能なサービスです。サーバのコンポーネントのファームウェアとデバイスは、Lifecycle Controller サービスで管理できます。Lifecycle Controller は、ファームウェアをアップデートする際に最適化アルゴリズムを使用して、再起動の回数を効率的に削減します。

Lifecycle Controller は、iDRAC7 以降のサーバーに対してモジュールアップデートサポートを提供します。

メモ: CMC は、1 対多ファームウェア アップデート ページでの PCIE SSD カードのファームウェア アップデートをサポートしていません。

メモ: Lifecycle Controller ベースのアップデート機能を使用する前に、サーバー ファームウェアのバージョンをアップデートしておきます。

メモ: コンポーネントのファームウェアをアップデートするには、サーバで CSIOR オプションが有効になっている必要があります。

CSIOR を有効にするには、次の手順を実行します。

- 第 12 世代サーバー以降 - 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。
- 第 13 世代サーバー - サーバーを再起動した後、プロンプトが表示されたら、F10 を押して Lifecycle Controller にアクセスします。**[ハードウェア構成]** > **[ハードウェア インベントリー]** の順に選択して、[**ハードウェア インベントリー**] ページに移動します。**ハードウェアインベントリ** ページで、**再起動時にシステムインベントリを収集** をクリックします。

Update from File メソッドを使用すれば、ローカルシステムに格納された DUP ファイルを使用して、サーバコンポーネントのファームウェアをアップデートすることができます。個々のサーバコンポーネントを選択し、必要な DUP ファイルを使用して、ファームウェアをアップデートすることができます。SD カードを使用して、48 MB 以上のメモリサイズの DUP ファイルを保存することで、多数のコンポーネントを一度に更新することができます。

メモ: 次に注意してください。

- **アップデートする個別のサーバー コンポーネントを選択する場合は、選択したコンポーネント間に依存関係がないことを確認してください。アップデートの際、他のコンポーネントに依存しているコンポーネントを選択すると、サーバの機能が急に中断する原因になることがあります。**
- **推奨される順序でサーバー コンポーネントをアップデートしてください。そうでないと、コンポーネントのファームウェア アップデートの処理に失敗する可能性があります。**

  サーバーコンポーネントファームウェアは常に以下の順序でアップデートしてください。

  - **BIOS**
  - **Lifecycle Controller**
  - **iDRAC**

シングル クリックですべてのブレードをアップデートします。または、**ネットワーク共有からアップデート**する方法を使用すれば、ネットワーク共有に保存されている DUP ファイルを使用してサーバー コンポーネントのファームウェアをアップデートすることができます。Dell Repository Manager (DRM) ベースのアップデート機能を使用すると、ネットワーク共有に保存されている DUP ファイルにアクセスして、1 回の操作でサーバー コンポーネントをアップデートできます。Dell Repository Manager を使用して、ファームウェア DUP とバイナリイメージのカスタムリモートリポジトリを設定し、ネットワーク共有で共有することができます。または、Dell Repository Manager (DRM) を使用して、利用可能な最新のファームウェアアップデートを確認します。Dell Repository Manager (DRM) では、最新の BIOS、ドライバ、ファームウェア、ソフトウェアにより、Dell システムが最新の状態になっていることを確認できます。サポートサイト (**support.jp.dell.com**) では、ブランドとモデルまたはサービスタグに基づいて、対象プラットフォームの入手可能な最新のアップデートを検索できます。アップデートをダウンロードすることも、検索結果からリポジトリを作成することもできます。DRM を使用して最新のファームウェア アップデートを検索する方法については、https://www.kb.dell.com/の『*Dell Repository Manager を使用して Dell サポート サイトで最新のアップデートを検索する*』を参照してください。DRM がリポジトリーを作成するための入力として使用するインベントリー ファイルを保存する方法については、「CMC Web インターフェイスを使用したシャーシ インベントリー レポートの保存」を参照してください。

メモ: [シングル クリック] ですべてのブレードをアップデートする方法には、次の利点があります。

- **最小のクリック数で、すべてのブレードサーバーのすべてのコンポーネントをアップデートすることが可能。**
- **すべてのアップデートは、ディレクトリにパッケージ化されています。これにより、各コンポーネントのファームウェアを個別にアップロードする必要はなくなります。**
- **サーバーコンポーネントをアップデートするためのより短時間かつ一貫的な方法。**
- **サーバーコンポーネントの必要なアップデートバージョンで標準イメージを維持することができ、一回の操作で複数のサーバーをアップデートするために使用することが可能。**
- **アップデートのディレクトリは、Dell Server Update Utility (SUU) のダウンロード DVD からコピーすることができます。または、Dell Repository Manager (DRM) で必要なアップデートバージョンを作成して、カスタマイズすることもできます。このディレクトリを作成するには、最新バージョンの Dell Repository Manager は必要ありません。ただし、Dell Repository Manager バージョン 1.8 では、シャーシ内のサーバからエクスポートされたインベントリに基づいて、リポジトリ (アップデートのディレクトリ) を作成するオプションがあります。Dell Repository Manger を使用してリポジトリーを作成する方法については、『*Dell Repository Manager Data Center バージョン 1.8 ユーザーズ ガイド*』と『*Dell Repository Manager Business Client バージョン 1.8 ユーザーズ ガイド*』を参照してください。どちらも dell.com/support/manuals にあります。**

Lifecycle Controller は、iDRAC によるモジュールアップデートサポートを提供します。サーバコンポーネントのファームウェアモジュールをアップデートする前に、CMC ファームウェアをアップデートすることを推奨します。CMC のファームウェアをアップデートした後、CMC Web インターフェイスの **[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 コンポーネントの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、サーバのすべてのコンポーネントモジュールを同時にアップデートすることを推奨します。これにより、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し、再起動の回数を減らすことができます。

CMC の Web インターフェイスを使用してサーバー コンポーネントのファームウェアをアップデートするには、**[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]** の順にクリックします。

サーバが Lifecycle Controller サービスをサポートしていない場合には、**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 **未サポート** と表示されます。最新世代のサーバでは、Lifecycle Controller ファームウェアをインストールし、iDRAC ファームウェアをアップデートして、サーバで Lifecycle Controller サービスを有効にしてください。旧世代のサーバでは、このアップグレードはできません。

Lifecycle Controller のファームウェアは、サーバーのオペレーティング システムで実行される、適切なインストール パッケージを使用してインストールされます。サポートされているサーバの場合は、`.usc` ファイル拡張子を持つ特別な修復またはインストール パッケージを使用できます。このファイルがあれば、iDRAC Web ブラウザー インターフェイス上で利用できるファームウェア アップデート機能を介して、Lifecycle Controller ファームウェアをインストールすることができます。

また、サーバー オペレーティング システムで実行される適切なインストール パッケージから Lifecycle Controller ファームウェアをインストールすることもできます。詳細については、『*Dell Lifecycle Controller ユーザーズ ガイド*』を参照してください。

Lifecycle Controller サービスがサーバーで無効になっている場合、**コンポーネント / デバイスファームウェアインベントリ** セクションに次のメッセージが表示されます。

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

メモ: URI に空白文字が含まれていると、「InstallFromURI」メソッドが機能しない場合があります。

ファームウェアが同じバージョンにアップデートされた場合、EMM ファームウェア不一致の非重大エラーが [**シャーシの正常性**] ページに表示されます。この問題を解決するには、EMM アップデート後に VRTX シャーシを再起動します。

メモ: Samsung PCIe NVMe SSD カードに関しては、ファームウェア アップデート チェック ボックスが、1 対多ファームウェア アップデートのページに表示されません。

サーバーコンポーネントのアップデート順序

個々のコンポーネントのアップデートを行う場合は、次の順序に従って、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アップデートする必要があります。

- iDRAC
- Lifecycle Controller
- 診断 (オプション)
- OS ドライバパック (オプション)
- BIOS
- NIC
- RAID
- その他のコンポーネント

メモ: 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を 1 度にアップデートする場合は、アップデート手順は Lifecycle Controller で処理されます。

Lifecycle Controller の有効化

サーバーへの電源投入時に次の操作を実行することによって Lifecycle Controller サービスを有効化することができます。

- iDRAC サーバーの場合、起動コンソールで **セットアップユーティリティ** にアクセスするには、<F2> キーを押します。
- **セットアップユーティリティ メインメニュー** ページで **iDRAC 設定** > **Lifecycle Controller** に移動し、**有効** をクリックします。**セットアップユーティリティ メインメニュー** ページに移動し、**終了** をクリックして設定を保存します。

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 と対応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、

- 『Lifecycle Controller-Remote Services クイックスタートガイド』を参照してください。
- delltechcenter.com/page/Lifecycle+Controller

サーバーコンポーネントアップデート ページでは、サーバー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の権限が必要です。

- CMC：**サーバー管理者** 権限。
- iDRAC：**iDRAC 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、どのタイプの Lifecycle Controller 操作用に対してもコンポーネントまたはデバイスを選択できません。

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

サーバーコンポーネントのアップデートのタイプを選択するには、次のようにします。

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. **アップデートのタイプの選択** セクションで、必要なアップデート方法を選択します。
   - **ファイルからアップデート**
   - **ネットワーク共有からアップデート**

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

全サーバー全体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メカニズムを提供します。

メモ: この機能を使用するには、Enterprise ライセンスが必要です。

サーバーコンポーネントのアップデート ページの **コンポーネント / デバイスのアップデートフィルタ** セクションでは、コンポーネントに基づいて情報のフィルタリングが可能ですが、これは **ファイルでアップデート** モードのみで使用可能です。

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。
- タイプやモデルに基づいて特定のコンポーネントまたはデバイスのカテゴリを絞り込むための、選択されたコンポーネントおよびデバイスの自動フィルタリング。

  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。

次に、フィルタリングメカニズム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、BIOS ファームウェアアップデートイメージ (DUP) の選択が、サーバーの正しいモデルと適合することが保証されます。

  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. 左ペインで **サーバー概要** に移動し、**アップデート** をクリックします。
2. **サーバーコンポーネントアップデート** ページの **コンポーネント / デバイス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**

   コンポーネント / デバイスのアップデートフィルタ セクションは、ファームウェアアップデートの **ファイルでアップデート** モードにのみ、表示されます。

   ファームウェアインベントリ セクションには、シャーシにあるすべてのサーバーから関連付けられたコンポーネントまたはデバイスのみが表示されます。ドロップダウンメニューからアイテムを選択した後は、リスト内にあるサーバーに関連付けられたコンポーネントまたはデバイスのみが表示されます。

   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。さらなるフィルタリングが行われ、モデル、タイプ、または何らか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場合もあります。たとえば、あるサーバーのひとつの 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 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** コマンドを実行します。

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

詳細については、**dell.com/support/manuals** にある『Chassis Management Controller for PowerEdge VRTX 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。

メモ: この機能を使用するには、Enterprise ライセンスが必要です。

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. 左ペインで **サーバー概要** をクリックし、**アップデート**をクリックします。
2. **サーバーコンポーネントアップデート** ページの **コンポーネント / デバイスファームウェアインベントリ** セクションで、ファームウェアインベントリの詳細を確認します。このページでは、次の情報を表示できます。
   - 現在 Lifecycle Controller サービスをサポートしないサーバーは、**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、サーバー上のその他コンポーネントおよびデバイスはサポートしません。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 が完全に動作可能になるまで待ってから、ページを更新してインベントリを再取得します。
- コンポーネントおよびデバイスのインベントリが、サーバーに物理的に取り付けられている状態を反映しない場合は、サーバーの起動プロセス中に Lifecycle Controller を呼び出します。この処置は、内蔵コンポーネントおよびデバイス情報の更新に役立ち、現在取り付けられているコンポーネントおよびデバイスを確認できるようにします。次の場合、インベントリはコンポーネントとデバイスの情報を正確に反映しません。
  - 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。

  この処置を自動化するため、iDRAC 設定ユーティリティは起動コンソールからアクセスできるオプションを提供します。

  a. iDRAC サーバーの場合、起動コンソールで **セットアップユーティリティ** にアクセスするには、<F2> を押します。
  b. **セットアップユーティリティメインメニュー** ページで、**iDRAC 設定** > **再起動時のシステムインベントリの収集** をクリックし、**有効** を選択して **システムセットアップメインメニュー** ページに戻ります。次に、**終了** をクリックして設定を保存します。
- 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 12. 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	シャーシ内でサーバーが装着されているスロットを表示します。スロット番号は 1~4 (シャーシ内の使用可能な 4 個のスロット用) の連番 ID で、シャーシ内のおけるサーバーの場所の識別に役立ちます。スロットに装着されているサーバーが 4 台未満の場合は、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。
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	サーバー上のコンポーネントおよびデバイスの情報を表示します。列幅が狭すぎる場合、マウスオーバーツールで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状態を表示します。ジョブ状態は継続的に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でファームウェアバージョンが変更された場合に備えて、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。現在の状況の隣には情報アイコンも表示され、現在のジョブ状態に関する追加情報を提供します。この情報は、アイコンをクリックする、またはカーソルを置くことで表示できます。
アップデート	サーバー上のファームウェアをアップデートするコンポーネントまたはデバイスをクリックして選択します。

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『Chassis Management Controller for PowerEdge VRTX 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シャーシインベントリレポートの保存

シャーシ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 **サーバー概要** 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** 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. **インベントリレポートの保存** をクリックします。
   Inventory.xml ファイルが、外部システムに保存されます。

   メモ: Dell Repository Manager アプリケーションは、シャーシ内で使用可能なすべてのブレードに対するアップデートのリポジトリを作成するために、*Inventory.xml* ファイルを入力として使用します。このリポジトリは、後ほどネットワーク共有にエクスポートすることができます。ネットワーク共有からアップデート モードのファームウェアアップデートは、すべてのサーバーのコンポーネントのアップデートにこのネットワーク共有を使用します。個々のサーバーで CSIOR を有効にし、シャーシハードウェアおよびソフトウェア設定への変更が行われるたびにシャーシインベントリレポートを保存する必要があります。

CMC ウェブインタフェースを使用したネットワーク共有の設定

ネットワーク共有の場所または資格情報を設定または編集するには、次のようにします。

1. CMC ウェブインタフェースのシステムツリーで **サーバ概要** に移動し、**ネットワーク共有** をクリックします。
   ネットワーク共有の編集 ページが表示されます。

   メモ: シャーシプロファイル、サーバープロファイル、および起動 ID プロファイル用に同じフォルダを使用しているときは、プロファイルが 100 個以上になるとパフォーマンスの問題が発生する場合があります。
2. **ネットワーク共有設定** セクションで、必要に応じて次の設定を行います。
   - プロトコル
   - IP アドレスまたはホスト名
   - 共有名
   - アップデートフォルダ
   - ファイル名 (オプション)

     メモ: ファイル名 の入力は、デフォルトのカタログファイル名が `catalog.xml` の場合に限り、省略可能です。カタログファイルの名前を変更した場合は、このフィールドに新しい名前を入力する必要があります。
   - プロファイルフォルダ
   - ドメイン名
   - ユーザー名
   - パスワード
   - SMB バージョン

   メモ: SMB バージョン オプションは、プロトコル タイプが CIFS の場合にのみ使用できます。

   メモ: ドメインに登録されている CIFS を使用しており、IP と CIFS のローカルユーザー資格情報を組み合わせて CIFS にアクセスする場合には、ドメイン名 フィールドへのホスト名またはホスト IP の入力は必須です。

   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. **ディレクトリのテスト** クリックして、ディレクトリが読み取りおよび書き込み可能であるかどうかを検証します。
4. **ネットワーク接続のテスト** をクリックして、ネットワーク共有の場所にアクセスできることを確認します。
   SMB バージョンを適用すると既存のネットワーク共有がマウント解除され、**ネットワーク接続のテスト** をクリックするか他の GUI ページに移動すると再度マウントされます。
5. **適用** をクリックして、ネットワーク共有のプロパティに変更を適用します。

   メモ:

   戻る をクリックして **サーバーコンポーネントアップデート** ページに戻ります。

Lifecycle Controller のジョブ操作

メモ: この機能を使用するには、Enterprise ライセンスが必要です。

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。

操作が別のセッションまたはコンテキストを介したスケジュールのために操作が送信されている最中に、別の操作が試行されることがあります。この場合、その状況と、その操作を送信できないことを示す確認メッセージが表示されます。この操作は、処理中の操作が完了するのを待ってから、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確認メッセージを承認するようにしてください。

サーバーコンポーネントファームウェアの再インストール

1 つ、または複数のサーバー全体で、選択されたコンポーネントまたはデバイス用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。ファームウェアイメージは、Lifecycle Controller 内にあります。

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、次の手順を実行します。

1. 左ペインで、**サーバー概要** > **アップデート** をクリックします。
2. **サーバーコンポーネントアップデート** ページの **アップデートタイプの選択** セクションで、**ファイルからアップデート** を選択します。
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オプションを選択します。
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** - サーバーをただちに再起動します。
   - **次の起動時** - サーバーを後ほど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。

メモ: この機能を使用するには、Enterprise ライセンスが必要です。

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、次の手順を実行します。

1. 左ペインで、**サーバー概要→ アップデート** をクリックします。
2. **サーバーコンポーネントアップデート** ページの **アップデートタイプの選択** セクションで、 **ファイルからアップデート** を選択します。
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オプションを選択します。
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** - サーバーをただちに再起動します。
   - **次の起動時** - サーバーを後ほど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全体で、選択されたコンポーネントまたはデバイスにファームウェアイメージの後続バージョン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 内で使用可能になっています。この機能を使用するには、Enterprise ライセンスが必要です。

メモ: iDRAC およびオペレーティングシステム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ファームウェアのアップデートを初期化する前に、ジョブキューをクリアすることをお勧めします。サーバー上のすべてのジョブのリストは、**Lifecycle Controller ジョブ** ページで使用できます。このページでは、単一または複数のジョブの削除、またはサーバー上の全ジョブのパージが可能です。

BIOS アップデートはサーバーのモデル固有です。場合によっては、サーバー上でのファームウェアアップデート用に単一のネットワークインタフェースコントローラ (NIC) デバイスが選択されていたとしても、そのサーバーにあるすべての NIC デバイスにアップデートが適用されることがあります。この動作は Lifecycle Controller の機能性、とりわけ Dell Update Package (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 Update Package (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これより大きい場合、ジョブ状態にはダウンロードの失敗が示されます。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 48 M を超えることがあります。このような場合には、それらのコンポーネントアップデートのうちの 1 つのアップデートが、アップデートファイルの切り捨てによって失敗します。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には、最初に Lifecycle Controller および 32 ビット診断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。これにはサーバーの再起動が不要で、比較的短時間で完了します。その後、その他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、ファイルからの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

ファイルからアップデート モードを使用して、サーバーコンポーネントファームウェアのバージョンをアップグレードするには、次のようにします。

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** 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. **アップデートタイプの選択** セクションで、**ファイルからアップデート** を選択します。詳細については、「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タイプの選択」を参照してください。
3. **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、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)。詳細については、「CMC ウェブ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」を参照してください。
4. **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。

5. 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。
6. 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。ファームウェアのアップデートは直ちに適用されます
   - **次回の再起動時** - サーバーの再起動は後で手動で行います。ファームウェアのアップデートは、次回の再起動時に適用されます。

   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必要ありません。

7. **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。

ネットワーク共有を使用したサーバーコンポーネントのシングルクリックアップデート

Dell Repository Manager と Dell PowerEdge VRTX のモジュラー型シャーシ統合を使用したネットワーク共有からのサーバーまたはサーバーコンポーネントのアップデートでは、カスタマイズされたバンドルファームウェアの使用によってアップデートが簡素化されるため、迅速かつ容易な導入が可能になります。ネットワーク共有からのアップデートは、NFS または CIFS のいずれかから、単一のカタログを使用して第 12 世代サーバーコンポーネントのすべてを同時にアップデートする柔軟性を実現します。

この方法は、Dell Repository Manager、および CMC Web インターフェースを使用してエクスポートしたシャーシインベントリファイルで、ユーザーが所有する接続済みシステムに対して、迅速かつ容易なカスタムリポジトリの構築法を提供します。DRM では、特定のシステム設定向けのアップデートパッケージのみを含む、完全にカスタマイズされたリポジトリを作成することができ、古くなったデバイス限定のアップデートを含むリポジトリ、またはすべてのデバイスに対するアップデートを含む 1 つのベースラインリポジトリを構築することもできます。また、必要なアップデートモードに基づいて、Linux または Windows 向けのアップデートバンドルを作成することも可能です。DRM では、リポジトリを CIFS または NFS 共有に保存することができ、CMC ウェブインタフェースでは、その共有のための資格情報と場所の詳細を設定することができます。その後、CMC ウェブインタフェースを使用することにより、単一のサーバーまたは複数のサーバーに対してサーバーコンポーネントのアップデートを実行することができます。

ネットワーク共有アップデートモードを使用するための前提条件

ネットワーク共有モード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は、次の前提条件が必要です。

- サーバーが第 12 世代以降に属し、iDRAC Enterprise ライセンスがある。
- CMC バージョンが 2.0 またはそれ以降のバージョンである。

- Lifecycle Controller がサーバーで有効になっている。
- 第 12 世代サーバーで iDRAC バージョン 1.50.50 以降を使用できる。
- Dell Repository Manager 1.8 以降がシステムにインストールされている。
- CMC 管理者権限を持っている。

CMC ウェブインタフェースを使用した、ネットワーク共有からの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

ネットワーク共有からアップデート モードを使用して、サーバーコンポーネントファームウェアのバージョンをアップグレードするには、次のようにします。

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. **アップデートタイプの選択** セクションで、**ネットワーク共有からアップデート** を選択します。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デートタイプの選択」を参照してください。
3. ネットワーク共有が接続されていない場合は、シャーシのネットワーク共有を設定します。ネットワーク共有の詳細を設定または編集するには、ネットワーク共有プロパティテーブルで **編集** をクリックします。詳細については、「CMC ウェブインタフェースを使用したネットワーク共有の設定」を参照してください。
4. コンポーネントとファームウェア詳細を含むシャーシインベントリファイルをエクスポートするには、**インベントリレポートの保存** をクリックします。
   Inventory.xml ファイルは外部システムに保存されます。Dell Repository Manager は *inventory.xml* ファイルを使用して、カスタマイズされたアップデートのバンドルを作成します。このリポジトリは、CMC によって設定された CIFS または NFS 共有に保存されます。Dell Repository Manager を使用したリポジトリの作成の詳細については、**dell.com/support/manuals** で利用できる『Dell Repository Manager Data Center バージョン 1.8 ユーザーズガイド』および『Dell Repository Manager Business Client バージョン 1.8 ユーザーズガイド』を参照してください。
5. ネットワーク共有で使用できるファームウェアアップデートを表示するには、**アップデートの確認** をクリックします。
   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 セクションには、シャーシ内にあるすべてのサーバーのコンポーネントおよびデバイスの現在のファームウェアバージョンと、ネットワーク共有で利用できる DUP のファームウェアバージョンが表示されます。

   メモ: スロットに対する 折りたたむ をクリックして、特定のスロットのコンポーネントとデバイスのファームウェアの詳細を折りたたみます。または、すべての詳細を再度表示するには、展開 をクリックします。
6. **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、**すべて選択 / 選択解除** のチェックボックスを選択して、サポートされているすべてのサーバーを選択します。あるいは、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したいサーバーのチェックボックスを選択します。サーバーの個々のコンポーネントを選択することはできません。
7. 次のオプションの 1 つを選択して、アップデートのスケジュール後にシステム再起動が必要かどうかを指定します。
   - 今すぐ再起動 — アップデートがスケジュールされており、サーバーが再起動します。アップデートはただちにサーバーコンポーネントに適用されます。
   - 次回の再起動時 — アップデートはスケジュールされていますが、次回のサーバー再起動時までは適用されません。
8. **アップデート** をクリックして、選択したサーバーのアップデート可能なコンポーネントのファームウェアのアップデートをスケジュールします。
   含まれているアップデートの種類に基づいてメッセージが表示され、続行してよいかの確認を求められます。
9. **OK** をクリックして続行し、選択したサーバーのファームウェアのアップデートをスケジュールします。メモ：

   メモ: ジョブのステータス 列には、サーバーにスケジュールされている操作のジョブのステータスが表示されます。ジョブのステータスは動的に更新されます。

サーバーコンポーネントのアップデートでサポートされているファームウェアバージョン

次の項では、CMC のサーバーコンポーネントのアップデートについて説明します。

次の表は、既存の CMC ファームウェアバージョンが 3.1 であり、サーバコンポーネントが N-1 バージョンから N バージョンにアップデートされるというシナリオに対してサポートされるサーバコンポーネントの CMC ファームウェアバージョンのリストです。

メモ: CMC ファームウェアのバージョンが 2.0 以降である場合、サーバーコンポーネントの N-1 バージョンから N バージョンへのファームウェアアップデートは、次の表に記載されている第 12 世代、第 13 世代、および第 14 世代の全サーバーに対して正常に行われます。

表 13. N バージョンへのサーバーコンポーネントアップデートでサポートされているサーバーコンポーネントのバージョン

プラットフォーム	サーバーコンポーネント	以前のコンポーネントのバージョン（N-1 バージョン）	アップデート後のコンポーネントのバージョン（N バージョン）
M520	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle Controller	2.52.52.52	2.60.60.60
	診断	4231A0	4247A1
	BIOS	2.4.2	2.6.1
	NIC	19.2.0	20.00.00.13
M620	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle Controller	2.52.52.52	2.60.60.60
	診断	4231A0	4247A1
	BIOS	2.5.4	2.6.1
M820	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle Controller	2.52.52.52	2.60.60.60
	診断	4231A0	4247A1
	BIOS	2.6.1	2.6.1
M630	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle Controller	2.52.52.52	2.60.60.60
	診断	4239.44	4239A36
	BIOS	2.6.0	2.7.1
M830	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle Controller	2.52.52.52	2.60.60.60
	診断	4239.44	4239A36
	BIOS	2.5.4	2.7.1
M640	iDRAC	3.15.15.15	3.21.21.21
	Lifecycle Controller	3.15.15.15	3.21.21.21
	診断	4301A13	4301A13
	BIOS	1.3.7	1.4.8

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

メモ: この機能を使用するには、Enterprise ライセンスが必要です。

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. 左ペインで、**サーバー概要** をクリックし、**アップデート** をクリックします。
2. **サーバーコンポーネントアップデート** ページで、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** 列でチェックボックスがジョブステータスの横に表示されている場合は、Lifecycle Controller ジョブが進行中で、現在の表示されている状態であることを意味します。そのジョブは、ジョブ削除操作の対象として選択できます。
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に対するジョブが削除されます。

CMC Web インターフェイスを使用したストレージコンポーネントのアップデート

必要なストレージコンポーネントの DUP がダウンロードされていることを確認してください。

ストレージコンポーネントをアップデートするには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** > **ストレージ** > **アップデート** をクリックします。
2. **ストレージコンポーネントアップデート** ページで **参照** をクリックします。
   アップロードするファイルの選択 ダイアログボックスが表示されます。
3. 必要な DUP ファイルが Dell サポートサイトからダウンロードされて保存された場所へ移動し、DUP ファイルを選択して **開く** をクリックします。
   DUP ファイル名とパスは **参照** フィールドに表示されます。
4. [**アップロード**] をクリックします。
   DUP が CMC にアップロードされます。[**ストレージ コンポーネント アップデート**] セクションには、ダウンロードされた DUP ファイルのサポート対象であるコンポーネントのみが表示されます。コンポーネントの現在のバージョン、使用可能な最新バージョン、および [**アップデート**] チェック ボックスが表示されます。
5. 必要なコンポーネントに適切な **アップデート** チェックボックスを選択します。
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用ファームウェアのアップデート処理が開始されます。進行状況は [**アップデート**] 列に表示されます。

   処置の完了後、ファームウェアアップデートの完了または失敗を示す適切なメッセージが表示されます。

メモ:

- **ファームウェアをアップデートする前に、サーバーの電源を切っておく必要があります。**
- **コンポーネントは、システム内の他の対応するコンポーネントを同じようにアップデートします。たとえば、SPERC のアップデートは既存の SPERC と同様に、EMM アップデートは内蔵 EMM と同様に実行されます。**
- **をクリックすると、異なるエンクロージャの HDD を表示します。**

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

次に関する情報の表示と正常性の監視を行うことができます。

- 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
- IO モジュール
- ファン
- 電源装置ユニット (PSU)
- 温度センサー
- ハードディスクドライブ
- LCD アセンブリ
- ストレージコントローラ
- PCIe デバイス

メモ: 外部コンポーネントの正常性は、既存のストレージ正常性を備えたストレージコンポーネントの全体の正常性および、VRTX の内蔵ストレージコンポーネントに影響します。つまり、外部コンポーネントは、シャーシ内のコンポーネントの正常性には影響しません。

トピック：

シャーシと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** ページにシャーシとそのコンポーネントの正常性が表示されます。シャーシとそのコンポーネントのグラフィカルなビューが表示されます。これは動的にアップデートされ、コンポーネントのサブグラフィックオーバーレイとテキストヒントは、現在の状態を反映して自動的に変更されます。

シャーシの正常性を表示するには、**シャーシの概要** をクリックします。シャーシ、アクティブおよびスタンバイ CMC、サーバモジュール、IO モジュール (IOM)、ファン、ブロワー、電源ユニット (PSU)、LCD アセンブリ、ストレージコントローラ、PCIe デバイスの全体的な正常性ステータスが表示されます。コンポーネントをクリックすると、各コンポーネントに関する詳細情報が表示されます。また、CMC ハードウェアログの最新のイベントも表示されます。詳細に関しては、『*Online Help*』(オンラインヘルプ) を参照してください。

メモ: シャーシで powercycle または racreset コマンドを実行すると、「オフライン状態」であるとの物理ドライブのアラートは削除されます。

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。すべてのアクティブ、重要、非重要なアラートが表示されます。

シャーシの図解

上の図はシャーシの正面図、下の図は背面図です。サーバー、DVD、HDD、KVM、および 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。青く描かれているのはコンポーネントの選択を示します。必要なコンポーネントのイメージをクリックすると選択されます。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、チャコールグレーの背景色で表示されます。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。コンポーネントにカーソルを合わせると、そのコンポーネントの追加情報を示すツールチップが表示されます。

表 14. 第 13 世代システムでのサーバアイコン状況

アイコン	説明
	サーバが存在しており、電源がオンで、正常に動作しています。
	サーバは存在するものの、電源はオフです。
	サーバは存在するものの、非重要エラーが報告されています。

表 14. 第 13 世代システムでのサーバアイコン状況（続き）

アイコン	説明
	サーバは存在するものの、重要エラーが報告されています。
	サーバが存在しません。

表 15. 第 14 世代システムでのサーバアイコン状況

アイコン	説明
	サーバが存在しており、電源がオンで、正常に動作しています。
	サーバは存在するものの、電源はオフです。
	サーバは存在するものの、非重要エラーが報告されています。
	サーバーは存在するものの、重要エラーが報告されています。
	サーバーは存在しません。

メモ: シャーシの電源がオフのときに第 14 世代 PowerEdge サーバを挿入すると、デフォルトではデルの第 13 世代 PowerEdge システムのサーバ状況アイコンが表示されます。

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 — ハードウェアログによって表示されているアクティブ、重要、非重要イベント、および時間によって変化するパフォーマンスデータが表示されます。
- プロパティ — 時間によって変化しない、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 — アクセス頻度の高いページに移動するためのリンクと、最も頻繁に実行されるアクションが表示されます。このセクションには、選択したコンポーネントに適用できるリンクのみが表示されます。

次の表は、ウェブインタフェースの**シャーシの正常性**ページに表示されるコンポーネントプロパティと情報のリストです。

メモ: Multi-Chassis Management（MCM）では、サーバーに関連付けられているクイック リンクはすべて表示されません。

表 16. コンポーネントのプロパティ

コンポーネント	正常性とパフォーマンスプロパティ	プロパティ	クイックリンク
LCD アセンブリ	• LCD の正常性 • シャーシの正常性	• シャーシの電源ボタン • コントロールパネル LCD のロック • LCD 言語 • LCD の向き	フロントパネル設定
アクティブおよびスタンバイ CMC	• 冗長性モード • MAC アドレス • IPv4 • IPv6	• ファームウェア • スタンバイファームウェア • 最後の更新 • ハードウェア	• CMC の状態 • ネットワーク • ファームウェアアップデート
すべてのサーバーと個々のサーバー	• 電源状況 • 電力消費量 • 正常性 • 割り当てられた電力 • 温度	• 名前 • モデル • サービスタグ • ホスト名 • iDRAC • CPLD • BIOS • OS • CPU 情報 • 総システムメモリ容量	• サーバー状態 • リモートコンソールの起動 • iDRAC GUI の起動 • サーバーの電源を切る • 正常なシャットダウン • リモートファイル共有 • iDRAC ネットワークの導入 • サーバーコンポーネントアップデート **メモ: サーバーの電源を切ると正常なシャットダウンのためのクイックリンクは、サーバーの電源状態がオンの場合にのみ表示されます。サーバーの電源状態がオフの場合は、[サーバーの電源を入れる] のクイック リンクが表示されます。**
KVM スロット	正常性	• KVM のマッピング • スロット 1：前面パネル USB/ビデオ有効 • スロット 2：前面パネル USB/ビデオ有効 • スロット 3：前面パネル USB/ビデオ有効 • スロット 4：前面パネル USB/ビデオ有効	フロントパネル設定

表 16. コンポーネントのプロパティ（続き）

コンポーネント	正常性とパフォーマンスプロパティ	プロパティ	クイックリンク
DVD スロット	• 正常性 • 電源状況	• DVD のマッピング • SLOT 1：DVD 有効 • SLOT 2：DVD 有効 • SLOT 3：DVD 有効 • SLOT 4：DVD 有効	フロントパネル設定
ディスクスロット	• 正常性 • 状態	• モデル • シリアル番号 • 電源状態 • ファームウェアバージョン • サイズ • タイプ	• 物理ディスクの状態 • 物理ディスクのセットアップ • この物理ディスクのコントローラを表示 • この物理ディスクの仮想ディスクを表示
電源装置	電源状態	容量	• 電源装置の状態 • 電力消費量 • システムバジェット
PCIe デバイス	• 取り付け済み • 割り当て済み	• モデル • サーバースロットのマッピング • ベンダー ID • デバイス ID • スロット タイプ • 割り当て済み電力 • ファブリック • 電源状態	• PCIe の状態 • PCIe セットアップ
ファン	• 速度 • PWM（最大に対する割合） • ファンオフセット	• 警告しきい値 • 重要しきい値	• ファンの状態 • ファン設定
送風装置	• 速度 • PWM（最大に対する割合） • 拡張冷却モード	• 警告しきい値 • 重要しきい値	• ファンの状態 • ファン設定
SPERC スロット	• 取り付け済み • 割り当て済み	• モデル • サーバースロットのマッピング • ベンダー ID • デバイス ID • スロット タイプ • 割り当て済み電力 • ファブリック • 電源状態	• コントローラの状態 • コントローラ設定
外付け共有 PERC 8 カードスロット	• 取り付け済み • 割り当て済み	• モデル • サーバースロットのマッピング • ベンダー ID • デバイス ID • スロット タイプ • 割り当て済み電力 • ファブリック • 電源状態	• PCIe スロットの状態 • PCIe セットアップ
IOM スロット	• 電源状況 • 役割	• モデル • サービスタグ	IOM 状態

表 16. コンポーネントのプロパティ（続き）

コンポーネント	正常性とパフォーマンスプロパティ	プロパティ	クイックリンク
			IOM GUI の起動

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. 左ペインの **サーバー概要** ツリーノードに、すべてのサーバー（スロット 01 からスロット 04）がサーバーリストに表示されます。サーバーがスロットにない場合は、対応するグラフィックのイメージがグレー表示になります。フルハイトサーバーがスロット 1 とスロット 3 にある場合は、スロット 3 のスロット名が **1 の拡張** として表示されます。
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置くと、ツールチップがサーバーのモデル名とサービスタグ番号（存在する場合）と共に表示されます。

シャーシ概要の表示

シャーシ概要の情報を表示するには、左ペインで、**シャーシ概要** > **プロパティ** > **概要** をクリックします。
シャーシ概要 ページが表示されます。このページの詳細については、『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情報と状態の表示

シャーシコントローラ情報と状態を表示するには、CMC ウェブインタフェースで、**シャーシ概要** > **シャーシコントローラ** をクリックします。
シャーシコントローラ状態 ページが表示されます。詳細については『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状態の表示

すべて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。

- **シャーシ概要** をクリックします。**シャーシ正常性** ページに、シャーシに取り付けられているすべてのサーバーの概要がグラフィック表示されます。サーバーの正常性状態は、サーバーサブグラフィックのオーバーレイによって示されます。シャーシ正常性の詳細については、『オンラインヘルプ』を参照してください。
- **シャーシ概要** > **サーバー概要** をクリックします。**サーバー状態** ページに、シャーシ内のサーバーの概要が示されます。詳細については『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** > > **正常性** と移動します。
   シャーシ正常性 ページは、シャーシにインストールされたすべてのサーバーをグラフィック表示します。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オーバーレイで示されます。カーソルをそれぞれのサーバーのサブグラフィック上へ動かします。そのサーバーについてテキストヒントまたはスクリーンヒントが表示され、追加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、I/O モジュール情報が右側に表示されます。詳細については、*オンラインヘルプ*を参照してください。
2. 左ペインで、**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（1~4）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、*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 ユーザーズガイド*』を参照してください。

IOM の情報および正常性状態の表示

CMC ウェブインタフェースで IOM の正常性状態を閲覧するには、次のいずれかを実行します。

1. **シャーシ概要** をクリックします。
   シャーシ正常性 ページが表示されます。左ペインのグラフィックは、シャーシの背面図、正面図、および側面図を表示し、IOM の正常性状態も含まれています。IOM 正常性状態は、IOM サブグラフィックのオーバーレイによって示されます。テキストヒントはその IOM の追加情報を示します。右ペインに IOM の情報を表示するには、IOM サブグラフィックをクリックします。
2. **シャーシ概要** > **I/O モジュール概要**に移動します。
   I/O モジュールステータス ページには、シャーシに関連する IOM の概要が記載されています。詳細については『Online Help』(オンラインヘルプ) を参照してください。

メモ: IOM/IOA のアップデートまたは電源サイクリングの後に、IOM/IOA のオペレーティングシステムが正しくも起動されていることを確認します。正しく起動されていない場合は、IOM の状態が「オフライン」と表示されます。

ファンの情報と正常性状態の表示

CMC は、システムイベントに基づいてファン速度を増減することにより、シャーシのファン速度を制御します。ファンは、低、中、高といった 3 つのモードで稼働することができます。ファンの設定の詳細については、『オンラインヘルプ』を参照してください。

RACADM コマンドを使用してファンのプロパティを設定するには、CLI インタフェースで次のコマンドを入力します。

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

RACADM コマンドの詳細については、**dell.com/cmcmanuals** にある『*Chassis Management Controller for PowerEdge VRTX 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: CMC はシャーシ内の温度センサーを監視し、必要に応じてファン速度を自動調整します。ただし、racadm fanoffset コマンドによって、最小ファン速度を維持するように上書きすることができます。このコマンドを使用して上書きすると、CMC は、シャーシにその速度でファンを動作させる必要がなくても、常に選択された速度でファンを稼働させます。

次のイベントが発生した場合、CMC はアラートを生成し、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。
- ファンが機能停止した。
- シャーシからファンが取り外された。

メモ: サーバーにおける CMC または iDRAC ファームウェアのアップデート中は、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。

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

1. **シャーシ概要** に移動します。
   シャーシ正常性 ページが表示されます。シャーシ図の下部にはシャーシの左側が表示され、これにはファンの正常性状態が含まれています。ファンの正常性状態は、ファンのサブグラフィックのオーバーレイで示されます。カーソルをファンのサブグラフィック上に移動します。テキストヒントがファンに関する追加情報を提供します。ファン情報を右ペインに表示するには、ファンのサブグラフィックをクリックします。
2. **シャーシ概要** > **ファン** に移動します。
   ファンス状態 ページには、シャーシ内のファンの状態、速度の測定値 (毎分の回転数、RPM)、およびしきい値が表示されます。ファンは 1 台、または複数台存在する場合があります。

   メモ: CMC とファン装置間で通信障害が発生した場合、CMC はファンユニットの正常性状態を取得または表示できません。

   メモ: ファンの両方がスロットに存在しない場合、またはファンが低速回転している場合には、次のメッセージが表示されます。

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

   詳細については『オンラインヘルプ』を参照してください。

ファンの設定

ファンオフセット — シャーシのストレージおよび PCIe 領域により高い冷却機能を提供する機能です。この機能によって、HDD、共有 PERC コントローラ、および PCIe カードスロットへの送風量を増やすことができます。ファンオフセットは、たとえば、通常よりも高い冷却能力を必要とするハイパワーまたはカスタム PCIe カードを使用するときに使用します。ファンオフセット機能には、オフ、低、中、高のオプションがあります。これらの設定は、それぞれ最大速度の 20%、50%、および 100% のファン速度オフセット (上昇) に対応します。また、オプションごとに最小速度設定もあり、低は 35%、中は 65%、および高は 100% となります。

たとえば、中のファンオフセット設定を使用すると、ファン 1~6 の速度が最大速度の 50% 上昇します。この上昇は、取り付けられているハードウェア構成に基づいた冷却のためにシステムによってすでに設定されている速度を上回ります。

ファンオフセットオプションのいずれかを有効にすると、電力消費が増加します。システム音は低オフセットで大きく、中オフセットでさらに大きく、高オフセットで著しく大きくなります。ファンオフセットオプションを無効にすると、ファン速度は、取り付けられたハードウェア構成のシステム冷却に必要なデフォルト速度まで低下します。

オフセット機能を設定するには、**シャーシ概要** > **ファン** > **セットアップ** と移動します。**詳細ファン設定** ページの **ファン設定** 表で、**ファンオフセット** に対応する **値** ドロップダウンメニューから、オプションを適切に選択します。

ファンオフセット機能の詳細については、『オンラインヘルプ』を参照してください。

RACADM コマンドを使用してこれらの機能を設定するには、次のコマンドを使用します。

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

ファンオフセット関連の RACADM コマンドの詳細については、dell.com/support/Manuals にある『Chassis Management Controller for PowerEdge VRTX 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。

拡張冷却モード (ECM) — PowerEdge VRTX シャーシ内に取り付けられたサーバーのための冷却能力を増加させる CMC の機能です。ECM の使用例は、高い環境温度での稼働、またはハイパワー (≥120 W) CPU が取り付けられたサーバーの使用などです。冷却能力の増加は、4 台のシャーシ送風装置モジューをより高速で稼働させることを可能にすることによって達成されます。その結果、ECM が有効化されているときは、電力消費量と騒音レベルが高くなる場合があります。

有効化されると、ECM はシャーシ内のサーバースロットへの冷却能力のみを増加させます。また、ECM がサーバーに対して追加冷却を常に提供するように設計されていないことに留意することも大切です。ECM が有効化されていても、追加冷却が必要な場合にのみ、送風装置速度の高速化が見られます。この状況の例には、高レベルのサーバー使用率または負荷、および周囲温度が高い環境が含まれます。

デフォルトで ECM はオフです。ECM が有効化されると、送風装置はブレードごとに約 20% 増しの送風を行うことができます。

ECM モードを設定するには、**シャーシ概要** > **ファン** > **セットアップ** と移動します。**詳細ファン設定** ページの **送風装置設定** 表で、**拡張冷却モード** に対応する **値** ドロップダウンメニューから、オプションを適切に選択します。

ECM 機能の詳細については、『オンラインヘルプ』を参照してください。

前面パネルプロパティの表示

前面パネルプロパティを表示するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** > **前面パネル** をクリックします。
2. **プロパティ** ページでは、次の項目を表示できます。
   - **電源ボタンのプロパティ**
   - **LCD のプロパティ**
   - **KVM のプロパティ**
   - **DVD ドライブのプロパティ**

KVM の情報および正常性状態の表示

シャーシに関連した KVM 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. **シャーシ概要** をクリックします。
   シャーシ正常性 ページが表示されます。左ペインに、シャーシの正面図と、KVM の正常性状態が表示されます。KVM の正常性状態は、KVM サブグラフィックのレイオーバーで示されます。ポインタを KVM 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 KVM に関する追加情報を提供します。KVM サブグラフィックをクリックすると、KVM 情報が右ペインに表示されます。
2. または、**シャーシ概要** > **前面パネル** をクリックします。

状態 ページの **KVM プロパティ** セクションで、シャーシに関連付けられた KVM の状態とプロパティを確認できます。詳細については『オンラインヘルプ』を参照してください。

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、次の手順を実行します。

1. 左ペインで **シャーシ概要** をクリックします。
   シャーシ正常性 ページが表示されます。左ペインには、シャーシの正面図が表示されます。LCD の正常性状態は、LCD サブグラフィックのオーバーレイで示されます。
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して、右ペインに LCD 情報を表示します。詳細については『オンラインヘルプ』を参照してください。

   または、**シャーシ概要** > **前面パネル** > **プロパティ** > **状態** に移動します。**状態** ページの **LCD のプロパティ** で、シャーシ上で使用可能な LCD の状態を表示できます。詳細については『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。

左ペインで、**シャーシ概要** > **温度センサー** をクリックします。
温度センサー状態 ページには、シャーシ全体 (シャーシおよびサーバー) の温度プローブの状態と読み取り値が表示されます。詳細については『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編集することはできません。しきい値を超える変化には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 環境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。

ストレージコンポーネントのストレージ容量と状態の表示

ストレージコンポーネントの容量およびフォールトトレランス状態を表示するには、次のいずれかを実行します。

1. **シャーシ概要** に移動します。
   シャーシ正常性 ページが表示されます。ストレージ容量の詳細、フォールトトレランスモード (アクティブ / パッシブ)、フォールトトレランス状態 (有効) に関する情報が右ペインに表示されます。このフォールトトレランス情報は、ストレージコンポーネントのフォールトトレランス機能が有効化されている時のみ表示されます。

   シャーシ図の下部分は、シャーシの左ビューを表示します。カーソルをストレージコンポーネントのサブグラフィックに重ねると、そのストレージコンポーネントに関する追加情報を提供するテキストヒントが表示されます。ストレージコンポーネントのサブグラフィックをクリックすると、右ペインに関連情報が表示されます。
2. または、左ペインで **シャーシ概要** > **ストレージ** > **プロパティ** > **状態** とクリックします。
   次の情報が記載された **ストレージ概要** ページが表示されます。
   - シャーシに取り付けられている物理ディスクドライブのグラフ概要と、各ドライブの状態。
   - すべてのストレージコンポーネントの概要。各コンポーネントには、それぞれのページにアクセスするためのリンクが付いています。
   - ストレージの使用済み容量と合計容量。
   - コントローラ情報。

     メモ: フォールトトレランスコントローラの場合、名前の形式は、共有 <*PERC 番号*> (内蔵 <番号>) になります。例えば、アクティブなコントローラは共有 PERC8 (内蔵 1)、ピアコントローラは共有 PERC8 (内蔵 2) となります。
   - 最近ログされたストレージイベント。

   メモ: 詳細については『オンラインヘルプ』を参照してください。

6

CMC の設定

Chassis Management Controller は、リモート管理タスクを実行するためのプロパティの設定、ユーザーのセットアップ、およびアラートの設定を可能にします。

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 のセットアップおよび基本的な設定の終了後、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。
- CMC にアクセスするインタフェースを設定します。
- LCD ディスプレイを設定。
- 必要に応じてシャーシグループをセットアップ。
- サーバー、I/O モジュール、または前面パネルを設定。
- VLAN を設定。
- 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。
- 必要に応じて電力制限ポリシーを設定。

メモ: いずれの CMC インタフェース (GUI および CLI) でも、プロパティ文字列に次の文字は使用できません。

- **&#**
- **< と > の同時使用**
- **; (セミコロン)**

トピック :

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。

シャーシ上にネットワークに接続されている CMC が 2 台 (アクティブとスタンバイ) 存在する場合、フェールオーバーが生じると、スタンバイ CMC がアクティブ CMC のネットワーク設定を自動的に引き継ぎます。

IPv6 が起動時に有効化されると、3 つのルータ要請がその後 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 13 秒以上ブロックされ、IPv6 ルータ要請が送信されます。このような場合、IPv6 ルータによってルータ広告が不要に送信されるまで、IPv6 接続性が制限される期間が生じる場合があります。

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. 左ペインで、**シャーシ概要** をクリックし、**ネットワーク** をクリックします。**ネットワーク設定** ページに現在のネットワーク設定が表示されます。
2. 必要に応じて、全般、IPv4、または IPv6 の設定を変更します。詳細については『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 `getniccfg` および `getconfig` サブコマンドと共に **cfgCurrentLanNetworking** グループからのオブジェクトを使用します。

IPv6 設定を表示するには、次の `getconfig` サブコマンドと共に **cfgIpv6LanNetworking** グループからのオブジェクトを使用します。

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、『Chassis Management Controller for PowerEdge VRTX 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 を有効または無効にするには、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 IPv4 アドレス指定を有効または無効にするには、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または無効にするには、次を入力します。

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

メモ: **次に注意してください。**

- **ネットワーク設定の変更から、その変更が適用されるまでには 30 秒の遅延があります。**
- **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 <static IP address>
racadm config -g cfgLanNetworking -o cfgNicGateway <static gateway>
racadm config -g cfgLanNetworking -o cfgNicNetmask <static subnet mask>
```

IPv6 では、CMC はデフォルトで IPv6 自動設定メカニズムから CMC IP アドレスを自動的に要求して取得します。

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

CMC ネットワークインタフェースアドレスの DHCP の有効化または無効化

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 DNS アドレス用 DHCP 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、プライマリおよびセカンダリ DNS サーバーアドレスが DHCP サーバーから取得されます。この機能を使用している間、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。

DNS アドレス機能用の DHCP を無効化し、優先および代替 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 に対して DNS アドレス機能用の DHCP を無効化し、優先および代替 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 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 アドレス機能向けの DCHP が無効化されない限り、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>
```

IPv4 および IPv6 DNS 設定の設定

- **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 Name (CMC 名)** — デフォルトでは、DNS サーバー上の CMC 名は cmc-<*service tag*> です。DNS サーバー上の CMC 名を変更するには、次を入力します。

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

ここで、<*name*> は最大で 63 文字の英数字とハイフンで指定します。たとえば、cmc-1, d-345 となります。

メモ: DNS ドメイン名が指定されていない場合、最大文字数は 63 文字です。ドメイン名が指定されている場合は、CMC 名の文字数に DNS ドメイン名の文字数を足した文字数が 63 文字以下である必要があります。

- **DNS Domain Name (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 <name>
```

ここで、<*name*> は最大で 254 文字の英数字とハイフンで指定します。たとえば、p45, a-tz-1, r-id-001 となります。

IPv4 と IPv6 での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

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機能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 <duplex mode>
```

ここで、

<*duplex mode*> 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 <speed>
```

ここで、

<*speed*> は 10 または 100 (デフォルト) です。

IPv4 と IPv6 での最大転送単位の設定

最大転送単位 (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に制限を設定できます。MTU を設定するには、次を入力します。

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

ここで、<*mtu*> は 576 ~ 1500 の数値です (両端を含み、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 の IP アドレスブロック機能およびユーザーブロック機能を利用すると、パスワード推測の試みによるセキュリティ問題を防止できます。この機能は広範な IP アドレス、ならびに CMC にアクセスできるユーザーをブロックできます。デフォルトでは、IP アドレスブロック機能は CMC で有効に設定されています。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 アドレスブロック機能およびユーザーブロック機能を利用する場合は、CMC ウェブインターフェイスまたは RADCADM を使用してオプションを有効にします。ログインロックアウトポリシー設定を行うと、特定のユーザーまたは IP アドレスにログインしようとして失敗する数を設定できます。この制限を超えると、ブロックされたユーザーは、ペナルティ時間が経過した後にのみログインできます。

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. 左側のペインで、**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、左側のペインで **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*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
- 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

仮想 LAN 機能では、複数 VLAN の同じ物理ネットワークケーブル上での共存、およびセキュリティまたは負荷管理の目的でネットワークのトラフィックを分離させることができます。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。

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仮想 LAN (VLAN) 機能を有効化します。

   ```
   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*> の有効値は 1 ~ 4000、および 4021 ~ 4094 の範囲の数値です。デフォルト値は 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 priority>
   ```

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

   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
   ```

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

CMC ウェブインタフェースを使用して CMC 用仮想 LAN (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。
   - 左ペインで、**シャーシ概要** をクリックし、**ネットワーク** > **VLAN** をクリックします。
   - 左ペインで、**シャーシ概要** > **サーバー概要** をクリックし、**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。各フィールドの詳細については、『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。

シャーシ概要 > **サーバー** > **セットアップ** > **VLAN** から、このページにアクセスすることもできます。

連邦情報処理標準（FIPS）

米国連邦政府の機関および請負契約業者は、通信インタフェースを搭載したすべてのアプリケーションでコンピュータのセキュリティ規格 Federal Information Processing Standards（FIPS）を使用します。140-2 は、レベル 1、レベル 2、レベル 3、レベル 4 の 4 つのレベルで構成されています。FIPS 140-2 シリーズは、すべての通信インタフェースに次のセキュリティプロパティが必要であると規定しています。

- 認証
- 機密性
- メッセージの整合性
- 否認防止
- 可用性
- アクセス制御

プロパティのいずれかが暗号アルゴリズムに依存している場合は、FIPS がこれらのアルゴリズムを承認する必要があります。

デフォルトでは、FIPS モードは無効になっています。FIPS が有効になっている場合、OpenSSL FIPS の最小キーサイズは SSH-2 RSA 2048 ビットです。

メモ: シャーシで FIPS モードが有効になっている場合、PSU ファームウェアアップデートはサポートされません。

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。

次の機能/アプリケーションは FIPS をサポートします。

- Web GUI
- RACADM
- WSMan
- SSH v2
- SMTP
- Kerberos
- NTP クライアント
- ネットワーク ファイルシステム

メモ: SNMP は FIPS に準拠していません。FIPS モードでは Message Digest Algorithm 5(MD5)認証以外のすべての SNMP 機能が機能します。

CMC ウェブインタフェースを使用した FIPS モードの有効化

FIPS を有効にするには、次の手順を実行します。

1. 左ペインで **シャーシ概要** 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. メニューバーで **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. **連邦情報処理標準（FIPS）** セクションで、**FIPS モード**ドロップダウンメニューから、**有効化**を選択してください。
   FIPS を有効にするとリ CMC がデフォルト設定にリセットされることを通知するメッセージが表示をされます。
4. **OK** をクリックして続行します。

RACADM を使用した FIPS モードの有効化

FIPS モードを有効にするには、次のコマンドを実行します

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

。

FIPS モードの無効化

FIPS モードを無効にするには、CMC を出荷時のデフォルト設定にリセットします。

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。
- ウェブサーバー — CMC ウェブインタフェースへのアクセスを有効にします。ウェブサーバーを無効にすると、リモート RACADM も無効になります。
- 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 — CMC によるリモートサーバーへのイベントのログを有効にします。この機能を使用するには、Enterprise ライセンスが必要です。

CMC には、クライアント間で暗号化されたデータをインターネット経由で受け入れて転送するための業界標準の SSL セキュリティプロトコルを設定したウェブサーバーが含まれています。ウェブサーバーには、デルの自己署名 SSL デジタル証明書 (サーバー ID) があり、クライアントからのセキュア HTTP 要求の受け入れと応答を担います。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。

ウェブ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。ウェブサーバーのリセットは、通常以下のいずれかのイベントの結果として発生します。

- 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 ウェブユーザーインタフェースまたは RACADM を介して変更された。
- ウェブサーバーポートの設定がウェブ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: サービス設定を変更するには、シャーシ設定管理者権限が必要です。

リモート Syslog は、追加の CMC ログターゲットです。リモート Syslog を設定したら、CMC によって生成される新しい各ログエントリが、それぞれの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伝送は 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. 左ペインで **シャーシ概要** をクリックし、**ネットワーク** > **サービス** をクリックします。**サービス管理** 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
   - Web サーバー
   - SSH
   - Telnet
   - リモート RACADM
   - snmp
   - リモート Syslog

各種フィールドについての情報は、『オンラインヘルプ』を参照してください。

3. **適用** をクリックしてから、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アップデートします。

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『Chassis Management Controller for PowerEdge VRTX 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、サーバーで非対応の機能に対するプロパティ値には N/A 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、次の手順を実行します。

1. 左ペインで **シャーシ概要** に移動し、**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。
2. **リムーバブルフラッシュメディア** ページで、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。
   - **アクティブコントロールメディアを修復する**
   - **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『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。

   2 つの CMC がシャーシに存在する場合、両方の CMC (アクティブおよびスタンバイ) にフラッシュメディアが含まれている必要があります。アクティブ CMC とスタンバイ CMC にフラッシュメディアが含まれていなければ、拡張ストレージ機能が劣化します。

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、シャーシ内のリードシャーシとすべてのメンバーシャーシの状態のグラフィカル表示を生成します。この機能を使用するには、Enterprise ライセンスが必要です。

シャーシグループの機能は以下のとおりです。

- 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、サーバーと入力 / 出力インベントリが利用可能です。
- 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可能です。

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セットアップするには、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. **セットアップ** > **グループ管理** とクリックします。
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。左ペインにグループ名とリードシャーシでグループが示され、未実装のメンバーシャーシが左ペインに表示されます。

シャーシグループへのメンバーの追加

シャーシグループの設定後、そのグループにメンバーを追加するには、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. **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、メンバーシャーシに対するシャーシ管理者権限を持つユーザー名を入力します。
6. **パスワード** フィールドに、対応するパスワードを入力します。
7. オプションとして、**新しいメンバーとリーダーのプロパティを同期** を選択して、リーダーのプロパティをメンバーにプッシュします。
8. **適用** をクリックします。
9. 最大の 8 メンバーを追加するには、手順 4~8 のタスクを完了します。新しい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。

   メモ: メンバー用に入力された資格情報は、メンバーシャーシとリードシャーシ間の信頼関係を確立するため、セキュアにメンバーシャーシに渡されます。この資格情報は、いずれのシャーシにも永続するものではなく、一度信頼関係が確立された後は、再度交換されることはありません。

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. 左ペインで、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。

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. 左ペインで、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ことを伝えます。このリードシャーシは、新しいグループのリーダーまたはメンバーに割り当てることができます。

ネットワーク問題によってリーダーとメンバーの間の通信ができない場合、メンバーシャーシがメッセージを受信しない可能性があります。その場合は、メンバーシャーシからメンバーを無効にして、削除プロセス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. 左ペインで、**シャーシ概要** > **セットアップ** > **グループ管理** をクリックします。
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へのアクセス

リードシャーシグループのページから、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 iDRAC サーバーのウェブページにアクセスできます。メンバーデバイスにリードシャーシと同じログイン資格情報が設定されている場合は、その資格情報を使用してメンバーデバイスにアクセスできます。

メモ: マルチシャーシ管理では、シングルサインオンおよびスマートカードログインはサポートされていません。リードシャーシからのシングルサインオンでのメンバーへのアクセスには、リードとメンバー間で共通のユーザー名またはパスワードが必要です。共通のユーザー名またはパスワードを使用できるのは、Active Directory ユーザー、ローカルユーザー、および LDAP ユーザーを使用する場合のみです。

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** セクションに表示されるシャーシイメージで、サーバーを選択します。
   c. **クイックリンク** 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。

      メモ: MCM では、サーバーに関連付けられたすべての クイックリンク は表示されません。

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

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 **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、『オンラインヘルプ』を参照してください。

MCM グループのサーバーインベントリ

グループは、0~8 個のシャーシグループメンバーを持つリードシャーシです。**シャーシグループ正常性** ページでは、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幅のサーバーモジュールを含む)。

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. 左ペインで、**グループ** を選択します。
2. **シャーシグループ正常性** ページで、**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、または保存するかを尋ねる **ファイルダウンロード** ダイアログボックスが表示されます。
3. **保存** をクリックして、サーバーモジュール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モジュールインベントリレポートを取得するには、シャーシグループのリーダー、シャーシグループのメンバーシャーシ、および関連シャーシ内のサーバーモジュール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、シャーシグループリーダーの通常のポーリング (30 秒ごと) 中に各シャーシグループメンバーによって最近返されたデータが含まれます。

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 **シャーシ電源状況オン** 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。

- **シャーシ電源状況オフ** 状況
- 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、シャーシの電源が再びオンになるまで、モデル番号はウェブインタフェースのどこにも表示されません。

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 17. サーバーモジュール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
Service Tag	1PB8VF1
総システムメモリ容量	4.0 GB

表 17. サーバーモジュールインベントリフィールドの説明（続き）

データフィールド	例
	メモ: メンバー上に VRTX CMC 1.0（以降）が存在している必要があります。存在しなければ、何も表示されません。
CPU の数	2 メモ: メンバー上に VRTX CMC 1.0（以降）が存在している必要があります。存在しなければ、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 VRTX CMC 1.0（以降）が存在している必要があります。存在しなければ、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 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 .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 にインポートした後で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、左ペインで **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. 左側のペイン **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。

シャーシ構成プロファイル

シャーシ設定プロファイルの機能では、ネットワーク共有またはローカル管理ステーションに保存されているシャーシ設定プロファイルを使用して、シャーシの設定ができるだけでなく、シャーシの設定の復元も可能です。

CMC ウェブインタフェースで **シャーシ設定プロファイル** のページにアクセスするには、システムツリーで **シャーシの概要** に移動し、**設定** > **プロファイル** の順にクリックします。**シャーシ設定プロファイル** のページが表示されます。

シャーシ設定プロファイル機能を使用して、次のタスクを実行することができます。

- ローカル管理ステーションのシャーシ設定プロファイルを使用してシャーシを設定し、初期設定を行います。
- 現在のシャーシ設定をネットワーク共有またはローカル管理ステーション上の XML ファイルに保存します。
- シャーシの設定を復元します。
- ローカル管理ステーションからネットワーク共有へシャーシのプロファイル (XML ファイル) をインポートします。
- ネットワーク共有からローカル管理ステーションへシャーシのプロファイル (XML ファイル) をエクスポートします。
- ネットワーク共有上に保管されたプロファイルを適用、編集、削除またはエクスポートします。

シャーシ設定の保存

現在のシャーシの設定を、ネットワーク共有またはローカル管理ステーション上の XML ファイルに保存することができます。保存できる設定には、CMC ウェブインタフェースと RACADM コマンドを使用して変更可能なすべてのシャーシのプロパティが含まれます。同一のシャーシ上に設定を復元するため、またはその他のシャーシを設定するために保存した XML ファイルを使用することもできます。

メモ: サーバーおよび iDRAC の設定は、シャーシの設定と一緒に保存または復元されません。

現在のシャーシの設定を保存するには、次のタスクを実行します。

1. **シャーシ設定プロファイル** のページに移動します。**保存およびバックアップ** > **現在の設定の保存** のセクションで、**プロファイル名** フィールドにプロファイルの名前を入力します。

   メモ: 現在のシャーシ構成を保存する際は、標準 ASCII 拡張文字セットがサポートされています。 ただし 、次の特殊文字は使用できません。

   “、,、*、>、<、\、/、:、および | はサポートされません。

2. **プロファイルタイプ** オプションで、次のプロファイルタイプのいずれかを選択します。
   - **置換** — このプロファイルタイプは、ユーザーパスワードおよびサービスタグなど書き込み専用の属性以外の CMC 全体構成の属性で構成されています。このプロファイルタイプは、IP アドレスなどの個人情報を含む完全なシャーシ設定を復元するバックアップファイルとして使用されます。
   - **クローン** — このプロファイルタイプには、すべての **置換** タイプのプロファイル属性が含まれます。MAC アドレスおよび IP アドレスなどの ID 属性は、安全を期すためにコメントアウトされています。このプロファイルタイプは新しいシャーシのクローン作成に使用されます。
3. **プロファイルの場所** ドロップダウンメニューから次のいずれかの場所を選択して、プロファイルを保存します。
   - **ローカル** — ローカル管理ステーションにプロファイルを保存します。

- **ネットワーク共有** — 共有されている場所にプロファイルを保存します。

4. **保存** をクリックして、選択した場所にプロファイルを保存します。
   操作が完了すると、Operation Successful のメッセージが表示されます。

   メモ: XML ファイルに保存されている設定を表示するには、保存プロファイル セクションで、保存されているファイルを選択して、プロファイルの表示 列で 表示 をクリックます。

シャーシ設定プロファイルの復元

バックアップファイル (.xml または .bak) をローカルの管理ステーションまたはシャーシの設定が保存されているネットワーク共有にインポートすることでシャーシの設定を復元することができます。設定には、CMC ウェブインタフェース、RACADM コマンド、または設定で利用可能なすべてのプロパティが含まれます。

シャーシを復元するには、次のタスクを実行します。

1. **シャーシ設定プロファイル** ページに移動します。**設定の復元** > **シャーシ設定の復元** のセクションで、**参照** をクリックして、保存されたシャーシ設定をインポートするためのバックアップファイルを選択します。
2. **設定の復元** をクリックして、暗号化されたバックアップファイル (.bak) または .xml の保存されたプロファイルのファイルを CMC にアップロードします。
   復元操作が正常に完了すると、CMC ウェブインタフェースはログインページに戻ります。

メモ: CMC の以前のバージョンのバックアップファイル (.bak) が FIPS が有効な CMC の最新バージョンにロードされている場合、すべての 16 の CMC ローカルユーザーのパスワードを再設定します。しかし、最初のユーザーのパスワードは「calvin」にリセットされます。

メモ: シャーシ構成プロファイルが、FIPS 機能をサポートしていない CMC から、FIPS が有効化されている CMC へインポートされている場合、FIPS は CMC で有効のまま保持されます。

メモ: シャーシ構成プロファイルで FIPS モードを変更する場合は、DefaultCredentialMitigation が有効です。

保存シャーシ設定プロファイルの表示

ネットワーク共有に保存されたシャーシ設定プロファイルを表示するには、**シャーシ設定プロファイル** ページに移動します。**シャーシ設定プロファイル** > **保存プロファイル** のセクションで、プロファイルを選択して、**プロファイルの表示** の列で **プロファイルの表示** をクリックします。**設定の表示** ページが表示されます。表示される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。

シャーシ設定プロファイルの適用

シャーシ設定プロファイルがネットワーク共有上に保存されたプロファイルとして存在する場合に、シャーシの設定をシャーシに適用することができます。シャーシ設定操作を始めるには、保存されているプロファイルをシャーシに適用します。

シャーシにプロファイルを適用するには、次のタスクを実行します。

1. **シャーシ設定プロファイル** ページに移動します。**保存プロファイル** のセクションで適用したい保存されたプロファイルを選択します。
2. **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。
3. **OK** をクリックして、シャーシにプロファイルを適用します。

シャーシ設定プロファイルのエクスポート

ネットワーク共有に保存されているシャーシ設定プロファイルを、管理ステーション上の指定し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、次のタスクを実行します。

1. **シャーシ設定プロファイル** ページに移動します。**シャーシ設定プロファイル** > **保存プロファイル** のセクションで必要なプロファイルを選択してから、**プロファイルのコピーのエクスポート** 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。

シャーシ設定プロファイルの編集

シャーシのシャーシ設定プロファイル名を編集することができます。

シャーシ設定プロファイル名を編集するには、次のタスクを実行します。

1. **シャーシ設定プロファイル** のページに移動します。**シャーシ設定プロファイル** > **保存プロファイル** のセクションで、必要なプロファイルを選択して、**プロファイルの編集** をクリックします。
   プロファイルの編集 ウィンドウが表示されます。
2. **プロファイル名** のフィールドに希望するプロファイル名を入力して、**プロファイルの編集** をクリックします。
   `Operation Successful` のメッセージが表示されます。
3. **OK** をクリックします。

シャーシ設定プロファイルの削除

ネットワーク共有に保存されているシャーシ設定プロファイルを削除することができます。

シャーシ設定プロファイルを削除するには、次のタスクを実行します。

1. **シャーシ設定プロファイル** のページに移動します。**シャーシ設定プロファイル** > **保存プロファイル** のセクションで、必要なプロファイルを選択して、**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。

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 カードをクエリすると、RACADM は取得した情報から `racadm.cfg` 設定ファイルを作成します。このファイルを 1 つ、または複数の CMC にエクスポートすることにより、お使いのコントローラを最短の時間で同じプロパティに設定できます。

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. 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
   ```

   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 config -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、ファイル名の変更、または別の場所への保存を行うことができます。

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。

CMC 設定ファイルの作成

CMC 設定ファイル <filename>.cfg は、単純なテキストファイルを作成するために racadm config -f <filename>.cfg コマンドと共に使用されます。このコマンドを使用すると、(.ini ファイルに類似した) 設定ファイルを構築し、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、『Chassis Management Controller for PowerEdge VRTX 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、.cfg ファイルが CMC に初めてロードされるときにそのファイルを解析して、有効なグループ名およびオブジェクト名が存在し、シンプルな構文規則に沿っていることを検証します。エラーはエラーを検知した行番号と共に示され、メッセージによりその問題が説明されます。正確性についてファイル全体が解析され、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、書き込みコマンドは CMC に転送されません。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、config サブコマンドで -c オプションを使用します。-c オプションを使用すると、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変更されたものです。変更されたオブジェクトが新しいインデックスを表す場合、設定中にそのインデックスが CMC に作成されます。
- 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。

  インデックスは作成したり、削除したりすることができます。時間が経過するにつれて、使用済みおよび未使用のインデックスでグループが断片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、管理されているすべての CMC 間でインデックスを完全に一致させる必要がないので、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、最初に使用できるインデックスに追加されます。1 つの CMC で正しく解析および実行される .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する必要がある場合、正しく実行されない可能性があります。
- 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 サブコマンドを使用して CMC を初期の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てください。オブジェクトおよびグループの詳細については、『Chassis Management Controller for PowerEdge VRTX 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。

  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 <filename> .cfg と入力すると、このコマンドは現在の CMC 設定用に .cfg ファイルを構築します。この設定ファイルは、独自の .cfg ファイルのサンプルおよび基礎として使用できます。

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 1 列目から開始する必要があります。他の列の「#」文字は、# という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しないで別の CMC に対して racadm config -f <filename> .cfg コマンドを実行することができます。

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 [文字は 1 列目にある必要があります。このグループ名は、そのグループ内の任意のオブジェクトの前に指定する必要があります。関連付けられたグループ名を含まないオブジェクトがあると、エラーが発生します。設定データは、『Chassis Management Controller for PowerEdge VRTX 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。次の例は、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を示しています。

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

- すべてのパラメータは、「object」、「=」、または「value」の間に空白を入れず、「object=value」のペアとして指定されます。値の後ろにある空白は無視されます。値の文字列内にある空白は変更されないまま残ります。= 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 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。インデックスが既に存在する場合は、そのインデックスが使用されるか、そのグループで最初に使用可能なインデックス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 1-4> <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 は設定ファイルを解析するときに停止し、エラーが発生したことを警告します。

  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 1-4> ""
```

  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 1-4>
```

- 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。これらの設定グループを別の CMC にクローンする必要がある場合は、キープロパティを設定してから、getconfig -f コマンドを実行する必要があります。または、getconfig -f コマンドを実行した後に、不足しているプロパティを設定ファイルに手動で入力することもできます。これは、すべての RACADM インデックス付きグループに適用されます。

  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 <variable> = <value> 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 <variable> = <value> 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。

このファイルを使用して、会社全体の変更をダウンロードしたり、racadm getconfig -f <myfile>.cfg< コマンドで新しいシステムをネットワーク経由で設定します。

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。

シャーシ設定プロファイルを使用した RACADM での複数の CMC の設定

シャーシ設定プロファイルを使用して、シャーシ設定プロファイルを XML ファイルとしてエクスポートしたり、別のシャーシにインポートしたりすることができます。

RACADM の get コマンド用をエクスポート操作に使用し、set コマンドをインポート操作に使用します。CMC からネットワーク共有またはローカル管理ステーションにシャーシのプロファイル (XML ファイル) をエクスポートしたり、ネットワーク共有またはローカル管理ステーションからプロファイル (XML ファイル) をインポートできます。

メモ: デフォルトでは、エクスポートはクローンタイプとして行われます。--clone を使用して XML ファイル内のクローンタイププロファイルを取得できます。

ネットワーク共有とのインポートまたはエクスポート操作は、ローカル RACADM またはリモート RACADM で行うことができます。それに対して、ローカル管理とのインポートまたはエクスポート操作はリモート RACADM インタフェースでのみ行うことができます。

シャーシ設定プロファイルのエクスポート

get コマンドを使用して、シャーシ設定プロファイルをネットワーク共有にエクスポートできます。

1. get コマンドを使用して、シャーシ設定プロファイルを clone.xml ファイルとしてエクスポートするには、次のように入力します。

```
racadm get -f clone.xml -t xml -l //xx.xx.xx.xx/PATH -u USERNAME -p PASSWORDCMC
```

2. get コマンドを使用して、シャーシ設定プロファイルを clone.xml ファイルとして NFS ネットワーク共有にエクスポートするには、次のように入力します。

```
racadm get -f clone.xml -t xml -l xx.xx.xx.xx:/PATH
```

リモート RACADM インタフェースを使用して、シャーシ設定プロファイルをネットワーク共有にエクスポートできます。

1. シャーシ設定プロファイルを clone.xml ファイルとして CIFS ネットワーク共有にエクスポートするには、次のように入力します。

```
racadm -r xx.xx.xx.xx -u USERNAMECMC -p PASSWORDCMC get -f clone.xml -t xml -l //
xx.xx.xx.xx/PATH -u USERNAME -p PASSWORD
```

2. シャーシ設定プロファイルを clone.xml ファイルとして NFS ネットワーク共有にエクスポートするには、次のように入力します。

```
racadm -r xx.xx.xx.xx -u USERNAMECMC -p PASSWORDCMC get -f clone.xml -t xml -l
xx.xx.xx.xx:/PATH
```

リモート RACADM インタフェースを使用して、シャーシ設定プロファイルをローカル管理ステーションにエクスポートすることができます。

1. clone.xml ファイルとして、シャーシ設定プロファイルをエクスポートするには、次のように入力します。

```
racadm -r xx.xx.xx.xx -u USERNAMECMC -p PASSWORDCMC get -f clone.xml -t xml
```

シャーシ設定プロファイルのインポート

set コマンドを使用して、シャーシ設定プロファイルをネットワーク共有から別のシャーシへインポートすることができます。

1. CIFS ネットワーク共有から、シャーシ設定プロファイルをインポートするには、次のように入力します。

```
racadm set -f clone.xml -t xml -l //xx.xx.xx.xx/PATH -u USERNAME -p PASSWORDCMC
```

2. NFS ネットワーク共有から、シャーシ設定プロファイルをインポートするには、次のように入力します。

```
racadm set -f clone.xml -t xml -l xx.xx.xx.xx:/PATH
```

リモート RACADM インタフェースを使用して、シャーシ設定プロファイルをネットワーク共有からインポートすることができます。

1. CIFS ネットワーク共有から、シャーシ設定プロファイルをインポートするには、次のように入力します。

```
racadm -r xx.xx.xx.xx -u USERNAMECMC -p PASSWORDCMC  set -f clone.xml -t xml -l //
xx.xx.xx.xx/PATH -u USERNAME -p PASSWORD
```

2. NFS ネットワーク共有から、シャーシ設定プロファイルをインポートするには、次のように入力します。

```
racadm -r xx.xx.xx.xx -u USERNAMECMC -p PASSWORDCMC set -f clone.xml -t xml -l
xx.xx.xx.xx:/PATH
```

リモート RACADM インタフェースを使用して、シャーシ設定プロファイルをローカル管理ステーションからインポートすることができます。

1. clone.xml ファイルとして、シャーシ設定プロファイルをエクスポートするには、次のように入力します。

```
racadm -r xx.xx.xx.xx -u USERNAMECMC -p PASSWORDCMC set -f clone.xml -t xml
```

構文解析規則

シャーシ設定プロファイルのエクスポートされた XML ファイルのプロパティを手動で編集することができます。

XML ファイルには次のプロパティが含まれています。

- **システム構成**：親ノードです。
- **コンポーネント**：プライマリの子ノードです。
- **属性**：名前と値があります。これらのフィールドは編集できます。たとえば、Asset Tag の値を次のように編集できます。

```
<Attribute Name="ChassisInfo.1#AssetTag">xxxxxx</Attribute>
```

XML ファイルの例は次のとおりです。

```
<SystemConfiguration Model="PowerEdge M1000e
"ServiceTag="NOBLE13"
TimeStamp="Tue Apr  7 14:17:48 2015" ExportMode="2">
<!--Export type is Replace-->
<!--Exported configuration may contain commented attributes. Attributes may be commented due
to dependency,
destructive nature, preserving server identity or for security reasons.-->
<Component FQDD="CMC.Integrated.1">
<Attribute Name="ChassisInfo.1#AssetTag">00000</Attribute>
<Attribute Name="ChassisLocation.1#DataCenterName"></Attribute>
<Attribute Name="ChassisLocation.1#AisleName"></Attribute>
<Attribute Name="ChassisLocation.1#RackName"></Attribute>
….
</Component>
</SystemConfiguration>
```

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. 左側のペインで、**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、*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、セッションの **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、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。

これらのオブジェクトの詳細については、**dell.com/support/manuals** にある『*Chassis Management Controller for PowerEdge VRTX 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

サーバーの次の設定を行うことができます。

- スロット名
- iDRAC ネットワーク設定
- DRAC 仮想 LAN タグ設定
- 最初の起動デバイス
- サーバー FlexAddress
- リモートファイル共有
- サーバークローンを使用した BIOS の設定

トピック：

スロット名の設定

スロット名は個別のサーバを識別するために使用します。スロット名を選択する際には、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 ~ 126) を最大 24 文字含めることができます。標準および特殊文字を名前に使用できます。
- スロット名は、シャーシ内で一意である必要があります。スロットには同じ名前を付けることはできません。
- 文字列では大文字と小文字が区別されません。`Server-1`, `server-1`, and `SERVER-1` は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-
  - DRAC-
  - MC-
  - シャーシ
  - Housing-Left
  - Housing-Right
  - Housing-Center
- 文字列 `Server-1` ~ `Server-4` は使用できますが、使用できるのは対応スロットのみです。例えば、`Server-3` はスロット 3 には有効な名前ですが、スロット 4 には無効です。ただし `Server-03` は、どのスロットでも有効な名前です。

  メモ: スロット名を変更するには、シャーシ設定管理者 権限が必要です。

ウェブインタフェースのスロット名の設定は、CMC にのみ存在します。サーバがシャーシから取り外されると、スロット名の設定とそのサーバとの関連付けはなくなります。

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上書きします。

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、次の手順を実行します。

1. 左ペインで、**シャーシ概要** > **サーバー概要** > **セットアップ** > **スロット名** に移動します。
2. **スロット名** ページの **スロット名** フィールドで、スロット名を編集します。

3. サーバのホスト名をスロット名として使用するには、**スロット名にホスト名を使用** オプションを選択します。これにより、サーバのホスト名（またはシステム名）が存在する場合は、静的なスロット名がそのホスト名（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.com/support/manuals の『*Dell OpenManage Server Administrator ユーザーズガイド*』を参照してください。
4. iDRAC DNS の名前をスロット名として使用するには、**スロット名に iDRAC DNS 名を使用** オプションを選択します。このオプションによって、iDRAC DNS 名がある場合は、その名前が静的スロットと入れ替わります。iDRAC DNS 名がない場合は、デフォルトのスロット名または編集されたスロット名が表示されます。

   メモ: スロット名に iDRAC DNS 名を使用 オプションを使用するには、シャーシ設定管理者 権限が必要です。

5. 設定を保存するには、**適用** をクリックします。

デフォルトのスロット名（サーバのスロット位置に基づいた SLOT-01～SLOT-04）をサーバに復元するには、**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

この機能を使用するには、Enterprise ライセンスが必要です。サーバーの iDRAC ネットワーク設定を行うことができます。後でインストールされるサーバー用には、QuickDeploy 設定を使用してデフォルトの iDRAC ネットワーク設定とルートパスワードを指定できます。これらのデフォルト設定は、iDRAC QuickDeploy の設定です。

iDRAC の詳細については、**dell.com/support/manuals** で『*iDRAC User's Guide*』（iDRAC ユーザーズガイド）を参照してください。

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。

iDRAC QuickDeploy の設定を有効にし、設定を行うには、次の手順を実行します。

1. 左ペインで、**サーバー概要** > **セットアップ** > **iDRAC** をクリックします。
2. [**iDRAC の導入**] ページの [**QuickDeploy 設定**] セクションで、次の表に記載されている設定を指定します。各フィールドの詳細については、*オンライン ヘルプ*を参照してください。

表 18. QuickDeploy 設定

設定	説明
サーバーが挿入される時の処置	リストから次のいずれかのオプションを選択します。 ・ 処置なし — サーバーが挿入されたときに処置は実行されません。 ・ QuickDeploy のみ — このオプションを選択して、新しいサーバがシャーシに挿入されたときに、iDRAC ネットワーク設定を適用します。指定された自動展開の設定は新規 iDRAC の設定に使用され、root パスワードの変更 が選択されている場合は root ユーザーパスワードが含まれます。 ・ サーバープロファイルのみ — このオプションを選択して、新しいサーバーがシャーシに挿入された時に、割り当てられたサーバープロファイルを適用します。 ・ QuickDeploy とサーバープロファイル — このオプションを選択して、新規サーバーがシャーシに挿入された時、まず最初に iDRAC ネットワーク設定を適用してから、割り当てられたサーバープロファイルを適用します。
サーバー挿入時に iDRAC root パスワードを設定する	このオプションを選択して、サーバーが挿入されたときに **iDRAC root パスワード** フィールドに入力された値と一致するように iDRAC root パスワードを変更します。
iDRAC root パスワード	[**サーバー挿入時に iDRAC root 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ると、このパスワードの値がサーバーの iDRAC root ユーザー パスワードに割り当てられます。パスワードには、印刷可能な 1～20 文字（空白含む）を使用することができます。
iDRAC root パスワードの確認	**パスワード** フィールドに入力したパスワードを再入力します。
iDRAC LAN の有効化	iDRAC LAN チャネルを有効または無効にします。デフォルトで、このオプションは選択されていません。

表 18. QuickDeploy 設定（続き）

設定	説明
iDRAC IPv4 の有効化	iDRAC で IPv4 を有効または無効にします。デフォルトでは、このオプションが選択されています。
iDRAC IPMI over LAN の有効化	シャーシに搭載されている各 iDRAC の IPMI over 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、このオプションが選択されています。
iDRAC IPv4 DHCP の有効化	シャーシ内の各 iDRAC の DHCP 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**]、[**QuickDeploy IP サブネット マスク**]、[**QuickDeploy IP ゲートウェイ**] のフィールドは無効になり変更できません。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ます。このオプションを選択するには、[**iDRAC IPv4 の有効化**] オプションを選択する必要があります。Quick Deploy IP アドレスには、2 と 4 の 2 つのオプションがあります。
開始 iDRAC IPv4 アドレス（スロット 1）	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 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することはありません。** たとえば、開始 IP アドレスが `192.168.0.250`、サブネット マスクが `255.255.0.0` の場合は、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` の場合、[**QuickDeploy 設定の保存**] または [**QuickDeploy 設定を使用した自動入力**] をクリックすると、エラー メッセージの「`QuickDeploy IP address range is not fully within QuickDeploy Subnet`」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	シャーシに存在するすべての DRAC に割り当てられる QuickDeploy デフォルトゲートウェイを指定します。
iDRAC IPv6 の有効化	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 自動設定の有効化	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。
CMC DNS 設定の使用	ブレードサーバーがシャーシに挿入されると、CMC DNS サーバー設定（IPv4 および IPv6）が iDRAC に通知されます。
iDRAC DNS 名の有効化	iDRAC DNS 名の有効化 を選択して、シャーシに挿入されているブレードサーバに iDRAC DNS 名のプレフィックスを適用します。デフォルトでは、iDRAC DNS 名の有効化 は無効になっています。
iDRAC DNS 名（プレフィックス）	iDRAC DNS 名のプレフィックスを設定できるのは、iDRAC DNS 名の有効化 が選択されている場合のみです。DNS 名のプレフィックスは、最長で 59 文字、最短で 1 文字にしてください。サポートされる文字は次のとおりです。 ・ 英数字：「a ~ b」または「A ~ B」 ・ 数字：「0 ~ 9」 ・ ハイフン：「-」 DNS 名のプレフィックスはハイフンで始まらないようにしてください。デフォルトのプレフィックスは「idrac」です。サーバプロファイルには、iDRAC DNS 名のプレフィックスのみが保存されます。

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 機能が実行されるのは、有効化されており、シャーシにサーバーを挿入されている場合のみです。[**サーバー挿入時に iDRAC root パスワードを設定する**] および [**QuickDeploy を有効にする**] が選択されている場合、LCD インターフェイスを使用してパスワードの変更を許可または許可しないように指示するプロンプトが表示されます。現在の iDRAC 設定とは異なるネットワーク設定がある場合、ユーザーはその変更の適用を受け入れるかどうか選択を求めるプロンプトが表示されます。

   メモ: LAN または IPMI over LAN の違いがある場合は、QuickDeploy IP アドレスの設定を受け入れるよう求められます。DHCP の設定が異なる場合は、DHCP QuickDeploy 設定を受け入れるよう求められます。

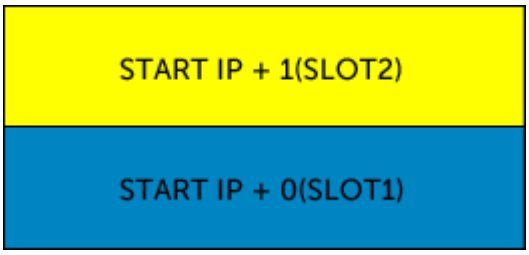
   QuickDeploy 設定を **iDRAC ネットワーク設定** セクションにコピーするには、**QuickDeploy 設定を使用して自動入力する** をクリックします。QuickDeploy ネットワーク構成設定が、 **iDRAC ネットワーク構成設定** テーブルの対応するフィールドにコピーされます。

   メモ: QuickDeploy フィールドへの変更は即座に反映されますが、iDRAC サーバー ネットワークの 1 つ以上の設定を変更した場合は、CMC から iDRAC に反映されるまでに数分かかることがあります。[更新] のクリックが早すぎると、1 台以上の iDRAC サーバーで、データが部分的にしか正しく表示されないことがあります。

サーバーへの QuickDeploy IP アドレスの割り当て

この図は、VRTX シャーシ内にハーフハイトサーバーが 4 台搭載されているときのサーバーに対する QuickDeploy IP アドレス割り当てを示しています。

次の図は、VRTX シャーシ内にフルハイトブレードが 2 台搭載されているときのサーバーに対する QuickDeploy IP アドレス割り当てを示しています。



個々のサーバー iDRAC の iDRAC ネットワーク設定の変更

この機能を使用すると、インストールされている各サーバーの iDRAC ネットワーク構成を設定できます。各フィールドに表示される初期値は、iDRAC から読み取られた現在の値です。この機能を使用するには、Enterprise ライセンスが必要です。

iDRAC ネットワーク設定を変更するには、次の手順を実行します。

1. 左ペインで [**サーバー概要**] をクリックし、**[セットアップ]** をクリックします。[**iDRAC の導入**] ページの [**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 DNS 名、IPv4 および IPv6 ネットワークの設定値が表示されます。
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: [LAN を有効にする] オプションを選択して、IPv4 または IPv6 設定を指定する必要があります。各フィールドの詳細については、*オンライン ヘルプ*を参照してください。

3. 設定を iDRAC に導入するには、[**iDRAC ネットワーク設定の適用**] をクリックします。[**QuickDeploy 設定**] に加えた変更も保存されます。

[**iDRAC ネットワーク設定**] の表には、今後のネットワーク設定値が反映されます。インストールされているサーバー用に表示される値は、現在インストールされている iDRAC ネットワーク設定と同じ場合と異なる場合があります。[**更新**] をクリックして、変更後のインストールされている各 iDRAC ネットワーク設定値で [**iDRAC の導入**] ページをアップデートします。

メモ: QuickDeploy フィールドへの変更は即座に反映されますが、iDRAC サーバー ネットワークの 1 つ以上の設定を変更した場合は、CMC から iDRAC に反映されるまでに数分かかることがあります。[更新] のクリックが早すぎると、1 台以上の iDRAC サーバーで、データが部分的にしか正しく表示されないことがあります。

RACADM を使用した iDRAC ネットワーク設定の変更

RACADM の `config` または `getconfig` コマンドでは、次の設定グループに対する `-m <module>`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と範囲の詳細については、**dell.com/support/manuals** にある『*Chassis Management Controller for PowerEdge VRTX 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 仮想 LAN タグの設定

仮想 LAN (VLAN) タグでは、同じ物理ネットワークケーブル上での複数 VLAN の共存、およびセキュリティまたは負荷管理を目的としたネットワークトラフィックの分離が可能です。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、コンポーネントを取り外した後もシャーシに残ります。

メモ: CMC を使用して設定された VLAN ID は、iDRAC が専用モードのときにのみ iDRAC に適用されます。iDRAC が共有 LOM モードである場合、iDRAC で行われた VLAN ID の変更は CMC GUI で表示されません。

RACADM を使用した iDRAC 仮想 LAN タグの設定

- 次のコマンドを使用して、特定サーバーの仮想 LAN 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 1~4 です。

  <*VLAN*> の有効値は 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 1~4 です。

  たとえば、次のとおりです。

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

ウェブインタフェースを使用した iDRAC 仮想 LAN タグの設定

サーバー用の 仮想 LAN (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。
   - 左ペインで、**シャーシ概要** > **ネットワーク** > **VLAN** をクリックします。
   - 左ペインで、**シャーシ概要** > **サーバー概要** をクリックし、**セットアップ** > **VLAN** をクリックします。
2. **VLAN タグ設定** ページの **iDRAC** セクションで、各サーバーに対して VLAN を有効にし、優先順位を設定して、ID を入力します。各フィールドの詳細については、『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。

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を示すもの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、そのサーバーの最初の起動デバイスとして使用されるデバイスです。このデバイスは、最初のデフォルト起動デバイスとして設定できるほか、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として設定することもできます。

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。システムの最初の起動デバイスを設定することもできます。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(**シャーシ概要** > **サーバー概要** > **セットアップ** > **最初の起動デバイス**) または BIOS 起動順序のどちらかで再度変更されるまでは、最初の起動デバイスとして維持されます。

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 19. 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 または 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起動ディスク上にあり、iDRAC GUI コンソールビューアで連結されます。
ローカル SD カード	ローカル SD カードから起動します (iDRAC 6 および iDRAC 7 システムをサポートするサーバーのみで可能)。
ローカルフロッピー	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。
リモートファイル共有	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。

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 権限または シャーシ設定システム管理者 権限、および iDRAC ログイン 権限を持っている必要があります。

複数のサーバーに最初の起動デバイスを設定するには、次の手順を実行します。

1. 左ペインで、**サーバー概要** > **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** 列で、サーバーに対応する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

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 が必要です。

個々のサーバーに最初の起動デバイスを設定するには、次の手順を実行します。

1. 左ペインで、**サーバー概要** をクリックし、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 **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。
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『Chassis Management Controller for PowerEdge VRTX 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 FlexAddress の設定

サーバーの FlexAddress の設定については、「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」を参照してください。この機能を使用するには、Enterprise ライセンスが必要です。

リモートファイル共有の設定

リモート仮想メディアファイル共有機能は、CMC を使用して、ネットワーク上の共有ドライブのファイルを 1 台以上のサーバにマップし、オペレーティングシステムを導入または更新します。接続されている場合、ローカルサーバでアクセスできるファイルと同様に、リモートファイルにアクセスすることができます。フロッピードライブと CD/DVD ドライブの 2 種類のメディアがサポートされています。

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 **サーバ管理者** の権限が必要です。この機能を使用するには、Enterprise ライセンスが必要です。

メモ: CIFS を使用しており、Active Directory ドメインの一部である場合には、イメージのファイルパスに IP アドレスとドメイン名を含めて入力してください。

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. 左ペインで、**サーバ概要** > **セットアップ** > **リモートファイル共有** をクリックします。
2. **リモートファイル共有の導入** ページで、適切なデータをフィールドに入力します。フィールドの説明については、『*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に接続するには、パス、ユーザー名、パスワードを入力します。操作を正しく実行すると、メディアにアクセスできます。

   接続されているリモートファイル共有の接続を解除するには、**接続解除** をクリックします。

   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: 導入 ボタンをクリックするとサーバが再起動されるため、前もって作業中のすべてのファイルを保存してください。

   導入 をクリックすると、次のタスクが実行されます。

   - **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。**
   - **サーバーの電源がオフになっている場合は、サーバーに電力が供給される。**

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 設定のみが含まれています。これらのプロファイルは PowerEdge VRTX 向け CMC バージョン 1.00 以降から生成されます。
- BIOS およびブート- このグループにはサーバーの BIOS およびブート設定のみが含まれています。これらのプロファイルは PowerEdge VRTX 向け CMC バージョン 1.00 以降から生成されます。
- すべての設定 — このバージョンには、サーバーと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。これらのプロファイルは、次のサーバーから生成されます。
  - CMC for PowerEdge VRTX バージョン 1.00 以降
  - iDRAC7 1.00.00 以降および 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
  - iDRAC8 および Lifecycle Controller 2.00.00.00 以降を搭載した第 13 世代サーバー

サーバー設定複製機能は iDRAC7 以降の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。
- サーバーの電源がオンになっている。

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。
- 管理ステーションまたは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管理ステーションまたは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。

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、左側のペインで **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。

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コピーする前に、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。

メモ: リモート共有を利用できる場合は、CMC 拡張ストレージおよびリモート共有を使用して、最大 100 個のプロファイルを保存できます。リモート共有の詳細については、「CMC ウェブインタフェースを使用したネットワーク共有の設定」を参照してください。

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、保存プロファイルへのアクセスが妨げられ、サーバー設定複製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** ページを開きます。**サーバープロファイル** セクションで **プロファイルの保存と適用** をクリックします。
2. 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。
   プロファイルの保存 セクションが表示されます。
3. プロファイルを保存する場所として、**拡張ストレージ** または **ネットワーク共有** を選択します。

   メモ: ネットワーク共有がマウントされており、アクセス可能な場合に限り、ネットワーク共有 オプションが有効化され、保存プロファイル に詳細が表示されます。ネットワーク共有が接続されていない場合、シャーシにはネットワーク共有を設定します。ネットワーク共有を設定するには、保存プロファイル セクションの 編集 をクリックします。ネットワーク共有の設定についての詳細は、「CMC ウェブインタフェースを使用したネットワーク共有の設定」を参照してください。

4. **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) を入力して、**プロファイルの保存** をクリックします。

   メモ: サーバープロファイルの保存時には、標準 ASCII 拡張文字セットがサポートされますが、次の特殊文字は使用できません。

)、“、.、*、>、<、\、/、:、|、#、?、および ,

   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。

プロファイルの適用

サーバー設定レプリケーションを実行できるのは、サーバー プロファイルが CMC 上の不揮発性メディアに保存されたプロファイルとして使用可能な場合、またはリモート共有に保存されている場合のみです。サーバー設定レプリケーション操作を開始するには、保存されたプロファイルを 1 台または複数のサーバーに適用できます。

メモ: サーバーが Dell Lifecycle Controller をサポートしていない場合、または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**] ページに移動します。[**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。

   メモ: プロファイルの選択 ドロップダウンメニューに、タイプ順に並べ替えられた使用可能なすべてのプロファイルが表示されます。これには、リモート共有および SD カードに保存されたプロファイルも含まれます。

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に関するメッセージとして、現在の設定が上書きされ、選択したサーバーが再起動されることが表示されます。操作を続行するかどうかのプロンプトが表示されます。

メモ: サーバー群でサーバー クローニング操作を実行するには、これらのサーバー群で CSIOR オプションが有効になっている必要があります。CSIOR オプションが無効化されている場合は、サーバー群で CSIOR が有効でないことを示す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させるには、サーバー群で CSIOR オプションが有効化されていることを確認してください。

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ますが、必要に応じて、サーバーが直ちに再起動される場合もあります。詳細については、*CMC のオンライン ヘルプ*を参照してください。

プロファイルのインポート

管理ステーション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。

保存されたプロファイルを CMC から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 **保存プロファイル** 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。
   上記フィールドについての情報は、『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

保存されたサーバープロファイルを、管理ステーションの指定されたファイルフォルダ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** ページに移動します。**保存プロファイル** セクションで必要なプロファイルを選択してから、**プロファイルのコピーのエクスポート** 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。

   メモ: ソースプロファイルが SD カード上にある場合、プロファイルをエクスポートすると説明が失われるというメッセージが表示されます。プロファイルのエクスポートを続行するには、**OK** をクリックします。

   ファイルの宛先を選択するように求めるメッセージが表示されます。
   - ソースファイルが SD カード上にある場合は、ローカルまたはネットワーク共有を選択します。

     メモ: ネットワーク共有がマウントされており、アクセス可能な場合に限り、ネットワーク共有 オプションが有効化され、保存プロファイル に詳細が表示されます。ネットワーク共有が接続されていない場合、シャーシにはネットワーク共有を設定します。ネットワーク共有を設定するには、保存プロファイル セクションの 編集 をクリックします。詳細については、「CMC ウェブインタフェースを使用したネットワーク共有の設定」を参照してください。
   - ソースファイルがネットワーク共有上にある場合は、ローカルまたは SD カードを選択します。

   上記フィールドについての情報は、『オンラインヘルプ』を参照してください。
3. 表示されたオプションに基づいて、宛先の場所として **ローカル**、**拡張ストレージ**、または **ネットワーク共有** を選択します。
   - **ローカル** を選択する場合は、ローカルディレクトリにプロファイルを保存できるダイアログボックスが表示されます。
   - **拡張ストレージ** または **ネットワーク共有** を選択する場合は、**プロファイルの保存** ダイアログボックスが表示されます。
4. **プロファイルの保存** をクリックして、選択した場所にプロファイルを保存します。

メモ: CMC ウェブインタフェースは、通常のサーバー設定プロファイル (サーバーのスナップショット) をキャプチャします。これは、ターゲットシステムでのレプリケーションに使用できます。ただし、RAID や ID 属性など一部の設定は、新しいサーバーに伝播されません。RAID 構成と ID 属性用の代替のエクスポートのモードの詳細については、DellTechCenter.com から *サーバーのサーバー設定プロファイルでのクローン作成*というホワイトペーパー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、またはリモート共有に保存されたサーバープロファイルの名前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** ページに移動します。**保存されたプロファイル** 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。
   サーバー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。

   メモ: SD カードに保存されたプロファイルに限り、プロファイルの説明を編集することができます。

   詳細については『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）またはネットワーク共有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 **保存プロファイル** 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『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** ページに移動します。**サーバープロファイル** セクションで、必要なサーバーの **サーバープロファイル** 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。

表示された設定の詳細については、『オンラインヘルプ』を参照してください。

メモ: CMC サーバー設定レプリケーション機能は、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 12 世代サーバー — サーバーの再起動後、会社のロゴが表示されたら、F2 を選択します。**iDRAC 設定** ページの左ペインで **Lifecycle Controller** をクリックしてから、**CSIOR** をクリックして変更を有効にします。
- 第 13 世代サーバー — サーバーの再起動後、プロンプトが表示されたら、F10 キーを押して Dell Lifecycle Controller にアクセスします。**ハードウェア構成** > **ハードウェアインベントリ** とクリックして、**ハードウェアインベントリ** ページに移動します。**ハードウェアインベントリ** ページで、**Collect System Inventory on Restart**（CSIOR）をクリックします。

保存プロファイル設定の表示

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。**保存プロファイル** セクションで、必要なサーバープロファイルの **プロファイルの表示** 列の **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。表示された設定についての詳細は、『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、サーバー設定操作から直接 10 件の最新プロファイルログエントリを表示します。各ログエントリには、重大度、サーバー設定複製操作が送信された日時、および複製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 ログでも使用できます。その他の使用可能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、『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 BIOS 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. 左ペインで、**シャーシ概要** > **サーバー概要** > **セットアップ** > **プロファイル** をクリックします。
2. **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** セクションから送信済みジョブのジョブ ID（JID）を書き取ります。

3. 左ペインで、**サーバー概要** > **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** 表内で同じ JID を検索します。CMC を使用した Lifecycle Controller ジョブの実行の詳細に関しては、「Lifecycle Controller ジョブ操作」を参照してください。
4. **ログの表示** リンクをクリックして、iDRAC Lifecycle Controller から特定のサーバーの *Lclogview* の結果を表示します。
完了または失敗の結果の表示内容は、特定のサーバーについて iDRAC Lifecycle Controller のログに表示される情報に似ています。

プロファイルの Quick Deploy

Quick Deploy 機能では、保存された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。スロットに挿入されたサーバー設定レプリケーションをサポートするサーバーは、いずれもそのスロットに割り当てられたプロファイルを使用して設定されています。Quick Deploy 処置を実行できるのは、**iDRAC の導入**ページの**サーバー挿入時の処置**オプションが**サーバープロファイル**オプション、または **Quick Deploy とサーバープロファイル**オプションに設定されている場合のみです。このオプションを選択することにより、新しいサーバーがシャーシに挿入された時に、割り当てられたサーバープロファイルを適用することができます。**iDRAC の導入**ページに移動するには、**サーバー概要** > **セットアップ** > **iDRAC** を選択します。導入可能なプロファイルは、SD カードに格納されています。Quick Deploy のプロファイルを設定するには、**シャーシ管理者**権限が必要です。

メモ:

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、**QuickDeploy 用のプロファイル** をクリックします。
現在のプロファイルの割り当てが、**プロファイルの割り当て** 列に含まれる選択ボックスのスロットに対して表示されます。
メモ: QuickDeploy 処置を実行できるのは、iDRAC の導入 ページで サーバー挿入時の処置 オプションが サーバープロファイル または Quick Deploy とサーバープロファイル に設定されている場合のみです。このオプションを選択することにより、新しいサーバーがシャーシに挿入された時に、割り当てられたサーバープロファイルを適用することができます。
2. ドロップダウンメニューから、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. **プロファイルの割り当て** 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。**
- **プロファイルの割り当てを 1 つ、または複数のスロットから削除するには、スロットを選択して 割り当ての削除 をクリックします。1 つ、または複数のスロットからプロファイルを削除すると、Quick Deploy プロファイル 機能が有効化されている時にスロットに挿入されたサーバーすべてのプロファイル内の設定が削除されることを警告するメッセージが表示されます。プロファイルの割り当てを削除するには、OK をクリックします。**
- **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、ドロップダウンメニューで 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導入されるときは、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。

メモ:

- **サーバーがスロットに挿入されているときにアクセスできないネットワーク共有上に割り当てられたプロファイルがある場合は、割り当てられたプロファイルがスロット <X> に対して使用可能ではないというメッセージが LCD に表示されます。**
- **ネットワーク共有がマウントされており、アクセス可能な場合に限り、ネットワーク共有 オプションが有効化され、保存プロファイル に詳細が表示されます。ネットワーク共有が接続されていない場合、シャーシにはネットワーク共有を設定します。ネットワーク共有を設定するには、保存プロファイル セクションの 編集 をクリックします。詳細については、「CMC ウェブインタフェースを使用したネットワーク共有の設定」を参照してください。**

起動 ID プロファイル

CMC ウェブインタフェースの **起動 ID 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。**サーバープロファイル** のページで、**起動 ID プロファイル** をクリックします。

起動 ID プロファイルには、サーバーを SAN ターゲットデバイスから起動するのに必要な NIC または FC の設定および固有の仮想 MAC と WWN が含まれています。これらは CIFS または NFS 共有を通じて複数のシャーシにわたって利用可能であるため、シャーシ内の故障しているサーバーから迅速にリモートで ID を同じシャーシまたは別のシャーシにある予備のサーバーに移動させることができます。これにより、故障しているサーバーのオペレーティングシステムとアプリケーションで起動することができるようになっています。この機能の主な利点は、すべてのシャーシにわたって共有されている固有の仮想 MAC アドレスプールを使用できることにあります。

この機能によって、サーバーが機能停止した場合に、物理的に介入することなく、オンラインでサーバーの操作を管理できるようになります。起動 ID プロファイル機能を使って、次のタスクを実行することができます。

- 初期セットアップ
  - 仮想 MAC アドレスの範囲を作成します。MAC アドレスを作成するには、シャーシ設定管理者およびサーバー管理者権限が必要です。
  - 起動 ID プロファイルテンプレートを保存し、各サーバーで使用される SAN 起動パラメータを編集し、含めることでネットワーク共有上の起動 ID プロファイルをカスタマイズすることができます。
  - 起動 ID プロファイルを適用する前に、初期設定を使用するサーバーを準備します。
  - 各サーバーに起動 ID プロファイルを適用し、それらを SAN から起動します。
- クイックリカバリ用のスペアスタンバイサーバー (1 つ、または複数) を設定します。
  - 起動 ID プロファイルを適用する前に、初期設定を使用するスタンバイサーバーを準備する。
- 次のタスクを実行することで、故障したサーバーの作業負荷を新しいサーバーで使用します。
  - 故障したサーバーが復帰する際に MAC アドレスが重複されないように、故障したサーバーの起動 ID をクリアします。
  - 故障したサーバーの起動 ID を予備スタンバイサーバーに適用します。
  - サーバーを新しい起動 ID で起動して作業負荷を素早く回復する。

起動 ID プロファイルの保存

起動 ID プロファイルを CMC ネットワーク共有に保存することができます。保存することのできるプロファイルの数は、利用可能な MAC アドレスにより異なります。詳細については、「*CMC ウェブインタフェースを使用したネットワーク共有の設定*」を参照してください。

Emulex Fibre Channel (FC) カードでは、オプション ROM の **SAN からの起動を有効化 / 無効化** 属性はデフォルトで無効になっています。SAN から起動するには、オプション ROM で属性を有効にし、サーバーへ起動 ID プロファイルを適用します。

プロファイルを保存するには、次のタスクを実行します。

1. **サーバープロファイル** のページに移動します。**起動 ID プロファイル** のセクションで、プロファイルを設定するのに必要な設定ができているサーバーを選択し、**FQDD** ドロップダウンメニューから FQDD を選択します。
2. **ID の保存** をクリックします。**ID の保存** セクションが表示されます。

   メモ: 起動 ID は、ネットワーク共有 オプションが有効であり、アクセス可能な場合にのみ、保存が可能で、詳細は 保存プロファイル のセクションに表示されます。ネットワーク共有 が接続されていない場合は、シャーシのネットワーク共有を設定します。ネットワーク共有を設定するには、保存プロファイル のセクションの 編集 をクリックします。詳細については、「*CMC ウェブインタフェースを使用したネットワーク共有の設定*」を参照してください。

3. **ベースプロファイル名** と **プロファイルの数** のフィールドでは、保存するプロファイルの名前とプロファイルの数を入力します。

   メモ: 起動 ID プロファイルの保存時には、標準 ASCII 拡張文字セットがサポートされますが、次の特殊文字は使用できません。

)、“、.、*、>、<、\、/、:、|、#、?、および ,

4. **仮想 MAC アドレス** ドロップダウンからベースプロファイル用の MAC アドレスを選択し、**プロファイルの保存** をクリックします。

   作成されるテンプレートの数は、ユーザーが指定するプロファイルの数で決まります。CMC は Lifecycle Controller と通信して、利用可能なサーバープロファイルの設定を取得し、名前付きのプロファイルとして保存します。名前ファイルのフォーマットは、`<base profile name>_<profile number>_<MAC address>` となっています。(例 : `FC630_01_0E0000000000`)

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、「**操作は正常に完了しました**」の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。

起動 ID プロファイルの適用

ネットワーク共有上で起動 ID プロファイルが保存プロファイルとして利用可能な場合に、起動 ID プロファイルの設定を適用することができます。起動 ID 設定操作を開始するには、保存プロファイルを 1 台のサーバーに適用します。

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。

サーバーにプロファイルを適用するには、次のタスクを実行します。

1. [**サーバー プロファイル**] ページに移動します。[**起動 ID プロファイル**] 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。

   メモ: プロファイルの選択 ドロップダウンメニューには、ネットワーク共有で利用可能な全てのプロファイルがタイプ別に並び替えられて表示されます。
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。
   ID の適用 オプションが有効となります。
3. **ID の適用** をクリックします。
   新しい ID 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。操作を続行するかどうかのプロンプトが表示されます。

   メモ: サーバーでサーバー設定のレプリケーション操作を行うには、当該サーバーで CSIOR オプションが有効になっている必要があります。CSIOR オプションが無効化されている場合は、当該サーバーで CSIOR が有効になっていないことを示す警告メッセージが表示されます。サーバー設定のレプリケーション操作を完了するには、サーバーの CSIOR オプションを有効にします。
4. **OK** をクリックして、選択したサーバーに起動 ID 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、直ちにサーバーが再起動されます。詳細については、*CMC のオンライン ヘルプ* を参照してください。

   メモ: 起動 ID プロファイルを一度に適用できるのは、サーバ内にある 1 つの NIC FQDD パーティションのみです。同じ起動 ID プロファイルを別のサーバにある NIC FQDD パーティションに適用するには、最初に適用されているサーバからクリアする必要があります。

起動 ID プロファイルのクリア

新しい起動 ID プロファイルをスタンバイサーバーに適用する前に、CMC ウェブインタフェースにある **ID のクリア** を使用して選択したサーバーの既存の起動 ID 設定をクリアすることができます。

起動 ID プロファイルをクリア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** ページに移動します。**起動 ID プロファイル** のセクションで、起動 ID プロファイルをクリアするサーバーを選択します。

   メモ: このオプションは、いずれかのサーバーが選択されており、その選択されたサーバーに起動 ID プロファイルが適用されている場合にのみ有効になります。
2. **ID のクリア** をクリックします。
3. **OK** をクリックして、選択したサーバーから起動 ID プロファイルをクリックします。
   このクリアの操作は、サーバーの I/O ID と永続性ポリシーを無効にします。クリアの操作が完了すると、サーバーの電源がオフになります。

保存起動 ID プロファイルの表示

ネットワーク共有に保存された起動 ID プロファイルを表示するには、**サーバープロファイル** ページに移動します。**起動 ID プロファイル** > **保存プロファイル** のセクションで、プロファイルを選択して、**プロファイルの表示** の列で **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。表示される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。

起動 ID プロファイルのインポート

管理ステーションに保存された起動 ID プロファイルをネットワーク共有へインポートすることができます。

管理ステーションから保存されたプロファイルをネットワーク共有にインポートするには、次のタスクを実行します。

1. **サーバープロファイル** のページに移動します。**起動 ID プロファイル** > **保存されたプロファイル** のセクションで **プロファイルのインポート** をクリックします。
   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。

起動 ID プロファイルのエクスポート

ネットワーク共有に保存されている起動 ID プロファイルを、管理ステーション上の指定し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、次のタスクを実行します。

1. **サーバープロファイル** のページに移動します。**起動 ID プロファイル** > **保存プロファイル** のセクションで、必要なプロファイルを選択して、**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。

起動 ID プロファイルの削除

ネットワーク共有に保存されている起動 ID 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、次のタスクを実行します。

1. **サーバープロファイル** のページに移動します。**起動 ID プロファイル** > **保存プロファイル** のセクションで、必要なプロファイルを選択して、**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。

仮想 MAC アドレスプールの管理

仮想 MAC アドレスプールの管理 を使用することによって、MAC アドレスを作成、追加、削除、非アクティブ化することができます。仮想 MAC アドレスプールでは、ユニキャスト MAC アドレスのみ使用することができます。CMC では、次の MAC アドレスの範囲が許可されています。

- 02:00:00:00:00:00 - F2:FF:FF:FF:FF:FF
- 06:00:00:00:00:00 - F6:FF:FF:FF:FF:FF
- 0A:00:00:00:00:00 - FA:FF:FF:FF:FF:FF
- 0E:00:00:00:00:00 - FE:FF:FF:FF:FF:FF

CMC ウェブインタフェースを使って、**仮想 MAC アドレスの管理** オプションを表示するには、システムツリーで **シャーシの概要** > **サーバーの概要** に移動します。**設定** > **プロファイル** > **起動 ID プロファイル** の順にクリックします。**仮想 MAC アドレスプールの管理** セクションが表示されます。

メモ: **仮想 MAC アドレスは、ネットワーク共有の `vmacdb.xml` ファイル内で管理されます。 非表示のロックファイル (`.vmacdb.lock`) が、ネットワーク共有に対して、削除または追加され、複数のシャーシからの起動 ID 操作が順序化されます 。**

MAC プールの作成

CMC ウェブインタフェースにある **仮想 MAC アドレスプールの管理** を使用して、ネットワーク内に MAC プールを作成することができます。

メモ: MAC プールの作成 セクションは、ネットワーク共有上に MAC アドレスデータベース (vmacdb.xml) がない場合にのみ表示されます。この場合、MAC アドレスの追加 および MAC アドレスの削除 オプションは使用できません。

MAC プールを作成するには、次の手順を実行します。

1. **サーバープロファイル** のページに移動します。**起動 ID プロファイル** > **仮想 MAC アドレスプールの管理** のセクションで、
2. **開始 MAC アドレス** のフィールドに、MAC アドレスプールの開始 MAC アドレスを入力します。
3. **MAC アドレスの数** のフィールドに、MAC アドレスの数を入力します。
4. **MAC プールの作成** をクリックして、MAC アドレスプールを作成します。
   ネットワーク共有で MAC アドレスデータベースが作成された後、**仮想 MAC アドレスプールの管理** に、ネットワーク共有に保存された MAC アドレスのリストとステータスが表示されます。このセクションで、MAC アドレスプールから MAC アドレスを追加または削除できるようになります。

MAC アドレスの追加

CMC ウェブインタフェースにある **MAC アドレスの追加** のオプションを使用して、ネットワーク共有へ MAC アドレスの範囲を追加することができます。

メモ: MAC アドレスプールにすでに存在する MAC アドレスを追加することはできません。この場合、新たに追加した MAC アドレスが、プール内に存在することを示すエラーが表示されます。

ネットワーク共有に MAC アドレスを追加するには、次の手順を実行します。

1. **サーバープロファイル** のページに移動します。**起動 ID プロファイル** > **仮想 MAC アドレスプールの管理** のセクションで、**MAC アドレスの追加** をクリックします。
2. **開始 MAC アドレス** のフィールドに、MAC アドレスプールの開始 MAC アドレスを入力します。
3. **MAC アドレスの数** のフィールドに、追加する MAC アドレスの数を入力します。
   有効な値は 1 から 3000 です。
4. **OK** をクリックして、MAC アドレスを追加します。

   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。

MAC アドレスの削除

CMC ウェブインタフェースにある **MAC アドレスの削除** のオプションを使用して、ネットワーク共有から MAC アドレスの範囲を指定して削除することができます。

メモ: MAC アドレスがノード上でアクティブになっている場合、またはプロファイルに割り当てられている場合は、削除することはできません。

ネットワーク共有から MAC アドレス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** のページに移動します。**起動 ID プロファイル** > **仮想 MAC アドレスプールの管理** のセクションで、**MAC アドレスの削除** をクリックします。
2. **開始 MAC アドレス** のフィールドに、MAC アドレスプールの開始 MAC アドレスを入力します。
3. **MAC アドレスの数** のフィールドに、削除する MAC アドレスの数を入力します。
4. **OK** をクリックして、MAC アドレスを削除します。

MAC アドレスの非アクティブ化

CMC ウェブインタフェースの **MAC アドレスの非アクティブ化** オプションを使用して、アクティブになっている MAC アドレスを非アクティブ化することができます。

メモ: サーバーが ID のクリア 処置に反応していない場合、または MAC アドレスがいずれのサーバーでも使用されていない場合にのみ、MAC アドレスの非アクティブ化 のオプションを使用してください。

ネットワーク共有から MAC アドレス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** のページに移動します。**起動 ID プロファイル** > **仮想 MAC アドレスプールの管理** のセクションで、非アクティブ化したいアクティブな MAC アドレスを選択します。
2. **MAC アドレスの非アクティブ化** をクリックします。

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に管理するため、CMC からは、サーバーの管理コントローラー (iDRAC) の Web ベース インターフェイスの起動ポイントが提供されます。

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 Web インターフェイスを起動できます。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 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。一度 iDRAC サイトにログオンすると、このユーザーには自動的に管理者権限が付与されます。これは、同じユーザーが iDRAC でアカウントを持たない場合や、そのアカウントが管理者権限を持たない場合でも同様です。
- CMC ユーザーで、サーバーの管理者権限は**有していない**が、同じアカウントが iDRAC にある場合は、シングル サイン オンで iDRAC に自動ログインできます。一度 iDRAC サイトにログオンすると、このユーザーには、その iDRAC アカウント用に作成された権限が付与されます。
- CMC ユーザーで、サーバーの管理者権限は有していない、または同じアカウントをその iDRAC で有していない場合は、シングル サイン オンでの iDRAC への自動ログインはされません。このユーザーが [**iDRAC GUI の起動**] をクリックすると、iDRAC のログイン ページに誘導されます。

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 において、パスワードが一致する同じログイン名を持っている場合です。ログイン名が同じでパスワードが一致しない場合、この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。

次の場合、[**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。

- サーバーがシャーシから取り外されている
- iDRAC の IP アドレスが変更されている
- iDRAC ネットワーク接続にエラーが発生している

MCM では、メンバー シャーシから iDRAC Web インターフェイスを起動しているとき、リーダー シャーシとメンバー シャーシのユーザー資格情報を同じにする必要があります。そうしないと、現在のメンバーシャーシのセッションが中止され、メンバーシャーシのログイン ページが表示されます。

サーバー状態ページからの 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、次の手順を実行します。

1. 左ペインで、**サーバー概要** を展開します。展開された **サーバー概要** リストに 4 つのサーバーがすべて表示されます。
2. iDRAC ウェブインタフェースを起動するサーバーをクリックします。
3. **サーバー状態** ページで、**iDRAC の起動** をクリックします。
   iDRAC ウェブインタフェースが表示されます。フィールドの説明については、『オンラインヘルプ』を参照してください。

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. 左ペインで **サーバー概要** をクリックします。
2. **サーバー状態** ページで、iDRAC ウェブインタフェースを起動するサーバーの **iDRAC の起動** をクリックします。

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。
- iDRAC 8 と iDRAC 7 をサポートするサーバー。

- サーバーの LAN インタフェースが有効である。
- 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起動することもできます。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。

シャーシ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、次の手順を実行します。

1. 左ペインで、**シャーシ概要** をクリックし、次に **プロパティ** をクリックします。
2. **シャーシ正常性** ページのシャーシ図で、指定の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** リンクをクリックしリモートコンソールを起動します。

サーバー状態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、次の手順を実行します。

1. 左ペインで **サーバー概要** を展開します。展開されたサーバーのリストに 4 つのサーバーがすべて表示されます。
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。
3. **サーバー状態** ページで、**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. 左ペインで、**サーバー概要** に移動し、**プロパティ** > **状態** 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. 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

シャーシ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。デバイスまたはサービスの状態が変更された、またはエラー状況が検出されると、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、そのフィルタがアラートメッセージ (電子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されている場合、アラートが電子メールアドレス、IP アドレス、外部サーバーなど、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. **シャーシイベントアラート** オプションを有効にします。
2. オプションとして、アラートをカテゴリまたは重要度でフィルタします。
3. E-メールアラートまたは SNMP トラップ設定を行います。
4. シャーシイベントアラートを有効にして、E-メールアラートまたは SNMP を設定済みの宛先に送信します。

トピック：

アラートの有効化または無効化

設定された宛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-メールアラートの宛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. 左ペインで、**シャーシ概要** > **アラート** をクリックします。
2. **シャーシイベント** ページの **シャーシアラート有効化** 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有効化するか、オプションの選択を外してアラートを無効化します。
3. 設定を保存するには、**適用** をクリックします。

アラートのフィルタ

カテゴリと重要度に基づいて、アラートをフィルタ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アラートのフィルタ

カテゴリと重要度に基づいてアラートをフィルタするには、次の手順を実行します。

メモ: シャーシイベントの設定変更を適用するには、アラート設定権限が必要です。

1. 左ペインで、**シャーシ概要** > **アラート** をクリックします。
2. **シャーシイベント** ページの **アラートフィルタ** セクションで、次のカテゴリの 1 つまたは複数を選択します。
   - **システム正常性**
   - **保管時**
   - **構成**
   - **監査**
   - **アップデート**
3. 次の重要度から 1 つまたは複数を選択します。

- **重要**
- **警告**
- **情報**

監視対象アラート セクションには、選択したカテゴリと重要度に基づいた結果が表示されます。このページのフィールドの説明については、『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。

RACADM を使用したイベントアラートの設定

イベントアラートを設定するには、`eventfilters` コマンドを実行します。詳細については、**dell.com/support//manuals** にある『Chassis Management Controller for PowerEdge VRTX 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 トラップ設定を設定する前に、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。

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. 左ペインで、**シャーシ概要** > **アラート** > **トラップの設定** をクリックします。
2. **シャーシイベントアラート送信先** ページで、次の値を入力します。
   - **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名を入力します。

     このコミュニティ文字列は、**シャーシ概要** > **ネットワーク** > **サービス** ページにある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アウトバウンドトラップのために使用するものです。**シャーシ概要** > **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 デーモンをクエリするために使用します。
   - **有効** で、送信先 IP に対応するオプションを選択して、トラップを受け取る IP アドレスを有効化します。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、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。

   メモ: SNMP と E-メールアラートのいずれも、設定できるフィルタマスクは 1 つだけです。フィルタマスクをすでに選択している場合は、タスク 2 を実行せずに手順 3 に進みます。

2. アラートの生成を有効にします。

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

3. `racadm eventfilters set` コマンドを実行することによって、イベントフィルタを指定します。
   a. 使用可能なアラート設定をすべてクリアするには、次のコマンドを実行します。`racadm eventfilters set -c cmc.alert.all -n none`
   b. 重要度をパラメータとして使用して設定します。たとえば次の場合、ストレージカテゴリのすべての情報イベントには処置として電源オフ、および通知として E-メールと SNMP が割り当てられます。`racadm eventfilters set -c cmc.alert.storage.info -n email,snmp`
   c. サブカテゴリをパラメータとして使用して設定します。たとえば次の場合、監査カテゴリ内のライセンスサブカテゴリ下にあるすべての設定には処置として電源オフが割り当てられ、すべての通知が有効化されます。`racadm eventfilters set -c cmc.alert.audit.lic -n all`
   d. サブカテゴリおよび重要度をパラメータとして使用して設定します。たとえば次の場合、監査カテゴリ内のライセンスサブカテゴリ下にあるすべての情報イベントには処置として電源オフが割り当てられ、すべての通知が無効化されます。`racadm eventfilters set -c cmc.alert.audit.lic.info -n none`
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 のタスクを実行します。

   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 <インデックス>` を入力します。インデックスが設定されていると、`cfgTrapsAlertDestIPAddr` オブジェクトおよび `cfgTrapsCommunityName` オブジェクトに値が表示されます。
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不明な場合は、次のコマンドを実行します。

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

電子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、または複数の電子メールアドレスに電子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電子メールを受け入れるように SMTP 電子メールサーバーを設定します。この機能は通常、セキュリティ上の理由で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設定する手順は、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、iDRAC から電子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 iDRAC 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: 電子メールアラートは 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. 左ペインで、**シャーシ概要** > **アラート** > **E-メールアラートの設定** をクリックします。
2. SMTP E-メールサーバー設定と、アラートを受信する E-メールアドレスを指定します。フィールドの説明については『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。フィルタマスクをすでに設定した場合は、手順 3 のタスクは実行しないでください。

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。イベントトラップのフィルタマスク表は、各イベントタイプ向け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 ホストをセットアップするには、次のコマンドを実行します。

```
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-メールアドレスを追加するには、手順 2～6 のタスクを実行します。

メモ: 手順 2～6 のコマンドは、指定するインデックス（1～4）に設定されている既存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 cfgEmailAlert -I <index>` を入力します。インデックスが設定されていると、`cfgEmailAlertAddress` オブジェクトおよび `cfgEmailAlertEmailName` オブジェクトに値が表示されます。

詳細については、**dell.com/support/manuals** にある『Chassis Management Controller for PowerEdge VRTX 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

CMC を使用したシステムの管理、およびシステムセキュリティの維持を行うために、特定の権限（役割ベースの権限）を持つユーザーアカウントをセットアップすることができます。デフォルトで、CMC はローカル管理者アカウントで設定されます。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ようにユーザーアカウントをセットアップすることができます。

最大 16 のローカルユーザーをセットアップ、または Microsoft Active Directory または LDAP などのディレクトリサービスを使用して追加ユーザーアカウントをセットアップすることができます。ディレクトリサービスを使用すると、認証されたユーザーアカウントを管理するための中枢的な場所が提供されます。

CMC は、関連する一連の権限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。役割は、利用可能な最大権限を定義します。

トピック：

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 **サーバーシステム管理者** 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 2 つの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を作成できません。また、サーバーユーザーがユーザー設定システム管理者を作成することもできません。このルールにより、サーバーのセキュリティと整合性が保護されます。

表 20. ユーザータイプ

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回復すると、以前に付与されたその他すべての権限が有効になります。
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。 ・ 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かないかに関係なく、追加または変更することができます。

表 20. ユーザータイプ（続き）

権限	説明
	サーバーを異なるシャーシに移動させると、サーバーは新しいシャーシのスロットに割り当て済みのスロット名および優先順位を引き継ぎます。以前のスロット名および優先順位は、以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を変更する。 • ユーザーの権限を変更する。 • ユーザーのログイン権限を有効または無効にするが、ユーザーの名前やその他の権限はデータベース内に保持する。
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** 権限を持つ CMC ユーザーがすべての電源関連の操作を実行できます。このような CMC ユーザーは、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発行すると、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、サーバー上のシステム管理者権限の欠如を埋め合わせます。 **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発行すると、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。これらの権限は、シャーシのユーザーがシャーシ上でサーバー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：

表 20. ユーザータイプ（続き）

権限	説明
	• 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、ファブリック A IOM をセットアップし、設定できます。
ファブリック B システム管理者	ユーザーはファブリック B をセットアップし、設定できます。これは、サーバー内の最初のメザニンカードに対応し、メインボードの共有 PCIe サブシステム内のファブリック B 回路に接続されます。
ファブリック C システム管理者	ユーザーはファブリック C をセットアップし、設定できます。これは、サーバー内の 2 番目のメザニンカードに対応し、メインボードの共有 PCIe サブシステム内のファブリック C 回路に接続されます。

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 21. 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 • 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
電力ユーザー	• 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
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
なし	権限の割り当てなし

表 22. 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	システム管理者の許可	パワーユーザーの許可	ゲストユーザーの許可
CMC ログインユーザー	有	有	有
シャーシ設定システム管理者	有	無	無
ユーザー設定システム管理者	有	無	無
ログのクリアシステム管理者	有	有	無
シャーシ制御システム管理者 (電源コマンド)	有	有	無
Server Administrator	有	有	無
テストアラートユーザー	有	有	無
デバッグコマンドシステム管理者	有	無	無
ファブリック A システム管理者	有	有	無

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を強くお勧めします。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。

ルート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. 左ペインで、**シャーシ概要** をクリックし、次に **ユーザー認証** をクリックします。
2. **ユーザー** ページの **ユーザー ID** 列で、**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。

3. **ユーザー設定** ページで、**パスワードの変更** オプションを選択します。
4. **パスワード** フィールドに新しいパスワードを入力し、同じパスワードを **パスワードの確認** に入力します。
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す。

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 ローカルユーザーを作成する前に、現行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、ウェブインタフェース、RACADM、WS-MAN などの CMC でセキュア化された任意のインタフェース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

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。

ローカル CMC ユーザーを追加し、設定するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** をクリックし、次に **ユーザー認証** をクリックします。
2. **ローカルユーザー** ページの **ユーザー ID** 列で、ユーザー ID 番号をクリックします。**ユーザー設定** ページが表示されます。

   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。

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、『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。適切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 を設定する場合、または RACADM の racresetcfg コマンドを使用した場合、現在のユーザーのみがパスワードが calvin を持つ root となります。racresetcfg サブコマンドは、すべての 設定パラメータをデフォルト値にリセットします。それまでに行った変更はすべて失われます。

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化する場合は、-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

CMC 設定に新しいユーザーを追加するには、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。

```
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
```

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のリストについては、『Chassis Management Controller for PowerEdge VRTX 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化されていないことを示します。

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、次のコマンドを実行します。

```
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『Chassis Management Controller for PowerEdge VRTX 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 を使用しているときは、各ユーザーを手動で個別に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ー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のユーザー設定を削除し、そのユーザー設定を工場出荷時のデフォルト値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: 特定のユーザー権限に対して有効なビットマスク値のリストについては、dell.com/support/manuals にある『Chassis Management Controller for PowerEdge VRTX 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化されてい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: 次のオペレーティングシステムでは、Active Directory を使用してユーザーを認識できます。

- **Microsoft Windows 2000**
- **Microsoft Windows Server 2003**
- **Microsoft Windows Server 2008**

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。

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 23. : 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	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	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 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、『*CMC オンラインヘルプ*』を参照してください。

1. 左ペインで、**シャーシ概要** に移動し、**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. **Microsoft Active Directory (標準スキーマ)** を選択します。標準スキーマ用に設定される設定が同じページに表示されます。

3. **共通設定** セクションで、次を指定します。
   - **Active Directory の有効化** を選択し、**AD タイムアウト** フィールドに Active Directory のタイムアウト値を入力します。
   - DNS ルックアップから Active Directory ドメインコントローラを取得するには、**DNS でドメインコントローラをルックアップする** を選択してから、次のいずれかを選択します。
     - **ログインからのユーザードメイン** - ログインユーザーのドメイン名を使って DNS ルックアップを実行します。
     - **ドメインを指定** - DNS ルックアップ用に使用するドメイン名を入力します。
   - CMC が指定された Active Directory ドメインコントローラのサーバーアドレスを使用できるようにするには、**ドメインコントローラのアドレスを指定する** を選択します。これらのサーバーアドレスは、ユーザーアカウントと役割グループが格納されているドメインコントローラのアドレスです。
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. **標準スキーマ役割グループ** 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** タブに移動します。**ネットワーク設定** 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** チェックボックスのチェックを外し、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 コマンドプロンプトで、次のコマンドを実行します。

- `config` コマンドを使用：

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1
racadm config -g cfgActiveDirectory -o cfgADType 2
racadm config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupName <common name of the
role group>
racadm config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupDomain <fully qualified
domain name>
racadm config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupPrivilege <Bit Mask Value
for specific RoleGroup permissions>
```

```
racadm config -g cfgActiveDirectory -o cfgADDomainController1 <fully qualified domain name
or IP address of the domain controller>
racadm config -g cfgActiveDirectory -o cfgADDomainController2 <fully qualified domain name
or IP address of the domain controller>
racadm config -g cfgActiveDirectory -o cfgADDomainController3 <fully qualified domain name
or IP address of the domain controller>
```

メモ: ドメインの FQDN ではなく、ドメインコントローラの FQDN を入力します。たとえば、dell.com ではなく servername.dell.com と入力します。

メモ:

3 つのアドレスのうち少なくとも 1 つを設定する必要があります。CMC は、正常に接続できるまで、設定された各アドレスに対して 1 つずつ接続を試みます。標準スキーマでは、これらはユーザーアカウントと役割グループが位置するドメインコントローラのアドレスです。

```
racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog1 <fully qualified domain name or
IP address of the domain controller>
racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog2 <fully qualified domain name or
IP address of the domain controller>
racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog3 <fully qualified domain name or
IP address of the domain controller>
```

メモ: グローバルカタログサーバーが標準スキーマに必要になるのは、ユーザーアカウントと役割グループが別個のドメイン内にある場合のみです。複数のドメインにある場合は、使用できるのはユニバーサルグループだけです。

メモ: 証明書の検証を有効にしている場合、このフィールドで指定する FQDN または IP アドレスは、ドメインコントローラ証明書のサブジェクトまたはサブジェクト代替名のフィールドの値と一致する必要があります。

SSL ハンドシェイク中の証明書の検証を無効にする場合は、次の RACADM コマンドを実行します。

- config コマンドを使用：racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0

この場合、認証局 (CA) 証明書をアップロードする必要はありません。

SSL ハンドシェイク中に証明書の検証を実施する場合は、次のコマンドを実行します (オプション)。

- config コマンドを使用：racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1

この場合、次の RACADM コマンドを実行して CA 証明書をアップロードする必要があります。

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

メモ: 証明書の検証が有効になっている場合、ドメインコントローラサーバーアドレスおよびグローバルカタログ FQDN を指定します。DNS が正しく設定されていることを確認してください。

拡張スキーマ Active Directory 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、または含めるデータの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。ユーザークラス属性の一例として、ユーザーの姓、名、電話番号などがあります。

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、Microsoft 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、お互いに競合しないことを保証できるようにしています。Microsoft 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。

メモ: RAC 権限オブジェクトは 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、または複数ドメインで設定することができます。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権限を与え、ユーザー 3 に RAC2 カードへのログイン権限を与えるなどです。

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. ユーザー 1 と ユーザー 2 をグループ 1 にグループ化します。
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。

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. ユーザー 1 と ユーザー 2 をグループ 1 にグループ化します。グループ 1 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。

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。

- DVD ドライブ:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools \Remote_Management_Advanced\LDIF_Files
- <DVD ドライブ>:\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リリースノート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 24. 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 25. 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

表 25. dellRacDevice クラス（続き）

OID	1.2.840.113556.1.8000.1280.1.7.1.1
SuperClasses	dellProduct
属性	dellSchemaVersion dellRacType

表 26. 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 27. 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 28. 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
SuperClasses	ユーザー
属性	dellRAC4Privileges

表 29. 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 30. 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
属性：dellIsLogClearAdmin **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

表 30. Active Directory スキーマに追加された属性のリスト（続き）

割り当てられた OID/ 構文オブジェクト識別子	単一値
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 **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 and Documentation』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 <DVDdrive>:\SYSMGMT\ManagementStation\support\OMActiveDirect ory_SnapIn64 にあります。

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、Microsoft のマニュアルを参照してください。

Active Directory への CMC ユーザーと権限の追加

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

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. **MMC コンソールルート** 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。

3. **新規オブジェクト** ページで、新しいオブジェクトの名前を入力します。この名前は、「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」で入力した CMC 名と同じであることが必要です。
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. **MMC コンソールルート** 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。
3. **新規オブジェクト** ページで、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の権限を割り当てます。CMC のユーザー権限の詳細については、 ユーザータイプ 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。
3. **新規オブジェクト** ページで、新しい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。お使いのシステムで Microsoft Windows 2000 以降のバージョンのオペレーティングシステムを実行している場合は、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。

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 Web インターフェイスを使用した拡張スキーマの Active Directory の設定

CMC Web インターフェイスを使用して 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: 各種フィールドについての情報は、*オンライン ヘルプ*を参照してください。

1. 左ペインで、**[シャーシ概要]** > **[ユーザー認証]** > **[シャーシ概要]** > **[ディレクトリー 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. **共通設定** セクションで、次を指定します。
   - **Active Directory の有効化** を選択し、**AD タイムアウト** フィールドに Active Directory のタイムアウト値を入力します。
   - DNS ルックアップから Active Directory ドメインコントローラを取得するには、**DNS でドメインコントローラをルックアップする** を選択してから、次のいずれかを選択します。
     - **ログインからのユーザードメイン** - ログインユーザーのドメイン名を使って DNS ルックアップを実行します。
     - **ドメインを指定** - DNS ルックアップ用に使用するドメイン名を入力します。
   - 指定された Active Directory ドメイン コントローラーのサーバー アドレスを CMC が使用可能にするには、**[ドメイン コントローラーのアドレスを指定する]** を選択します。これらのアドレスは、CMC デバイス オブジェクトと関連オブジェクトが存在するドメイン コントローラーのアドレスとなります。
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。ファイルのフル パスおよび完全なファイル名と拡張子を含んだ絶対ファイル 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ことは推奨されません。
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。
   [適用] をクリックした後、CMC Web サーバーが自動的に再起動します。
9. CMC Web インターフェイ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 アドレスに対する **DHCP を使用する** が有効の場合は、次のいずれかを行います。
    - **DHCP を使用して DNS サーバーアドレスを取得する** を選択して、DHCP サーバーが DNS サーバーアドレスを自動的に取得できるようにします。
    - **DHCP を使用して DNS サーバーアドレスを取得する** チェックボックスをオフにしたままで、フィールドにプライマリおよび代替 DNS サーバーの IP アドレスを入力して DNS サーバーの IP アドレスを手動で設定します。
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 コマンドを使用して CMC Active Directory を拡張スキーマで設定するには、コマンドプロンプトを開き、次のコマンドを入力します。

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1
racadm config -g cfgActiveDirectory -o cfgADType 1
racadm config -g cfgActiveDirectory -o cfgADRacName <RAC common name>
racadm config -g cfgActiveDirectory -o cfgADRacDomain < fully qualified rac domain name >
racadm config -g cfgActiveDirectory -o cfgADDomainController1 < fully qualified domain name
or IP Address of the domain controller >
racadm config -g cfgActiveDirectory -o cfgADDomainController2 < fully qualified domain name
or IP Address of the domain controller >
racadm config -g cfgActiveDirectory -o cfgADDomainController3 < fully qualified domain name
or IP Address of the domain controller >
```

メモ: 3 つのアドレスのうち少なくとも 1 つを設定する必要があります。CMC は、正常に接続できるまで、設定された各アドレスに対して 1 つずつ接続を試みます。拡張スキーマでは、これらはこの CMC デバイスがあるドメインコントローラの FQDN または IP アドレスです。

ハンドシェイク中の証明書の検証を無効にする場合は、次のコマンドを実行します (オプション)。

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

メモ: この場合、CA 証明書をアップロードする必要はありません。

SSL ハンドシェイク中に証明書の検証を実施する場合は、次のコマンドを実行します (オプション)。

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

この場合、CA 証明書をアップロードする必要があります。

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

メモ: 証明書の検証が有効な場合、ドメインコントローラサーバーのアドレスおよび FQDN を指定します。DNS が正しく設定されていることを確認してください。

次の RACADM コマンドの使用はオプションです。

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

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。

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ためにユーザー認証とユーザー承認の 2 つのフェーズが使用されます。

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 サーバーを検索する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。

   メモ: Windows ベースのディレクトリサーバーでは、匿名ログインは許可されていません。そのため、バインド DN 名とパスワードを入力します。

2. ユーザーログインに基づいて、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。システムがバインドできない場合は、ログインが失敗します。
4. 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。ユーザードメインは管理者が設定できます。
2. ユーザーが所属するユーザーグループごとに、適切なユーザーアクセス権と権限をユーザーに付与します。

CMC ウェブ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 権限が必要です。

1. 左ペインで、**シャーシ概要** > **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: 各種フィールドについての情報は、『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 名>* 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。

6. **LDAP 役割グループの設定** ページで、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. **証明書検証を有効にする** オプションを選択した場合、**証明書を管理** 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 証明書を指定し、**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
  ```

CMC は、オプションとして SRV レコードのために DNS サーバーをクエリするように設定することができます。`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 レコードのための DNS の検索には、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 コマンドの詳細については、**dell.com/support/manuals** にある『Chassis Management Controller for PowerEdge VRTX 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。

SSO は認証方法として kerberos を使用するため、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 要素認証は、ユーザーがパスワードまたは PIN、および秘密キーまたはデジタル証明書を含む物理カードを所有することを必要とするため、高レベルのセキュリティを提供します。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の信頼性を確認します。

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フェースに対しても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、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 についての情報は、Microsoft ウェブサイトを参照してください。

トピック：

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: Microsoft 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。Microsoft Windows 2008 で Active Directory を使用している場合は、SP1 と共に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

- 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) のために Kerberos レルムとキー配付センター (KDC) をセットアップ。
- 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)。

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。ユーザーアカウントへのサービスプリンシパル名 (SPN) バインドの作成、および信頼情報の MIT スタイルの Kerberos keytab ファイルへのエクスポートには、ktpass ツール (サーバーインストール CD/DVD の一部として Microsoft から使用可能) が使用されます。ktpass ユーティリティの詳細については、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** オプションで使用する Active Directory ユーザーアカウントを作成する必要があります。この名前は、生成した keytab ファイルのアップロード先となる CMC DNS 名と同じ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。

```
ktpass -princ HTTP/cmcname.domainname.com@DOMAINNAME.COM -mapuser keytabuser -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -pass * -out c:\krbkeytab
```

メモ: `cmcname.domainname.com` には RFC で必要とされるとおり小文字を使用し、`@REALM_NAME` には大文字を使用する必要があります。さらに、CMC は Kerberos 認証用に DES-CBC-MD5 タイプおよび AES256–SHA1 タイプの暗号化もサポートします。

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おり、安全な場所に保管する必要があります。*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 の設定については、「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 の設定については、「拡張スキーマ Active Directory 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、および 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** 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

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てください。

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。

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、『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のセットアップのために Active Directory を設定している間に、次の追加手順を実行します。
   - 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を有効にする** オプションを選択します。

  メモ: これら 2 つのオプションが選択されても、セキュアシェル (SSH)、Telnet、シリアル、リモート RACADM などのすべてのコマンドライン帯域外インタフェースは変化しません。

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 <user>@<domain>
```

   ここで、*<user>* は有効な Active Directory ユーザーアカウントです。

   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、dell.com/support/manuals にある『Chassis Management Controller for PowerEdge VRTX 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. 左ペインで、**シャーシ概要** > **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 ファイルが正常にアップロードされたかどう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 ユーザーの 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 config -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た CMC での RACADM コマンドの使用方法については、『Chassis Management Controller for PowerEdge VRTX 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。

トピック：

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ための組み込み connect コマンド。これは `racadm connect` 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 コマンドラインインタフェースコマンド

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 31. 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、その後にサブコマンドが続きます。詳細については、『Chassis Management Controller for PowerEdge VRTX 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。詳細については、「connect 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」を参照してください。 **メモ: connect RACADM コマンドを使用することもできます。**
`exit、logout、quit`	これらすべてのコマンドは同じ処理を実行し、現在のセッションを終了してログインコマンドラインインタフェースに戻ります。

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。

管理ステーションが Microsoft Windows XP または Microsoft Windows Server 2003 を実行している場合は、CMC Telnet セッションで文字の問題が発生する可能性があります。この問題は、return キーが応答せずにパスワードプロンプトが表示されないという、ログインのフリーズとして生じることがあります。

この問題を解決するには、**support.microsoft.com** から hotfix 824810 をダウンロードしてください。詳細については、Microsoft Knowledge Base の記事 824810 も参照できます。

コマンドラインインタフェースでは、racadm コマンドを使用して、`racadm getconfig -g cfgSessionManagement` のようにセッションタイムアウトを管理することができます。詳細については、『*Chassis Management Controller Version for Dell PowerEdge VRTX 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 での SSH の使用

SSH は Telnet セッションと同じ機能をもつ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、SSH バージョン 2 とパスワード認証をサポートしています。SSH はデフォルトで CMC で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、SSH クライアントはエラーメッセージを発行します。メッセージテキストはクライアントによって異なり、CMC によって制御されません。RACLog メッセージを確認して、障害の原因を特定してください。

メモ: Windows では `OpenSSH` を 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。`Putty.exe` を使用して `OpenSSH` を実行することもできます。Windows のコマンドプロンプトで `OpenSSH` を実行しても、完全には機能しません。一部のキーが応答せず、グラフィックは表示されません。Linux を実行しているサーバ上では、任意のシェルから SSH クライアントサービスを実行して、CMC に接続することができます。

同時に 4 つの SSH セッションがサポートされます。セッションのタイムアウトは `cfgSsnMgtSshIdleTimeout` プロパティによって制御されます。racadm のコマンドを使用すれば、`getconfig -g cfgSessionManagement` のようにして、複数のセッションのタイムアウトを確認することができます。

```
$ racadm getconfig -g cfgSessionManagement
cfgSsnMgtWebserverTimeout=1800
cfgSsnMgtTelnetIdleTimeout=1800
cfgSsnMgtSshIdleTimeout=1800
cfgSsnMgtRacadmTimeout=60
```

RACADM コマンドの詳細については、dell.com/support/Manuals の『*Chassis Management Controller for PowerEdge VRTX 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 は、SSH 経由での公開キー認証 (PKA) もサポートしています。この認証方式では、ユーザー ID とパスワードを埋め込んだり、プロンプトに対して入力したりする必要がないため、SSH スクリプトによる自動化が向上しています。詳細については、『SSH による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。

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 32. 暗号化スキーム

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

表 32. 暗号化スキーム（続き）

スキームの種類	スキーム
	• 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と共に使用できる公開キーは、最大 6 個まで設定できます。キーを誤って上書きしたり削除したりするのを防ぐため、公開キーを追加または削除する前に `view` コマンドを使って設定済みのキーを確認してください。サービスユーザー名は、SSH 経由で CMC にアクセスするとき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 を正しく設定し、使用すれば、CMC へのログイン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のセットアップに大変便利です。

メモ: この機能を管理するための GUI サポートはありません。使用できるのは RACADM のみです。

新しい公開キーを追加するときは、そのキーを追加するインデックスに既存のキーが存在していないことを確認してください。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。SSH インタフェースが有効化されている限り、新しいキーは追加されてすぐに自動で有効化されます。

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 で使用されるのは最初の 16 文字のみであることに注意してください。すべての PKA ユーザーがログインにサービスユーザー名を使用するため、CMC は RACADM `getssninfo` コマンドの使用時における SSH ユーザーの識別に公開キーコメントを使用します。

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、『Chassis Management Controller for PowerEdge VRTX 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。

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 CLI を使用する方法の 2 つの方法があります。

このセクションでは、両方のアプリケーションに当てはまる、パブリック/プライベートキーのペアを生成する簡単な手順について説明します。これらのツールの付加的な、または高度な使用方法については、アプリケーションのヘルプを参照してください。

PuTTY Key Generator を使用して、Windows を実行しているクライアント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。RSA キーのサイズは 1024 ~ 4096 です。

メモ:

- **推奨される DSA キーの長さは 1024 です。**
- **1024 未満、または 4096 を超えるサイズのキーを追加すると、CMC がメッセージを表示しない場合がありますが、これらのキーでログインしようとすると、CMC が応答しなくなります。**

- **2048 より大きい DSA キーにする場合は、次の RACADM コマンドを使用します。CMC は 4096 までのキー強度の RSA キーを容認しますが、推奨されるキー強度は 1024 です。**

```
racadm -r 192.168.8.14 -u root -p calvin sshpkauth -i svcacct -k 1 -p 0xfff -f
dsa_2048.pub
```

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。

   キーをセキュリティ保護するパスフレーズを入力することもできます。プライベートキーは保管しておきます。

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。たとえば、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オプション `-f` を使用して、CMC に公開キーを追加するには、コマンドラインインタフェースコンソールで次を入力します。

```
racadm sshpkauth -i svcacct -k 1 -p 0xfff -f <公開キーファイル>
```

メモ: **リモート RACADM ではファイルのアップロードオプションしか使用できません。詳細については、『Chassis Management Controller for PowerEdge VRTX 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、次のコマンドを実行します。

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

すべての公開キーを削除するには、次のコマンドを実行します。

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

ターミナルエミュレーションソフトウェアの設定

CMC は、次のいずれかのタイプ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の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)。

次の副項にあるタスクを完了して、必要なタイプのターミナルソフトウェアを設定します。

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、同じ基本的な設定が必要です。他のバージョンの Minicom を設定するには、本ユーザーズガイドの「必要な Minicom 設定」の項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 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>` を入力し、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. Minicom を終了するには、<Ctrl><a>、<x>、<Enter> を押します。

    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 33. 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	有
ソフトウェアフロー制御	無
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。

connect コマンドを使用したサーバーまたは入出力モジュールの接続

CMC は、サーバーまたは I/O モジュールのシリアルコンソールをリダイレクトするための接続を確立できます。

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。

- CMC コマンドラインインタフェース (CLI) または RACADM `connect` コマンド。RACADM コマンドの実行の詳細については、『Chassis Management Controller for PowerEdge VRTX 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 I/O 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 起動画面および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。シャーシ上には IOM が 1 つ存在します。

注意: CMC シリアルコンソールからの実行時は、CMC がリセットされるまで `connect -b` オプションの接続が維持されます。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` オプションは未処理のバイナリデータを渡し、`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に接続した場合、DTR 信号が遷移しても (たとえば、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る)、アプリケーションは終了しません。

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。

IOM に接続するには、次を入力します。

```
connect switch-n
```

ここで、`n` は IOM ラベル A1 です。

connect コマンドで IOM を参照する場合、IOM は次の表にあるとおりにマップされます。

表 34. スイッチへの IO モジュールのマッピング

IO モジュールラベル	スイッチ
A1	switch-a1 または switch- 1

メモ: IOM 接続はシャーシごとに同時に 1 つしか存在できません。

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。

管理対象サーバーのシリアルコンソールに接続するには、`connect server-n` コマンドを実行します。ここで *n* は 1~4 です。また、`racadm connect server-n` コマンドも使用できます。`-b` オプションを使用してサーバーに接続する場合、バイナリ通信が前提とされ、エスケープ文字は無効になります。iDRAC を使用できない場合、`No route to host` (ホストへのルートなし) 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を有効にする必要があります。また、ターミナルエミュレータウィンドウを 80 x 25 に設定する必要もあります。それ以外の設定では、ページの文字が正しく表示されません。

メモ: BIOS セットアップのページでは、一部のキーが動作しません。そのため、<Ctrl> <Alt> <Delete> などに対して適切なキーボードショートカットを入力します。必要なキーボードショートカットは、最初のリダイレクト画面に表示されます。

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

iDRAC ウェブインタフェースを使用して、リモートコンソールセッションによる管理下システムへの接続を実行できます(**dell.com/support/manuals** にある『iDRAC ユーザーズガイド』を参照)。

デフォルトでは、BIOS のシリアル通信は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. 管理下サーバーの電源をオンにします。
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** に移動し、<Enter> を押します。ダイアログボックス内のシリアル通信リストに次のオプションが表示されます。
   - **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**

   これらのオプション間を移動するには、矢印キーを押します。

   メモ: COM1 経由のコンソールリダイレクトでオン オプションが選択されていることを確認してください。
4. **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。
5. 変更を保存して終了します。

   管理下システムが再起動します。

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を設定するときは、リダイレクトされたコンソールが表示されるウィンドウまたはアプリケーションを 25 行 x 80 桁に設定して、テキストが正しく表示されるようにします。異なる設定をすると、テキストの一部がずれて表示されます。

`/etc/grub.conf` ファイルを次のように編集します。

1. ファイル内の一般設定セクションを見つけ、次の 2 行を新たに入力します。

```
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/sdal # initrd /boot/initrd-version.img # #boot=/dev/sda default=0
timeout=10 #splashimage=(hd0,2)/grub/splash.xpm.gz serial --unit=1 --speed=57600 terminal --
timeout=10 serial title Red Hat Linux Advanced Server (2.4.9-e.3smp) root (hd0,0) kernel /boot/
vmlinuz-2.4.9-e.3smp ro root= /dev/sda1 hda=ide-scsi console=ttyS0 console= ttyS1,57600
initrd /boot/initrd-2.4.9-e.3smp.img title Red Hat Linux Advanced Server-up (2.4.9-e.3)
root (hd0,00) kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 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 画面がコンソールリダイレクトで表示されません。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 の使用

この項では、FlexAddress および FlexAddress Plus と設定について説明しています。

メモ: FlexAddress 機能を使用するにはエンタープライズライセンスがインストールされている必要があります。

トピック：

FlexAddress について

サーバーが交換されても、スロットの FlexAddress はそのサーバースロット用にそのまま維持されます。サーバーが新しいスロットまたはシャーシに挿入された場合は、新しいスロット用にそのシャーシで FlexAddress 機能が有効化されている場合を除き、サーバー割り当ての WWN/MAC が使用されます。サーバーを取り外すと、サーバー割り当てアドレスに戻ります。新しいサーバーを識別するために、各ファブリックの導入フレームワーク、DHCP サーバー、およびルータを再設定する必要はありません。

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 アドレスが割り当てられます。FlexAddress なしでは、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 アドレスが変更され、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 アドレスを特定のスロットに割り当て、工場出荷時のアドレス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 アドレスは変わりません。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限って行われるため、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。

CMC VRTX シャーシは SD カードが搭載された状態で出荷され、FlexAddress、FlexAddress Plus、および拡張ストレージ機能をサポートします。VRTX シャーシが 2 台目の CMC (オプション) と共に出荷された場合、2 台目の CMC には拡張ストレージのみをサポートする SD カードが装備されています。

メモ:

- **SD カードに格納されているデータは暗号化されており、どのような方法でも複製または改ざんすることはできません。これらによって、システム機能が妨げられ、システムの誤作動を招く可能性があるためです。**
- **SD カードの使用は、1 台のシャーシに限定されています。別のシャーシ上で同じ SD カードを使用することはできません。**

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、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> + <mac_count>  - 1 = <mac_end>
```

たとえば、次のとおりです。

```
(starting_mac)00188BFFDCFA + (mac_count)0xCF - 1 = (ending_mac)00188BFFDDC8
```

。

メモ: SD カードの内容が誤って変更されることを防ぐため、SD カードはロックしてから USB メモリカードリーダーに挿入してください。SD カードのロックは、CMC に挿入する前に解除してください。

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 アクティブ化状態の表示

機能カードには、FlexAddress 、FlexAddress Plus、および拡張ストレージのうち、ひとつまたは複数の機能が含まれています。

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** 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。

SD 機能カードの状態を表示するには、以下の RACADM コマンドを実行します。

```
racadm featurecard -s
```

次のメッセージが表示されます。

```
Active CMC:
The feature card inserted is valid, serial number CN0H871T1374036T00MXA00
The feature card contains the following feature(s)
       FlexAddress: bound
       FlexAddressPlus: bound
       ExtendedStorage: bound
Standby CMC:
The feature card contains the following feature(s)
       ExtendedStorage: bound
```

メモ: セカンダリ CMC はオプションで、スタンバイ CMC の出力は、スタンバイ CMC がシャーシ内で使用可能な場合に限り、表示されます。

表 35. 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
No feature card inserted.	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。
The feature card inserted is valid and contains the following feature(s) FlexAddress: bound.	処置の必要はありません。
The feature card inserted is valid and contains the following feature(s) FlexAddress: bound to another chassis, svctag=ABC1234, SD card SN = 1122334455.	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。
The feature card inserted is valid and contains the following feature(s) FlexAddress: not bound.	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

表 35. featurecard -s コマンドによって返される状態メッセージ（続き）

状態メッセージ	処置
	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。

```
Feature Name = FlexAddress
       Date/time Activated = 05 Oct 2013 - 11:50:49
       Feature installed from SD-card serial number = CN0H871T1374036T00MXA00

       Feature Name = FlexAddressPlus
       Date/time Activated = 05 Oct 2013 - 11:50:49
       Feature installed from SD-card serial number = CN0H871T1374036T00MXA00

       Feature Name = ExtendedStorage
       Current Status = redundant, active
       Date/time Activated = 05 Oct 2013 - 11:50:58
       Feature installed from SD-card serial number = CN0H871T1374036T00MXA00
```

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
No features active on the chassis
```

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。

```
ERROR: One or more features on the SD card are active on another chassis
```

feature コマンドおよび featurecard コマンドの詳細については、サポートサイトで利用可能の『Chassis Management Controller for PowerEdge VRTX 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 アドレスを、シャーシ提供の WWN/MAC アドレス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。

メモ: racresetcfg サブコマンドを使用して、CMC の FlexAddress を工場出荷時設定の「無効」にリセットすることができます。RACADM 構文は、次のとおりです。

```
racadm racresetcfg -c flex
```

FlexAddress 関連の RACADM コマンドの詳細およびその他工場出荷時のデフォルト設定のプロパティに関しては、dell.com/cmcmanuals にある『*PowerEdge VRTX RACADM 用シャーシ管理コントローラコマンドラインリファレンスガイド*』を参照して下さい。

設定を開始する前に、サーバーの電源を切断する必要があります。FlexAddress はファブリック単位で有効または無効にすることができます。さらに、この機能はスロット単位でも有効または無効にすることができます。ファブリック単位でこの機能を有効にした後、有効にするスロットを選択できます。たとえば、ファブリック A が有効になっていると、有効な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。

メモ: FlexAddress は、次回の再起動までサーバーモジュール上で有効になりません。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電源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を投入する必要があります。電源切断および電源投入シーケンスが完了すると、シャーシ割り当ての MAC アドレスが Wake-On-LAN (WOL) 機能で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

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。

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. 左ペインで、**サーバー概要** > **セットアップ** > **FlexAddress** をクリックします。
2. **FlexAddress の導入** ページの **シャーシ割り当て WWN/MAC のファブリックの選択** 画面で、FlexAddress を有効にするファブリックタイプ (**ファブリック A** または **iDRAC**) を選択します。無効にするには、オプションをクリアします。
3. **シャーシ割り当て WWN/MAC のスロットの選択** ページで、FlexAddress を有効にするスロットに対して **有効** オプションを選択します。無効にするには、オプションをクリアします。

   メモ: 次に注意してください。

   - **スロットが選択されていないと、選択されたファブリックに対して FlexAddress は有効になりません。**
   - **どのファブリックも選択されていないときにサーバースロットが選択および適用されると、`No fabrics selected! FlexAddress will not be used on this chassis.` というメッセージが表示されます。FlexAddress を正常に設定するには、ファブリックとスロットの両方を選択してください。**
   - **スレーブスロットへの FlexAddress 設定は許可されません。CMC ウェブインターフェースではこのオプションはグレー表示されます。サーバーのスレーブスロットに関連する Ethernet デバイスが、マスタースロットの設定を継承します。**
4. 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 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#>* = 1 or 4 および *<state>* = 0 or 1 です。

0 は無効、1 は有効を示します。

setflexaddr コマンドの詳細については、『Chassis Management Controller for PowerEdge VRTX 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: Dell PowerEdge VRTX と共に FlexAddress または FlexAddressPlus 機能をご購入いただいた場合、これらの機能は事前にインストール済みで、全スロットおよびファブリックで有効化されています。この機能のご購入には、dell.com でデルにお問い合わせください。

メモ: racresetcfg サブコマンドを使用して、CMC の Flex Address を工場出荷時設定の「無効」にリセットすることができます。RACADM 構文は、次のとおりです。

```
racadm racresetcfg -c flex
```

FlexAddress 関連の RACADM コマンドの詳細およびその他工場出荷時のデフォルト設定のプロパティに関しては、dell.com/cmcmanuals にある『*PowerEdge VRTX RACADM 用シャーシ管理コントローラコマンドラインリファレンスガイド*』を参照して下さい。

ワールド ワイド名またはメディア アクセス制御 (MAC) アドレスの表示

[**WWN/MAC サマリー**] ページで、シャーシ内のスロットのワールド ワイド名 (WWN) 設定とメディア アクセス制御 (MAC) アドレスを確認します。

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 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が FlexAddress 用に有効化されていることを示します。FlexAddress 機能は、シャーシ内の各種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、およびスロット固定の 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化されます。

メモ: FlexAddress 機能の詳細については、「FlexAddress について」を参照してください。

WWN または MAC アドレスの情報の表示

シャーシ内の各サーバー スロットまたはすべてのサーバーに対するネットワーク アダプターの WWW/MAC アドレス インベントリーを表示することができます。インベントリーには次が含まれます。

- ファブリックの設定

  メモ:
  - ファブリック A には、取り付けられている入力 / 出力ファブリックのタイプが表示されます。ファブリック A が有効になっている場合、未使用スロットにはファブリック A 用にシャーシ割り当ての MAC アドレスが表示されます。
  - 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 はファブリックとして扱われます。
  - コンポーネントに関連付けられたチェックボックスが選択されている場合は、ファブリックが FlexAddress または FlexAddressPlus に対して有効化されていることを示します。
- NIC アダプター ポートで使用中のプロトコル。たとえば、LAN、ISCI、FCoE などです。
- シャーシ内のスロットのファイバー チャネル ワールド ワイド名 (WWN) 設定および MAC (メディア アクセス制御) アドレス。
- MAC アドレスの割り当てタイプおよび現在アクティブなアドレス タイプ (サーバー割り当て、FlexAddress、または I/O アイデンティティー MAC)。黒色のチェック 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、シャーシ割り当て、リモート割り当てのいずれか) を示します。
- パーティショニングをサポートしているデバイスの NIC パーティションのステータス

WWN/MAC アドレス インベントリーは、Web インターフェイスまたは RACADM CLI を使用して表示することができます。インターフェイスに基づいて MAC アドレスをフィルタリングし、特定の機能やパーティションに対してどの WWN/MAC アドレスが使用されているかを確認できます。アダプターで NPAR が有効になっている場合は、どのパーティションが有効または無効かを確認できます。

Web インターフェイスを使用して、次に対する WWN/MAC アドレス情報を表示できます。

- 特定スロット — **サーバー概要** > **スロット <x>** > **セットアップ** > **FlexAddress** をクリックして、**FlexAddress** ページを開きます。

- すべてのスロットおよびサーバー - **[サーバー概要]** > **[プロパティ]** > **[WWN/MAC]** をクリックして、[**WWN/MAC サマリー**] ページを開きます。

両方のページから、WWN/MAC アドレス情報を基本モードまたは拡張モードで表示できます。

- **基本モード** - このモードでは、サーバー スロット、ファブリック、プロトコル、WWN/MAC アドレスおよびパーティション状態を表示させることができます。WWN/MAC アドレスのボックスには、アクティブな WWN/MAC アドレスのみが表示されます。表示されたフィールドの一部またはすべてを使用して、次のフィルタリングができます。
- **詳細モード** - このモードでは、基本モードで表示されるすべてのフィールド、およびすべての MAC タイプ (サーバー割り当て、FlexAddress、および I/O アイデンティティー) を表示することができます。表示されたフィールドの一部またはすべてを使用してフィルタリングができます。

WWN/MAC アドレス情報は、基本モードと詳細モードの両方で、折りたたまれた状態で表示されます。対応するスロットのプラス記号をクリックするか、[**すべて展開/折りたたむ**] をクリックして、特定のスロットまたはすべてのスロットについての情報を表示します。

シャーシ内の全サーバーの WWN/MAC アドレス情報をローカルフォルダにエクスポートすることも可能です。

各種フィールドについての情報は、*オンライン ヘルプ*を参照してください。

Web インターフェイスを使用した基本 WWN または MAC アドレス情報の表示

各サーバースロット、またはシャーシ内の全サーバーの WWN/MAC アドレスを基本モードで表示するには、次の手順を実行します。

1. **サーバー概要** > **プロパティ** > **WWN/MAC** をクリックします。
   WWN/MAC サマリ ページに、WWN/MAC アドレス情報が表示されます。

   または、**[サーバー概要]** > **[スロット<x>]** > **[セットアップ]** > **[FlexAddress]** をクリックして、特定のサーバー スロットの WWN/MAC アドレス情報を表示します。[**FlexAddress**] ページが表示されます。
2. **WWN/MAC アドレス** 表で **エクスポート** をクリックして、ローカルに WWN/MAC アドレスを保存します。
3. 対応するスロットのプラス記号をクリック、または [**すべて展開/折りたたむ**] をクリックして、WWN/MAC アドレス テーブル内の特定のスロット、またはすべてのスロットについての属性のリストを展開または折りたたみます。
4. **表示** ドロップダウンメニューから **基本** を選択して、WWN/MAC アドレスの属性をツリービューで表示します。
5. **サーバースロット** ドロップダウンメニューから、それぞれ **すべてのサーバー** または特定のスロットを選択して、すべてのサーバーまたは特定のスロット内のサーバーに対する WWN/MAC アドレスの属性を表示します。
6. **ファブリック** ドロップダウンメニューから、1 つのファブリックタイプを選択して、そのサーバーに関連付けられているすべて、または特定タイプの管理ファブリックまたは I/O ファブリックの表示します。
7. **プロトコル** ドロップダウンメニューから、**すべてのプロトコル** またはリストされているネットワークプロトコルのいずれかを選択して、選択したプロトコルに関連付けられているすべての MACS または MAC を表示します。
8. **WWN/MAC アドレス** フィールドに MAC アドレスの一部、または全体を入力して、特定の MAC アドレスに関連付けられたスロットのみを表示します。
9. **パーティションの状態** ドロップダウンメニューから、パーティションの状態を選択して、選択したパーティション状態のサーバーを表示します。

各種フィールドについての情報は、*オンライン ヘルプ*を参照してください。

Web インターフェイスを使用した詳細 WWN/MAC アドレス情報の表示

各サーバースロット、またはシャーシ内の全サーバーの WWN/MAC アドレスを詳細モードで表示するには、次の手順を実行します。

1. **サーバー概要** > **プロパティ** > **WWN/MAC** をクリックします。
   WWN/MAC サマリ ページに、WWN/MAC アドレス情報が表示されます。
2. **表示** ドロップダウンメニューから **詳細** を選択して、WWN/MAC アドレスの属性を詳細ビューで表示します。
   [**WWN/MAC アドレス**] テーブルには、サーバー スロット、ファブリック、プロトコル、WWN/MAC アドレス、パーティションの状態、MAC アドレス割り当てタイプ (サーバー割り当て、FlexAddress、または I/O アイデンティティー MAC) が表示されます。黒色のチェック 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、シャーシ割り当て、リモート割り当てのいずれか) を示します。

3. **WWN/MAC アドレス** 表で **エクスポート** をクリックして、ローカルに WWN/MAC アドレスを保存します。
4. スロットに対する ＋ をクリックするか、または [**すべて展開/折りたたむ**] をクリックして、WWN/MAC アドレス テーブル内の特定のスロット、またはすべてのスロットについての属性リストを展開または折りたたみます。
5. **サーバースロット** ドロップダウンメニューから、それぞれ **すべてのサーバー** または特定のスロットを選択して、すべてのサーバーまたは特定のスロット内のサーバーに対する WWN/MAC アドレスの属性を表示します。
6. **ファブリック** ドロップダウンメニューから、1 つのファブリックタイプを選択して、そのサーバーに関連付けられているすべて、または特定タイプの管理ファブリックまたは I/O ファブリックの表示します。
7. **プロトコル** ドロップダウンメニューから、**すべてのプロトコル** またはリストされているネットワークプロトコルのいずれかを選択して、選択したプロトコルに関連付けられているすべての MACS または MAC を表示します。
8. **WWN/MAC アドレス** フィールドで MAC アドレスを入力して、特定の MAC アドレスに関連付けられたスロットのみを表示します。
9. **パーティションの状態** ドロップダウンメニューから、パーティションの状態を選択して、選択したパーティション状態のサーバーを表示します。

   特定のパーティションが無効化されていると、状態が **無効** と表示され、そのパーティションを表示している行がグレー表示になります。

各種フィールドについての情報は、*オンライン ヘルプ*を参照してください。

RACADM を使用した WWN または MAC アドレス情報の表示

RACADM を使用してすべてのサーバーまたは特定のサーバーの WWN/MAC アドレス情報を表示するには、`getflexaddr` および `getmacaddress` サブコマンドを使用します。

シャーシ全体の FlexAddress を表示するには、次の RACADM コマンドを使用します。

```
racadm getflexaddr
```

特定スロットの 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 [-i <slot#>]
```

ここで、*<slot#>* は 1~4 の値です。

NDC または LOM MAC アドレスを表示するには、次の RACADM コマンドを使用します。

```
racadm getmacaddress
```

シャーシの MAC アドレスを表示するには、次の RACADM コマンドを使用します。

```
racadm getmacaddress -m chassis
```

すべてのサーバーの iSCSI MAC アドレスを表示するには、次の RACADM コマンドを使用します。

```
racadm getmacaddress -t iscsi
```

特定サーバーの iSCSI MAC を表示するには、次の RACADM コマンドを使用します。

```
racadm getmacaddress [-m <module> [-x]] [-t iscsi]
```

ユーザー定義の MAC および WWN アドレスを表示するには、次の RACADM コマンドを使用します。

```
racadm getmacaddress -c io-identity
```

```
racadm getmacaddress -c io-identity -m server -2
```

すべての LOM またはメザニンカードのコンソール指定の MAC/WWN を表示するには、次の RACADM コマンドを実行します。

```
racadm getmacaddress -c all
```

シャーシ割り当ての WWN/MAC アドレスを表示するには、次の RACADM コマンドを使用します。

```
racadm getmacaddress -c flexaddress
```

すべての LOM またはメザニンカードの MAC/WWN アドレスを表示するには、次の RACADM コマンドを実行します。

```
racadm getmacaddress -c factory
```

すべての iDRAC/LOM/ メザニンカードのイーサネットおよび iSCSI MAC/WWN アドレスを表示するには、次の RACADM コマンドを実行します。

```
racadm getmacaddress -a
```

`getflexaddr` および `getmacaddress` サブコマンドの詳細については、『Chassis Management Controller for PowerEdge VRTX 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。

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 36. 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。	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)` `FlexAddress: bound to another chassis, svctag = <Service tag Number> SD card SN = <Valid flex address serial number>`
同じサービスタグにバインドされている アクティブ CMC モジュールの SD カード。	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)` `FlexAddress: bound`
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。	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)` `FlexAddress:not bound`
何らかの理由 (SD カードが挿入されていない、破損した SD カード、機能の非アクティブ化後、SD カードが異なるシャーシにバインドされている) で FlexAddress 機能がシャーシ上でアクティブではない。	`$racadm setflexaddr [-f <fabricName> <slotState>]` `$racadm setflexaddr [-i <slot#> <slotstate>]`	`ERROR: Flexaddress feature is not active on the chassis`
ゲストユーザーによるスロット / ファブリックへの FlexAddress の設定試行。	`$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`

表 36. FlexAddress コマンドと出力（続き）

状況	コマンド	出力
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。	`$racadm setflexaddr -i 1 1`	`ERROR: Unable to perform the set operation because it affects a powered ON server`
CMC Enterprise ライセンスがインストールされていないときの、スロットまたはファブリックの Flexaddress 設定変更。	`$racadm setflexaddr -i<スロット番号> <状況>` `$racadm setflexaddr -f<FabricName> <status>`	`ERROR: SWC0242 : A required license is missing or expired. Obtain an appropriate license and try again, or contact your service provider for additional details.` **メモ: この問題を解決するには、FlexAddress の有効化 ライセンスが必要です。**

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

ファブリックの管理

シャーシはファブリック A というファブリックタイプをサポートしています。ファブリック A は単一の I/O モジュールによって使用され、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ます。

シャーシに存在する I/O モジュール（IOM）は 1 個だけで、パススルーまたはスイッチモジュールになります。この I/O モジュールはグループ A に分類されます。

シャーシ IOM は **ファブリック** と呼ばれる離散データパスが使用されます。このファブリックには A という名前が付けられており、イーサネットのみをサポートします。各サーバー IO アダプタ（メザニンカードまたは LOM）には、機能に応じて 2 個または 4 個のポートを搭載できます。メザニンカードスロットには、PCIe カード（IO モジュールではなく）に接続される PCIe 拡張カードが装着されます。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導入するときは、最大の可用性のために、バンク 1 および 2 の間にそれらの冗長リンクをスパンします。離散 IOM はファブリック識別子で識別されます。

メモ: CMC CLI では、IOM は規則に従って「switch」とされます。

トピック：

- 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 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

初回電源投入シナリオ

シャーシが電源に接続され、オンにされたとき、I/O モジュールはサーバーよりも優先されます。IOM は他よりも先に電源がオンになります。このとき、ファブリックタイプの検証は実行されません。

IOM の電源がオンになった後、サーバーの電源がオンにされ、次に CMC によってサーバーのファブリックの整合性が検証されます。

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は、「IOM の情報および正常性状態の表示」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 の電源がオンになっている事を確認してください。

グループ A 内の IOM のネットワーク設定を設定するには、ファブリック A システム管理者の権限が必要です。

メモ: イーサネットスイッチの場合、帯域内（VLAN1）と帯域外の管理 IP アドレスは同じにすることも、同じネットワーク上にすることもできません。同じにすると、帯域外 IP アドレスが設定されなくなります。デフォルトの帯域内管理 IP アドレスについては、IOM の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 Web インターフェイスを使用した IOM 用ネットワークの設定

I/O モジュールのネットワーク設定を行うには、次の手順を実行します。

1. 左ペインで [**シャーシ概要**] をクリックし、[**I/O モジュール概要**] をクリックして [**セットアップ**] をクリックします。あるいは、唯一使用可能な I/O モジュールである [**A**] のネットワーク設定を設定するには [**A ギガビット イーサネット**] をクリックし、[**セットアップ**] をクリックします。
   I/O モジュール ネットワーク設定の構成 ページで、適切なデータを入力し、**適用**をクリックします。
2. 許可されている場合は、IOM のルート パスワード、SNMP RO コミュニティー文字列、および Syslog サーバー IP アドレスを入力します。フィールドの説明については、『*CMC オンライン ヘルプ*』を参照してください。

   メモ: CMC 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 アドレス設定を恒久的に保存するには、`connect switch` コマンド (または `racadm connect switch` RACADM コマンド) を入力するか、IOM GUI へのダイレクト インターフェイスを使用して、起動設定ファイルにこのアドレスを保存する必要があります。

   メモ: SNMP コミュニティ文字列の長さは、33 ~ 125 文字の ASCII 値の範囲で設定できます。

3. **適用** をクリックします。
   ネットワーク設定が IOM 用に設定されます。

   メモ: 許可されている場合は、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の設定値にリセットできます。

RACADM を使用した IOM 用ネットワークの設定

RACADM を使用して、IOM にネットワークを設定するには、日付と時刻を設定します。『Chassis Management Controller for PowerEdge VRTX 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 -u <ユーザー名> -p <パスワード>
```

```
racadm deploy -m switch -u -p <パスワード> -v SNMPv2 <snmp コミュニティ文字列> ro
```

```
racadm deploy -a [サーバー|スイッチ] -u <ユーザー名> -p <パスワード>
```

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

電力の管理と監視

PowerEdge VRTX シャーシは、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、電力効率のよいサーバー環境のさらなる強化が可能になります。

PowerEdge VRTX 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 VRTX モジュラーエンクロージャは AC 電力を利用し、その負荷をすべてのアクティブな内蔵電源装置ユニット（PSU）に分散します。システムは、最大 4800 ワットの AC 電力を供給することが可能であり、その電力はサーバーモジュールおよび関連するエンクロージャインフラストラクチャに割り当てられます。ただし、この容量はユーザーが選択する冗長性ポリシーに応じて異なります。

PowerEdge VRTX 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 2 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 **OpenManage Power Center（OMPC）**を介して制御することもできます。OMPC 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
- 動的電源供給（DPSE）

OMPC 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。

トピック：

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

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が AC 電源障害に耐えることのでき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、AC 電源グリッド、ケーブル配線と電源供給、または PSU 自体に起因することが考えられます。

グリッド冗長性に対応するようシステムを設定する場合、PSU はグリッドに分割されます：スロット 1 および 2 の PSU は第 1 グリッド、スロット 3 および 4 の PSU は第 2 グリッドに振り分けられます。CMC マネジャーは、いずれかのグリッドが故障した場合、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。グリッド 冗長性は個々の PSU の故障にも耐えます。

メモ: グリッド冗長性の役割のひとつは、電源グリッド全体に障害が発生してもサーバーがシームレスに稼動するようにすることですが、グリッド 冗長性を維持するために使用できる電力は、2 つのグリッドの容量がほぼ同等の場合に最大となります。

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にのみ実現されます。

グリッド冗長性レベル

グリッド冗長として使用するには、各グリッドにつき 1 台の PUS が必要最低限の構成です。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、各レッグの 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。

冗長性喪失イベントを警告するように設定されている場合には、CMC が AC 冗長性を維持できなくなると、E-メールまたは SNMP アラート (またはその両方) が管理者に送信されます。

この構成で 1 台の PSU が機能しなくなると、その障害の発生した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、冗長グリッドにある PSU (障害状態ではない場合) が、システムを中断なしで機能させるために役立ちます。1 台の PSU が機能を停止すると、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、グリッド冗長性の状態は **なし** として報告され、シャーシの正常性は **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。

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。

グリッド冗長性とは異なり、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 スロット位置に設置する必要がありません。

メモ: Dynamic Power Supply Engagement (DPSE) を使用すると、PSU をスタンバイ状態にすることができます。スタンバイ状態とは、電源を供給していない PSU の物理状態のことです。DPSE を有効にすると、追加の PSU がスタンバイモードになるため、効率性を高めて節電することができます。

メモ: エンクロージャの電源をオフにしている間は、モジュラーエンクロージャの冗長性ポリシーを変更してください。

動的電源供給

デフォルトでは、動的電源供給 (DPSE) モードは無効になっています。DPSE は、シャーシに電力を供給する PSU の電力効率を最適化することにより、電力を節約します。これにより、PSU の寿命も延び、発熱も低減されます。この機能を使用するには、Enterprise ライセンスが必要です。

CMC はエンクロージャの電力割り当て全体を監視し、PSU をスタンバイ状況にして、シャーシの全電力割り当てを少数の PSU で供給するようにします。オンライン PSU は高利用率での動作時に効率が良くなることから、オンライン PSU の効率が向上し、スタンバイ PSU の寿命が延びます。

残りの PSU を最大効率で動作させるには、次の電源冗長性モードを使用します。

- DPSE を使用した **PSU 冗長性** モードは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に必要とされ、もう 1 台は PSU 故障時における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。
- DPSE を使用した **グリッド冗長性** モードでは、少なくとも 2 台の PSU (各電源グリッドごとに 1 台) がアクティブです。グリッド冗長性は、部分的に載荷されたモジュラーエンクロージャ構成に対する効率性と最大可用性の平衡も保ちます。
- DPSE を無効化すると、4 台 の PSU すべてがアクティブになって負荷を共有することから、効率性が最も低くなり、各電源装置の活用率が減少する結果となります。

DPSE は、上記で説明した 2 つの電源装置冗長設定 (**電源装置冗長性** および **グリッド冗長性**) の両方に有効化することが可能です。

メモ: 2 台の PSU 構成モードでは、サーバーの負荷によっては、いずれの PSU もスタンバイモードに移行できない場合があります。

- **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源供給に必要な PSU に加え、常にもう 1 台の PSU の電源をオンにして **オンライン** とマークしておきます。電力使用率が監視され、システム全体の負荷に応じて 1 台の PSU をスタンバイ状況に移行することが可能です。4 台の PSU 構成では、少なくとも 2 台の PSU の電源が常にオンになります。

  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、オンライン PSU 1 台の損失に対応可能であり、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。
- **AC 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 PSU 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、PSU が **スタンバイ** 状況に移行されます。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反映するため、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、1 つのグリッド全体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が上昇により、**スタンバイ** 状態の 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 が有効になっている状況では、電力需要が 2 つの電源冗長性ポリシーモードの両方で上昇した場合、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

次の表に示すように、シャーシのデフォルトの冗長性設定は、シャーシに搭載されている PSU の数によって異なります。

表 37. 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 2 台	DC 冗長性	無効
PSU 4 台	DC 冗長性	無効

グリッド冗長性

4 台の PSU による グリッド冗長性モードでは、4 台すべての PSU がアクティブです。2 台の PSU を 1 つの AC 電源グリッドに接続し、残り 2 台の PSU をもう 1 つの AC 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果的に機能させるには、均衡のとれた台数の PSU 一式が個別の AC グリッドに適切にケーブル配線されている必要があります。

一方の AC グリッドが故障した場合、機能している AC グリッド上にある PSU がサーバーやインフラストラクチャに中断を生じることなく電力供給を引き継ぎます。

注意: グリッド冗長性モードでは、均衡のとれた台数の PSU 一式が必要です (各グリッドに少なくとも 1 台の PSU)。この条件を満たさない場合、グリッド冗長性は不可能です。

電源装置冗長性

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 のうちいずれかが故障してもサーバーまたはシャーシの電源がオフにならないことを確実にします。電源装置の冗長性モードには、少なくとも 2 台の PSU が必要です。追加の PSU が存在する場合、これらは DPSE が有効になるときに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がオフになる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、および需要に応じた異なるモジュールへの電力の再割り当てを可能にします。

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、ストレージアダプタ、PCIe カード、物理ディスク、メイン基板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 4 台装備できます。詳細については、**dell.com/support/manuals** にある『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。

エンクロージャ内でサーバーの電源がオンになると、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供給し、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た後、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。実際の電力要件に基づいて、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。サーバーが割り当てられた電力を完全に使用していると、iDRAC が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、サーバー上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 VRTX 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割り当てに役立てるため、PowerEdge VRTX では、シャーシ全体の AC 電力利用が特定のしきい値内に留ま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、I/O モジュール、ストレージアダプタ、物理ディスクドライブ、メイン基板、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後、エンクロージャ内のサーバーの電源がオンになります。システム入力電力上限は、「電力負荷」より低く設定することはできません。電力負荷とは、インフラストラクチャに割り当てられた電力と電源の入ったサーバーに割り当てられた最小電力の合計です。

メモ: 電力上限機能を使用するには、Enterprise ライセンスが必要です。

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。

シャーシ内における追加サーバー、共有 HDD、PCIe カード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、ファンをより高速で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、ストレージアダプタ、PCIe カード、物理ディスク、メイン基板の装着や、PSU の台数、タイプ、構成によっても、モジュラーエンクロージャの電力需要が増加します。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 5000 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
- I/O モジュールの電源オフ
- ストレージアダプタ、PCIe カード、物理ディスクドライブ、およびメイン基板の電源オフ
- 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、シャーシの電源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 4 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、メイン基板、物理ディスクドライブ、ストレージアダプタには、最高の優先順位が与えられます。CMC が優先順位の高いデバイス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。

サーバーへの優先度レベルの割り当て

追加の電力が必要なとき、サーバー優先度レベルによって CMC がどのサーバーからの電力を利用するかが決定されます。

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 権限が必要です。

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

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. 左ペインで、**サーバー概要** > **電源** > **優先度**をクリックします。
   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. **優先度** ドロップダウンメニューから、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

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 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*> (1~4) 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。

たとえば、スロット 4 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 cfgServerPriority -i 4 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

左ペインで、**シャーシ概要** > **電源** > **電源監視** をクリックします。電源監視 ページに電源正常性、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『オンラインヘルプ』を参照してください。

メモ: 電源装置下でも電源情報性状態を確認することができます。

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
```

AC 電源リカバリー

システムの AC 電源が中断した場合、シャーシは AC 電源が失われる前の以前の電源状態に復元されます。以前の電源状態への復元は、デフォルトの動作です。次の要因が原因で中断が発生する可能性があります。

- 電源の停止
- 電源ケーブルが電源装置ユニット (PSU) から引き出されます
- 配電ユニット (PDU) の停止

バジェット/冗長性の設定 > **AC 電源リカバリを無効化**オプションが選択されている場合、シャーシは AC リカバリ後の電源がオフのままになっています。

ブレードサーバーの自動電源投入が設定されていない場合、手動で電源を入れる必要があることがあります。

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状態を表示するには、左ペインで **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** ページには、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『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 CMC に進み、ログインした後、次を入力します。

```
racadm getpbinfo
```

getpbinfo の詳細 (出力の詳細を含む) については、『Chassis Management Controller for PowerEdge VRTX 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。

冗長性ステータスと全体的な電源正常性

冗長性ステータスは、全体的な電源正常性を判断する要因の 1 つです。電源冗長性ポリシーがグリッド冗長性などに設定されており、冗長性のある状態でのシステム動作が冗長性ステータスで示されている場合、全体的な電源正常性は通常は **OK** です。シャーシに設置された PSU が何らかの理由で故障した場合、シャーシの全体的な電源正常性ステータスは**非重大**と表示されます。ただし、グリッド冗長性の動作条件が満たされない場合、冗長性ステータスは**いいえ**とされ、全体的な電源正常性は**重大**とされます。その理由は、構成された冗長性ポリシーに従ってシステムが動作できないためです。

アクティブ CMC は、スタンバイ CMC から正常性ステータスをポーリングして、シャーシが冗長であるかを判断します。ネットワーク ケーブルを外すと、30 秒後にシャーシのフェールオーバーがトリガーされます。そして、スタンバイ CMC がアクティブになります。ネットワークが停止すると、最初アクティブ CMC であったものが約 3 分後に起動して、スタンバイ CMC になります。このスタンバイ CMC による正常性監視タスクは、5 分後に再開されます。スタンバイで何らかの正常性の変更がある場合、スタンバイの安定後にのみ処理されます。アクティブ CMC による冗長性の判断は、8 分半待機する必要があります。正常性の変更による何らかのフェールオーバーを開始する場合は、事前に冗長性ステータスが正常であることを確認してください。

メモ: 冗長性ポリシーをグリッド冗長性に変更したりグリッド冗長性から変更したりした場合、そうした条件についての事前チェックを CMC は実行しません。そのため、冗長性ポリシーの設定は、即時に冗長性喪失または条件回復をもたらす可能性があります。

PSU 障害発生後の電力管理

電力不足イベント (PSU 障害など) が発生すると、CMC はサーバーへの電力供給を削減します。電力の削減後、CMC はシャーシの電力需要を再評価します。電力要件が引き続き満たされない場合、CMC は優先順位の低いサーバーの電源をオフにします。ただし、この処理はお使いの CMC で設定した電源冗長性ポリシーに基づいて実行されます。冗長サーバーは、サーバーのパフォーマンスに影響を与えることなく、電力の喪失に対応することができます。

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。

PSU を取り外した後の電力の管理

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 を取り外す場合、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オフにする場合があります。

制限

- CMC は、優先順位の高いサーバーの電源をオンにするための優先順位の低いサーバーの *自動*電源オフをサポートしませんが、ユーザーが電源をオフにすることはできます。
- 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、「デフォルトの冗長性設定」にリストされている 2 つの設定のどちらでも選択することができます。

新規サーバーの電源供給ポリシー

電源をオンにした新規サーバーがシャーシに利用できる電力を超えると、CMC は優先順位の低いサーバーに対する電力を減らす可能性があります。これは、システム管理者が、サーバーにフル電力を割り当てるために必要な電力を下回る電力制限をシャーシに設定している場合や、シャーシ内のすべてのサーバーが高い電力を必要とする状況で電力が不足する場合に発生します。優先順位の低いサーバーに割り当てられた電力を削減しても充分な電力を解放できない場合は、新規サーバーの電源をオンにすることができません。

これは、システム管理者が、サーバーに対するフル電源割り当てよりも低い電力制限をシャーシに設定しているか、高電力を必要とするサーバーに利用可能な電力が不十分である場合に発生します。

次の表は、前述したシナリオで新しいサーバーの電源をオンにしたときに CMC が行う処置を説明しています。

表 38. 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
有	節電は不要	許可
無	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 拒否

PSU の機能が停止すると、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が劣化する、または極端な場合には、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 の電源オフまたは 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 39. 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	Disabled（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	Disabled（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。
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。

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 40. 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	電源装置が存在します。
取り外し	電源装置は存在しません。
AC 入力受信	電源装置への電源入力が復元されました。
AC 入力喪失	電源装置への電源入力が失われました。
DC 出力生成	電源装置は正常に動作しています。
DC 出力喪失	電源装置に障害が発生しました。

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 41. 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	Power supply redundancy is lost.（電源装置の冗長性が失われました。）
冗長性回復	電源装置は冗長です。

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 4 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、KVM、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、要件に基づいて異なる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
- 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
- AC 電源リカバリを無効にする

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 は優先順位の高いサーバーおよびシャーシ内のその他モジュールのために電力を解放するために、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。

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。たとえば、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、2 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 4800W に制限されています。

最大節電モード

これは、グリッド冗長性または PSU 冗長性のために有効化されます。CMC は以下の場合に最大節電を実現します。

- 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。

メモ: シャーシ上で最大節電モード (MPCM) が有効になっていると、ブレードサーバーからのすべての電源要求は拒否されます。iDRAC でアクションが発生しているか、ブレードサーバーでホストに電源サイクルの開始を要求している場合、ブレードサーバーに電源は入りません。

電源バジェットを維持するためのサーバー電力の低減

CMC は、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*の範囲内に維持するために追加の電力が必要なとき、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、新しいサーバーが起動すると、CMC は新しいサーバーにより多くの電力を供給するため、優先順位が低いサーバーへの電力を削減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、サーバーのパフォーマンスを低下させます。

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 操作

デフォルトで、110V PSU AC 操作機能が使用可能です。ただし、110V と 220V 操作の組み合わせはサポートされません。両方の電圧の入力が CMC によって検出されると、一方の電圧値のみが選択され、もう一方の電圧レベルに接続されている電源装置の電源がオフにされて、機能していないと表示されます。

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、「電力の管理と監視」を参照してください。

外部電源管理

CMC 電源管理は、オプションとして OpenManage Power Center (OMPC) から制御することができます。詳細については、『OMPC 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、OMPC は次を管理します。

- 対応 VRTX サーバーのサーバー電源
- 対応 VRTX 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する
- 動的電源供給

OPMC は次に、シャーシインフラストラクチャと前世代のサーバーノードへの電力の割り当て後に使用できるバジェットから、対応 VRTX サーバーノード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。すべての対応 VRTX 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: 電源管理処置を実行するには、シャーシ設定システム管理者 権限が必要です。

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. 左ペインで、**シャーシ概要** > **電源** > **設定** をクリックします。
2. **バジェット / 冗長性設定** ページで、次のプロパティのいずれかまたはすべてを必要に応じて選択します。各フィールドの説明については、『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**
   - **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: 電源管理処置を実行するには、シャーシ設定システム管理者 権限が必要です。

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、*<value>* は 1 (グリッド冗長性)、2 (電源装置冗長性) です。デフォルト値は 2 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>
     ```

     この *<value>* は 938 ~ 4800W の数値で、ワット単位での最大電力上限を示しています。デフォルトは 4800 です。

     たとえば、次のコマンドは最大電力バジェットを 4800 ワットに設定します。

     ```
     racadm config -g cfgChassisPower -o cfgChassisPowerCap 4800
     ```
   - 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
     ```
   - 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
     ```
   - 電力リモートログの間隔を確認するには、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、以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 ホストへのロギン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。詳細については、リモート Syslog 設定手順を参照してください。

- Open Manage Power Center (OPMC) によるリモート電源管理を有効にするには、次を入力します。

```
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、『Chassis Management Controller for PowerEdge VRTX 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。

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、PSU) におけるいくつかの電力管理処置をリモートで実行することを可能にします。

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 権限が必要です。

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. 左ペインで、**シャーシ概要** > **電源** > **制御**をクリックします。
   シャーシーの電源制御 ページが表示されます。
2. 次のいずれかの電源制御操作を選択します。
   各オプションの情報は『オンラインヘルプ』を参照してください。
   - **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**
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 <処置>
```

ここでの <*処置*> 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: モジュラー ブレード サーバーは、CMC の再起動またはフェールオーバー中はスロットル状態になります。

メモ: **電源管理処置を実行するには、シャーシ設定システム管理者 権限が必要です。**

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. 左ペインで、**サーバー概要** > **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. **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、『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 (たとえば、サーバーのリセット) を実行します。

IOM での電源制御操作の実行

IOM はリモートでリセットまたは電源投入できます。

メモ: **電源管理処置を実行するには、シャーシ設定システム管理者 権限が必要です。**

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

I/O モジュールで電源制御操作を実行するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** > **I/O モジュール概要** > **電源** をクリックします。
2. **電源制御** ページで、IOM に対する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 (パワーサイクル)。
3. **適用** をクリックします。

RACADM を使用した IOM での電源制御操作の実行

RACADM を使用した IOM での電源制御操作を実行するには、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 chassisaction -m switch <処置>
```

ここで、<処置> は実行する操作 (power cycle) を示します。

15

シャーシストレージの管理

Dell PowerEdge VRTX 上では、次の操作を実行できます。

- 物理ディスクドライブとストレージコントローラの状態の表示。
- コントローラ、物理ディスクドライブ、仮想ディスク、およびエンクロージャのプロパティの表示。
- コントローラ、物理ディスクドライブ、および仮想ディスクのセットアップ。
- 仮想アダプタの割り当て。
- コントローラ、物理ディスクドライブ、および仮想ディスクのトラブルシューティング。
- ストレージコンポーネントのアップデート。
- フォールトトレランスモードでの共有ストレージコントローラの使用。
- 共有 PERC8（内蔵 2）の有効化または無効化。

メモ: 仮想ディスクが最初に作成されている場合は、高速初期化または完全初期化は表示されません。

トピック：

ストレージコンポーネントの状態の表示

ストレージコンポーネントの状態を表示するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** > **ストレージ** > **プロパティ** > **ストレージ概要** をクリックします。
2. **ストレージ概要** ページでは、次を表示することができます。
   - シャーシに取り付けられている物理ディスクドライブのグラフ概要と、各ドライブの状態。
   - すべてのストレージコンポーネントの概要。各コンポーネントには、それぞれのページにアクセスするためのリンクが付いています。
   - ストレージの使用済み容量と合計容量。
   - コントローラ情報。

     メモ: フォールトトレランスコントローラの場合、名前の形式は、共有 <*PERC 番号*> (内蔵 <番号>)になります。例えば、アクティブなコントローラは共有 PERC8 (内蔵 1)、ピアコントローラは共有 PERC8 (内蔵 2)となります。

     メモ: セカンダリ PERC が無効化されている場合、その名前は 無効 PERC (内蔵 2) と表示されます。
   - 最近ログされたストレージイベント。

   メモ: 詳細については『オンラインヘルプ』を参照してください。

ストレージトポロジの表示

ストレージトポロジを表示するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** > **ストレージ** > **プロパティ** > **トポロジ** をクリックします。
2. **トポロジ** ページで、**<コントローラ名>** をクリックして対応するページを表示します。

   メモ: この CMC に関連付けられたストレージデバイスの制御をアクティブに行っているコントラーラ、およびスタンバイとして機能しているパッシブコントローラの名前を表示できます。
3. 取り付けられている各コントローラの下で、**仮想ディスクを表示**、**<エンクロージャ名>**、および **物理ディスクを表示** のリンクをクリックして、それぞれのページを開きます。

CMC ウェブインタフェースを使用した SPERC のフォールトトレランストラブルシューティング情報の表示

SPERC のフォールトトレラント機能の正しい機能性を示す属性を表示するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** > **ストレージ** > **トラブルシューティング** > **セットアップのトラブルシューティング** をクリックします。
   ストレージセットアップのトラブルシューティング ページが表示されます。
2. **ストレージセットアップのトラブルシューティング** ページでは、次の操作を行うことができます。
   - 電源アイコンを ⊞ をクリックして、内蔵コントローラがフォールトトレラントモードにあるときの次の属性を表示します。
     - 2 つの共有 PERC が検出された。
     - 2 つのエキスパンダが検出された
     - 共有 PERC (複数) とエキスパンダ (複数) が正しくケーブル配線されている
     - 共有 PERC (複数) 上の正しいファームウェア
     - エクスパンダ (複数) 上の正しいファームウェア
     - シャーシインフラストラクチャ上の正しいファームウェア
     - 共有 PERC (複数) に同じ設定がある : SPERC (複数) に同じ設定があるかどうかを示します。
   - 電源アイコンを ⊞ をクリックして、内蔵コントローラがフォールトトレラントモードにないときの次の属性を表示します。
     - 1 つの共有 PERC が検出された
     - 1 つのエキスパンダが検出された
     - 共有 PERC とエキスパンダが正しくケーブル配線されている
   - 電源アイコンを ⊞ をクリックして、外付けコントローラがフォールトトレラントにあるときの次の属性を表示します。
     - 2 つの共有 PERC が検出された
     - 共有 PERC が異なるファブリックにインストールされている

- 共有 PERC および EMM が正しく接続されている
- 共有 PERC 上のファームウェアが正しい
- 共有 PERC の設定が同一である

- 電源アイコンを ⊞ をクリックして、外付けコントローラがフォールトトレラントモードにないときの次の属性を表示します。
  - 1 つの共有 PERC が検出された
  - 1 つのエキスパンダが検出された
  - 共有 PERC とエキスパンダが正しくケーブル配線されている
- フォールトトレラント条件が満たされているかどうかを示す各属性の状態を表示します。

  メモ: フォールトトレランス環境内の属性が条件と一致しない場合は、今すぐアップデート オプションがその属性に表示されます。

メモ: 方法を学ぶ オプションが、一部の属性に対して表示されます。属性に関する詳細については、方法を学ぶ をクリックしてください。

3. 属性の条件を満たすには、**今すぐアップデート** をクリックします。
   ストレージコンポーネントアップデート ページが表示され、属性の条件を満たすために、必要なストレージコンポーネントをアップデートすることができます。

CMC Web インターフェイスを使用したスロットへの仮想アダプターの割り当て

仮想アダプター機能を使用すると、取り付けられているストレージを 4 台のサーバーで共有できます。仮想ディスクをサーバー スロットにマップするには、最初に仮想ディスクを仮想アダプター (VA) にマッピングし、次に仮想アダプター (VA) をサーバー スロットにマッピングします。

- VA をサーバー スロットに割り当てる前に、次を確認してください。
  - サーバー スロットが空、またはスロット内のサーバーの電源がオフになっている。
  - VA がサーバーまたはスロットからマップ解除されている。
  - 影響を受けるすべてのサーバーの電源がオフになっている。
- 仮想ディスクが作成され、これらの割り当て先は、**仮想アダプター 1**、**仮想アダプター 2**、**仮想アダプター 3**、**仮想アダプター 4** のいずれかとされます。詳細については、「仮想ディスクへの仮想アダプター アクセス ポリシーの適用」を参照してください。

メモ:

- **一度に 1 つのサーバーにマッピングできるのは仮想アダプタ 1 つのみです。**
- **適切なライセンスがない場合は、VA – サーバー割り当てのマップ解除、または VA のデフォルトサーバーへのマップしか行うことができません。**
- **デフォルトのマッピングは VA1 - サーバースロット 1、VA2 - サーバースロット 2、VA3 - サーバースロット 3、および VA4 - サーバースロット 4 です。**
- **フル ハイト サーバーが挿入されている場合、上部スロットには VA がマッピングされているのに対し、下部スロットには何もマッピングされていません。たとえば、スロット 1 のフル ハイトにおいて、VA1 はスロット 1 に割り当てられており、VA3 は未マップのままです。**
- **システムにエンタープライズ ライセンスがある場合は、4 つの VA のうちどの VA でもサーバー スロットに割り当てることができます。ただし、それでも一度にマップできるのは 1 台のサーバーに対して 1 つの仮想アダプターのみです。**
- **仮想アダプタのルールが、外部および内蔵共有ストレージアダプタに適用されます。**

サーバースロットに対して仮想アダプタをマップまたはマップ解除するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** > **ストレージ** > **セットアップ** > **仮想化** をクリックします。
   ストレージ仮想化 ページが表示されます。
2. 必要な割り当てタイプを選択するには、**割り当てモード : 仮想ディスクから仮想アダプタ** 表から次を選択します。
   - **単一の割り当て** - これを選択して、1 つの仮想ディスクを 1 つの仮想アダプタに割り当てます。
   - [**複数割り当て**] - 1 つの仮想ディスクを複数の仮想アダプターに割り当てます。画面上に表示される手順を読んでから、このオプションを選択して下さい。

メモ: **[複数の割り当て] モードは、サーバーにクラスター サービスがインストールされている場合にのみ選択します。クラスター サービスがインストールされていない状態でこのモードを使用すると、データの破損や損失の原因になる場合があります。**

メモ: **CMC Web インターフェイスで、[割り当てモード] が [単一割り当て] に設定されているとき、1 つの仮想ディスクを複数の仮想アダプターに割り当てることができます。**

3. [**マップされた仮想アダプター**] テーブルの [**処置**] ドロップダウン リストから、次のオプションの 1 つを選択し、[**適用**] をクリックします。
   - **<スロット番号>** - VA が割り当てられる必要があるスロットを選択します。
   - **マップ解除** - これを選択して、スロットに対する VA 割り当てを解除します。

   選択した処置に基づいて、選択したサーバーに対する VA のマッピングまたはマッピング解除が行われます。

   メモ: **下部スロット (3 または 4) のサーバーに割り当てられた VA があるものとします。ハーフ ハイト サーバー (スロット 3 または 4) をフル ハイト サーバーに交換した場合、このフル ハイト サーバーは下部スロットに割り当てられた VA にはアクセスしません。ハーフ ハイト サーバーを挿入し直すことで、この VA へのアクセスが提供されます。**

   ブレードに対して PERC 仮想コントローラブをマッピングまたはマッピング解除します。

   - 個々の外部共有 PERC 8 カードには 4 つの仮想アダプター (VA) があります。システムに 1~2 枚の外部共有 PERC 8 カードが存在する場合、共有モードでは 4 つの仮想アダプターのうち 1 つをマッピングまたはマッピング解除できます。
   - 外付け PCIE スロットが共有アダプタで占有されている場合、仮想アダプタマッピングにより、共有ストレージ VA プールの最新の詳細または情報を取得できます。
   - 共有アダプターが外部 PCIE スロットを占有している場合、共有デバイスはサポートされません。共有アダプターを使用する場合の共有デバイスのサポートは、共有ストレージの VA プールを変更することで行えます。

ストレージコントローラでのフォールトトレランス

高可用性 (HA) ストレージは、複数の内蔵コンポーネントの使用、およびストレージリソースへの複数のアクセスポイントの使用を可能にします。ストレージコンポーネントが機能停止した場合、サーバーは、使用可能なデータへの 2 番目の重要コンポーネントまたはパスによってサポートされます。高可用性は、水面下でサービスを復元することによってダウンタイムを最小限に抑え、これは多くの場合は機能障害がはっきりと表れる前に行われますが、ダウンタイムを排除するわけではありません。フォールトトレランス (FT) は、ストレージシステム内の、バックアップコンポーネントとして動作するように設定され、スタンバイモードに保たれる冗長コンポーネントを活用します。フォールトトレランスモードのストレージコントローラは、ストレージサービスの中断を防ぎ、機能停止したコンポーネントのサービスを自動的に引き継ぎます。冗長コンポーネント (コントローラ) は通常のの動作状況では使用されないため、フェールオーバープロセス中、パフォーマンスの一貫性が維持されます。

フォールトトレランスを備えた高可用性には以下のような利点があります。

- コントローラが機能停止した場合でも、すべてのストレージアプリケーションにアップタイムを提供。
- シャーシの重要機能へのアクセスを常時提供。
- コントローラが機能停止、または故障したときに、サーバーが状況に対処することを可能にする。
- コンポーネント冗長性を利用する。

コントローラのフォールトトレランス機能を使用することにより、アクティブおよびパッシブ (ピア) コントローラを持つことによって達成される共有ストレージに関連するタスクを管理できます。アクティブコントローラは、アクティブであり、ストレージ関連プロセスのすべてを監視するコントローラです。アクティブコントローラが機能停止した場合に、ピアホットスペアとして動作しているパッシブコントローラがその機能をシームレスに引き継ぐため、両コントローラの稼働状態はコントローラ間で伝達されます。

メモ: **CMC は、SR-IOV 対応ファームウェアを持つ共有 PERC 8 用のフォールトトレランスデータを表示します。非 SR-IOV カードが共有ストレージスロットに接続されている場合、カードに電源が投入されず、アラートが生成されます。**

メモ: **CMC の設定をリセットする CMC のリセットなどの操作は、外部フォールトトレラント構成をリセットします。この結果、PERC モードが「安全モード」に変更されます。外部 PERC でフォールトトレランスを無効にしてください。**

セキュリティキーの不一致

暗号化 keyID と **パスフレーズを**を使用して、コントローラーのセキュリティキーを作成できます。コントローラは、セキュリティキーの作成中に使用される**パスフレーズ**のみを比較し、2 つのコントローラに同じセキュリティキーがあるかどうかを特定します。したがって、クラスタへの参加する 2 つのコントローラは異なる **暗号化キー ID** を使用している場合でも、同じパスフレーズを使用している限り、フォールトトレラントです。

セキュリティキーの不一致が 2 つのピアコントローラ間で検出された場合、フォールトトレラントモードが「劣化」に変更されます。重要アラートが**シャーシの正常性**ページに表示され、監視が適切なドライブの関連付けを表示しないことがあります。

セキュリティキーの不一致が検出された場合、コントローラで他のストレージセキュリティ操作を実行する前に、コントローラのセキュリティキーの作成、変更、または削除を実行することによりキーの不一致を解決します。不一致が解決された後、シャーシの電源サイクルを実行します。2 つの非高可用性コントローラを組み合わせる前に、一致するようにキーに変更します。このアクションにより、クラスタに参加する各コントローラに関連付けられる安全なドライブのインポートが容易になります。

外部コントローラについては、フォールトトレランス用のケーブル接続を行う前に、一致するようにキーを変更します。セキュリティキーを変更すると、クラスタに参加する各コントローラに関連付けられる安全なドライブのインポートが容易になります。

CMC ウェブインタフェースを使用したセキュリティキーの不一致の解決

CMC ウェブインタフェースを使用して、セキュリティキーの不一致を解決するには、次の操作を実行します。

1. サーバモジュールの電源をオフにします。
2. **サーバー概要** > **電源** > **制御** > **サーバーの電源をオフにする**をクリックします。
3. 既存の非フォールトのフォールトトレラントコントローラの 1 つまたは両方を変更して、キーが一致するようにします。
4. シャーシの電源を切ってすぐ入れなおします。
5. コントローラのキーが一致しているかどうかを確認します。

CMC ウェブインタフェースを使用したコントローラプロパティの表示

コントローラプロパティを表示するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** > **コントローラ** をクリックします。
2. **コントローラ** ページの **コントローラ** セクションで、コントローラの基本プロパティを確認できます。ただし、詳細なプロパティを表示するには、 。

   メモ: コントローラがフォールトトレランスモードの場合、フォールトトレランスの状態とモードに関する次の情報も表示されます。

   - **フォールトトレランスモード - 共有、アクティブ / パッシブ**
   - **フォールトトレランス状態 - 正常 / 通常、または喪失 / 劣化**
   - **ピアコントローラ - 2 台のコントローラによってサポートされるフォールトトレランスモードの場合、ピア (スタンバイ) として機能するコントローラの名前を示します。**

   メモ: ピアコントローラが無効な場合、その名前は 無効 PERC (内蔵 2) または無効 PERC(SPERC スロット 6)として表示されます。状態が 不明 と表示され、これはピアコントローラがオフになっていることを示します。

   コントローラに関する詳細については、『オンラインヘルプ』を参照してください。

RACADM を使用したコントローラプロパティの表示

RACADM を使用してコントローラプロパティを表示するには、コマンド `racadm raid get controllers -o` を実行します。

詳細については、『Chassis Management Controller for PowerEdge VRTX 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。

外部設定のインポートまたはクリア

外部ディスクはシャーシに挿入されている必要があります。

外部設定をインポートまたはクリアするには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** > **ストレージ** > **コントローラ** > **セットアップ** をクリックします。
2. **コントローラ設定** ページの **外部設定** セクションで、各コントローラに対して次をクリックします。

- **外部設定のクリア**。既存のディスク設定をクリアします。
- **インポート/回復**。外部設定を持つディスクをインポートします。

メモ: 特定の仮想ディスクのディスクを削除し、コントローラをリセットし、ドライブを 1 つずつ再挿入すると、異なるサイズと状態の複数の仮想ディスクインスタンスが 外部設定 ページに表示されます。インポートアクティビティが完了すると、仮想ディスクの正しい状態とサイズが表示されます。

ストレージコントローラの設定

ストレージコントローラの既存プロパティを変更したり、新しく取り付けられたストレージコントローラの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ストレージコントローラの設定

少なくとも 1 台のストレージコントローラがシャーシに取り付けられていることを確認してください。

ストレージコントローラを設定するには、次の手順を実行します。

1. CMC ウェブインタフェースで、**シャーシ概要** > **ストレージ** > **コントローラ** > **セットアップ** と進みます。
2. **コントローラセットアップ** ページで、**コントローラ** ドロップダウンメニューからコントローラを選択します。

   メモ: 次に注意してください。

   - **ストレージコントローラがフォールトトレランスモードで、また両方に同じファームウェアバージョンがある場合、両方のコントローラがドロップダウンメニューに単一のデバイスとして表示されます。例えば、共有 PERC8 (内蔵 1) または共有 PERC8 (内蔵 2) または共有 PERC8 (SPERC スロット 5) または共有 PERC8 (SPERC スロット 6) と表示されます。2 つのコントローラの設定が異なる場合は、設定非互換 メッセージが表示されます。フォールトトレランスコントローラのプロパティは、両方のコントローラでプロパティが同じになるように設定することができます。このモードのコントローラは個別のプロパティを持つことができません。**
   - **異なるファームウェアバージョンで 2 番目のストレージコントローラがインストールされている場合、ドロップダウンメニューにコントローラが 2 つのコンポーネントとして表示されます。例えば、共有 PERC8 (内蔵 1)、共有 PERC8 (内蔵 2) は、共有 PERC8 (SPERC スロット 5) と共有 PERC8 (SPERC スロット 6) などです。**

   選択したコントローラの属性値が表内でアップデートされます。
3. 適切なデータを入力または選択して、**適用** をクリックします。

   メモ: 属性およびその他のフィールドの説明については、*『オンラインヘルプ』*を参照してください。

   新しく設定されたプロパティが選択したコントローラに適用され、**現在値** フィールドに、その属性のアップデートされた値が表示されます。

RACADM を使用したストレージコントローラの設定

RACADM コマンドを実行してストレージコントローラをセットアップするには、次の構文を使用します。

```
racadm raid ctrlprop:RAID.ChassisIntegrated.1-1 [-rebuild <value>] [-bgi <value>] [-
reconstruct <value>] [-checkconsistency <value>] [-ccmode {abortonerror | normal}] [-
copybackmode {off | on | onwithsmart}] [-lb {auto | disabled}] [-prunconfigured {yes | no}]
```

詳細については、『Chassis Management Controller for PowerEdge VRTX 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。

共有 PERC コントローラ

内蔵共有 PERC が 2 つインストールされているシステムの場合、**フォールトトレラント** モードから **非フォールトトレラント** モードに操作モードを変更することができるか、またはこの逆に、2 番目の内部共有 PERC 8 コントローラを有効または無効にすることにより、ウェブインタフェースまたは RACADM CLI を使用できます。

内部共有 PERC 8 コントローラの場合、2 つ目の内蔵コントローラを無効にすることができます。2 つ目の内蔵コントローラが無効になった後、最初の内蔵コントローラはフォールトトレラントモードではありません。2 つ目の内蔵コントローラが有効になると、2 本の内蔵コントローラは、デフォルトでフォールトトレラントモードです。2 つ目の内蔵コントローラは、`racadm raid disableperc:RAID.ChassisIntegrated.2-1` コマンドで無効にできます。

外付けエンクロージャの場合、`racadm raid disableperc: RAID.ChassisSlot.5-1 and racadm raid disableperc: RAID.ChassisSlot.6-1` コマンドをそれぞれ使って、スロット 5 とスロット 6 の外付け共有 PERC 8 カードの両方を無効にできます。

RACADM コマンドラインインタフェースから `racadm raid get controllers` コマンドを実行して、お使いのシステム上の共有 PERC コントローラの数をリストします。このコマンドが `RAID.ChassisIntegrated.1-1` のみをリストする場合、お使いのシステムには単一の共有 PERC コントローラがあります。このコマンドが `RAID.ChassisIntegrated.1-1`、`RAID.ChassisIntegrated.2-1` をリストする場合、お使いのシステムには 2 台の共有 PERC コントローラがあります。

スロット 5 とスロット 6 の 2 番目の内蔵共有 PERC 8 および外付け共有 PERC 8 カードは、有効または無効にできます。

CMC ウェブインタフェースを使用して操作モードを変更するには、左ペインで **シャーシ概要** > **ストレージコントローラ** と移動して **コントローラトラブルシューティング** ページに移動し、**RAID コントローラの無効化** または **RAID コントローラの有効化** オプションを選択します。

RACADM CLI を使用して動作モードを変更するには、次の手順を実行します。

- 2 番目の内蔵共有 PERC8 が無効な場合、`racadm raid enableperc:RAID.ChassisIntegrated.2-1` コマンドを実行して、**内蔵 2 共有 PERC 8** および **フォールトトレランス**モードを有効にすることができます。
- `racadm raid enableperc:RAID.ChassisSlot.6-1` コマンドを実行して、スロット 6 で**外付け共有 PERC8** を有効にします。
- `racadm raid disableperc:RAID.ChassisIntegrated.2-1` コマンドを実行して、**2 番目の内蔵共有 PERC8** および **フォールトトレラントス**モードを無効にします。

メモ:

- **enable** または **disable** コマンドを実行する前に、シャーシの電源をオンにし、すべてのサーバーモジュールの電源をオフにする必要があります。シャーシでは、この操作の一環として自動的にパワーサイクルが行われます。共有 PERC の動作モードの変更後は、トラブルシューティング ページを使用する、または **racadm racreset** コマンドを実行して CMC のリセットを行うことが推奨されます。
- デフォルトで、2 番目の内蔵 PERC 8 カードが検出された場合は、そのモードが高可用性モードを表示します。
- 外付けスロットで SPERC を有効にしても、フォールトトレランスを有効になりません。
- 外付け共有 PERC8 に対してフォールトトレラントモードを有効にするには、「*RACADM を使用した外付け RAID コントローラのフォールトトレランスを有効または無効にする*」セクションを参照します。

CMC ウェブインタフェースを使用した RAID コントローラの有効化または無効化

2 台の共有 PERC8 コントローラを搭載した VRTX シャーシでは、内蔵 1 PERC アダプタがアクティブで、すべてのサーバーモジュールがオフになっているときに、内蔵 2 PERC アダプタを有効または無効にすることができます。フォールトトレランスのためには、両方のアダプタが有効になっている必要があります。**コントローラのトラブルシューティング** ページでは、ピアコントローラの有効化または無効化が可能です。

メモ: データの損失を防ぐには、コントローラの有効化または無効化操作を実行する前に、次を行ってください。

- **再構築やコピーバックといったすべての操作を完了する。**
- **データボリュームが最適状態であることを確認する。**

メモ: 次の場合、2 つ目の PERC アダプタを有効にする間に警告メッセージが表示され、フォールトトレラントの状態が劣化状態になります。

- **PERC アダプタの設定のいずれかが変更された。**
- **ファームがウェアアップデートされた。**

フォールトトレラントシステム設定をフォールトトレラントモードに設定するには、共有 PERC のファームウェアおよび設定が一致していることを確認します。

ピアコントローラは、次の状況下に限り、無効にすることができます。

- シャーシ内のすべてのサーバーの電源が切れている。
- 内蔵 1 PERC が現在アクティブなコントローラである。

  メモ: 内蔵 1 PERC が現在アクティブなコントローラではない場合は、シャーシのパワーサイクルを実行してこのコントローラをアクティブにします。
- 両方の CMC にこの機能をサポートする同じファームウェアバージョンがある。

メモ: 内蔵 2 PERC を無効にした後に CMC カードを交換するには、CMC カードをシステム内のアクティブ CMC コントローラカードとして割り当てる前に、ファームウェアバージョン 1.35 以降でカードをアップデートすることをお勧めします。この処置を実行する前に、メッセージが表示されます。

CMC ウェブインタフェースを使用してフォールトトレラントモードのピアコントローラを有効または無効にするには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** > **ストレージ** > **コントローラ** > **トラブルシューティング** をクリックします。
2. **コントローラトラブルシューティング** ページで、内蔵 2 PERC に対応する **処置** ドロップダウンメニューから次のいずれかを選択し、**適用** をクリックします。
   - **RAID コントローラを無効にする** — フォールトトレラントモードでピアコントローラを無効にします。
   - **RAID コントローラの有効化** — フォールトトレラントモードのピアコントローラを有効化します。内蔵 2 PERC がすでに無効になっている場合、ドロップダウンメニューの **RAID コントローラの有効化** オプションが使用可能になります。
   - 外付け共有 PERC 8 カードコントローラを有効または無効にするには、次の手順を実行します。
     - **コントローラトラブルシューティング** ページで、スロット 5 またはスロット 6 の外付け共有 PERC 8 カードに対応する **処置** ドロップダウンメニューから次のいずれかを選択し、**適用** をクリックします。
       - **RAID コントローラを無効する** — RAID コントローラを無効にします。
       - **RAID コントローラを有効にする** — RAID コントローラを有効にします。PERC がすでに無効になっている場合、ドロップダウンメニューの **RAID コントローラを有効にする** オプションが使用可能になります。
   - **設定のリセット** — このオプションを選択して、仮想ドライブを削除し、コントローラに接続されたすべてのホットスペアの割り当てを解除します。ただし、これで削除されるのは構成からのディスクのみであり、データは削除されません。メモ：構成をリセットしても、外部構成は削除されません。外部設定のクリアを使用してリセットします。
   - **TTY ログのエクスポート** — このオプションを選択して、ローカルシステム上の TTY ログをエクスポートします。メモ：コントローラから収集された TTY ログには、ドライブから取得したデータが含まれていません。SAS アドレスなどのデータが含まれている可能性があります。
   - **フォールトトレランスを有効にする** — このオプションを選択すると、外付け PERC のフォールトトレランスモードを有効にすることができます。またこの処置を実行すると、外付け共有 PERC 9 がリセットされます。
   - **フォールトトレランスを無効にする** — このオプションを選択すると、外付け PERC のフォールトトレランスモードを無効にすることができます。またこの処置を実行すると、外付け共有 PERC 9 がリセットされます。

     メモ:
     - **無効化された PERC については、その他オプション (設定のリセット、TTY ログのエクスポート、固定キャッシュの破棄、RAID コントローラの無効化) のいずれもドロップダウンメニューで利用できません。**
     - **デフォルトでは、内蔵されている 2 つの共有ストレージアダプタが高可用性モードで検出されます。**
     - **外部共有コントローラが接続された後、その上でフォールトトレランスモードを有効にする必要があります。**
     - **フォールトトレランスを有効にする と フォールトトレランスを無効にする は、外付け共有 PERC 8 カードについてのみ表示されます。 外付け共有 PERC 8 カードのデフォルトモードは、非フォールトトレラントモードです。**

メモ: ピアコントローラの有効化または無効化により、シャーシのパワーサイクルが開始されます。変更が反映されるのは、パワーサイクル完了後のみです。

RACADM を使用して RAID コントローラの有効または無効にする

RACADM を使用してピアコントローラを有効化するには、CMC にシリアル /Telnet/SSH テキストコンソールを開き、ログインして次のように入力します。

```
racadm raid enableperc:<AdapterFQDD>
```

ピアコントローラを無効化するには、次を入力します。

```
racadm raid disableperc:<AdapterFQDD>
```

メモ: RACADM インタフェースを使用したこの機能の詳細については、『*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。

RACADM を使用した外付け RAID コントローラのフォールトトレランスを有効または無効にする

フォールトトレランスを有効にするには、次の手順を実行します。

```
racadm raid controllers: <FQDD of External Shared PERC8> -p HighAvailabilityMode ha
```

フォールトトレランスを無効にするには、次の手順を実行します。

```
racadm raid set controllers: <FQDD of External Shared PERC8> -p HighAvailabilityMode None
```

CMC ウェブインタフェースを使用した物理ディスクプロパティの表示

物理ディスクがシャーシに取り付けられていることを確認してください。

物理ディスクドライブのプロパティを表示するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** > **ストレージ** > **物理ディスク** に移動します。
   プロパティ ページが表示されます。
2. すべての物理ディスクドライブのプロパティを表示するには、**物理ディスク** セクションで ＋。

   メモ: 内蔵共有アダプタのフォールトトレラントモードに表示されるのは、次の値です。

   - **アクティブコントローラ - 共有 PERC8 (内蔵 1)**
   - **冗長 /フェイルオーバーコントローラ - 共有 PERC8 (内蔵 2)**

   外付け共有アダプタのフォールトトレラントモードに表示されるのは、次の値です。

   - **アクティブコントローラ - 共有 PERC8 (SPERC、スロット 5)**
   - **冗長/フェールオーバーコントローラ - 共有 PERC8 (SPERC、スロット 6)**

   また、次のフィルタを使用して、特定の物理ディスクドライブのプロパティを表示することできます。

   - **物理ディスク基本フィルタ** オプションの **グループ基準** ドロップダウンメニューから、**仮想ディスク**、**コントローラ**、または **エンクロージャ** を選択し、**適用** をクリックします。
   - **詳細フィルタ** をクリックし、各種属性の値を選択して、**適用** をクリックします。

RACADM を使用した物理ディスクドライブプロパティの表示

RACADM を使用して物理ディスクドライブのプロパティを表示するには、コマンド `racadm raid get pdisks -o` を実行します。

詳細については、『Chassis Management Controller for PowerEdge VRTX 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。

物理ディスクと仮想ディスクの識別

LED 点滅機能の有効化または無効化についての詳細は、次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 LED 点滅の設定
- RACADM を使用した LED の点滅の設定

CMC Web インターフェイスを使用したグローバルホット スペアの割り当て

グローバルホットスペアを割り当てまたは割り当て解除するには、次の手順を実行します。

1. 左ペインで、**[シャーシ概要]** > **[ストレージ]** > **[物理ディスク]** > **[セットアップ]** の順にクリックします。
   物理ディスクの設定ページが表示されます。
2. **物理ディスクの構成**セクションで、**物理ディスクのアクション**ドロップダウンメニューから、**未割り当て**を選択するか、物理ディスクドライブのそれぞれに対して**グローバルホットスペア**を選択し、**適用**をクリックします。

メモ: グローバルホットスペアの割り当ては、対応するコントローラに少なくとも 1 つの仮想ディスクが存在する場合にのみ行うことができます。

RACADM を使用したグローバルホットスペアの割り当て

RACADM を使用してグローバルホットスペアを割り当てるには、コマンド `racadm raid hotspare: -assign yes -type ghs` を実行します。

RACADM コマンドの使用の詳細については、『Chassis Management Controller for PowerEdge VRTX 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。

物理ディスクの回復

物理ディスクを回復するには、以下を実行します。

1. CMC ウェブインタフェースで、**シャーシ概要** > **ストレージ** > **物理ディスク** > **セットアップ** と移動します。
2. **セットアップ** ページの **物理ディスクの回復** セクションの下で回復する必要がある物理ディスクを選択し、ドロップダウンメニューから **ドライブの再構築**、**再構築のキャンセル**、または **オンラインに強制** を適切に選択して **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仮想ディスクプロパティの表示

仮想ディスクが作成されていることを確認してください。

仮想ディスクプロパティを表示するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** > **ストレージ** > **仮想ディスク** > **プロパティ** をクリックします。
2. **プロパティ** ページの **仮想ディスク** セクションで、 をクリックします。また、次のフィルタを使用して、特定の仮想ディスクプロパティを表示することもできます。
   - **基本仮想ディスクフィルタ** セクションの **コントローラ** ドロップダウンメニューから、コントローラ名を選択し、**適用** をクリックします。
   - **詳細フィルタ** をクリックし、各種属性の値を選択して、**適用** をクリックします。

RACADM を使用した仮想ディスクプロパティの表示

RACADM を使用して仮想ディスクプロパティを表示するには、コマンド `racadm raid get vdisks -o` を実行します。

詳細については、『Chassis Management Controller for PowerEdge VRTX 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 Web インターフェイスを使用した仮想ディスクの作成

デフォルトでは、CMC は初期化せずに仮想ディスクを作成します。ただし、初期化せずに作成される仮想ディスクに対しては、高速初期化オプションを選択できます。高速初期化プロセスでは、仮想ディスクの最初と最後の 8 MB がクリアされ、すべてのブート レコードやパーティション情報が削除されます。高速初期化を実行するには、**シャーシ設定管理者権限**が必要です。

物理ディスクがシャーシに取り付けられていることを確認してください。

メモ: 仮想ディスクを削除すると、その仮想ディスクはコントローラの設定から削除されます。

仮想ディスクを作成するには次のように入力します。

1. 左ペインで、**[シャーシ概要]** > **[ストレージ]** > **[仮想ディスク]** > **[作成]** の順にクリックします。
2. **仮想ディスクの作成**ページで、**RAID レベル**セクションから、RAID レベルを選択します。
3. **物理ディスクの選択**セクションから、選択した RAID レベルに基づいて物理ディスクドライブの数を選択します。
4. **設定の構成**セクションで、適切なデータを入力し、**初期化**および **仮想ディスクの暗号化**オプションを選択してから、**仮想ディスクの作成**をクリックします。

   CMC では、仮想ディスクの作成中に、新しいオプション (初期化) が提示されます。このオプションを利用すると、高速初期化なしで仮想ディスクを作成できます。デフォルトでは、仮想ディスク作成は高速初期化ありで行われます。

   [**初期化**] オプションを利用すると、初期化せずに仮想ディスクを作成できます。このオプションは、仮想ディスクの作成時に高速初期化プロセスがデフォルトで起動するのを無効にします。

   仮想ディスクの暗号化オプションを利用すると、自己暗号化ドライブ (SED) で安全な仮想ディスクを作成できます。

   メモ: 仮想ディスクの暗号化オプションは、暗号化キーがコントローラの設定ページにある特定のコントローラに設定されている場合のみが有効にされます。

暗号化キーの管理

コントローラ上に作成される暗号またはセキュリティキーは、SED で作成される仮想ディスクを保護するために、アクセスをロック、またはロック解除されます。暗号化対応コントローラに対して 1 つのキーの暗号化のみが作成できます。暗号化キーは、**コントローラのセットアップ**ページで、暗号化キー識別子とパスフレーズを入力することにより作成できます。CMC を利用すると、暗号化キーのパスフレーズを変更したり、暗号化キーを削除することもできます。

CMC ウェブインタフェースを使用した暗号化キーの作成

暗号化キーが**未設定**の場合に、コントローラーに対する暗号またはセキュリティキーを作成できます。

暗号化キーを作成するには、次の手順を実行します。

1. 左側のペインで、**ストレージ** > **コントローラ** > **セットアップ**を選択してください。
2. **セキュリティキー**ドロップダウンから、**セキュリティキーの作成**を選択します。
   ポップアップウィンドウが表示されます。
3. セキュリティキーとパスワードを入力して、**OK** をクリックします。
4. **コントローラのセットアップ**ページで、**適用**をクリックします。
   暗号化キーが作成されると、**セキュリティキー**のステータスが**有効**に変更されます。

RACADM を使用した暗号化キーの作成

RACADM コマンドを実行して暗号化キーを作成するには、次の構文を使用します。

```
racadm raid createsecuritykey:RAID.ChassisIntegrated.1-1 -key <Key id> -passwd <passphrase>
```

詳細については、『*Chassis Management Controller for PowerEdge VRTX 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暗号化キー識別子の変更

コントローラの暗号化キー識別子とパスフレーズを変更できます。

暗号化キー識別子とパスフレーズを変更するには、次の操作を実行します。

1. 左側のペインで、**ストレージ** > **コントローラ** > **セットアップ**を選択してください。
2. **セキュリティキー**ドロップダウンから、**セキュリティキーの修正**を選択します。
   ポップアップウィンドウが表示されます。
3. 新しい暗号化キー識別子と既存と新規のパスフレーズを入力し、**OK** をクリックします。
4. **コントローラのセットアップ**ページで、**適用**をクリックします。

RACADM を使用した暗号化識別子キーの修正

RACADM コマンドを実行して暗号化キー識別子とパスフレーズを変更するには、次の構文を使用します。

```
racadm raid modifysecuritykey:RAID.ChassisIntegrated.1-1 -key <Key id> -oldpasswd
<oldpassphrase> -newpasswd <newpassphrase>
```

詳細については、『*Chassis Management Controller for PowerEdge VRTX 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暗号化キーの削除

コントローラの暗号化キーは、保護された仮想ディスクがそれと関連付けられていない場合のみを削除できます。

暗号化キーを削除するには、次の手順を実行します。

1. 左側のペインで、**ストレージ** > **コントローラ** > **セットアップ**を選択してください。
2. **セキュリティキー**ドロップダウンから、**セキュリティキーの削除**を選択します。
   確認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。
   暗号化キーを削除した後、仮想ディスクの一部ではないすべての SED がセキュアに消去されます。詳細については、*オンラインヘルプ*を参照してください。

RACADM を使用した暗号化キーの削除

RACADM コマンドを実行して暗号化キーを削除するには、次の構文を使用します。

```
racadm raid deletesecuritykey:RAID.ChassisIntegrated.1-1
```

詳細については、『*Chassis Management Controller for PowerEdge VRTX 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。

仮想ディスクの暗号化

コントローラで暗号化キーを設定した後に、SED で作成された仮想ディスクを暗号化できます。暗号化を実行するときには、メッセージが必ず CMC **ログ**に記録されます。仮想ディスクを暗号化できます。

- セキュリティキーが、コントローラに設定されます。
- 仮想ディスク上のすべてのドライブは SED です。

1 つの仮想ディスクを暗号化すると、同じディスクグループのすべての仮想ディスクで暗号化が有効になります。

仮想ディスクを暗号化するには、**シャーシ設定管理者**の権限が必要です。

CMC ウェブインタフェースを使用する仮想ディスクの暗号化

既存の仮想ディスクを暗号化するには、次の操作を実行します。

1. 左ペインで、**Chassis ストレージ** > **仮想ディスク** > **管理**の順にクリックします。
2. **仮想アクション**ドロップダウンリストから、**仮想ディスク**を選択し、**適用**をクリックします。

メモ: 仮想ディスクの暗号化オプションは、安全でない仮想ディスクが SED で設定されている場合にのみ使用できます。

RACADM を使用した仮想ディスクの暗号化

RACADM コマンドを実行して仮想ディスクを暗号化するには、次の構文を使用します。

```
racadm raid encryptvd:Disk.Virtual.0:RAID.ChassisIntegrated.1-1
```

詳細については、『*Chassis Management Controller for PowerEdge VRTX 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。

外部設定のロック解除

セキュア仮想ディスクの一部であるドライブが、セキュアドライブと呼ばれます。セキュアドライブは、1 つのコントローラから別のコントローラに移行できます。宛先コントローラに対して異なる暗号化またはセキュリティキーが設定されると、これらのドライブのセキュリティステータスが「ロック済み」として表示され、「外部設定のプレビュー」の一部として表示されません。「外部構成のインポート」は、これらの外部ドライブを検知しません。

ロック解除コマンドを実行している間は、これらのドライブにソースコントローラパスフレーズとキー ID を提供します。ロック解除後も、これらのドライブは「外部コントローラキー」によって引き続き保護されます。ただし、既存の「外部設定のプレビュー」で外部ドライブを検索する際にこれらのドライブを表示することができます。これらのセキュアドライブでインポートを行ったり、外部設定をクリアしたりすることができます。

異なるセキュリティキーを持つ外部ドライブを複数のコントローラから移行する場合は、別のコントローラから移行されたドライブのロックを解除する前に、一方の外部コントローラからドライブのセットをロック解除し、インポートまたはクリアします。これにより、コントローラにロックを解除されたがインポートまたはクリアされなかったドライブがある場合は、コントローラ上でロックの解除はできません。

ドライブがいったんロック解除されると、CMC ウェブインタフェースまたは RACADM を使用して外部構成をインポートすることができます。

コントローラの電源がロックの解除後およびインポートフェーズ前に循環される場合、ドライブは再びロックされます。

システムに複数の外部構成がある場合は、外部設定のロックを解除する前に、各外部設定のロックを解除し、インポートします。

ロック解除に使用するキー ID は、キー ID が一致するドライブを識別するためだけに使用されます。一致するドライブが検出された後は、パスフレーズは、ドライブのロック解除に使用されます。

CMC Web インターフェイスを使用した外部設定のアンロック

外部設定をアンロックするには、次の手順を実行します。

1. 左ペインで、**[シャーシ概要]** > **[ストレージ]** > **[コントローラー]** > **[セットアップ]** をクリックします。
2. **[セットアップ]** ページに移動します。
3. **[アンロックをするにはここをクリック]** をクリックします。
   [物理ディスク] ページが表示されます。
4. アンロックする物理ディスクを選択します。
5. 物理ディスクがキー識別子に関連付けられているかを確認します。
6. **[アクション]** ドロップダウンで、**[ドライブのアンロック]** を選択します。
   セキュリティ キー フレーズの入力を求めるダイアログ ボックスが表示されます。
7. **[セキュリティ キーのパスフレーズ]** テキスト ボックスにパスフレーズを入力します。

8. パスフレーズを再入力して、[**アンロック**] をクリックします。
物理ドライブはアンロックされ、このドライブは [**物理ディスクの回復**] リストに表示されません。

RACADM を使用した外部設定のロック解除

RACADM コマンドを実行して外部設定のロックを解除するには、次の構文を使用します。

```
racadm raid unlock:<Controller FQDD> -key <Key id> -passwd <passphrase>
```

詳細については、『*Chassis Management Controller for PowerEdge VRTX 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。

暗号消去

暗号消去オプションを用いると、セキュアな SED 上のデータを安全に消去できます。セキュアなデータは、仮想ディスクの削除後もドライブ上に存在し続け、脅威にさらされた状態になっています。暗号消去は、次の条件で使用できます。

- セキュアなドライブを廃棄/再利用するために、データを削除するとき。
- セキュアでロックされた外部設定をインポートする必要がない場合に、データを安全に消去するとき。
- パスフレーズを紛失した場合に、ロックされたドライブを回復するとき。

1 つまたは複数の SED 物理ディスクの暗号消去を実行することができます。

注意: 暗号消去タスクを実行すると、物理ディスク上のすべてのデータが消去されます。

暗号消去の実行

物理ディスクが仮想ディスクの一部である場合、暗号消去を実行する前に、仮想ディスクから削除します。

暗号消去を実行します。

1. 左側のペインで、**ストレージ** > **物理ディスク** > **セットアップ**を選択してください。
物理ディスクの設定ページが表示されます。
2. データを消去する物理ディスクを選択します。
3. **物理ディスクのアクション**ドロップダウンリストから、**暗号消去**を選択し、**適用**をクリックします。
メッセージが表示され、操作の確認が求められます
4. **はい**をクリックして続行します。
選択した物理ディスクからのすべてのデータが削除されます。

仮想ディスクへの仮想アダプタアクセスポリシーの適用

物理ディスクドライブがインストールされており、仮想ディスクが作成されていることを確認します。

仮想アダプタアクセスポリシーを適用するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** > **ストレージ** > **仮想ディスク** > **割り当て** をクリックします。
2. **仮想ディスクの割り当て** ページの **仮想アダプタのアクセスポリシー** セクションで、**仮想アダプタ <番号>** ドロップダウンメニューから各物理ディスクドライブについて **フルアクセス** を選択します。
3. **適用** をクリックします。

これで、仮想アダプタをサーバースロットに割り当てることができます。詳細については、本ユーザーズガイドのスロットへの仮想アダプタの割り当ての項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仮想ディスクプロパティの変更

仮想ディスクプロパティを変更するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** > **ストレージ** > **仮想ディスク** > **管理** をクリックします。
2. **仮想ディスクの管理** ページの **仮想ディスク処置** ドロップダウンメニューから、次の処置のいずれかを選択し、**適用** をクリックします。
   - **名前の変更**
   - **削除**

   メモ: 削除を選択した場合、仮想ディスクを削除するとその仮想ディスク内で使用可能なデータが恒久的に削除されることを示す次のメッセージが表示されます。

   ```
   Deleting the virtual disk removes the virtual disk from the controller's configuration.
   Initializing the virtual disk permanently erases data from the virtual disk.
   ```

   - **ポリシーの編集：読み取りキャッシュ**
   - **ポリシーの編集：書き込みキャッシュ**
   - **ポリシーの編集：ディスクキャッシュ**
   - **初期化：高速**
   - **初期化：完全**
   - **仮想ディスクの暗号化**

エンクロージャ管理モジュール

エンクロージャ管理モジュール (EMM) は、エンクロージャのデータパスおよびエンクロージャ管理タスクを提供します。EMM は、エンクロージャコンポーネントおよびドライブへのアクセス権の監視と制御を行います。

EMM は、ホストサーバーに対してエンクロージャの属性と状態を通信します。 EMM モジュールは、エンクロージャの次のコンポーネントを監視します。

- ファン
- 電源装置
- 温度プローブ
- 物理ディスクの挿入または取り外し
- エンクロージャ上の LED

EMM のステータスおよび属性を表示する

EMM ステータスには、EMM の正常性が表示されます。EMM には、エンクロージャから固有のステータス値が含まれます。最大 2 つの EMM が許可されます。 エンクロージャファームウェアは、各 EMM のステータスを作成します。

ウェブインタフェースを使用した EMM のステータスおよび属性の表示

EMM のステータスおよび属性を表示するには、次の手順を実行します。

シャーシ概要 → **ストレージ** → **エンクロージャ** → **プロパティ** の順にクリックします。 **エンクロージャページ**には、シャーシのエンクロージャの EMM ステータスおよび属性が表示されます。内蔵エンクロージャまたは外付けエンクロージャを展開して、EMM のステータスおよび属性を表示します。 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 を使用して EMM のステータスおよび属性を表示する

EMM のステータスを表示するには、 `racadm raid get emms -o -p Status` コマンドを使用します。

EMM の属性を表示するには、 `racadm raid get emms -o` コマンドを使用します。

詳細については、**dell.com/support/manuals** にある『*Chassis Management Controller for PowerEdge VRTX 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。

エンクロージャのステータスおよび属性の表示

CMC には、物理コンポーネントに基づいて、エンクロージャの正常性が表示されます。共有ストレージに接続されているエンクロージャのデータが CMC に表示されますが、少数の PCIe カードに接続されている外付けエンクロージャは表示されません。エンクロージャのステータスと属性を表示するには、CMC ログイン権限が必要です。

ウェブインタフェースを使用したエンクロージャのステータスおよび属性の表示

エンクロージャのステータスおよび属性を表示するには、次の手順を実行します。

シャーシ概要 → **ストレージ** → **エンクロージャ** → **プロパティ** をクリックします。**エンクロージャページ** には、シャーシのエンクロージャの正常性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。

メモ: EMM、PSU、ファンが取り外されても、プライマリステータスが変化しない場合には、エンクロージャのロールアップステータスが重要になります。CMC またはシャーシの電源を入れ直すと、プライマリステータスも重要に変わります。

RACADM を使用したエンクロージャのステータスと属性の表示

エンクロージャのステータスを表示するには、`racadm raid get enclosures –o –p Status` コマンドを使用します。

エンクロージャの属性を表示するには、`racadm raid get enclosures –o` コマンドを使用します。

詳細については、**dell.com/support/manuals** にある『*Chassis Management Controller for PowerEdge VRTX 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。

コネクタごとに 2 つまでのエンクロージャをレポートする

各外付け共有 PERC8 カードは、コネクタごとに最大 2 つのエンクロージャをサポートしています。ただし、制限が異なる構成が 2 つあります。1 つの PERC(非フォールトトレラント)構成で、カード 1 枚につき最大 2 台のエンクロージャを接続することができます。冗長ケーブル接続のため、フォールトトレラント外付け PERC 8 カードは、フォールトトレラントペアごとに最大 2 台のエンクロージャをサポートします。

コネクタ上で 3 つ以上のエンクロージャが検出された場合、警告メッセージがシャーシログに記録されます。 これはシャーシの正常性に影響し、アクティブなアラートまたはシャーシログエントリを提供します。

エンクロージャの資産タグと資産名の設定

エンクロージャを識別するには、エンクロージャの資産名と資産タグを設定します。

メモ:

- **無効な値を入力した場合、エラーが表示されます。**
- **最初に、ファームウェアに保存された値が表示されます。**
- **エンクロージャの資産タグと資産名を設定するには、シャーシ設定権限が必要です。**
- **資産タグおよび資産名を設定できるのは、外部エンクロージャのみです。**

ウェブインタフェースを使用したエンクロージャの資産タグと資産名の設定

エンクロージャの資産タグと資産名を設定するには、**シャーシ概要** → **ストレージ** → **エンクロージャ** → **セットアップ**の順にクリックします。 **資産タグ** と **資産名** を適切なフィールドに入力し、 **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。

RACADM を使用したエンクロージャの資産タグと資産名の設定

エンクロージャの資産タグを設定するには、`racadm raid set enclosures: Enclosure.External.0-0:RAID.ChassisSlot.5-1 –p AssetTag <value>` コマンドを使用します。

エンクロージャの資産名を設定するには、`racadm raid set enclosures: Enclosure.External.0-0:RAID.ChassisSlot.5-1 –p AssetName <value>` コマンドを使用します。

詳細については、**dell.com/support/manuals** にある『*Chassis Management Controller for PowerEdge VRTX 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。

エンクロージャの温度プローブステータスと属性の表示

温度プローブステータスには、エンクロージャの温度センサーの状態が表示されます。センサーには、エンクロージャから固有のステータス値を含みます。4 つまでの温度センサーまたはプローブが許可されており、エンクロージャファームウェアが各センサーの状態を作成します。プローブステータスを表示するには、CMC ログイン権限が必要です。

ウェブインタフェースを使用したエンクロージャの温度プローブステータスおよび属性の表示

エンクロージャの温度プローブステータスおよび属性を表示するには、次の手順を実行します。

シャーシ概要 → **ストレージ** → **エンクロージャ** → **プロパティ**の順にクリックします。 **エンクロージャページ**には、シャーシのエンクロージャの温度プローブの正常性状態と属性が表示されます。外付けエンクロージャを展開して、エンクロージャの PSU の状態を表示します。 詳細については、『*CMC オンラインヘルプ*』を表示してください 。

RACADM を使用したエンクロージャの温度プローブ属性の表示

エンクロージャの温度プローブ属性を表示するには、`racadm raid get tempprobes -o` コマンドを使用します。詳細については、**dell.com/cmcmanuals** にある『*Chassis Management Controller for PowerEdge VRTX 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。

エンクロージャの温度警告しきい値の設定

温度警告しきい値では、エンクロージャ温度が警告としてレポートするしきい値を変更することができます。

メモ:

- **無効な値を入力した場合はエラーが表示されます。**
- **最初に、ファームウェア に保存された値が表示されます。**
- **エンクロージャの資産タグと資産名を設定するには、シャーシ設定権限が必要です。**

ウェブインタフェースを使用したエンクロージャの温度警告しきい値の設定

エンクロージャの温度警告しきい値を設定するには、次の手順を実行します。

シャーシ概要 → **ストレージ** → **エンクロージャ** → **セットアップ**の順に選択します。**エンクロージャ** ドロップダウンメニューからエンクロージャを選択し、温度センサー 2 と 3 の警告しきい値の上限と下限の適切な値を入力します。**資産タグ** と **資産名** を適切なフィールドに入力し、**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。

RACADM を使用したエンクロージャ温度警告しきい値の設定

エンクロージャ内の温度プローブの最小警告しきい値を設定するには、 `racadm raid set tempprobes:TempSensor.Embedded.0:Enclosure.External.1-0:RAID.ChassisSlot.6-1 -p MinimumWarningThreshold <value>` コマンドを使用します。

エンクロージャ内の温度プローブの最大警告しきい値を設定するには、 `racadm raid set tempprobes:TempSensor.Embedded.0:Enclosure.External.1-0:RAID.ChassisSlot.6-1 -p MaximumWarningThreshold <value>` コマンドを使用します。

詳細については、**dell.com/support/manuals** にある『*Chassis Management Controller for PowerEdge VRTX 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。

エンクロージャのファンステータスおよび属性を表示する

ファンステータスと属性には、エンクロージャのステータスが表示され、固有のステータス値を含みます。2 つまでのファンが許可されており、エンクロージャファームウェアが各ファンのステータスを作成します。ファンステータスを表示するには、CMC ログイン権限が必要です。

メモ: PSU が欠落している場合は、PSU に対応するファンには重要ステータスが表示されます。

ウェブインタフェースを使用してエンクロージャのファンステータスおよび属性を表示する

PSU のステータスおよび属性を表示するには、次の手順を実行します。

シャーシ概要 → **ストレージ** → **エンクロージャ** → **プロパティ**の順にクリックします。 **エンクロージャページ**には、エンクロージャのファンの正常性状態と属性が表示されます。外付けエンクロージャを展開して、エンクロージャのファンの状態を表示します。詳細については、『*CMC オンラインヘルプ*』を表示してください。

RACADM を使用したエンクロージャのファンステータスおよび属性の表示

ファンのステータスを表示するには、 `racadm raid get fans -o -p Status` コマンドを使用します。

ファンの属性を表示するには、`racadm raid get fans -o` コマンドを使用します。

詳細については、**dell.com/support/manuals** にある『*Chassis Management Controller for PowerEdge VRTX 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エンクロージャプロパティの表示

エンクロージャプロパティを表示するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** > **ストレージ** > **エンクロージャ** > **プロパティ** をクリックします。
2. **プロパティ** ページの **エンクロージャ** セクションで、 をクリックして、物理ディスクドライブとそれらの状態、物理ディスクドライブスロットの概要、および詳細プロパティをグラフィカルに表示します。

16

PCIe スロットの管理

デフォルトでは、すべてのスロットがマップ解除されています。次を実行することができます。

- シャーシ内の全 PCIe スロットの状態の表示。
- サーバーに対する PCIe スロットを割り当ておよび割り当て解除。

PCIe スロットをサーバーに割り当てる前に、次を考慮してください。

- 空の PCIe スロットを電源がオンになっているサーバーに割り当てることはできません。
- サーバーに割り当てられたアダプタがある PCIe スロットは、現在割り当てられているサーバー (ソース) の電源がオンになっている場合、別のサーバーに割り当てることはできません。
- サーバーに割り当てられたアダプタがある PCIe スロットは、電源がオンになっている別のサーバー (ターゲット) に割り当てることはできません。

割り当てられている PCIe スロットをサーバーから削除する前に、以下の点を考慮します。

- PCIe スロットが空の場合、サーバーの電源がオンになっていても、スロットをサーバーから割り当て解除できます。
- PCIe スロットにアダプタがあり、その電源がオンになっていない場合、サーバーの電源がオンになっていてもサーバーから割り当て解除できます。このような状況は、スロットが空で割り当てられているサーバーの電源がオンになっている状態でユーザーが空のスロットにアダプタを挿入すると発生することがあります。

外付け PCI アダプタをブレードに対してマッピングまたはマッピング解除します。

- アダプタは常に非共有デバイスとして電源が入っています。そのため、アダプタは 1 つのサーバーにマッピングされています。
- 外付け PCIE スロットが共有アダプタで占有されている場合、挿入されたアダプタの前のマッピングは変化しません。
- 外付け PCIE スロットが共有アダプタで占有されている場合、PCIE スロットはブレードサーバーに対してマッピングまたはマッピング解除できない可能性があります。ユーザーが共有アダプタに対してマッピングまたはマッピング解除しようとすると、EEMI メッセージがログに記録されます。

サーバーに対する PCIe スロットの割り当ておよび割り当て解除についての詳細は、『オンラインヘルプ』を参照してください。

メモ:

- **ライセンスがない場合は、フルハイトサーバーには最大 4 個の PCIe スロットを割り当てることができ (上部スロットへ 2 個、拡張スロットへ 2 個)、ハーフハイトサーバーでは 2 台の PCIe デバイスを割り当てることができます。**
- **外付け共有 PERC 8 カードデバイスがついた外付け PCIE のプロパティは、専用のデバイスと区別できます。これらの共有デバイスには、専用デバイスとは異なるプロパティがあります。**
- **外付け SPERC の場合は、共有のステータスが表示されます。外付け共有 PERC 8 のマッピングまたはマッピング解除オプションは使用できません。**

トピック :

CMC ウェブインタフェースを使用した PCIe スロットプロパティの表示

- 8 個の PCIe スロットすべてについての情報を表示するには、左ペインで **シャーシ概要** > **PCIe 概要** をクリックします。必要なスロットに対し、 をクリックしてプロパティをすべて表示します。
- 1 個の PCIe スロットについての情報を表示するには、**シャーシ概要** > **PCIe スロット <番号>** > **プロパティ** > **状態**をクリックします。

メモ: ユーザーインタフェースは、専用アダプタで外部 PCIE スロットから取り付けられた SPERC (またはその他の共有) デバイスを含む外部 PCIe スロットを、これらのデバイスが持つ異なるプロパティから判断して区別しています。

CMC ウェブインタフェースを使用したサーバーへの PCIe スロットの割り当て

PCIe スロットをサーバーに割り当てるには、次の手順を実行します。

- 左ペインで、**シャーシ概要** > **PCIe 概要** > **セットアップ** > **マッピング：PCIe スロットからサーバースロット** をクリックします。**マッピング：PCIe スロットからサーバースロット** ページの **処置** 列内にある **処置** ドロップダウンメニューから、適切なサーバー名を選択し、**適用** をクリックします。

次に注意してください。

- ライセンスがないと、ハーフハイトサーバーにマップすることができる PCIe スロットの最大数は 2 個です。フルハイトサーバーが取り付けられている場合、PCIe スロットを上部サーバースロットに 2 個、および下部（拡張）サーバースロットに 2 個と、1 台のフルハイトサーバーにつき 4 個の PCIe スロットをマップすることができます。
- サーバースロットは、8 個の PCIe スロットのうちどのスロットにもマップすることができます。
- フルハイトサーバーでは上部メザニンと下部メザニンの両方が装着済みです。装着済みでない場合は、POST 中、<F 1> または <F 2> がページ上に表示された時にいずれかのキーを押す事ができるように、POST が停止されます。
- フルハイトサーバーの場合、PCIe スロットは上部メザニンへ最大 2 個、下部メザニンへ最大 2 個マップすることができます。デフォルトで、サーバースロット 3 へのすべての PCIe のマッピングは、下部メザニンにマップされます。
- サーバースロット番号は、スロット 01、スロット 02 といった具合に表示されます。フルハイトサーバーの場合、スロット名は、スロット 01 の拡張、スロット 02 の拡張といったように拡張と表示されます。
- ホスト名を選択する場合は、スロット名の代わりにホスト名が表示されます。
- CMC は、システムイベントログ（SEL）、SNMP、および電子メールのインタフェースを介してアラート機能を提供します。

サーバーへの PCIe デバイスの割り当ての詳細については、『オンラインヘルプ』を参照してください。

RACADM を使用した PCIe スロットの管理

RACADM コマンドを使用してサーバーに対する PCIe スロットの割り当て、または割り当て解除を行うことができます。したりすることができます。ここにコマンドの一部を紹介します。RACADM コマンドの詳細については、dell.com/support/Manuals にある『Chassis Management Controller for PowerEdge VRTX 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。

- サーバーに対する PCIe デバイスの現在の割り当てを表示するには、次のコマンドを実行します。

```
racadm getpiecfg -a
```

- FQDD を使用して PCIe デバイスのプロパティを表示するには、次のコマンドを実行します。

```
racadm getpciecfg [-c <FQDD>]
```

たとえば、PCIe デバイス 1 のプロパティを表示するには、次のコマンドを実行します。

```
racadm getpciecfg -c PCIE.ChassisSlot.1
```

- サーバースロットに PCIe アダプタスロットを割り当てるには、次のコマンドを実行します。

```
racadm setpciecfg assign [-c <FQDD>] [i <server slot>]
```

- たとえば、サーバースロット 2 に PCIe スロット 5 を割り当てるには、次のコマンドを実行します。

```
racadm setpciecfg assign -c PCIE.ChassisSlot.5 -i 2
```

- サーバーから PCIe スロット 3 の割り当てを解除するには、次のコマンドを実行します。

```
racadm setpciecfg unassign -c pcie.chassisslot.3
```

PCIe 電源ライドスルー

CMC VRTX 内の新しく割り当てられた PCIe カードは、サーバーノードへの電源投入前に検出および初期化する必要があります。検出および初期化プロセスには次の手順が含まれます。

- 取り付けられたカードの検出とインベントリ
- サーバーモジュールへの公開のための PCIe カードの準備

- サーバー BIOS による設定のための複数のカードの準備
- ブレードノードへの電源投入前の全カードの初期化

これらのプロセスはすべて完了に数秒かかるため、PCIe カードの初期化に遅延を生じます。CMC VRTX の PCIe ライドスルー機能は、このプロセスのサイクル時間を短縮します。PCIe ライドスルー機能は、次を可能にします。

- サーバーノードへの電源投入が迅速化されるため、PCIe カードへの電源投入も迅速化されます。
- 次のシナリオにおいて、PCIe カードの電源オン状態が事前設定された時間分延長されます。
  - 関連するサーバーの電源がオフになった後
  - アダプタ検出プロセスの終了後
- カードの電源オン準備完了状態は、検出プロセス後、事前設定された時間分延長されます。この延長により、一般タイプのパワーサイクルシナリオの遅延を排除することができます。カードは、ノード割り当てと電源投入を待つ準備完了状態のままとなります。カードは設定時間を超えると電源オフになります

。

メモ: 期間終了時、PCIe カードの電源がオフになります。ライドスルーモードのアダプタはすべて、シャーシのドアが開いたときにも常に電源が切れます。

メモ:

- **CMC の電力が不足すると、CMC はライドスルーモードの全アダプタをオフにすることで、これらのアダプタに割り当てられているすべての電力を開放します。電源が復旧されると、PCIe スロットに電力が再度割り当てられます。この電力復元により、カードは遅延なくサーバー割り当ての準備完了状態になります。**
- **共有モードとして電源が入っているすべての外部 PCIE アダプタはライドスループロセスから除外されます。共有デバイスとして共有アダプタの電源がオンになると、シャーシの電源がオフになるまで、電源オン状態のままです。**

CMC ウェブインタフェースを使用した PCIe ライドスループロパティの表示

PCIe ライドスループロパティを表示するには、左側のペインで **シャーシ概要** > **PCIe 概要** をクリックします。**PCIe 状態** ページが表示されます。**一般設定** セクションに次の PCIe ライドスループロパティ状態が表示されます。

- **ライドスルー状態** - 有効または無効
- **ライドスルータイムアウト** - ライドスルー機能が有効化されている時間を示します。

RACADM を使用した PCIe ライドスループロパティ状態の表示

PCIe 電源ライドスループロパティに関する情報を表示するには、次のコマンドを入力します。

```
racadm getpciecfg -r
```

詳細については、『Chassis Management Controller for PowerEdge VRTX 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 PCIe ライドスループロパティの設定

CMC VRTX の PCIe ライドスループロパティを設定するには、次の手順を実行します。

1. 左ペインで **シャーシ概要** > **セットアップ** > **ライドスルー** とクリックします。
   PCIe ライドスルー設定 ページが表示されます。
2. PCIe ライドスルー機能を有効化または無効化するには、**PCIe ライドスルーの有効化** オプションを選択またはクリアします。

   メモ: デフォルトではライドスルー機能が有効化されており、期間は 300 秒に設定されています。

3. **タイムアウト** フィールドに、ライドスルー機能を有効にする時間を入力します。

ゼロ（0）または 60～1800 秒の値を入力します。ゼロは無限のタイムアウトを示します。

4. **適用** をクリックします。

RACADM を使用した PCIe ライドスループロパティ状態の設定

PCIe 電源ライドスループロパティは、次のコマンドを実行することによって設定できます。

- ライドスルー機能を無効にするには、`racadm setpciecfg ridethru-d` コマンドを実行します。
- ライドスルー機能を有効にするには、`racadm setpciecfg ridethru –e` コマンドを実行します。
- ライドスルータイムアウトプロパティをリセットするには、`racadm setpciecfg ridethru-t<timeout>` コマンドを実行します。
- 許容タイムアウト範囲を設定するには、`racadm setpciecfg help ridethru` コマンドを実行します。

詳細については、『Chassis Management Controller for PowerEdge VRTX 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。

17

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モートシステム上でのリカバリ、および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。

メモ: WinRM の Microsoft のサポートは、Windows 10 クライアントでは使用できません。WinRM の代わりに Power Shell を使用してください。

トピック：

システム管理者パスワードを忘れた場合のリセット

管理タスクの実行には、**Administrator** 権限を持つユーザー資格情報が必要です。CMC ソフトウェアにはユーザー アカウントのパスワードを保護するセキュリティ機能があり、管理者アカウントのパスワードを忘れた場合には、これを無効にすることができます。管理者アカウントのパスワードを忘れた場合は、CMC 基板の J_PWORD ジャンパーを使用すると回復できます。

CMC 基板には、次の図に示すように 2 ピンのパスワード リセット コネクターがあります。ジャンパーがリセット コネクターに取り付けられている場合、デフォルトの管理者アカウントとパスワードが有効になり、`username: root` と `password: calvin` のデフォルト値に設定されます。

表 42. CMC パスワードジャンパの設定

ジャンパー コマンド	ジャンパーの画像	ジャンパーの状態	ジャンパー リセット ステータス
J_PWORD		(デフォルト)	パスワードリセット機能は無効です。

表 42. CMC パスワードジャンパの設定（続き）

ジャンパー コマンド	ジャンパーの画像	ジャンパーの状態	ジャンパー リセット ステータス
			パスワードリセット機能は有効です。

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。

J_PWORD 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。

```
username: root
```

```
password: calvin
```

アカウントが削除されたかどうか、またはパスワードが変更されたかどうかに関わらず、管理者アカウントはリセットされます。

メモ: J_PWORD ジャンパが取り付けられると、次のように（設定プロパティ値ではなく）デフォルトのシリアルコンソール設定が使用されます。

```
cfgSerialBaudRate=115200
```

```
cfgSerialConsoleEnable=1
```

```
cfgSerialConsoleQuitKey=^\
```

```
cfgSerialConsoleIdleTimeout=0
```

```
cfgSerialConsoleNoAuth=0
```

```
cfgSerialConsoleCommand=""
```

```
cfgSerialConsoleColumns=0
```

次の手順で、システム管理者パスワードを忘れた場合のリセット方法を説明します。

1. ハンドルの CMC リリース ラッチを押し、モジュールの前面パネルを引きます。CMC モジュールをエンクロージャから引き出します。
   メモ: 静電気放出（ESD）により CMC が損傷するおそれがあります。特定の条件下で、ESD が身体または物体に蓄積され、CMC に放電することがあります。ESD による損傷を防ぐため、シャーシの外側にある CMC を取り扱う際は、身体から放電される静電気に対して予防策を講じてください。
2. ジャンパーを使用して**パスワードのリカバリー** ヘッダー ピンを短絡させます。
3. パスワード リセット コネクターからジャンパー プラグを取り外し、2 ピンのジャンパーを挿入してデフォルトの管理者アカウントを有効にします。CMC 基板上のパスワード ジャンパーの位置は、次の図で確認できます。
4. CMC モジュールをエンクロージャに挿入します。取り外したケーブルを元どおりに取り付けます。
   メモ: 残りの手順が完了するまで、CMC モジュールがアクティブ状態になっていることを確認します。
5. CMC の再起動が完了するまで待ちます。Web インターフェイスのシステム ツリーで、[**シャーシの概要**] に移動し [**電源**] > [**制御**] をクリックして、[**CMC のリセット（ウォーム ブート）**] を選択、[**適用**] をクリックします。
6. デフォルトの管理者ユーザー名「root」とパスワード「calvin」を使用してアクティブな 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。
7. システム管理者パスワードの作成を含む、必要な管理処置を実行します。
8. ハンドルの CMC リリース ラッチを押し、モジュールの前面パネルを引きます。CMC モジュールをエンクロージャから引き出します。
9. **パスワードのリカバリー** ヘッダーから 2 ピン ジャンパーを取り外し、ジャンパー プラグを元に戻します。
10. CMC モジュールをエンクロージャに挿入します。取り外したケーブルを元どおりに取り付けます。手順 4 を繰り返して、ジャンパーのない CMC モジュールをアクティブ CMC にします。

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、『PowerEdge VRTX の 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。

表 43. サブシステム用 racadm コマンド

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	getssninfo
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	getraclog
システムイベントログ	getsel

SNMP Management Information Base ファイルのダウンロード

CMC SNMP Management Information Base (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 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. 左ペインで、**シャーシ概要** > **ネットワーク** > **サービス** > **SNMP** をクリックします。
2. **SNMP 設定** セクションで、**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?

- 電源がオンになっている場合、オペレーティングシステムは機能していますか、無反応ですか、それとも機能が停止していますか?
- 電源がオフになっている場合、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 **グリッド冗長性** 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 2 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 2 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 **グリッド 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。(完全なグリッド冗長性動作のため、4 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、**グリッド冗長性** 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挿入しましたが、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の設定をチェックします。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る場合があります。
  - **解決策 B：** 最大節電の設定をチェックします。これが設定されていると、この問題が発生します。詳細については、電源設定を参照してください。
  - **解決策 C：** 新しく挿入したサーバーと関連付けられているサーバースロットの電力優先順位を確認し、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 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 <数値> 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 <数値> 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 4 台の電源装置での **グリッド冗長性** 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。**グリッド冗長性** ポリシーでは、左側 2 台の電源装置がひとつの AC グリッドに接続され、右側 2 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、PSU 2 と PSU 3 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で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：** 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には、シャーシに少なくとも 3 台の電源装置が装備され、PUS 障害がサーバー動作に影響しないように **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。

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の情報には、ハードウェアログおよびシャーシログを表示することができます。

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
```

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、左ペインで **シャーシ概要** > **ログ** をクリックします。**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 という単語で示されます。日付 / 時刻のエントリは昇順で表示されます。日付 / 時刻 列に <システム起動> が表示される場合は、日付または時刻が利用できない、モジュールの電源オンまたは電源オフ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。

メモ: ハードウェアログをクリアするには、ログのクリア管理者 権限が必要です。

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
```

シャーシログの表示

CMC は、シャーシ関連のイベントのログを生成します。CMC は、システムイベントログ (SEL)、SNMP、および電子メールのインタフェースを介してアラート機能を提供します。

SPERC は、1 つ、または複数の PowerEdge サーバーの電源が入っている間に挿入します。

メモ:

- **シャーシログをクリアするには、ログのクリア管理者 権限が必要です。**

RACADM を使用したシャーシログの表示

RACADM を使用してシャーシ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 chassislog view
```

このコマンドにより、最新のシャーシログエントリが 25 件表示されます。

シャーシログの表示に使用可能なオプションを表示するには、次のコマンドを実行します。

```
racadm chassislog help view
```

ウェブインタフェースを使用したシャーシログの表示

シャーシログを表示、保存、クリアすることができます。ログは、ログタイプとフィルタに基づいて絞り込むことができます。また、キーワードによる検索を実行したり、指定した期間のログを表示したりすることも可能です。

左ペインで、**シャーシ概要** > **ログ** > **シャーシログ** をクリックします。**シャーシログ** 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シャーシ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。

診断コンソールの使用

高度な技術を持つユーザーである、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。

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. 左ペインで、**シャーシ概要** > **トラブルシューティング** > **診断** をクリックします。
   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、『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 CMC のリセット、または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サーバーの仮想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 CMC のリセットで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。

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. 左ペインで、**シャーシ概要** > **トラブルシューティング** > **コンポーネントのリセット** をクリックします。
   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 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 / フェールオーバー** 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。ただし、スタンバイ CMC が存在しない場合は、使用可能な CMC が再起動されます。
3. サーバーを仮想的に再装着するには、**サーバーの仮想的な再装着** セクションで、再装着するサーバーを選択し、**選択の適用** をクリックします。

   詳細については『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

これはライセンスが必要な機能です。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を保存または復元するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** > **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。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場合に限り、後から使用することができます。
2. シャーシ設定を復元するには、「復元」セクションで **参照** 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。**
   - **Flexaddress 情報、サーバープロファイル、および拡張ストレージは、シャーシ設定と一緒に保存または復元されません。**

ネットワークタイムプロトコル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 2~3 分かかる場合があります。2~3 分経過しても変更されない場合は、問題のトラブルシューティングが必要な場合があります。CMC は、次の理由でクロックを同期化できない場合があります。

- ネットワークタイムプロトコル (NTP) サーバー 1、NTP サーバー 2、および NTP サーバー 3 の設定に問題がある。
- 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。

NTP に関連する問題のトラブルシューティングを行うには、CMC トレースログの情報をチェックしてください。このログには NTP に関連する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類似し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
```

このコマンドの出力には、問題のデバッグに有用な詳細な NTP 統計が含まれています。

Windows ベースの NTP サーバーを設定する場合は、ntpd の MaxDist パラメータを増やすと役立つ場合があります。デフォルト設定には大部分の NTP サーバーと連動するために十分大きな設定が必要であるため、このパラメータを変更する前に、変更によるすべての影響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 コマンドの入力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、コンポーネントの次の状態を示します。

- 緑色 LED の点灯は、コンポーネントの電源がオンになっていることを示します。緑色 LED の点滅が示すのは、重大ではあるがルーチン的なイベントの発生で、その間ユニットの動作はできなくなります。これは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、ユーザーによる設定が可能で、識別用に使用されます。設定の詳細については、「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」を参照して下さい。

表 44. 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	ステータス
CMC	緑色、点灯	電源オン
	青色、点灯	ファームウェアのアップロード中 ファームウェアのアップデートは正常
	電源オフ	ファームウェアのアップデートが進行中
	緑色、消灯	電源オフ
	青色、点灯	アクティブ

表 44. LED の色と点滅パターン（続き）

コンポーネント	LED の色、点滅パターン	ステータス
	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
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
送風装置	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
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

表 44. LED の色と点滅パターン（続き）

コンポーネント	LED の色、点滅パターン	ステータス
	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
エンクロージャ	青	ホストサーバーがエンクロージャを識別している場合
	橙色	オンになっているかリセット、障害状態

無応答 CMC のトラブルシューティング

いずれのインターフェイス（Web インターフェイス、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

カードの左側には LED が 2 個あります。

- 左上の LED - 電源状態を示します。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。
- 左下の LED - この 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。アクティブ CMC では青色の LED が点灯します。冗長の 2 つの CMC 構成の場合は、スタンバイ CMC で右上の緑色の LED だけが点灯されます。

ネットワーク問題のトラブルシューティング

内蔵 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。『*Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド*』の「`gettracelog`」コマンド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 の内蔵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。

コントローラのトラブルシューティング

コントローラをトラブルシューティングするには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** > **ストレージ** > **コントローラ** > **トラブルシューティング**をクリックします。
2. **コントローラトラブルシューティング** ページで、各コントローラに対応する **処置** ドロップダウンリストから次のいずれかを選択し、**適用** をクリックします。
   - **設定のリセット** - 仮想ディスクとホットスペアを削除します。ただし、ディスク上のデータは消去されません。

     メモ: PERC 構成のリセットは、PERC コントローラの固定キャッシュがある場合はそれを破棄します。
   - **TTY ログのエクスポート** - ストレージコントローラからの TTY デバッグログがローカルシステムにエクスポートされます。
   - **固定キャッシュの破棄** - RAID コントローラキャッシュに保存されているデータを削除します。

     メモ: 固定キャッシュが存在する場合、それをクリアするオプションが存在します。固定キャッシュが存在しない場合は、このオプションは表示されません。
   - **RAID コントローラを無効にする** — ピアコントローラを無効にします。このオプションは、共有 PERC 8 (内蔵 2) と外付け共有 PERC 8 のドロップダウンメニューにのみあります。
   - **RAID コントローラを有効にする** — ピアコントローラを有効にします。**RAID コントローラを有効にする** オプションはドロップダウンメニューに表示されます。

     メモ:

     無効化された PERC については、その他オプション (設定のリセット、TTY ログのエクスポート、固定キャッシュの破棄、RAID コントローラの無効化) のいずれもドロップダウンメニューで利用できません。
   - **フォールトトレランスを有効にする** — 外付け共有 PERC 8 カードのフォールトトレランスモードを有効にします。
   - **フォールトトレランスを無効にする** — 外付け共有 PERC 8 カードのフォールトトレランスモードを無効にします。

     メモ: フォールトトレランスを有効にする と フォールトトレランスを無効にする は、外付け共有 PERC 8 カードについてのみ表示されます。 外付け共有 PERC 8 カードのデフォルトモードは、非フォールトトレラントモードです。

メモ:

- **ブレードに電源が入っている状態では、エラーメッセージが表示されます。**
- **ブレードの電源が入っている状態では、このコマンドは失敗します。**

フォールトトレラントのシャーシにおけるエンクロージャのホットプラグ

1. スロット 5 と 6 のシャーシがフォールトトレラントではないことを確認します。
2. エンクロージャを切断します。
3. スロット 5 と 6 の状態をフォールトトレラントモードに変更します。
4. エンクロージャのケーブルをフォールトトレラントとなるように再接続します。

エンクロージャの切断後、エンクロージャの再接続前に、シャーシの電源を循環させます。シャーシの電源が循環されるまでドライブが以前の SCSI-3 予約を保持しているためです。

18

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。

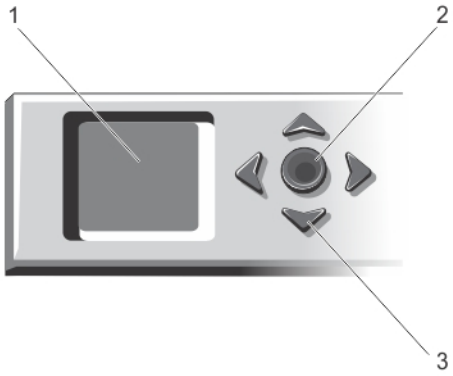


図 4. LCD ディスプレイ

1. LCD 画面
2. 選択（「チェック」）ボタン
3. スクロールボタン（4）

トピック：

- LCD のナビゲーション
- 診断
- 前面パネル LCD 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（次に進む）と左（前に戻る）の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、右の矢印ボタンで、選択したメニュー項目や画面上のアイコンを変更できます。選択した項目は、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 45. 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。

表 45. LCD パネルのナビゲーション用アイコン（続き）

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
		**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。
		**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。

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。

- **KVM マッピング** - サーバーに対して KVM をマッピングまたはマッピング解除するオプションがあります。
- **DVD マッピング** - このオプションは、DVD ドライブがインストールされている場合のみ **メインメニュー** に表示されます。
- **エンクロージャ** - シャーシの状態情報を表示します。
- **IP サマリ** - CMC IPv4、CMC IPv6、iDRAC IPv4、および iDRAC 4 IPv6 の情報を表示します。
- **設定** - **LCD 言語**、**シャーシの向き**、**デフォルト LCD 画面**、および **ネットワーク設定** などのオプションがあります。

KVM マッピングメニュー

このページを使用することにより、KVM からサーバーへのマッピング情報の表示、KVM への別のサーバーのマップ、または既存の接続のマッピング解除を行うことができます。サーバー用に KVM を使用するには、メインメニューから **KVM マッピング** を選択し、適切なサーバーに移動して、中央の **チェック** ボタンを押します。

DVD マッピング

このページを使用することにより、DVD からサーバーへのマッピング情報の表示、別のサーバーのシャーシ上 DVD ドライブへのマップ、または既存の接続のマッピング解除を行うことができます。サーバーが DVD にアクセスできるようにするには、メインメニューから **DVD マッピング** を選択し、必要なサーバーまで移動して、中央の **チェック** ボタンを押します。

DVD ドライブをサーバースロットにマップできるのは、そのサーバースロットに対して DVD が有効になっている場合のみです。DVD ドライブは、いずれのサーバースロットからも使用されないように、マッピングを解除することもできます。DVD ドライブとメイン基板との間で SATA ケーブルが正しく接続されていないと、DVD ドライブの正常性が重要状態になります。DVD ドライブの正常性が重要状態の場合、サーバーは DVD ドライブにアクセスできません。

メモ: DVD マッピング機能は、DVD ドライブが取り付けられている場合にのみ、LCD の メインメニュー 画面に表示されます。

エンクロージャメニュー

この画面から、次の画面に移動できます。

- **前面状態**
- **背面状態**
- **側面状態**
- **エンクロージャ状態**

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。

IP 概要メニュー

IP 概要 画面には、CMC (IPv4 および IPv6) と、シャーシに取り付けられている各サーバーの 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。

設定

設定 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。

- **LCD 言語** - 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。
- **シャーシの向き** - シャーシの取り付け方向に基づいて、**タワーモード** か **ラックモード** を選択します。
- **デフォルト LCD 画面** - LCD パネルにアクティビティがない場合に表示される画面 (**メインメニュー**、**前面状態**、**背面状態**、**側面状態**、または **カスタム**) を選択します。
- **ネットワーク設定** - これを選択して CMC のネットワーク設定を行います。この機能の詳細については、「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」を参照してください。

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** 画面に戻る場合は **戻る** アイコンをハイライト表示します。

選択をアクティブにするには、中央のボタンを押します。

LCD 言語

LCD 言語 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. 中央ボタンを押します。**確定** アイコンがハイライト表示されます。
3. 中央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**
- **前面状態** (シャーシの前面図)
- **背面状態** (シャーシの背面図)
- **側面状態** (シャーシの左側面図)
- **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が水色でハイライト表示されます。

1. 上下の矢印キーを使って、デフォルトに設定する画面をハイライト表示します。
2. 中央ボタンを押します。**確定** アイコンがハイライト表示されます。
3. 中央ボタンを再度押して変更を確定します。**デフォルト画面** が表示されます。

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。シャーシやサーバーあるいはシャーシ内の他の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** では、背景が橙色のアイコンがメニューアイテム (エンクロージャ) の横に表示され、正面、背面、側面あるいはエンクロージャーのステータスを指します。

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。

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 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 46. CMC の状態

アイテム	説明
名前 / 場所	例： CMC1、CMC2
エラーなし	エラーがない場合は「エラーなし」と表示されます。エラーがある場合は、重大なエラー メッセージが最初に表示され、続いて警告関連のメッセージが表示されます。
ファームウェアバージョン	アクティブ CMC にのみ表示されます。スタンバイ CMC にはスタンバイが表示されます。
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。
MAC: <アドレス>	CMC の MAC アドレスが表示されます。

表 47. シャーシまたはエンクロージャ状態

アイテム	説明
ユーザー定義名	例：「Dell ラック システム」。CMC CLI または Web インターフェイスで設定できます。
エラーメッセージ	エラーがない場合は「エラーなし」と表示されます。エラーがある場合は、重大なエラー メッセージが最初に表示され、続いて警告関連のメッセージが表示されます。
モデル番号	例：「PowerEdgeM1000」。
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、グリッド冗長、または DC 冗長

表 48. ファン状態

アイテム	説明
名前 / 場所	例：ファン 1、ファン 2 など。

表 48. ファン状態（続き）

アイテム	説明
エラーメッセージ	エラーがない場合は「エラーなし」と表示されます。エラーがある場合は、重大なエラー メッセージが最初に表示され、続いて警告関連のメッセージが表示されます。
RPM	現在のファン速度（RPM）です。

表 49. PSU 状態

アイテム	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「エラーなし」と表示されます。エラーがある場合は、重大なエラー メッセージが最初に表示され、続いて警告関連のメッセージが表示されます。
ステータス	オフライン、オンライン、またはスタンバイ - PSU の電源状態を示します。
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 50. IOM 状態

アイテム	説明
名前 / 場所	IOM A
エラーメッセージ	エラーがない場合は「エラーなし」と表示されます。エラーがある場合は、重大なエラー メッセージが最初に表示され、続いて警告関連のメッセージが表示されます。
ステータス	オフまたはオン - IOM が機能しているかどうかを示します。
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 タイプの 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 51. KVM マッピングの状態

アイテム	説明
サーバー <番号 >	KVM をマップすることができるサーバーのリストが表示されます。
エラーメッセージ	エラーがない場合は「エラーなし」と表示されます。エラーがある場合は、重大なエラー メッセージが最初に表示され、続いて警告関連のメッセージが表示されます。
マップ済み	KVM にマップされているサーバーのリストが表示されます（存在する場合）。
スロット <番号>	KVM がマップされているサーバースロットを示します。表示形式は、SLOT-<*01 to 04*>になります。
マップされていない	KVM がどのサーバーにもマップされていない場合に表示されます。

表 52. DVD マッピングの状態

アイテム	説明
サーバー <番号 >	DVD をマップすることができるサーバーのリストが表示されます。
エラーメッセージ	エラーがない場合は「エラーなし」と表示されます。エラーがある場合は、重大なエラー メッセージが最初に表示され、続いて警告関連のメッセージが表示されます。
マップ済み	DVD にマップされているサーバーのリストが表示されます（存在する場合）。
スロット <番号>	DVD のマップ先のサーバー スロットを示します。表示形式は、SLOT-<*01 to 04*>になります。
マップされていない	KVM がどのサーバーにもマップされていない場合に表示されます。

表 53. 送風装置の状態

アイテム	説明
名前 / 場所	例：送風装置 1、送風装置 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」と表示されます。エラーがある場合は、重大なエラー メッセージが最初に表示され、続いて警告関連のメッセージが表示されます。
RPM	現在の送風装置速度（RPM）

表 54. SPERC の状態

アイテム	説明
SPERC：< 番号 >	SPERC 名を SPERC n の形式で表示します（n は SPERC 番号）。例：SPERC 1、SPERC 2 などです。
エラーメッセージ	エラーがない場合は「エラーなし」と表示されます。エラーがある場合は、重大なエラー メッセージが最初に表示され、続いて警告関連のメッセージが表示されます。
稼働状態	オフまたはオン - SPERC が機能しているかどうかを示します。
名前：< 名前 >	共有 PERC の名前です。例：SPERC
正常性状態	OK
ファームウェアバージョン	SPERC バージョン
製造元	製造元の名前
状態	オフライン、オンライン、またはスタンバイ - SPERC の電源状態を示します。

表 55. PCIe カードの状態

アイテム	説明
PCIe カード <*番号*>	PCIe カード名を PCIe Card <*n*>の形式で表示します（n は PCIe カード番号）。例：PCIe Card 1、PCIe Card 2 などです。
エラーメッセージ	エラーがない場合は「エラーなし」と表示されます。エラーがある場合は、重大なエラー メッセージが最初に表示され、続いて警告関連のメッセージが表示されます。
稼働状態	オフまたはオン - PCIe カードが機能しているかどうかを示します。
名前：< 名前 >	PCIe カードの名前です。
サーバーにマップ済み	マップ済み、またはマップされていません。

表 56. ハードディスクドライブの状態

アイテム	説明
ハードディスクドライブ：< 番号 >	ハード ディスク ドライブ名を Hard Disk Drive <*n*>の形式で表示します（n はハード ディスク ドライブ番号）。例：Hard Disk Drive 1、Hard Disk Drive 2 などです。
エラーメッセージ	エラーがない場合は「エラーなし」と表示されます。エラーがある場合は、重大なエラー メッセージが最初に表示され、続いて警告関連のメッセージが表示されます。
電源状態	スピンアップ、移行、またはスピンダウン - ハードディスクドライブの電源状態を示します。
製造元	製造元の名前
容量	ハードディスクドライブの使用可能なストレージ容量（GB）

表 56. ハードディスクドライブの状態（続き）

アイテム	説明
ファームウェアバージョン	ハードディスクドライブのファームウェアバージョン
状態	オフライン、オンライン、またはスタンバイ - ハードディスクドライブの電源状態を示します。

表 57. サーバー状態

アイテム	説明
名前 / 場所	例：サーバー 1、サーバー 2 など。
エラーなし	エラーがない場合は「エラーなし」と表示されます。エラーがある場合は、重大なエラー メッセージが最初に表示され、続いて警告関連のメッセージが表示されます。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。例：SLOT-01 **メモ: この表は、CMC CLI または CMC Web インターフェイスを介して設定できます。**
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。
iDRAC DNS 名	iDRAC サーバの DNS 名を表示します。
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 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 をサポートしている場合にのみ表示されます。現在の IPv6 対応状態を表示します。
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	この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）。
自動検出ステータス	サーバーの自動検出のステータスを表示します。

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 の起動が完了した場合にのみ表示されます。この機能の詳細については、『*PowerEdge VRTX の 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。

19

よくあるお問い合わせ（FAQ）

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
- リモートシステムの管理と復元
- Active Directory
- FlexAddress と FlexAddressPlus
- IOM

トピック：

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)
```

このメッセージは何を意味しますか?

別のコマンドは、CMC がリセットを完了した後でのみ、発行される必要があります。

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 - `ERROR: <message>` といった構文、入力ミス、名前の誤りなどの問題です。

  RACADM `help` サブコマンドを使用して、正しい構文と使用方法を表示します。たとえば、シャーシログのクリアでエラーが発生した場合は、次のサブコマンドを実行します。

  ```
  racadm chassislog help clear
  ```

- CMC 関連のエラーメッセージ - CMC が処置を行うことができない問題です。次のエラーメッセージが表示されます。

  ```
  racadm command failed.
  ```

シャーシに関する情報を表示するには、次のコマンドを入力します。

```
racadm gettracelog
```

ファームウェア 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。

$ プロンプトに戻るには、<Ctrl>–d を入力します。

`$ logout` および `$ quit` コマンドの使用中に、`Not Found` というエラーメッセージが表示されます。

リモートシステムの管理と復元

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 ウェブサーバーのリセット後は、リモート RACADM サービスとウェ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 1 分ほどかかる場合があります。

CMC ウェブサーバーは次の状況が発生するとリセットされます。

- CMC ウェブユーザー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 ファイル) 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。

使用している DNS サーバーが 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。

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。

CMC ウェブインタフェースへのアクセス時に、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る。

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にデフォルトの CMC サーバー証明書が含まれています。この証明書が使用されると、デフォルト証明書が CMC のホスト名 (たとえば IP アドレス) に一致しない場合、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. 左ペインで、**シャーシ概要** をクリックします。
2. **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 に CMC を登録** オプションを選択します。
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。

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 証明書サービスが使用された場合、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 コマンドを実行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 ?

- 元の機能カードが対象のシャーシまたは別のシャーシ上のアクティブな CMC にある場合は、ウェブインタフェースには次のエラーメッセージが表示されます。
  - `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`

この場合元の機能カードは、デルサービスに依頼して元のシャーシサービスタグを別のシャーシに移入するよう再プログラムした上で、元の機能カードを搭載した CMC をそのシャーシ上で有効にする以外は、そのシャーシでも他のシャーシでも無効化できません。

- 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?

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オフにする必要があります。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。

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。ブラウザからログオフし、再起動してください。

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 を実行する前には、シャーシの電源をオフにす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。

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上にないアドレスに設定。