Dell Chassis Management Controller Version 2.21 for PowerEdge FX2 and FX2s

ユーザーズガイド

December 2019
Rev. A00

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 EMC PowerEdge FX2/FX2s 向け Dell Chassis Management Controller（CMC）は、**PowerEdge FX2/FX2s** 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 管理者は以下が可能です。

- インベントリの表示。
- 設定および監視タスクの実行。
- 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に対するアラートの有効化。
- PCIe のマッピング情報を表示し、PCIe スロットを再割り当てします。
- シャーシ内の iDRAC と I/O モジュールへの 1 対多の管理インタフェースの提供。

CMC は、サーバに対し、複数のシステム管理機能を提供します。電源および温度の管理は CMC の基本的な機能です。その機能は次のとおりです。

- 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冷却ファンの機能性を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を提供し、ステータスまたはエラーを報告します。
- 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 FX2/FX2s 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との間の 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。
  - PCIe スロット。

温度、ハードウェアの誤った構成、停電、およびファン速度などの警告やエラーについて、電子メールアラートまたは SNMP トラップアラートを送信するように CMC を設定することができます。

メモ: 本書では「ストレージスレッド」および「ストレージモジュール」が同じ意味で使用されています。

トピック：

- Dell EMC サポートサイトからのドキュメントへのアクセス

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。

本リリースの新機能

Dell EMC PowerEdge FX2/FX2s 向け CMC の本リリースは次の機能をサポートしています。

- 米国カリフォルニア州の「SB-327」規制に準拠するための、強制的なパスワード変更の有効化。
- CLI コマンドを使用した、SSH 自己署名キーの再生成。
- OpenSSH オープンソース パッケージのバージョン 7.9p1 へのアップデート。
- OpenSSH オープンソース パッケージのバージョン 1.0.2r へのアップデート。

管理機能

CMC は次の管理機能を提供します。

- 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。
- SNMP、ウェブインタフェース、KVM、内蔵 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、ストレージスレッド、およびシャーシインフラストラクチャ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。
- マルチノードスレッドの導入。PowerEdge FM120x4 はマルチノードスレッドです。
- シャーシ電力制限の監視。
- 拡張 WWN/MAC アドレスインベントリに対する iDRAC IO アイデンティティ機能のサポート。
- FlexAddress 機能 — 特定のスロットに対して、工場で割り当てられたワールドワイドネーム / メディアアクセスコントロール (WWN/MAC) ID のシャーシに割り当てられた WWN/MAC ID への置き換え
- シャーシのコンポーネントステータスおよび状態のグラフィック表示。
- 単一およびマルチスロットサーバーのサポート。
- 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。
- 最大 19 台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。

  メモ: マルチシャーシ管理は IPv6 ネットワークではサポートされていません。
- FX2s シャーシ内のストレージスレッドを管理するためのローカルおよびリモート iDRAC RACADM プロキシ機能。

セキュリティ機能

CMC は次のセキュリティ機能を提供しています。

- パスワードレベルのセキュリティ管理 — リモートシステムへの無許可のアクセスを防止。

- 次による一元ユーザー認証：
  - 標準スキーマまたは拡張スキーマ（オプション）を使用する Active Directory。
  - ハードウェアに保存されたユーザー ID とパスワード。
- 役割ベースの権限 — システム管理者が各ユーザーに特定の権限を設定可能。
- ウェブインタフェースを介したユーザー 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。
- CMC 署名済みイメージ — デジタル署名によって、検知されていない変更からファームウェアイメージを保護するために使用されます。

シャーシの概要

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。

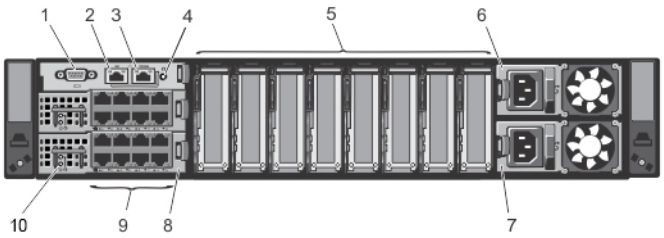


図 1. シャーシの背面パネル

表 1. シャーシ背面パネル - コンポーネント

アイテム	インジケータ、ボタン、またはコネクタ
1	シリアルコネクタ
2	イーサネットコネクタ Gb1
3	イーサネットコネクタ STK/Gb2（スタック）
4	システム識別ボタン
5	ロープロファイル PCIe 拡張スロット
6	電源ユニット（PSU1）
7	電源ユニット（PSU2）
8	I/O モジュール（2）
9	I/O モジュールポート
10	I/O モジュールインジケータ

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。

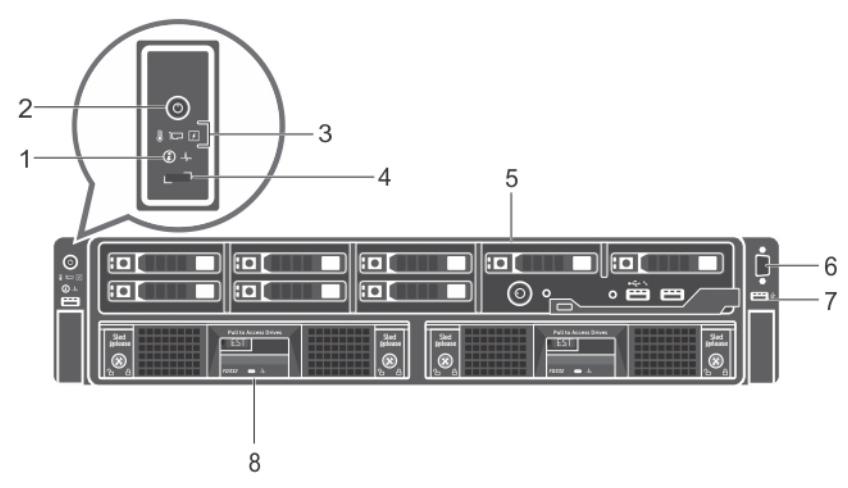


図 2. シャーシの前面パネル

表 2. シャーシの前面パネル - コンポーネント

アイテム	インジケータ、ボタン、またはコネクタ
1	システム識別ボタン
2	エンクロージャ電源インジケータ、電源ボタン
3	診断インジケータ
4	KVM 選択ボタン
5	コンピュートスレッド
6	ビデオコネクタ
7	USB コネクタ
8	ストレージスレッド

対応リモートアクセス接続

次の表では、対応リモートアクセス接続をリストします。

表 3. 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。CMC には、次の 2 つの RJ-45 Ethernet ポートがあります。 ○ Gb1（アップリンクポート） ○ Gb2（スタッキングまたはケーブル統合ポート）。STK/Gb ポートは、CMC NIC のフェールオーバー用にも使用できます。 **メモ:** NIC フェールオーバーを実装するには、CMC 設定がデフォルトの **スタッキング** から **冗長** に変更されているようにしてください。 **注意: NIC のフェールオーバーを実装するために CMC の設定がデフォルトのスタッキングから冗長に変更されていない場合に、STK/Gb2 ポートを管理ネットワークに接続すると、予想できない結果になります。デフォルトのスタッキングモードで Gb1 ポートと STK/Gb2 ポートを同じネットワーク（ブロードキャストドメイン）に接続すると、ブロードキャストストームが生じる可能性があります。また、CMC 設定が冗長モードに変更されていても、シャーシ間が**

表 3. 対応リモートアクセス接続（続き）

接続	機能
	スタッキングモードでデイジーチェーン接続されている場合に、ブロードキャストストームが発生する可能性があります。ケーブル配線モデルが、意図した用途の CMC 設定と一致しているようにしてください。 • DHCP サポート。 • SNMP トラップおよび E-メールイベント通知。 • iDRAC および I/O モジュール（IOM）用のネットワークインタフェース。 • システム起動、リセット、電源投入、シャットダウンコマンドを含む Telnet/SSH コマンドコンソールおよび RACADM CLI コマンドのサポート。
シリアルポート	• システム起動、リセット、電源投入、シャットダウンコマンドを含む シリアルコンソールおよび RACADM CLI コマンドのサポート。 • 特定タイプの IOM へのバイナリプロトコルによる通信を行うために特別に設計されたアプリケーション用バイナリ交換のサポート。 • シリアルポートは、connect（または racadm connect）コマンドを使ってサーバーのシリアルコンソールまたは I/O モジュールに内部的に接続可能。

対応プラットフォーム

CMC は、**PowerEdge FX2** および **FX2s** シャーシ モデルをサポートしています。サポートされているプラットフォームは、PowerEdge FC430、PowerEdge FC630、PowerEdge FM120x4、PowerEdge FC830、PowerEdge FC640、PowerEdge FD332 です。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/cmcmanuals** にある『*Dell Chassis Management Controller（CMC）Version 2.0 for Dell PowerEdge FX2/FX2s リリース ノート*』を参照してください。

対応 Web ブラウザー

対応 Web ブラウザーの最新情報については、**dell.com/cmcmanuals** にある『*Dell Chassis Management Controller（CMC）for Dell PowerEdge FX2/FX2s バージョン 2.21 リリース ノート*』を参照してください。

- 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+
```

対応ファームウェアバージョン

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

表 4. BIOS、iDRAC、および Lifecycle Controller 用の最新ファームウェアバージョン

サーバー	BIOS	iDRAC	Lifecycle Controller
PowerEdge FC830	2.7.1	2.52.52.52	2.52.52.52
PowerEdge FC630	2.7.1	2.52.52.52	2.52.52.52
PowerEdge FC430	2.7.1	2.52.52.52	2.52.52.52
PowerEdge FM120	1.70	2.52.52.52	2.52.52.52
PowerEdge FC640	1.37	3.18.18.18	3.18.18.18

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

次の表は、CMC PowerEdge FX2/FX2s ファームウェアのバージョンが 2.0 から 2.1 にアップデートされる一方で、サーバコンポーネントが次のバージョンにアップデートされない場合に、サポートされるサーバコンポーネントのファームウェアバージョンのリストです。

表 5. 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）
FD332	SAS RAID FW	25.2.2-0004	25.4.0.0015
FC430	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
FC630	iDRAC	2.52.52.52	2.52.52.52
	Lifecycle Controller	2.52.52.52	2.52.52.52
	診断	4239.44	4239A36
	BIOS	2.6.0	2.7.1
FC830	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
FM120x4	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle Controller	2.52.52.52	2.60.60.60
	診断	4231A0	4247A1
	BIOS	1.6.0	1.7.0
FC640	iDRAC	3.15.15.15	3.21.21.21

表 5. 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（続き）

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）
	Lifecycle Controller	3.15.15.15	3.21.21.21
	診断	4301A13	4301A13
	BIOS	1.3.7	1.4.8

サポートされるネットワークアダプタ

以下の表には、PowerEdge FX2/FX2s でサポートされるネットワークアダプタがリストされています。

表 6. PowerEdge FX2/FX2s でサポートされるネットワークアダプタ

	プラットフォーム			
モデル	FC430	FC630	FC830	FC640
5718 DP 1G	有	有	無	有
57810S 10G SFP+	無	有	無	有
57810S 10G BASE-T	無	有	無	有
5719 QP 1G	有	有	有	有
5720 DP 1G	有	無	無	有
57416 DP 10G	無	無	無	有
57414 DP 25G	無	無	無	有
57412 DP 10G	無	無	無	有
BCOM QP 1G	有	有	有	有
LightPulse LPE12002 FC8 HBA	有	有	有	有
LightPulse LPe15002B-M8–D DP 8G Gen 5	有	有	有	有
LPe16002 デュアルポート FC 16 HBA	有	有	有	有
LightPulse LPE12000 FC 8 HBA	無	有	有	有
LightPulse LPe 15000B-M8–D SP 8G Gen 5	無	有	有	有
LPE 16000 シングルポート FC 16 HBA	無	有	有	有
LPE 31K0 FC16 1P	無	有	有	有
LPE32002 FC32 2P	無	有	有	有
LPE31K2 FC16 2P	有	有	有	有
LPE 32000 FC32 1P	無	有	有	有
OCe 14102–UX-D 10GbE CNA	無	無	無	無
OCe 14102–U1–D 10GbE CNA	有	有	有	有
OCe 14102–U1–D 10GbE CNA	有	有	有	有
X540 DP 10G BASE-T	有	有	有	有
i350 DP 1G	有	有	有	有
i350 QP 1G	有	有	有	有

表 6. PowerEdge FX2/FX2s でサポートされるネットワークアダプタ（続き）

	プラットフォーム			
モデル	**FC430**	**FC630**	**FC830**	**FC640**
X520 DP 10G SFP+	無	有	無	有
X710 DP 10GBE SFP+ (Fortville)	有	有	有	有
CX3 DP 40GbE QSFP+	有	有	有	有
CX3 DP 10GbE DA/SFP+	有	有	有	有
CX3 MCX354–A-FCBT	無	無	無	無
QLE2560 FC8 シングル HBA	無	有	有	有
578 10S 10G BASE-T	有	有	有	有
QLE2660 SP FC 16 HBA	無	有	有	有
QLE2662 DP FC16 HBA	有	有	有	有
QLG SFP DP 10G	無	無	無	有
QLG BT DP 10G	無	無	無	有
QLE2560 FC 8 HBA	無	有	有	有
QLG SFP DP 25G	無	無	無	有
QLE2562 FC8 HBA	有	有	有	有
QLE2690 FC16 SP HBA	無	有	有	有
QLE2742 FC32 SFP+ HBA	無	有	有	有
QLE2740 FC32 SP HBA	無	有	有	有
QLE2692 FC16 DP HBA	有	有	有	有
PCIE SF852P DP 10G	有	有	有	有
INTEL OPA x16 LP	無	無	有	有

ライセンスの管理

使用可能な CMC 機能は、購入したライセンス（CMC Express または CMC Enterprise）に応じて異なります。CMC を設定または使用できるインターフェイスでは、ライセンス機能のみを使用できます。たとえば、CMC Web インターフェイス、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 Web インターフェイスおよび RACADM を介して使用できます。

ストレージスレッドのライセンス

CMC での RAID コントローラーの管理用に、ストレージ スレッド ライセンスを購入することもできます。ストレージ スレッド ライセンスは、工場出荷時にインストールすることも、オンラインで購入することも可能です。サポート対象のストレージ スレッド ライセンスのタイプは次のとおりです。

- RAID コントローラー 1 台と HBA コントローラー 1 台（RAID/HBA）
- 両方の RAID コントローラ

ストレージ スレッドのライセンスは、1 台または 2 台の RAID コントローラーに対して使用できます。ライセンスが単一のコントローラー上の RAID に割り当てられた場合、ライセンスは最初のコントローラーにのみ適用されます。ストレージ スレッドのライセンスを削除すると、RAID データが失われる可能性があります。

ストレージ スレッドのライセンスはストレージ スレッドに固有のもので、ストレージ スレッドのサービス タグに関連付けられます。たとえば、シャーシ間でストレージ スレッドを移動した場合、ライセンスもストレージ スレッドと一緒に移動されます。ストレージ スレッド ライセンスのマスター コピーは、永続ストアに格納されます。詳細については、**dell.com/support/manuals** にあ

る『*Dell Chassis Management Controller for PowerEdge FX2/FX2s 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。

ストレージスレッドライセンスのアクティビティのすべてのログメッセージは、CMC ログファイルに保存されます。

メモ: FD33xS および FD33xD RAID コントローラを HBA モードから RAID モードに変更するには、ストレージスレッドライセンスが必要です。

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。このライセンスはストレージスレッドには適用できません。
- 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。

メモ: 評価およびサイトライセンスは CMC にのみ適用されます。

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いてください。詳細については、「ライセンスの取得」の項、および **dell.com/support** 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 — CMC とストレージスレッドの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ーフェイスを使用して 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。

  ストレージ スレッドの電源がオフのときに、シャーシにインストールされているライセンスを、ストレージ スレッドにインポートすることも可能です。ストレージ スレッドのライセンスをすでに取得済みの場合、新しいライセンスをインポートする前に、既存のライセンスを削除します。インポートされたライセンスは CMC License Manager とストレージ スレッド永続ストアに保存されます。ライセンスされた機能は、ホスト サーバーの再起動時に RAID がリセットされた場合にのみ使用できます。ストレージ スレッドのライセンスは、ターゲット デバイスにのみインポートすることができます。

- 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次のとおりです。
  `<EntitlementID>.xml`
- 削除 — コンポーネントまたはストレージ スレッドが欠落している場合に、そのコンポーネントまたはストレージ スレッド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、製品の基本機能が有効になります。

  ストレージ スレッドのライセンス削除は、ストレージ スレッドの電源がオフの場合にのみ行えます。削除したライセンスは、ストレージ スレッド永続ストアおよび License Manager から削除されます。

- 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。

ストレージ スレッドの場合、新しいライセンスによって、CMC License Manager とストレージ スレッド永続ストアの既存のライセンスは上書きされます。ライセンスを置き換える前に、ストレージ スレッドの電源を切ってください。ライセンスされた機能が使用可能となるのは、次回のホスト再起動時に RAID コントローラーがリセットされた後のみです。

- 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、更新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換できます。詳細については、**WWW.DELL.COM/SUPPORT/LICENSING/US/EN/19** にあるデルのソフトウェア ライセンス管理ポータルを参照してください。
- 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: 詳細オプションで正しいページが表示されるようにするため、セキュリティ設定の信頼済みサイトのリストには ***.dell.com** を追加す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。

  メモ: PowerEdge FM120x4 のライセンスを、PowerEdge FC630 にインストールしようとすると、ライセンスのインストールに失敗します。ライセンス付与の詳細については、『*Integrated Dell Remote Access Controller (iDRAC) ユーザーズ 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 7. ライセンスタイプに基づいている CMC の機能

機能	Express	Enterprise
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
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
CMC 設定バックアップ	無	有
CMC 設定復元	有	有
リモート Syslog	無	有
ディレクトリサービス	無	有
シングルサインオンサポート	無	有
2 要素認証	無	有
PK 認証	無	有
リモートファイル共有	無	有
エンクロージャレベルの電力制限	無	有

表 7. ライセンスタイプに基づいている CMC の機能（続き）

機能	Express	Enterprise
Multi-chassis management(マルチシャーシ管理)	無	有
FlexAddress の有効化	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

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 8. 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のローカライズバージョンの表示

CMC ウェブインタフェースのローカライズバージョンを表示するには、ウェブブラウザのマニュアルをお読みください。ローカライズバージョンを表示するには、ブラウザを希望の言語に設定します。

対応管理コンソールアプリケーション

CMC は、Dell OpenManage Console との統合をサポートします。詳細については、**dell.com/support/manuals** で入手できる OpenManage Console 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 FX2/FX2s 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『*Dell Chassis Management Controller for PowerEdge FX2/FX2s 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

デル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以外にも、**dell.com/support/manuals** から次のガイドにアクセスできます。

- 『*CMC FX2/FX2s Online Help*』(CMC FX2/FX2s オンラインヘルプ) では、ウェブインタフェースの使用方法について説明しています。このオンラインヘルプにアクセスするには、CMC ウェブインタフェースで **Help (ヘルプ)** をクリックしてください。
- 『*Chassis Management Controller Version 2.0 for Dell PowerEdge FX2/FX2s RACADM Command Line Reference Guide*』(Dell PowerEdge FX2/FX2s 向け Chassis Management Controller バージョン 2.0 RACADM コマンドラインリファレンスガイド) には、FX2/FX2s 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** にある『*Dell Chassis Management Controller (CMC) for Dell PowerEdge FX2/FX2s Version 2.0 Release Notes*』(Dell PowerEdge FX2/FX2s 向け Dell Chassis Management Controller (CMC) バージョン 2.0 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 8 (iDRAC) User's Guide*』(Integrated Dell Remote Access Controller 7 (iDRAC) ユーザーズガイド) には、管理下システムでの iDRAC8 のインストール、設定、およびメンテナンスに関する情報が記載されています。
- 『*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*』は、システムアップデート対策の一環としての Dell Update Packages の入手方法と使い方を説明しています。
- Dell 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には、CMC PowerEdge FX2/FX2s がインストールされているシステムに関する詳細が記載されています。

- システムに付属している「安全にお使いただくために」には安全や規制に関する重要な情報が記載されています。規制に関する詳細な情報については、**www.dell.com/regulatory_compliance** にある 法規制の順守ホームページを参照してください。保証に関する情報は、このマニュアルに含まれているか、別の文書として同梱されています。
- 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『Glossary』(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 QR コード (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

次のリンクを使用して、必要なドキュメントにアクセスします。

- Dell EMC エンタープライズシステム管理のマニュアル — **www.dell.com/SoftwareSecurityManuals**
- Dell EMC OpenManage マニュアル — **www.dell.com/OpenManageManuals**
- Dell EMC リモートエンタープライズシステム管理のマニュアル — **www.dell.com/esmmanuals**

- iDRAC マニュアル — **www.dell.com/idracmanuals**
- Dell EMC OpenManage Connections エンタープライズ システム管理のマニュアル — **www.dell.com/OMConnectionsEnterpriseSystemsManagement**
- Dell EMC Serviceability Tools マニュアル — **www.dell.com/ServiceabilityTools**
- 1. **www.support.dell.com** にアクセスします。
  2. **すべての製品を参照** 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。
     - **統計**
     - **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**
     - **公共機関向けソリューション**
     - **ユーティリティ**
     - **メインフレーム**
     - **保守ツール**
     - **仮想化ソリューション**
     - **オペレーティングシステム**
     - **サポート**
  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。

トピック：

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。

シャーシ設定のチェックリスト

次のタスクによって、シャーシを正確に設定することができます。

1. ブラウザを使用する CMC と管理ステーションは、同一のネットワーク上にあることが必要です。このネットワークを管理ネットワークと呼びます。イーサネットネットワークケーブルを、**GB1** とラベル付けされたポートから管理ネットワークに接続します。

   管理ネットワーク：CMC、iDRAC（各サーバ上）、およびスイッチ I/O モジュール用のネットワーク管理ポートは、PowerEdge FX2/FX2s シャーシ内の共通内部ネットワークに接続されています。これにより、管理ネットワークをサーバデータネットワークから分離できます。

   アプリケーションネットワーク：管理対象サーバへのアクセスは 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。これにより、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。シャーシ管理へのアクセスが中断されないようにするため、このトラフィックを分離することは重要です。

   メモ: シャーシ管理を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の潜在的なトラフィックのため、内部管理ネットワーク上の管理インタフェースは、サーバ向けのトラフィックにより飽和状態になる可能性があります。その場合、CMC と iDRAC との間の通信に遅延が発生します。こうした遅延は、稼動中の iDRAC をオフライン状態だと CMC が見なしたりするなど、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 と iDRAC のトラフィックをそれぞれ異なる VLAN に分離するという選択肢もあります。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可能です。
2. STK/Gb2 ポートは、CMC NIC のフェールオーバー用にも使用できます。NIC フェールオーバーを実装するには、CMC 設定がデフォルトの **スタッキング** から **冗長** に変更されているようにしてください。詳細については、「管理ポート 2 の設定」を参照してください。

   注意: NIC のフェールオーバーを実装するために CMC の設定がデフォルトのスタッキングから冗長に変更されていない場合に、STK/Gb2 ポートを管理ネットワークに接続すると、予想できない結果になります。デフォルトのスタッキングモードで Gb1 ポートと STK/Gb2 ポートを同じネットワーク（ブロードキャストドメイン）に接続すると、ブロードキャストストームが生じる可能性があります。また、CMC 設定が冗長モードに変更されていても、シャーシ間がスタッキングモードでデイジーチェーン接続されている場合に、ブロードキャストストームが発生する可能性があります。ケーブル配線モデルが、意図した用途の CMC 設定と一致しているようにしてください。
3. 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 I/O モジュールに接続します。
4. シャーシにサーバーを挿入します。
5. シャーシを電源に接続します。

6. シャーシの電源をオンにするには、電源ボタンを押すか、タスク 6 を完了してから次のインタフェースを使用します。Web インターフェイスを使用して、**[シャーシ概要]** > **[電源]** > **[制御]** > **[電源制御オプション]** > **[システムの電源を入れる]** の順に移動します。**適用** をクリックします。

   コマンド ライン インターフェイスを使用してシャーシの電源をオンにすることも可能で、その場合は `racadm chassisaction powerup` コマンドを使用します。

   メモ: サーバーの電源は入れないでください。

7. デフォルトの CMC のネットワーク設定は、静的な CMC IP アドレス 192.168.0.120 です。DHCP へネットワーク設定を変更する場合には、CMC のシリアルポートにシリアルケーブルを接続します。シリアル接続についての詳細は、「管理ステーションからのリモートアクセスソフトウェアの使用」の項に記載されているシリアルインタフェース / プロトコルセットアップを参照してください。

   シリアル接続が確立したら、ログインして `racadm setniccfg –d` コマンドを使用し、ネットワーク設定を DHCP に変更します。CMC で DHCP サーバから IP アドレスを取得するには、約 30 ~ 60 秒かかります。

   DHCP が割り当てた CMC IP アドレスを表示するには、次のいずれかの方法を使用します。

   - CMC とのシリアル接続を使用して CMC IP アドレスを表示するには、次の手順を実行します。
     a. シャーシ背面にあるシリアルコネクタに、シリアル Null モデムケーブルの一端を接続します。
     b. ケーブルのもう一端を管理システムシリアルポートに接続します。
     c. 接続確立後、デフォルトのルートアカウント資格情報を使用して CMC にログインします。
     d. `racadm getniccfg` コマンドを実行します。

        表示された出力で、**現在の IP アドレス** を検索します。

   - KVM を使用してサーバーを接続することによって CMC IP アドレスを表示するには、次の手順を実行します。
     a. KVM を使用して、シャーシ内のサーバーに接続します。

        メモ: KVM 経由でネットワークに接続する方法の詳細については、「KVM を使用したサーバーへのアクセス」を参照してください。
     b. サーバーの電源を入れます。
     c. サーバーが UEFI (Unified Extensible Firmware Interface) モードで起動するように設定されていることを確認します。
     d. F2 を押して、セットアップユーティリティ ページにアクセスします。
     e. **セットアップユーティリティ** ページで、**iDRAC 設定** > **システム概要** をクリックします。

        CMC IP アドレスが **Chassis Management Controller** セクションに表示されます。

        iDRAC GUI の **[iDRAC 設定]** ページの詳細については、『*Dell Integrated Dell Remote Access Controller (iDRAC) ユーザーズガイド*』を参照してください。

8. デフォルトのルート アカウント資格情報を入力し、Web ブラウザーを使用して CMC IP アドレスに接続します。
9. 必要に応じて iDRAC ネットワークを設定します。デフォルトでは、iDRAC LAN は固定 IP が設定された状態で有効化されています。**Enterprise ライセンス** を使用してデフォルトの固定 IP アドレスを判別するには、**[サーバー概要]** > **[セットアップ]** > **[iDRAC]** の順に移動します。**Express ライセンス** を使用して固定 IP アドレスを判別することもできます。その場合は、**[サーバー概要]** > **[サーバー スロット]** > **[セットアップ]** > **[iDRAC]** の順に移動します。
10. CMC Web インターフェイスで、IO モジュールに外部管理 IP アドレス (該当する場合) 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。
11. デフォルトのルート アカウント資格情報を使用して Web インターフェイス経由で各 iDRAC に接続し、必要な設定を行います。
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: デフォルトのローカルアカウント資格情報は、root (ユーザー名) と calvin (パスワード) です。

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。

デイジーチェーン FX2 CMC ネットワーク接続

ラック内に複数のシャーシがある場合は、最大 10 台のシャーシをデイジー チェーン構成にすることで、管理ネットワークへの接続数を減らすことができます。必要とされる管理ネットワークのアップリンク接続数を 10 から 1 に減らすことができます。

シャーシをデイジーチェーン接続する場合、GB はアップリンク ポート、STK はスタッキング (ケーブル統合) ポートになります。GB ポートを管理ネットワーク、またはネットワークに近いシャーシの CMC の STK ポートに接続します。STK ポートはチェーンまたはネットワークから離れた GB ポートにのみ接続してください。

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

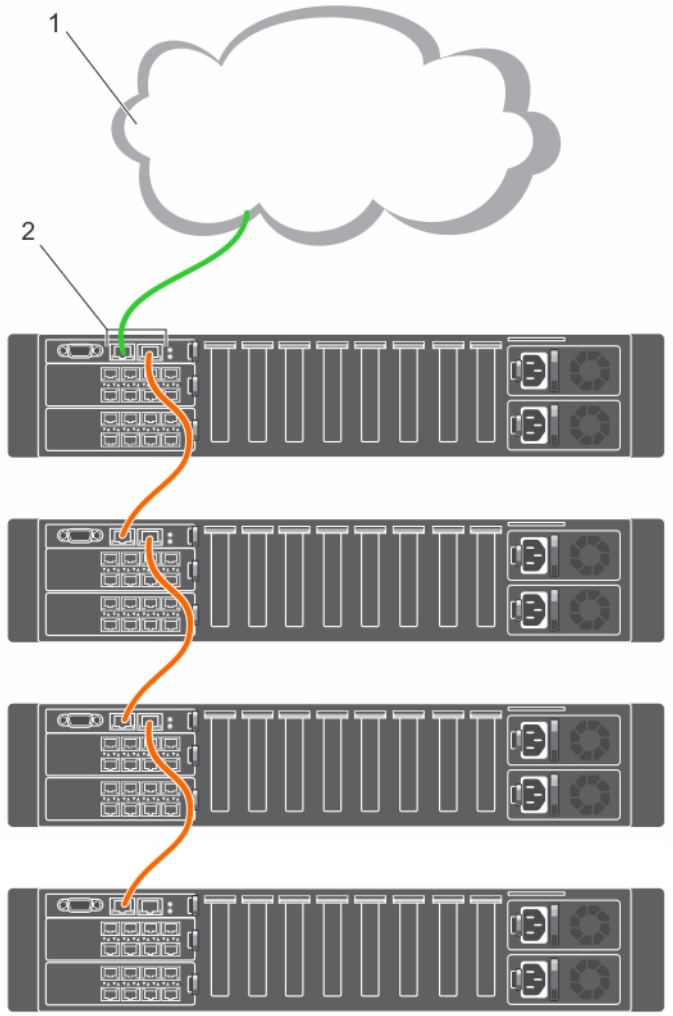
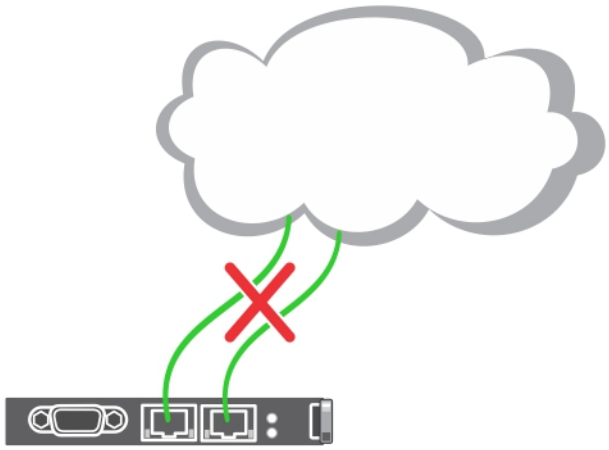


表 9. デイジーチェーンのストレージスレッド

図のコンポーネント番号	コンポーネント名
1	管理ネットワーク
2	アクティブ CMC

次の図は、スタッキングモードでの CMC の間違ったケーブル接続の例を示します。



4 つの FX2 CMC モジュールをデイジーチェーン接続するには、以下の手順に従います。

1. 最初のシャーシの FX2 CMC の GB ポートを管理ネットワークに接続します。
2. 2 つ目のシャーシの FX2 CMC の GB ポートを最初のシャーシの FX2 CMC の STK ポートに接続します。
3. 3 つ目のシャーシがある場合は、そのシャーシの FX2 CMC の GB ポートを 2 つ目のシャーシの FX2 CMC の STK ポートに接続します。
4. 4 つ目のシャーシがある場合は、そのシャーシの FX2 CMC の GB ポートを 3 つ目のシャーシの FX2 CMC の STK ポートに接続します。

注意: CMC の STK ポートは、管理ネットワークには絶対に接続しないでください。必ず別のシャーシの GB ポートに接続してください。STK ポートを管理ネットワークに接続すると、ネットワークが中断してデータが失われる可能性があります。GB と STK を同じネットワーク (ブロードキャスト ドメイン) にケーブル接続すると、ブロードキャスト ストームが発生する可能性があります。

メモ: STK ポートが別の CMC にチェーン接続されている CMC をリセットすると、チェーンの後半に表示される CMC のネットワークが中断される可能性があります。子 CMC でネットワーク リンクが失われたことを示すメッセージがログ記録される場合があります。

メモ: シャーシをまとめてデイジーチェーン接続する場合は、すべてのシャーシが同じ VLAN ID を共有していることを確認してください。

管理ステーションからのリモートアクセスソフトウェアの使用

CMC には、各種リモートアクセスソフトウェアを使用して管理ステーションからアクセスすることができます。次のリストは、お使いのオペレーティングシステムから使用できるデル提供のリモートアクセスソフトウェアの一覧です。

表 10. CMC インタフェース

インタフェース / プロトコル	説明
シリアル	CMC は、ターミナルエミュレーションソフトウェアを使用して起動することが可能なシリアルテキストコンソールをサポートします。CMC への接続に使用できるターミナルエミュレーションソフトウェアの例をいくつか紹介します。 ● Linux Minicom ● Hilgraeve の Windows 向けハイパーターミナル シリアル Null モデムケーブル (両端に存在) の一方をシャーシ背面のシリアルコネクタに接続し、ケーブルのもう一方を管理ステーションのシリアルポートに接続します。ケーブル接続についての詳細は、「シャーシ概要」の項でシャーシ背面パネルを参照してください。

表 10. CMC インタフェース（続き）

インタフェースノプロトコル	説明
	次のパラメータを使用してターミナルエミュレーションソフトウェアを設定します。 ● ボーレート：115200 ● ポート：COM 1 ● データ：8 ビット ● パリティ：なし ● 停止：1 ビット ● ハードウェアフロー制御：はい ● ソフトウェアフロー制御：いいえ
リモート RACADM CLI	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 インターフェイスを使用し、HTTPs チャネルも使用します。–r オプションは、ネットワーク経由で RACADM コマンドを実行し、CMC IP、ユーザー名、パスワードが必要となります。 お使いの管理ステーションからリモート RACADM を使用するには、システムに付属する『Dell Systems Management Tools and Documentation』DVD を使用してリモート RACADM をインストールします。リモート RACADM の詳細については、
Web インターフェイス	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。Web インターフェイスは 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 Web ブラウザーから NIC インターフェイスを介してアクセスします。対応する Web ブラウザーのリストは、Dell サポート サイト **dell.com/support/manuals** の『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。
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。
SNMP	Simple Network Management Protocol（SNMP）は、ネットワーク上のデバイスを管理するための一連のプロトコル定義です。CMC は SNMP へのアクセスを提供し、これによって、システム管理情報用の CMC のクエリに SNMP ツールを使用することが可能になります。CMC MIB ファイルは、CMC Web インターフェイスで **[シャーシ概要]** > **[ネットワーク]** > **[サービス]** > **[SNMP]** の順に移動してダウンロードできます。CMC MIB の詳細については、『*Dell OpenManage SNMP リファレンス ガイド*』を参照してください。 次の例は、CMC からシャーシ サービス タグを取得するための `net-snmp snmpget` コマンドの使用方法を示しています。 `snmpget -v 1 -c <CMC community name> <CMC IP address>.1.3.6.1.4.1.674.10892.2.1.1.6.0`
WSMan	WSMan Services は、一対多のシステム管理タスクを実行するため、Web Services for Management（WSMan）プロトコルをベースとしています。CMC Services 機能を使用するには、WinRM クライアント（Windows）や OpenWSMan クライアント（Linux）などの WSMan クライアントを使用することができます。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 の情報は、管理下システムで変更可能なセマンティックや情報の種類を定義します。 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。

表 10. CMC インタフェース（続き）

インタフェースノプロトコル	説明
	メモ: 転送セキュリティのために使用される SSL ポートは、CMC HTTPS ポートと同じです。 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 Web 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 WS-Management 仕様：**www.dmtf.org/standards/wbem/wsman** 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 set winrm/config @{MaxTimeoutms ="80000"}」を使用しても、WinRM ツールのバグのため、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 分以上かかる可能性のあるコマンドには 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。

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。

リモート RACADM のインストール

お使いの管理ステーションからリモート RACADM を使用するには、システムに付属する『*Dell Systems Management Tools and Documentation*』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ています。

- 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 Software コンポーネントのインストールの詳細については、**dell.com/support/manuals** にある『*Dell OpenManage のインストールおよびセキュリティ ユーザーズ ガイド*』を参照してください。また **support.dell.com** から最新バージョンの Dell DRAC ツールをダウンロードすることもできます。

Windows 管理ステーションへのリモート RACADM のインストール

DVD を使用する場合は、***<path>*\SYSMGMT\ManagementStation\windows\DRAC*<.msi file name>*** を実行します。

dell.com/support からソフトウェアをダウンロードした場合は、

1. ダウンロードしたファイルを解凍し、提供された **.msi** ファイルを実行します。
   ダウンロードしたバージョンに応じて、ファイルの名前は DRAC.msi、RACTools.msi、または RACTools64Bit.msi となります。
2. ライセンス契約に同意し、**次へ** をクリックします。
3. ソフトウェアをインストールする場所を選択し、**次へ** をクリックします。
4. **インストール** をクリックします。

インストールウィンドウが表示されます。

5. **終了** をクリックします。

管理者のコマンドプロンプトを開いて、`racadm` と入力し、**Enter** を押します。RACADM のヘルプ手順が表示される場合は、ソフトウェアが正しくインストールされていることを意味しています。

Linux 管理ステーションへのリモート RACADM 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 and Documentation*』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 の自動マウントが `-noexec mount` オプションで行われます。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** ディレクトリーに移動します。RAC ソフトウェアをインストールするには、次のコマンドを入力します。

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

5. RACADM コマンドのヘルプを参照するには、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 FX2/FX2s 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 サブコマンドの使用対象となるフォルダーへの「書き込み」権限が必要です。たとえば、`racadm getconfig -f <file name>`とします。

Linux 管理ステーションからのリモート 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。

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。

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 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場所とシャーシ名 (デフォルト名は **Dell cmc-"サービスタグ"**) を設定できます。たとえば、シャーシ名での SNMP クエリでは、設定する名前が返されます。

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 にログインしている際にシャーシ名を表示できます。[**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** および **setchassisname** コマンドを参照してください。

たとえば「`racadm setsysinfo –c chassisname`」や「`racadm setsysinfo –c chassislocation`」のように入力します。

詳細については、『*Chassis Management Controller for PowerEdge FX2/FX2s 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 インターフェイ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 FX2/FX2s 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。

たとえば、`racadm setractime -l 20140207111030` のように入力します。

日付と時刻を読み取るには、`racadm getractime` コマンドを使用します。

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、ストレージスレッド、I/O モジュール）の LED を点滅させることができます。

メモ: これらの設定を変更するには、CMC の **デバッグ管理者** 権限が必要です。

コンピュートスレッドが識別操作を実行すると、接続されたストレージスレッドの前方の LED も識別パターンで点滅します。ストレージスレッドがスプリットシングルモードで、2 つのコンピュートノードに接続されている場合は、2 つのコンピュートノードのいずれかが識別操作を実行していれば、識別パターンで点滅します。

コンピュートスレッド、ドライブまたはエンクロージャに iDRAC または OMSS を使用して識別操作を開始する場合、これらに関連付けられているストレージスレッドも識別操作を実行します。

メモ: 識別操作にストレージスレッドのみを選択することはできません。

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。

コンポーネント LED の点滅を有効にするには、それぞれのコンポーネントを選択してから **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、サーバーの選択を解除してから **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` の *n* は 1~4 (PowerEdge FM120x4) で、`server-nx` の *n* は 1~4、*x* は a から b (PowerEdge FC630) です。
- `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

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。

前面パネルの設定

前面パネル ページを使用して、次を設定することができます。

- 電源ボタン
- KVM

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。

KVM を使用したサーバーへのアクセス

Web インターフェイスからサーバーを KVM にマップするには、次の手順を実行します。

1. シャーシの前面にあるビデオコネクタにモニタを接続し、USB コネクタにキーボードを接続します。
2. 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。
3. **前面パネル設定** ページの **KVM 設定** セクションで、**KVM マッピングの有効化** オプションを選択します。
4. **フロントパネル設定** ページの **KVM 設定** セクションにある **マップ済み KVM** オプションで、ドロップダウンリストから必要なサーバーを選択します。
5. **適用** をクリックします。

racadm を使用してサーバーを KVM にマップするには、`racadm config -g cfgKVMInfo -o cfgKvmMapping [server slot #]`コマンドを使用します。

racadm を使用して現在の KVM マッピングを表示するには、`racadm getconfig -g cfgKVMInfo` を使用します。

サーバーモードでのシャーシ管理の設定

この機能を使用すると、シャーシ共有コンポーネントおよびラックサーバーとしてのシャーシノードを管理および監視することができます。この機能が有効な場合、iDRAC RACADM プロキシ、ブレードサーバーのオペレーティングシステム、Lifecycle Controller を使用して次の操作を行えます。

- シャーシのファン、電源装置、温度センサーの監視と管理
- CMC ファームウェアのアップデートと設定

CMC ウェブインタフェースを使用したサーバーでのシャーシ管理の設定

サーバーモードでシャーシ管理を有効にするには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** > **セットアップ** > **一般** をクリックします。
2. **一般シャーシ設定** ページの **サーバーモードでのシャーシ管理** ドロップダウンから、次のモードのいずれかを選択します。
   - **なし** — このモードでは、iDRAC、OS または Lifecycle Controller 経由でシャーシコンポーネントを監視または管理することができません。
   - **監視** — このモードでは、シャーシコンポーネントを監視することができますが、iDRAC、OS、iDRAC RACADM プロキシ、または Lifecycle Controller 経由でファームウェアアップデートを実行することはできません。
   - **管理と監視** — このモードでは、iDRAC、OS、iDRAC RACADM、または Lifecycle Controller 経由でシャーシコンポーネントを監視し、DUP を使用して CMC ファームウェアをアップデートすることができます。

RACADM を使用したサーバーモードでのシャーシ管理の設定

サーバーで、シャーシ管理を RACADM を使用して有効にするには、次のコマンドを使用します。

- サーバーモードでのシャーシ管理を無効にするには、次のコマンドを使用します。

```
racadm config -g cfgRacTuning - cfgRacTuneChassisMgmtAtServer 0
```

- サーバーモードでのシャーシ管理を監視に変更するには、次のコマンドを使用します。

```
racadm config -g cfgRacTuning - cfgRacTuneChassisMgmtAtServer 1
```

- サーバーモードでのシャーシ管理を管理および監視に変更するには、次のコマンドを使用します。

```
racadm config -g cfgRacTuning - cfgRacTuneChassisMgmtAtServer 2
```

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。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。

トピック：

SSH 経由の公開キー認証の設定

SSH インターフェイス経由でサービス ユーザー名と併用できる公開キーは、最大 6 個まで設定できます。意図しないキーの上書きや削除を防止するため、公開キーを追加または削除する際は、事前に `view` コマンドを用い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、キーの追加先インデックスに、既存のキーが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の確認は行われません。SSH インターフェイ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、RACADM `getssninfo` コマンド使用時における SSH ユーザーの識別に、CMC では公開キー コメントが使用されます。

たとえば、コメント PC1 およびコメント PC2 を持つ 2 つの公開キーが設定されている場合は、次のようになります。

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

`sshpkauth` の詳細については、『*Chassis Management Controller for PowerEdge FX2/FX2s 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。

本項では、両方のアプリケーションで公開 / 秘密キーペアを生成する簡単な手順について説明します。これらのツールの使用法の詳細については、アプリケーションヘルプを参照してください。

PuTTY Key Generator を使用して、Windows 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 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 のキーサイズが 1024 ~ 4096 であることを確認します。

   メモ:
   - 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でもログインに失敗します。
   - 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。

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。秘密キーを保存したことを確認します。

4. 公開キーの使用方法には 2 つのオプションがあります。
   - 公開キーをファイルに保存し後でアップロードします。
   - テキストオプションを使用してアカウントを追加する場合に、**公開キーの貼り付け** ウィンドウからテキストをコピーして貼り付けます。

Linux を実行するシステム用の公開キーの生成

Linux クライアント用の ssh-keygen アプリケーションは、グラフィカルユーザーインタフェースのないコマンドラインツールです。ターミナルウィンドウを開き、シェルプロンプトで次を入力します。

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

ここで、

`-t` は 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。コマンドの完了後、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 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、対応ウェブブラウザ が設定されており、必要な権限で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: セキュリティを強化するために、初期設定時に root アカウントのデフォルトパスワードを変更することをお勧めします。

メモ: 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場合は、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>

     メモ: CMC ユーザー名には、英数字と特定の特殊文字のみが使用可能です。アットマーク (@) および次の特殊文字は使用できません。

     - スラッシュ (/)
     - バックスラッシュ (\ )
     - セミコロン (;)
     - バッククォート (')
     - 引用符 (")
   - 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* はドメインの名前、*port number* は HTTPS ポート番号を示します。
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の設定後、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。

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。

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 \
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。

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
WSMan	4

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
- I/O モジュール

以下のサーバーコンポーネントのファームウェアをアップデートできます。

- BIOS
- iDRAC7
- iDRAC8
- 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
- RAID コントローラ

トピック：

署名済みの CMC ファームウェアイメージ

CMC ファームウェアには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憑性を確実にするため、署名検証手順を実行します。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。ファームウェアアップデートには、アップグレードとダウングレードが含まれます。

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。

シャーシのファームウェアのアップデートは、次の順で行うことが推奨されます。

- ブレードコンポーネントファームウェア
- CMC ファームウェア
- シャーシインフラストラクチャファームウェア

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**

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 getversion` コマンドを使用して、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。その他の RACADM コマンドに関する詳細については、『*Dell Chassis Management Controller for PowerEdge FX2/FX2s 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 を使用して、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。

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。

メモ: ファームウェアイメージファイルに検証署名が含まれていない、または無効もしくは壊れている検証署名が含まれている場合は、CMC ファームウェアをアップデートすることはできません。

メモ: 以前のバージョンで計算された署名を現在の CMC ファームウェアで認識できない場合、CMC ファームウェアをその以前のバージョンにダウングレードすることはできません。

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 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。

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 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。

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: 2400W AC PSU によってサポートされるシャーシでは、2400W AC PSU でサポートされないバージョンでファームウェアをアップデート / ダウングレードしようとすると、エラーメッセージが表示されます。2400W AC PSU は CMC 1.40-A00 以降のイメージに対応しています。

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。

ウェブインタフェースを使用した CMC ファームウェアのアップデート

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

1. 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 の **ターゲットのアップデート** 列から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、管理ステーション上または共有ネットワーク上にあるファームウェアイメージファイルへのパスを入力、または **参照** 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名は `fx2_cmc.bin` です。
4. **ファームウェアアップデートを開始する** をクリックし、**はい** をクリックします。**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ステータス情報が表示されます。ステータスインジケータは、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。ファームウェアの各種状態の詳細については、『オンラインヘルプ』を参照してください。
5. CMC では、ファームウェアアップデート処理の最終段階中、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。数分後、CMC が再起動したときに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。

   メモ: ファームウェアのアップデート後、ウェブブラウザ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をクリアする手順については、ウェブブラウザのオンラインヘルプを参照してください。

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、**ファイル転送と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、ファイル転送中にのみ使用できます。
- **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: 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。

たとえば、`racadm fwupdate <options> <firmware image>`とします。

RACADM コマンドの詳細については、『*Chassis Management Controller for PowerEdge FX2/FX2s 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: 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。

DUP を使用した CMC のアップデート

次のコンポーネント経由で、Dell Update Package (DUP) を使用して CMC のファームウェアをアップデートすることができます。

- iDRAC RACADM プロキシ

- ブレードサーバのオペレーティングシステム
- Lifecycle Controller

iDRAC 経由での CMC のアップデートに関する詳細については、『Integrated Dell Remote Access Controller ユーザーズガイド』を参照してください。

DUP を使用して CMC をアップデートする前に、次を確認します。

- ローカルシステムまたはネットワーク共有で、CMC ファームウェアパッケージが DUP として使用可能である。
- **サーバーモードでのシャーシ管理** が **管理と監視** に設定されている。

  詳細については、「サーバーモードでのシャーシ管理の設定」を参照してください。
- OS または Lifecycle Controller 経由のアップデートについては、iDRAC オプションの **OS/USC 経由の共有コンポーネントアップデートの有効化** を有効にする必要があります。このオプションを有効にする方法の詳細については、『Integrated Dell Remote Access Controller ユーザーズガイド』を参照してください。

メモ: DUP を使用して CMC をアップデートするときは、CMC イメージで使用できる IOM コプロセッサへのアップデートは次回のシャーシ電源投入サイクルで適用されます。

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、メインボード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前に、必要に応じてシャーシ内のすべてのサーバーの電源をオフにします。

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。

アップデートの完了時には、シャーシ全体がリセットされるため、CMC への接続が失われます。ウェブインタフェースを更新して、再度ログインしてください。**シャーシ概要** > **シャーシコントローラ** と移動します。

アップデートの完了後、アップデートされたメインボードファームウェアのバージョンが表示されます。

。

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のファームウェアをアップデートするには、`fwupdate` サブコマンドを使用します。

たとえば、`racadm fwupdate <options> <firmware image>`とします。

RACADM コマンドの使用の詳細については、『*Chassis Management Controller for PowerEdge FX2/FX2s 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: 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には、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。

サーバー iDRAC ファームウェアのアップデート

iDRAC 8 または iDRAC 7 のファームウェアをアップデートすることができます。この機能を使用するには、次が必要です。

- Enterprise ライセンスを持っている。
- iDRAC7 ファームウェアバージョンが 1.57.57 以降である。
- iDRAC8 ファームウェアバージョンが 2.05.05 以降である。

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。

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**。
   - **シャーシ概要** > **シャーシコントローラ** > **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. iDRAC または iDRAC8 ファームウェアをアップデートするには、**iDRAC<リビジョン番号> Enterprise 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。

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、サーバの Lifecycle Controller 機能を利用しています。

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。Lifecycle Controller を使用してファームウェアをアップデートするには、iDRAC ファームウェアがバージョン 2.3 以降でなければなりません。

Dell Update Packages (DUP) は、Lifecycle Controller を使用したファームウェアのアップデートを行う際に使用されます。オペレーティングシステム ドライバー パックのコンポーネント DUP がこの制限を超えているため、拡張ストレージ機能を使用して個別にアップデートする必要があります。

メモ: Lifecycle Controller ベースのアップデート機能を使用する前に、サーバのファームウェアのバージョンをアップデートする必要があります。また、サーバー 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 ファームウェアもアップデートしてください。

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]** の順に選択して、[**CSIOR**] を有効にし、変更を保存します。
- 第 13 世代サーバ — サーバを再起動した後、プロンプトが表示されたら、F10 キーを押して 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。

  - iDRAC
  - Lifecycle Controller
  - BIOS

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**] 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、Dell Tech Center で、http://en.community.dell.com/TECHCENTER/EXTRAS/M/WHITE_PAPERS/20438118/DOWNLOAD 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。

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更新した後、CMC の 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]** をクリックします。

サーバーで Lifecycle Controller サービスに対応していない場合は、[**コンポーネント/デバイスのファームウェア インベントリー**] 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ーの場合、 `.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、ネイティブの 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 の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場合、「InstallFromURI」メソッドが機能しないことがあります。

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
- BIOS
- 診断 (オプション)
- OS ドライバパック (オプション)
- RAID
- NIC
- CPLD
- 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。
- System Services 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をキャンセルし、キューから削除できるようになります。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』、または **delltechcenter.com/page/Lifecycle+Controller** を参照してください。

- **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 の場合：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 **サーバー概要** に移動し、**アップデート** > **サーバーコンポーネントアップデート** 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、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た情報のフィルタが可能ですが、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。

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。

   - 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、ファームウェアインベントリ用のページを更新してインベントリを再取得します。
   - iDRAC のファームウェアのみを直接アップデートできる代替ページへのハイパーリンクが表示されます。このページでは、iDRAC ファームウェアのアップデートのみをサポートしており、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。
   - コンポーネントおよびデバイスのインベントリ内容が、サーバーに物理的に取り付けられている内容を正しく反映していない場合は、サーバーの起動プロセス中に Lifecycle Controller を呼び出す必要があります。これは、内部の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。この状況は、次の場合に発生します。

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

     iDRAC 設定ユーティリティに対するこのアクションを自動化するには、起動コンソールからアクセスできるオプションがあります。

     a. 起動コンソールで、<F2> を押して **セットアップユーティリティ** にアクセスします。
     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	シャーシ内のサーバーが装着されているスロットを表示します。スロット番号はシャーシ内で使用できる 4 つのスロットに対する連番 ID です。 ● 1、1a、1b、1c、1d ● 2、2a、2b、2c、2d ● 3、3a、3b、3c、3d ● 4、4a、4b、4c、4d この付番スキームは、シャーシ内にあるサーバーの位置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

表 12. コンポーネントおよびデバイス情報（続き）

フィールド	説明
	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 インベントリーを表示するには、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 FX2/FX2s 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. **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 Web インターフェイ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 Web インターフェイスのシステム ツリーで [**サーバー概要**] 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。
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: デフォルトのカタログ ファイル名が catalog.xml の場合のみ、[**ファイル名**] はオプションです。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 for Dell PowerEdge FX2/FX2s のオンライン 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 の場合：iDRAC の設定権限および iDRAC へのログイン。

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、適切なタイプをクリックします。
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、適切なタイプをクリックします。
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グレード

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 85 MB 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 85 MB 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、**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、「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_Stmp_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」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 キーショートカットを使用して、該当するサーバー全体におけるアップデート用コンポーネントまたはデバイスのタイプを選択します。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** 列の関連するチェックボックスを有効化することによって、必要なコンポーネントまたはデバイスを選択します。

   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は、単一 DUP、または組み合わされた DUP のいずれもアップデートサイズ制限を無視できます。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** — 直ちに再起動します。ファームウェアアップデートは即時に適用されます
   - **次回の再起動時** — サーバーを後ほど手動で再起動します。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 FX2/FX2s 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。

- サーバーに iDRAC Enterprise ライセンスがある。
- サーバー上で Lifecycle Controller が有効になっている。
- 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、**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アップデートのスケジュールを完了します。
   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。

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。

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。

- 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
- PCIe デバイス
- ストレージスレッド

トピック：

シャーシとコンポーネント概要の表示

CMC Web インターフェイ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、CMC、サーバー モジュール、IO モジュール (IOM)、ファン、電源供給ユニット (PSU)、ストレージ スレッド、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。詳細については、『*Dell Integrated Dell Remote Access Controller (iDRAC) ユーザーズ ガイド*』を参照してください。

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

シャーシは正面、背面、上部から見た図で示されています (それぞれ上のイメージと下のイメージ)。サーバおよび KVM は前面図、残りのコンポーネントは背面図で示されています。青色の表示はコンポーネントの選択を示し、必要なコンポーネントイメージをクリックすることで制御されます。シャーシにコンポーネントが存在する場合、そのコンポーネントタイプのアイコンが、図中のコンポーネントが取り付けられている場所 (スロット) に表示されます。空の場所は、背景色が濃い灰色で表示されます。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には、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、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。

第 13 世代システムでのサーバアイコン状況

イメージ	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。
	サーバは存在するものの、重要エラーが報告されています。

第 14 世代システムでのサーバアイコン状況

イメージ	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。
	サーバは存在するものの、重要エラーが報告されています。

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、Web インターフェイスの [**シャーシの正常性**] ページに表示されるコンポーネントの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 13. 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
CMC	• MAC アドレス • IPv4 • IPv6	• 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

表 13. 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
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（オペレーティングシステム） • 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、代わりに [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。
すべてのストレージと個別のストレージスレッド	正常性	• 名前 • モデル • サービスタグ • 資産タグ • コントローラの数 ○ 物理ディスクスロット ○ サーバーに接続済み ○ コントローラモード機能 • イントルージョン状態	• ストレージアレイの状態 • ストレージアレイセットアップ
電源供給ユニット	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 • マッピング • ベンダー ID • デバイス ID • スロット タイプ • モジュールタイプ • ファブリック • 電源状態	• PCIe の状態 • PCIe セットアップ

表 13. 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
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
IOM スロット	• 電源状況 • 役割	• モデル • サービスタグ	IOM 状態

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** ツリーノードで、すべてのサーバー（SLOT-01～SLOT-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存在しない場合、図解内の対応するイメージがグレー表示されます。
2. カーソルをサーバーのスロット名またはスロット番号の上に置くと、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。

ストレージモデル名とサービスタグの表示

各ストレージスレッドのモデル名とサービスタグは、次の手順で表示することができます。

1. 左ペインの **サーバー概要** ツリーノードの下に、すべてのストレージスレッドがリスト表示されます。ストレージスレッドがスロットに存在しない場合、図内の対応するイメージはグレー表示されます。
2. ストレージスレッドのスロット番号にカーソルを置きます。
   使用可能であれば、ツールヒントがストレージスレッドのモデル名およびサービスタグ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、*CMC for Dell PowerEdge FX2/FX2s のオンライン 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 コントローラー情報と状態を表示するには、CMC Web インターフェイスで、**[シャーシ概要]** > **[シャーシ コントローラー]** 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、*CMC for Dell PowerEdge FX2/FX2s のオンライン 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、『CMC for Dell PowerEdge FX2/FX2s 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。

ストレージスレッドの情報および正常性状態の表示

ストレージスレッド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]** > **[サーバー概要]** をクリックし、ストレージ スレッドを選択します。
[ストレージ アレイの状態] ページには、ストレージ スレッド プロパティと、コンピュート スレッドに接続されたストレージ ノードのリストが表示されます。詳細については、*オンライン ヘルプ*を参照してください。

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。カーソルをそれぞれの IOM サブグラフィックの上に動かしてください。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 モジュール状態 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『CMC for Dell PowerEdge FX2/FX2s 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 つのモードで稼働させることができます (ファンオフセット)。ファンの設定に関する詳細については、『*CMC for Dell PowerEdge FX2/FX2s 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/support/manuals にある『Chassis Management Controller for PowerEdge FX2/FX2s 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の速度を自動調整します。このコマンドを使用して上書きすると、シャーシの必要性に関わらず、CMC は常に選択された速度でファンを稼働することになります。ただし、racadm `fanoffset` コマンドによって、最小限のファン速度を維持できるよう上書きすることが可能です。

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。シャーシ図の上部右側にはシャーシの上部左側が表示され、これにはファンの正常性ステータスが含まれています。ファンの正常性ステータスは、ファンのサブグラフィックの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動かすと、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 — この機能を使用すると、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 オフセットの使用例となるのは、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 カードを使用する場合です。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。ただし構成によっては、低、中、高の各オプションでの最小速度の方が、これらの値よりも高速になる場合があります。

たとえば、ファン オフセットを中に設定した場合、ファン速度は最大速度の 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。

いずれかのファン オフセット オプションを有効にすると、消費電力は増加します。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が無効化されているときは、取り付けられたハードウェア構成のためのシステム冷却に必要なデフォルト速度までファン速度が低減されます。

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]** の順に移動します。[**詳細ファン設定**] ページで、[**ファン オフセット**] に対応する [**値**] ドロップダウン リストから、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>]
```

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**
   - **KVM のプロパティ**
   - **フロントパネルインジケータ**

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。

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。

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。

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、リモートで管理できるように CMC のネットワークを設定する必要があります。この初期設定によって、CMC へのアクセスを有効にする TCP/IP ネットワークパラメータが割り当てられます。

CMC の設定、または CMC RACADM への初期アクセスのセットアップは、ウェブインタフェースを使用して行うことができます。

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。
- 必要に応じてシャーシグループを設定。
- 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。
- ストレージスレッドの追加と設定。

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 NIC アドレス用 DHCP 機能が動的ホスト構成プロトコル (DHCP) サーバーからの IP アドレスに対する要求と取得を自動で行います。この機能はデフォルトで無効になっています。

DHCP を有効にして、DHCP サーバーから自動的に IP アドレスを取得することができます。

DNS IP アドレス用 DHCP の有効化または無効化

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 アドレス用 DHCP 機能を有効化し、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 1
```

IPv6 のために DNS アドレス用 DHCP 機能を有効化し、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 1
```

静的 DNS 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-address> racadm config -g
cfgLanNetworking -o cfgDNSServer2 <IPv4-address>
```

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

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。

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

IPv4 設定を表示するには、オブジェクト `cfgCurrentLanNetworking` に次のサブコマンドを併用します。

- `getniccfg`
- `getconfig`

IPv6 設定を表示するには、`cfgIpv6LanNetworking` に `getconfig` サブコマンドを併用します。

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 FX2/FX2s 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 ネットワークインタフェースを無効にすると、無効化操作が次の処置を実行します。

- iDRAC および IOM 管理を含む、帯域外シャーシ管理に対するネットワークインタフェースアクセスの無効化。
- ダウンリンク状態検知の阻止。

  CMC ネットワークアクセスのみを無効にするには、CMC IPv4 と CMC IPv6 の両方を無効にします。

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: 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 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>
```

DHCP は、デフォルトで無効になっています。DHCP を有効にして、iDRAC または CMC IPv4 アドレス、サブネットマスク、およびゲートウェイの割り当てに DHCP サーバを使用するには、次のように入力します。

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

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>
```

IPv4 および IPv6 DNS 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 名** - デフォルトでは、DNS サーバ上の CMC 名は cmc-<*サービスタグ*> です。DNS サーバ上の CMC 名を変更するには、次のように入力します。

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

  ここで、< *name* > は 63 文字以内の英数字とハイフンによる文字列です。たとえば、cmc-1、d-345 のように指定します。

  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 文字以内である必要があります。
- **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、次のように入力します。

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

  ここで、< *name* > は 254 文字以内の英数字とハイフンによる文字列です。たとえば、p45、a-tz-1、r-id-001 のように指定します。

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

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

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

```
racadm config -g cfgNetTuning -o cfgNetTuningNicAutoneg 0
racadm config -g cfgNetTuning -o cfgNetTuningNicFullDuplex <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。

管理ポート 2 の設定

CMC の 2 個目のネットワークポートは、ケーブル本数削減のための CMC のデイジーチェーン接続用に使用、またはネットワークのフェイルオーバー操作用に冗長ポートとして使用することができます。**管理ポート 2** は、トップオブラック (TOR) スイッチまたは別のスイッチに接続することも可能です。2 つの CMC NIC ポートを同じサブネットに接続するという必須条件はありません。

管理ネットワークポート冗長用に CMC を実際に事前設定しておかなければ、CMC をその用途のためにケーブル接続することはできません。CMC は、展開のために標準のシングルネットワーク接続を使用する必要があり、その後で 2 つめの冗長接続が可能となります。

メモ: 管理ポート 2 が冗長向けに設定されいるが、スタッキング向けにケーブル配線されているというときは、ダウンストリーム CMC (TOR スイッチから離れているもの) のネットワークリンクがなくなります。

メモ: 管理ポート 2 がスタッキング向けに設定されているが、冗長向けにケーブル配線されている (TOR スイッチへの 2 つの接続) というときは、ルーティングループによってネットワークストームが発生する可能性があります。

冗長操作を指定するには、`racadm config -g cfgNetTuning -o cfgNetTuningNicRedundant 1` コマンドを使用します。

スタッキング操作を指定するには、`racadm config -g cfgNetTuning -o cfgNetTuningNicRedundant 0` コマンドを使用します。

管理ポート 2 はデフォルトでスタッキング用に設定されています。

CMC ウェブインタフェースを使用した管理ポート 2 の設定

CMC ウェブインタフェースを使用して管理ポ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** > **ネットワーク** とクリックし、**ネットワーク** タブをクリックします。
2. **ネットワーク設定** ページにある **一般設定** セクションの **管理ポート 2** の横で、**冗長** または **スタッキング** のいずれかを選択します。
3. **変更の適用** をクリックします。
   - 管理ポート 2 が冗長向けに設定されいるが、スタッキング向けにケーブル配線されているというときは、ダウンストリーム CMC (トップオブラックスイッチから離れているもの) のネットワークリンクがなくなります。
   - 管理ポート 2 がスタッキング向けに設定されているが、冗長向けにケーブル配線されている (TOR スイッチへの 2 つの接続) というときは、ルーティングループによってネットワークストームが発生する可能性があります。

RACADM を使用した管理ポート 2 の設定

冗長操作を指定するには、`racadm config -g cfgNetTuning -o cfgNetTuningNicRedundant 1` コマンドを使用します。

スタッキング操作を指定するには、`racadm config -g cfgNetTuning -o cfgNetTuningNicRedundant 0` コマンドを使用します。

管理ポート 2 はデフォルトでスタッキング用に設定されています。

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。
- リモート 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。

メモ: SSH、Telnet、HTTP、または HTTPS の CMC サービスポート番号を変更する場合は、ポート 111 などの OS サービスで一般的に使用されるポートは使用しないでください。http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml で、Internet Assigned Numbers Authority（IANA）予約済みポートを参照してください。

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 および iDRAC の通信用の予約済みネットワークポートは 21、68、69、123、161、546、801、4003、4096、5985 ~ 5990、6900、および 60106 です。

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 FX2/FX2s 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。

サーバーのファームウェアが特定の機能をサポートしていない場合、その機能に関連した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 を用いてリモート syslog を非対応の iDRAC で有効にすると、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、『CMC for Dell PowerEdge FX2/FX2s オンラインヘルプ』を参照してください。
3. **適用** をクリックして選択したオプションを適用します。

シャーシ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シャーシのウェブページを開くには、クィック起動リンクを使用することができます。
- 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 19 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。

   メモ: シャーシグループが作成されると、ツリー構造の **シャーシ概要** アイテムが、リードシャーシの名前と置き換えられます。

シャーシグループへのメンバーの追加

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

1. リーダーシャーシにシャーシ管理者権限でログインします。
2. システムツリーでリードシャーシを選択します。
3. **セットアップ** > **グループ管理** とクリックします。
4. **グループ管理** にある **ホスト名 /IP アドレス** フィールドで、メンバーの IP アドレスまたは DNS 名を入力します。

メモ: MCM が正しく機能するには、すべてのグループメンバーとリーダーシャーシで、デフォルトの HTTPS ポート（443）を使用する必要があります。

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、**新しいメンバーをリーダープロパティと同期** 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。シャーシグループへのメンバーの追加については、「新しいメンバーとリーダーシャーシのプロパティの同期」を参照してください。
8. **Apply（適用）** をクリックします。
9. 最大の 19 の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 Web ページの起動

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 Web 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 Web 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認証情報が設定されている場合は、その認証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: シングル サインオンおよびスマート カード ログインは、マルチ シャーシ管理で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 サインオンでメンバーを起動するには、リードとシャーシ間で共通したユーザー名/パスワードが必要です。共通のユーザー名/パスワードの使用は、Active Directory、ローカル、および LDAP ユーザーでのみ機能します。

メンバーデバイスに移動するには、次の手順を実行します。

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

   リーダーとシャーシの両方で、FIPS が有効になっている場合、または無効になっている場合に、[**CMC の起動**] を用いたメンバー シャーシへのログインを試みると、[**シャーシ グループの正常性**] ページに誘導されます。そうでない場合は、メンバー シャーシの [**ログイン**] ページに誘導されます。

   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**] というラベルが付いたボックスで、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。

新しいメンバーとリーダーシャーシのプロパティの同期

リーダーのプロパティを、グループに新しく追加されたメンバーシャーシに適用することができます。新しいメンバーのプロパティとリーダーのプロパティを同期するには、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. ツリー構造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** ページで、新しいメンバーをグループに追加するときに、**新しいメンバーとリーダーのプロパティを同期** を選択します。
5. **適用** をクリックします。リーダーのプロパティがメンバーに適用されます。

同期後、シャーシ内の複数のシステムの以下の設定サービスプロパティが影響を受けます。

表 14. 設定サービスプロパティ

プロパティ	ナビゲーション
SNMP 設定	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。
シャーシのリモートロギング	左ペインで、**シャーシ概要** > **ネットワーク** > **サービス** > **リモート Syslog** をクリックします。
LDAP サービスおよび Active Directory サービスを使用したユーザー認証	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。
シャーシアラート	左ペインで、**シャーシ概要** をクリックし、次に **アラート** をクリックします。

MCM グループのサーバーインベントリ

グループは、0 ~ 19 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。
- 空のスロットと拡張スロット。

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。

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インポート

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ローカル管理ステーションにインポートすることができます。

リモートファイル共有に保存されているプロファイルを CMC にインポートするには、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、[**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。

メモ: RACADM を使用して、シャーシ設定プロファイルをインポートすることができます。詳細については、『Chassis Management Controller for Dell PowerEdge M1000e 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。

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。

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>
```

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. CMC への Telnet/SSH テキストコンソールを開いて、ログイン後、次を入力します。

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

   メモ: getconfig -f を使用して CMC の設定をファイルにリダイレクトする機能は、リモート RACADM インタフェースでのみサポートされています。

3. テキストのみのエディタ (オプション) を使用して設定ファイルを変更します。設定ファイルに特殊なフォーマット文字を使用すると、RACADM データベースが破損する可能性があります。
4. 新しく作成した設定ファイルを使ってターゲット CMC を変更します。 コマンドプロンプトで、次のコマンドを入力します。

   ```
   racadm 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、CMC の CMC 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。

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 列目で始まる必要があります。他の列の「#」文字は、「#」文字として扱われます。

  一部のモデム パラメーターには、文字列に「#」文字が含まれる場合があります。エスケープ文字は必要ありません。racadm getconfig -f <filename> .cfg コマンドで .cfg を生成し、エスケープ文字を追加せずに別の 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。

グループ名を示す右カッコ ([ ) は 1 列目にある必要があります。このグループ名は、そのグループ内の他のオブジェクトよりも前に指定する必要があります。関連するグループ名が含まれていないオブジェクトは、エラーを生成します。設定データは、『*iDRAC および CMC 向け RACADM コマンド ライン リファレンス ガイド*』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。値の後にあるスペースは無視されます。値の文字列内にあるスペースは変更されません。=の右側の文字はそのまま使用されます (例 : 2 つ目の=、#、[、] など)。これらの文字は、有効なモデム チャット スクリプト文字です。

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

- .cfg パーサはインデックス オブジェクト エントリーを無視します。

  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、それが使用されます。インデックスがない場合は、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ーが作成されます。

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

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

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

- インデックス付きグループの行を.cfg ファイルから削除することはできません。テキスト エディタを用いてこの行を削除すると、RACADM は設定ファイルの解析時に停止し、エラーを警告します。

  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 1-16> ""
  ```

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

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

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

- インデックス付きグループの場合、オブジェクト アンカーは [ ] ペアに後続する最初のオブジェクトである必要があります。次に示すのは、現在のインデックス付きグループの例です。

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

- リモート RACADM を使用して設定グループをファイル内に取り込むときに、グループ内のキー プロパティが設定されていない場合、その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。あるいは、getconfig -f コマンドを実行した後で、必要な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、RACADM インデックス付きグループのすべてに適用されます。

  次は、この動作と対応するキープロパティを示したインデックス化されたグループを一覧にしたものです。

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

CMC IP アドレスの変更

設定ファイルで CMC の IP アドレスを変更する場合は、不必要なすべての <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=192.x.x.x
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。

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 VLAN 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。また、標準文字や特殊文字も使用できます。
- 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-`
  - `Chassis`
  - `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 に対しては有効な名前ですが、スロット 4 に対しては無効な名前です。ただし `Server-03` は、どのスロットに対しても有効な名前です。

  メモ: スロット名を変更するには、**シャーシ設定管理者** 権限が必要です。

Web インターフェイ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 Web インターフェイスで行ったスロット名の設定は、iDRAC インターフェイスに表示されている名前の変更を常に上書きします。

CMC Web インターフェイ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]** の順に移動します。
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** の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 の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-4) 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。後でインストールする予定のサーバには、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設定できます。これらのデフォルトの設定が iDRAC QuickDeploy 設定です。

iDRAC の詳細については、dell.com/support/manuals で『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 15. 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 15. 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 オプションには、4 と 2 の 2 つの値があります。
予約済み QuickDeploy IP アドレス	シャーシ内で iDRAC 用に予約された静的 IPv4 アドレスの件数を選択します。**iDRAC IPv4 アドレス（スロット 1）を開始中** から始まる IPv4 アドレスは予約済みとみなされ、同じネットワーク内の他の場所では使用されないと想定されます。QuickDeploy 機能は、予約済み静的 IPv4 アドレスがないスロットに挿入されたサーバに対しては動作しません。
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` でサブネット マスクが `255.255.0.0` の場合は、スロット 4c 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際に、iDRAC に伝達された CMC DNS サーバの設定（IPv4 と IPv6）を有効にします。
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 名を適用します。iDRAC DNS プレフィックスを指定することができます。CMC によりスロット名が追加されます。たとえば、iDRAC DNS プレフィックスが「DNSNAME」の場合、iDRAC DNS 名にスロット名が追加され、「DNSNAME-SlotN」になります。 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。

表 15. QuickDeploy 設定（続き）

設定	説明
	• 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。

   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。

サーバーに対する QuickDeploy IP アドレス割り当て

次の表は、FX 2/FX2s シャーシ内にあるスレッドに基づいたサーバーへの QuickDeploy IP アドレスの割り当て方法を示したものです。

- シャーシ内に 2 台のフルワイドスレッド：

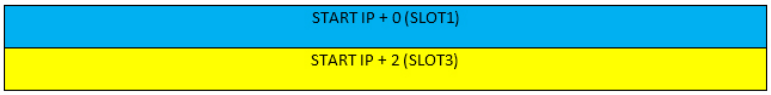


図 3. シャーシ内に 2 台のフルワイドスレッド

- シャーシ内に 4 台のハーフワイドスレッド：

図 4. シャーシ内に 4 台のハーフワイドスレッド

- シャーシ内に 8 台のクォーターワイドスレッド：

  メモ: **予約済み QuickDeploy IP アドレス**は、最低 8 に設定する必要があります。

図 5. シャーシ内に 8 台のクォーターワイドスレッド

- シャーシ内に 4 台の FM120x4 スレッド：

  メモ: **予約済み QuickDeploy IP アドレス**を 16 に設定する必要があります。

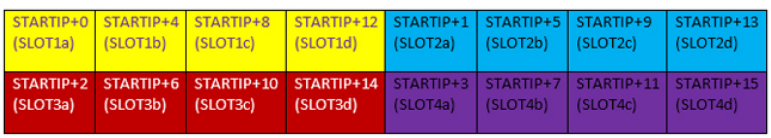


図 6. シャーシ内に 4 台の FM120x4 スレッド

- 上段列にはクォーターワイドスレッドのみ、下段列にはハーフワイドスレッドのみを搭載：

  メモ: **予約済み QuickDeploy IP アドレス**は、最低 8 に設定する必要があります。

図 7. 上段列にあるクォーターワイドスレッドと下段列にあるハーフワイドスレッド

- 上段列にはフルワイドスレッドのみ、下段列にはハーフワイドスレッドのみを搭載：

図 8. 上段列にあるフルワイドスレッドと下段列にあるハーフワイドスレッド

- 上段列にはフルワイドスレッド、下段列にはクォータースレッドのみを搭載：

  メモ: 予約済み QuickDeploy IP アドレスは、最低 8 に設定する必要があります。

図 9. 上段列にあるフルワイドスレッドと下段列にあるクォーターワイドスレッド

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、*CMC for Dell PowerEdge FX2/FX2s のオンライン 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 `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および範囲の詳細については、**dell.com/support/manuals** にある『*Dell Integrated Dell Remote Access Controller(iDRAC)RACADM コマンド ライン リファレンス ガイド*』および『*Chassis Management Controller for PowerEdge FX2/FX2s 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 VLAN タグの設定

VLAN を使用すると、複数の仮想 LAN を同じ物理ネットワークケーブル上に共存させ、セキュリティや負荷管理の目的でネットワークトラフィックを分離することができます。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。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。

メモ: CMC からの iDRAC VLAN 設定は、iDRAC での iDRAC NIC の選択がシャーシ (専用) LOM モードに設定されている場合にのみ有効となります。

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

ウェブインタフェースを使用した iDRAC VLAN タグの設定

サーバーに 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。詳細については、『CMC for Dell PowerEdge FX2/FX2s オンラインヘルプ』を参照してください。
3. 設定を保存するには、**適用** をクリックします。

RACADM を使用した iDRAC VLAN タグの設定

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

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

  <*n*> の有効値は 1~4 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 1~16 です。

  たとえば、次のとおりです。

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

最初の起動デバイスの設定

各サーバーについて、CMC の最初の起動デバイスを指定できます。これはサーバーの実際の最初の起動デバイスでなくてもよく、またそのサーバー上に存在するデバイス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設定できます。また、サーバーの最初の起動デバイスも設定できます。システムは、次回および後続の再起動時に選択されたデバイスから起動し、そのデバイスは CMC ウェブインタフェースまたは BIOS 起動順序から再び変更されない限り、BIOS 起動順序の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。

最初の起動デバイスには、次のデバイスを設定することができますが、デバイスを最初の起動デバイスとして設定するには、**デフォルト** を選択します。

サーバー上で実行されているファームウェアバージョンが最初の起動デバイスで使用可能なバージョンと同じである場合に、サーバーのファームウェアバージョンが上書きされないようにするには、**なし** を選択します。

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 16. 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	ハードディスクドライブを使用して起動します。
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。
BIOS セットアップ	BIOS セットアップ中に起動します。
仮想フロッピー	仮想フロッピーディスクから起動します。
仮想 CD/DVD	仮想 CD ドライブまたは DVD ドライブから起動します。
ローカル SD カード	ローカル SD (セキュアデジタル) カードから起動します。
リモートファイル共有	リモートファイル共有から起動します。
BIOS 起動マネージャ	BIOS 起動マネージャを使用して起動します。
Lifecycle Controller	Lifecycle Controller を使用して起動します。
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。

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 FX2s 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。

スレッドのネットワークアップリンクの設定

スレッドネットのワークアップリンクを設定することができるのは、内蔵ネットワークスイッチを搭載した PowerEdge FM120x4 スレッドのみです。

スレッドのネットワークアップリンクを設定するには、**シャーシ概要** > **サーバー概要** > **セットアップ** > **スレッドのネットワークアップリンク** の順に移動します。

スレッドのネットワークアップリンク設定プロパティで、次の値のいずれかを選択します。

- **標準 (集約)**: 4 つのすべての IOM アップリンクポートが単一のトランクグループに設定されており、すべての LOM がそのグループにマップされているアップリンク設定です。この値がデフォルトで選択されています。
- **ネットワークアダプタ隔離 (セキュリティ強化)**: 標準設定と似たアップリンク設定ですが、ローカルノード間のルーティングを設定することはできません。
- **孤立ネットワーク** : 各ノードの LOM 1 が IOM A1 に、LOM2 が IOM A2 にマップされているアップリンク設定です。
- **強化ネットワークアダプタ孤立** : マルチテナント設定でのセキュリティ強化のためのアップリンク設定です。この設定では、各ノードの LOM にマップされた専用の IOM ポートで個々のネットワークアダプタが分離されます。 各ノード上の LOM 1 のみが動作可能です。

メモ: CMC バージョン 1.3 以降からダウングレードする際に、**スレッドのネットワークアップリンク設定** が **強化ネットワークアダプタ孤立** に設定されている場合は、CMC 1.2 以前のバージョンでは、**スレッドのネットワークアップリンク設定** が空白になります。CLI では、コマンドの出力として、無効な値である「4」が表示されます。

```
$ getconfig -g cfgRacTuning -o cfgRacTuneSledNetworkUplink
```

リモートファイル共有の導入

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。

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、**サーバー概要** > **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、各フィールドに適切なデータを入力します。フィールドの説明に関する詳細については、*CMC for Dell PowerEdge FX2/FX2s のオンライン ヘルプ*を参照してください。
3. リモート ファイル共有に接続するには、[**接続**] をクリックします。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。

   前に接続した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 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。

サーバー設定複製を使用したプロファイル設定の実行

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

- BIOS — このグループにはサーバーの BIOS 設定のみが含まれます。
- BIOS および起動 — このグループには、サーバーの BIOS および起動設定が含まれます。
- 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。
  - iDRAC7 1.57.57 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 2.05.05 および Lifecycle Controller 2.00.00.00 以降を搭載した第 13 世代サーバー

サーバークローニング機能は iDRAC7 および iDRAC8 サーバーをサポートします。古い世代の RAC サーバーもリストされますが、メインページではグレー表示になり、この機能の使用には有効化されません。

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。iDRAC7 サーバーではバージョン 2.05.05、iDRAC8 サーバーでは 2.05.05 が必要です。
- 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導入する。
- 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。

プロファイルページへのアクセス

プロファイル ページを使用して、1 台または複数のサーバーに対して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 **プロファイル** ページにアクセスするには、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。**プロファイル** ページが表示されます。

保存済みプロファイルの管理

BIOS プロファイルは編集、表示、または削除することができます。保存されている CMC のプロファイルを管理するには、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. **プロファイル** ページの **プロファイルの適用** セクションで、**プロファイルの管理** をクリックします。**BIOS プロファイルの管理** ページが表示されます。

- プロファイルを編集するには、**編集** をクリックします。
- BIOS 設定を表示するには、**表示** をクリックします。
- プロファイルを削除するには、**削除** をクリックします。フィールドの説明については、『CMC for Dell PowerEdge FX2/FX2s オンラインヘルプ』を参照してください。

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: リモート共有を使用できる場合は、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。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、保存プロファイルにアクセスできなくなり、サーバークローニング機能が無効になります。

プロファイルを追加するには、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。**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。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. **プロファイル名** および **説明** フィールドに、プロファイル名と説明 (オプション) を入力し、**プロファイルの保存** をクリックします。

   メモ:

   サーバープロファイルを保存するときにプロファイル名でサポートされていない文字には、ハッシュ (#)、コンマ (,)、疑問符 (?) があります。

   標準 ASCII 拡張文字セットがサポートされており、次の特殊文字、

)、“、.、*、>、<、\、/、:、および | はサポートされません。

   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

サーバークローニングは、サーバープロファイルが CMC 上の不揮発性メディアで保存されたプロファイルとして使用できる、またはリモート共有に保存されている場合にのみ可能です。サーバークローニング操作を開始するには、保存されたプロファイルを 1 台または複数台のサーバーに適用することができます。

プロファイルの適用 表に、サーバーごとの操作ステータス、スロット番号、スロット名、モデル名が表示されます。

メモ: サーバーが 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** ページに進みます。**プロファイルの保存と適用** セクションで、選択したプロファイルを適用するサーバーを 1 台または複数台選択します。
   プロファイルの選択 ドロップダウンメニューが有効化されます。
   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、リポジトリおよび 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は現在の設定を上書きし、選択したサーバーを再起動するという警告メッセージが表示されます。操作を続行する場合は、それを確認するプロンプトが表示されます。
   メモ: サーバークローニング操作をサーバーで実行するには、サーバーに対する CSIOR オプションが有効になっている必要があります。CSIOR オプションが無効の場合、CSIOR がサーバーに対して有効になっていないという警告メッセージが表示されます。ブレードのクローニング操作を完了するためには、サーバーで CSIOR オプションを有効化するようにしてください。
4. **OK** をクリックして、選択したサーバーにプロファイルを適用します。
   選択したプロファイルがサーバーに適用されます。サーバーは、必要に応じて直ちに再起動される場合があります。詳細については、『CMC for Dell PowerEdge FX2/FX2s 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。
   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警告メッセージが表示されます。**OK** をクリックして、プロファイルのエクスポートを続行します。

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。

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. 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。
   BIOS プロファイルの編集 — <プロファイル名> セクションが表示されます。
2. 必要に応じてサーバープロファイルの名前と説明を編集し、**プロファイルの編集** をクリックします。

   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、『*Online Help*』（オンラインヘルプ）を参照してください。

メモ: CMC サーバー設定複製機能は、**Collect System Inventory on Restart (CSIOR)**）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、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。

CSIOR を有効にするには、次の手順を実行します。

1. 第 12 世代サーバー — サーバーを再起動した後、F2 セットアップから、**iDRAC 設定** > **Lifecycle Controller** を選択して **CSIOR** を有効にし、変更を保存します。
2. 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 キーを押して、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**と選択して、**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、**再起動時のシステムインベントリの収集**をクリックします。

保存済み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 **プロファイルの表示** 列で **表示** をクリックします。**設定の表示** ページが表示されます。表示された設定に関する詳細については、*CMC for Dell PowerEdge FX2/FX2s のオンライン ヘルプ*を参照してください。

プロファイルログの表示

プロファイルログを表示するには、**サーバープロファイル** ページで、**最近のプロファイルログ** セクションを確認します。このセクションは、サーバークローニング操作から直接 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、サーバー設定レプリケーション操作提出の日時、およびレプリケーションログメッセージの説明が表示されます。ログエントリは、RAC ログでも使用可能です。その他のエントリを表示するには、**プロファイルログに移動** をクリックします。**プロファイルログ** ページが表示されます。詳細については、*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** の順にクリックします。
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** の順にクリックします。**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ついては、「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、特定のサーバーでの iDRAC Lifecycle Controller の Lclogview の結果を表示します。
   特定のサーバーでの操作完了または失敗の結果表示は、iDRAC Lifecycle Controller 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**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。**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 カードに含まれています。

メモ: Quick Deploy 用プロファイル をセットアップするには、**シャーシ管理者** 権限が必要です。

サーバープロファイルのスロットへの割り当て

サーバープロファイル ページでは、サーバープロファイルをスロットへ割り当てることができます。プロファイルをシャーシスロットへ割り当てるには、以下の手順を実行します。

1. **サーバープロファイル** ページで、**QuickDeploy 用のプロファイル** セクションをクリックします。
   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: Quick Deploy 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したスロットに適用されます。

メモ: FM120x4 スレッドが挿入されると、サーバースロットに割り当てられている保存されたプロファイルが、4 台のサーバーすべてに適用されます。

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 XML 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展開されるときは、アプリケーションの進捗と結果がプロファイルログに維持されます。

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。

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、『*Dell PowerEdge FX2/FX2s 向け 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 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を提供します。

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。iDRAC サイトの表示後、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、iDRAC のアカウントを持たない同じユーザーや、アカウントに管理者権限のない場合でも同様です。
- サーバーの管理者権限を **持たない** CMC ユーザーでも、iDRAC に同じアカウントがある場合は、シングル サインオンで iDRAC に自動ログインできます。iDRAC のサイトが表示されたら、iDRAC アカウントに対して作られた権限が許可されます。
- サーバーの管理者権限を持たない CMC ユーザーでも、iDRAC に同じアカウントがある場合は、シングル サインオンで iDRAC に自動ログインできます。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 にパスワードが一致する同じログイン名を持っているということです。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た
- iDRAC の IP アドレスが変更された
- iDRAC ネットワーク接続にエラーが発生した

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 GUI の起動** をクリックします。
   iDRAC Web インタフェースが表示されます。フィールドの説明についての情報は、『CMC for Dell PowerEdge FX2/FX2s 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。

サーバーステータスページからのリモートコンソールの起動

個別にサーバーのリモートコンソールを起動するには：

1. 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。

メモ: リモートコンソールの起動 ボタンまたはリンクが有効になるのは、サーバーに Enterprise ライセンスがインストールされている場合のみです。

8

ストレージスレッドの設定

FX2s シャーシで使用されるハーフ幅ストレージスレッドには以下が含まれます。

- 1 つまたは 2 つの RAID コントローラ
- 最大 16 台のディスクドライブ

2 つの RAID コントローラが格納されている個々のストレージスレッドを、次のモードで動作するように設定できます。

- スプリットシングル
- スプリットデュアル
- 結合

メモ: シャーシのスロット 1 はストレージスレッドのための有効な場所ではないため、ストレージスレッドを挿入しないようにしてください。

メモ: 本項は、デュアルコントローラストレージモジュールにのみ適用されます。

メモ: iDRAC Comprehensive Embedded Management（CEM）を使用して、ストレージ スレッドの設定とモニターを行うこともできます。詳細については、『*Integrated Dell Remote Access Controller（iDRAC）ユーザーズ ガイド*』を参照してください。

トピック：

スプリットシングルモードのストレージスレッドの設定

スプリットシングルモードでは、2 台の RAID コントローラが 1 つのコンピュートスレッドにマップされます。両方のコントローラが有効で、各コントローラは 8 台のディスクドライブに接続されます。

スプリットデュアルモードでのストレージスレッドの設定

スプリットデュアルモードでは、ストレージスレッドの両方の RAID コントローラが 2 つのコンピュートスレッドに接続されます。

ストレージスレッドがフル幅の PowerEdge FC830 スレッドの下に取り付けられている場合は、スプリットデュアルモードで構成できます。ただし、コントローラは 1 台のコンピュートスレッドにのみ接続され、そのコンピュートスレッドのみが報告されます。

ストレージスレッドがデュアルモードで設定され、2 台のコンピュートスレッドに接続できない場所にある場合、2 番目のコントローラはどのコンピュートスレッドにも接続されません。

設定を変更するには、**シャーシ設定管理者** 権限を持っている必要があり、コンピュートスレッドの電源をオフにする必要があります。

結合モードでのストレージスレッドの構成

結合モードでは、RAID コントローラは単一のコンピュートスレッドにマップされます。ただし、1 つのコントローラだけが有効化され、すべてのディスクドライブはそのコントローラに接続されます。

CMC ウェブインタフェースを使用したストレージスレッドの設定

1. 左ペインで、**シャーシ概要** > **サーバー概要** をクリックし、ストレージスレッドをクリックします。
   ストレージスレッドの詳細が表示されます。
2. 右側のメニューから、 **設定** をクリックします。
   ストレージ設定 ページが表示されます。

   シャーシの正常性 ページ上でストレージスレッドを選択することで、**ストレージ設定** ページにアクセスすることもできます。**クイックリンク** で、 **ストレージアレイのセットアップ** をクリックしてください。
3. **コンポーネント** で、次のオプションの 1 つを選択します。
   - **分割デュアルホスト**
   - **分割シングルホスト**
   - **結合**

   メモ: ストレージスレッドを設定する前に、コンピュートスレッドの電源をオフにします。ページの一番上の **サーバーの電源制御** をクリックして、コンピュートスレッドの電源をオフにします。詳細については、オンラインヘルプを参照してください。
4. **適用** をクリックします。

RACADM を使用したストレージスレッドの設定

`config` または `getconfig` RACADM コマンドと `cfgStorageModule` オプションを使用して、ストレージ スレッドとコンピュート スレッドを接続できます。詳細については、**dell.com/support/manuals** にある『*Chassis Management Controller for PowerEdge FX2/FX2s RACADM コマンド ライン リファレンス ガイド*』の「**getstoragemoduleinfo**」の項を参照してください。

iDRAC RACADM プロキシを使用したストレージスレッドの管理

iDRAC RACADM プロキシ機能を使用すると、CMC がネットワークにない場合に、iDRAC RACADM を介して FX2s シャーシのストレージスレッドを管理できます。

ローカルで iDRAC にアクセスするには、次のコマンドを使用します。

```
racadm <command> --proxy
```

例：`racadm getractime --proxy`

iDRAC RACADM にリモートからアクセスすることもできます。詳細については、『*Integrated Dell Remote Access Controller 8 (iDRAC8) バージョン 2.10.10.10 RACADM コマンド ライン インターフェイス リファレンス ガイド*』の「*RACADM プロキシ*」の項を参照してください。

メモ: 今回のリリースでサポートされるのは、ローカルおよびリモート RACADM プロキシのみです。

ストレージアレイステータスの表示

左ペインで、**シャーシ概要** > **サーバー概要** > **< ストレージスレッド >** をクリックします。 右ペインに **ストレージアレイステータス** ページが表示されます。**ストレージアレイの状態** ページに **シャーシの正常性** ページからアクセスすることもできます。

1. **シャーシの正常性** ページで、前面パネルの画像にあるストレージスレッドをクリックします。
   ストレージスレッドの詳細が右ペインの下部に表示されます。
2. **クイックリンク** で、**ストレージアレイステータス** を選択します。

詳細については『オンラインヘルプ』を参照してください。

9

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。システムコンポーネントの状態が事前定義された状態を超過すると、イベントが発生します。イベントがイベントフィルタに一致し、そのフィルタがアラートメッセージ (E-メールアラートまたは SNMP トラップ) を生成するように設定されている場合、アラートが E-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

設定された送信先にアラートを送るには、グローバルアラートオプションを有効にする必要があります。このプロパティは個々のアラート設定を上書きします。

SNMP または E-メールアラートの送信先がアラートを受信するように設定されていることを確認してください。

CMC ウェブインタフェースを使用したアラートの有効化または無効化

アラートの生成を有効化または無効化するには、次の手順を実行します。

1. 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。

RACADM を使用したアラートの有効化または無効化

アラートの生成を有効または無効にするには、`cfgAlertingEnable` RACADM オブジェクトを使用します。詳細については、『*Dell Chassis Management Controller for PowerEdge FX2/FX2s 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。

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。

メモ: SNMP プロトコルとトラップの形式の設定についての詳細は、『*Dell Chassis Management Controller for PowerEdge FX2/FX2s 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 SNMP トラップアラート送信先の設定

CMC ウェブインタフェースを使用して IPv4 または IPv6 アラート宛先を設定するには、次の手順を実行します。

1. システムツリーで**シャーシ概要**に移動し、**アラート** > **トラップ設定**をクリックします。
   シャーシイベントアラート送信先 ページが表示されます。
2. 以下を入力します。
   - **送信先** フィールドに、有効な IP アドレスを入力します。ドットで 4 つに区切られた IPv4 フォーマット、標準 IPv6 アドレス表記、または FQDN (例 : `123.123.123.123`、`2001:db8:85a3::8a2e:370:7334`、または `dell.com`) を使用してください。

     ネットワーキング技術またはインフラストラクチャと一貫性のあるフォーマットを選択します。テストトラップ 機能では、現在のネットワーク設定に不適当な選択項目は検出されません (IPv4 専用の環境で IPv6 送信先を使用する場合など)。
   - **コミュニティ文字列** フィールドに、 送信先管理ステーションが属する有効なコミュニティ文字列 を入力します。

     このコミュニティ文字列は、**シャーシ** > **ネットワーク** > **サービス** ページのコミュニティ文字列とは異なります。SNMP トラップのコミュニティ文字列は、CMC が管理ステーション宛の送信トラップに使用するものです。**シャーシ** > **ネットワーク** > **サービス** ページのコミュニティ文字列は、管理ステーションが CMC の SNMP デーモンにクエリを行うために使用します。

     メモ: CMC はデフォルトの SNMP コミュニティ文字列に public を使用しています。高いセキュリティを確保するため、デフォルトのコミュニティ文字列を変更し、空以外の値を設定することをお勧めします。
   - **有効** で、トラップ受信用に有効にする IP アドレスの、送信先 IP に対応するチェックボックスを選択します。IP アドレスは最大 4 つまで指定できます。
3. 設定を保存するには、**適用** をクリックします。
4. IP アドレスが SNMP トラップを受信しているかどうかを確認するには、**SNMP トラップのテスト** 列の **送信** をクリックします。

   IP アラート送信先が設定されます。

RACADM を使用した SNMP トラップアラート送信先の設定

RACADM を使用して IP アラート送信先を設定するには、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-メールアラートの両方とも、設定できるフィルタマスクは 1 つだけです。フィルタマスクを既に選択している場合は、手順 2 を省略することができます。
2. アラートの生成を有効にします。

   ```
   racadm config -g cfgAlerting -o cfgAlertingEnable 1
   ```
3. 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。
4. 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 3 で指定したインデックス値です。

5. 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。

メモ: CMC はデフォルトの SNMP コミュニティ文字列に public を使用しています。高いセキュリティを確保するため、デフォルトのコミュニティ文字列を変更し、空以外の値を設定することをお勧めします。

トラップアラートの送信先 IP アドレスは 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 2~5 を繰り返します。

メモ: 手順 2~5 のコマンドは、指定されたインデックス (1~4) の既存設定のすべてを上書きします。インデックスに以前設定した値があるかどうかを判断するには、racadm getconfig -g cfgTraps -i <index> を入力します。インデックスが設定されていると、cfgTrapsAlertDestIPAddr および cfgTrapsCommunityName オブジェクトに対して値が表示されます。

6. アラート送信先へのイベントトラップをテストするには、次を入力します。

```
racadm testtrap -i <index>
```

ここで、<index> は 1~4 の値で、テストするアラート送信先を表します。

インデックス番号がわからない場合は、次を入力します。

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

E-メールアラートの設定

CMC が環境についての警告やコンポーネント障害などのシャーシイベントを検出した場合、1 つ、または複数の E-メールアドレスに E-メールアラートを送信するように設定できます。

CMC の IP アドレスから送信された E-メールを受け入れるように SMTP E-メールサーバーを設定する必要があります。この機能は通常、セキュリティ上、ほとんどのメールサーバーでオフになっています。これをセキュアな方法で行うための手順は、SMTP サーバーに同梱のマニュアルを参照してください。

メモ: メールサーバーが Microsoft Exchange Server 2007 である場合、CMC 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 CMC ドメイン名が設定されていることを確認してください。

メモ: E-メールアラートは IPv4 および IPv6 アドレスの両方をサポートします。IPv6 を使用する場合には、DRAC DNS ドメイン名を指定する必要があります。

ご利用のネットワークに定期的に IP アドレスを解放し、異なるアドレスで更新する SMTP サーバーが存在する場合、指定した SMTP サーバーの IP アドレスが変更されるときに、このプロパティ設定が機能しない期間が生じます。そのような場合は、DNS 名を使用してください。

CMC ウェブインタフェースを使用した E-メールアラートの設定

ウェブインタフェースを使用して E-メールアラートを設定するには、次の手順を実行します。

1. システムツリーで **シャーシ概要** に移動し、**アラート** > **電子メールアラート設定** をクリックします。
2. アラートの受信用 SMTP E-メールサーバー設定および E-メールアドレスを指定します。フィールドの詳細については、『CMC オンラインヘルプ』を参照してください。
3. 設定を保存するには、**適用** をクリックします。
4. **E-メールのテスト** で **送信** をクリックして、指定した E-メールアラートの宛先にテスト E-メールを送信します。

RACADM を使用した E-メールアラート設定の設定

RACADM を使用して、テスト E-メールをアラートの送信先 E-メールアドレスに送信するには、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
```

3. 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 はインデックス番号を用いて、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。

4. 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。

5. 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 メール名に使用できるのは 32 文字以内の、英数字、ハイフン、下線、ピリオドです。スペースは使用できません。

6. SMTP ホストを設定します。

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

ここで host.domain は FQDN です。

E メール アラートを受け取る送信先 E メール アドレスは、最大 4 件設定できます。E メール アドレスをさらに追加するには、手順 2~5 を繰り返します。

メモ: 手順 2~5 のコマンドは、指定するインデックス (1~4) の既存設定をすべて上書きします。インデックスに以前設定された値があるかどうかを判断するには、「xracadm getconfig -g cfgEmailAlert – I *<index>*」と入力します。インデックスが設定済みの場合は、cfgEmailAlertAddress および cfgEmailAlertEmailName オブジェクトの値が表示されます。

詳細については、**dell.com/support/manuals** で入手可能な『*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。

10

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、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 はデフォルトのルートアカウントで設定されています。管理者は、他のユーザーによる CMC へのアクセスを許可するようにユーザーアカウントを設定することができます。

最高 16 のローカルユーザーをセットアップしたり、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、追加のユーザーアカウントをセットアップできます。ディレクトリサービスの使用は、認証されたユーザーアカウントを管理するための中心点を提供します。

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 ユーザーに**サーバ管理者**権限が付与されている場合を除き、CMC ユーザーに付与された権限がサーバ上の同じユーザーに自動的に転送されるわけではありません。つまり、CMC Active Directory ユーザーと iDRAC Active Directory ユーザーは、Active Directory ツリーの異なるブランチに位置している、ということです。ローカルサーバユーザーを作成するには、ユーザー設定で直接サーバにログインする必要があります。ユーザー設定では、CMC からサーバユーザーを作成することもその逆も実行できません。このルールにより、サーバのセキュリティと整合性が保護されます。

表 17. 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。 ユーザーには、CMC ログインユーザー権限がなくとも他の権限を付与することが可能です。この機能は、ユーザーが一時的にログインを禁止されている場合に便利です。そのユーザーの CMC ログインユーザー権限が復元しても、その前に与えられていた他の権限はすべて保持されます。
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に適用されますが、正確にはサーバそのものではなく、スロットに関連付けられるシャーシプロパティです。そのため、サーバがスロットにあるかどうかに関係なく、スロット名とスロットの優先順位を追加または変更できます。 • AD 証明書の管理、AD グループ、ドメイン、権限の設定など、Active Directory（AD）に関連付けられています。

表 17. 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。以前のスロット名と優先順位は、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**権限が付与されている CMC ユーザーは電源設定を行うことができます。ただし、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**権限が付与されている CMC ユーザーは、電源関連の操作をすべて行うことができます。電源オン、電源オフ、パワーサイクルなどのシャーシ電力操作を制御できます。 **メモ:** 電源設定を行うには、**シャーシ設定システム管理者** 権限が必要です。
Server Administrator	これは、CMC ユーザーにシャーシ内に存在する任意のサーバー上の任意の操作を実行する全権利を与える包括的な権限です。 **サーバシステム管理者**権限が付与されているユーザーがサーバ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に送信します。つまり、**サーバシステム管理者**権限は、サーバにおけるシステム管理者権限の欠如を無視します。 **サーバーシステム管理者** 権限がない場合、シャーシで作成されたユーザーは以下のすべての条件が満たされた場合にのみ、サーバー上でコマンドを実行することができます。 • 同じユーザー名がサーバー上に存在する • サーバー上の同じユーザー名は同じパスワードが所有する必要がある。 • ユーザーはコマンドを実行する権限を持っている **サーバシステム管理者**権限が付与されていない CMC ユーザーがサーバ上で実行する処置を発行する場合、CMC はユーザーのログイン名とパスワードを入力して対象のサーバにコマンドを送信します。ユーザーがサーバ上に存在しない場合、またはパスワードが一致しない場合、ユーザーは処置を実行できません。 ユーザーが対象のサーバに存在し、パスワードが一致する場合、サーバはユーザーがそのサーバ上でが付与されている権限を返します。CMC ファームウェアはサーバ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判断します。
	次のリストに、サーバシステム管理者に付与されているサーバ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： • 電源オン

表 17. ユーザータイプ（続き）

権限	説明
	• 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。

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 18. 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 19. 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

表 19. 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（続き）

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
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

root 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 ユーザーを追加して設定するには、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 を設定している場合、または RACADM の `racresetcfg` コマンドを使用した場合、唯一の現行ユーザーアカウントはデフォルトのルートアカウントです。`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。

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 20. : 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。

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。

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。

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。

CMC にアクセスするための汎用 LDAP ディレクトリの設定

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。

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。

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

       < *Search Domain* > はクエリ内で使用するルートレベルドメイン、< *Service Name* > はクエリ内で使用するサービス名です。

       例えば次のようになります。

       ```
       _ldap._tcp.dell.com
       ```

       `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. **証明書の検証有効** オプションを選択した場合、 **証明書の管理** セクションで、SSL ハンドシェイク中に LDAP サーバー証明書を検証する CA 証明を指定し、**アップロード** をクリックします。証明書が CMC にアップロードされ、詳細が表示されます。
9. **適用** をクリックします。
   汎用 LDAP ディレクトリサービスが設定されました。

RACADM を使用した汎用 LDAP ディレクトリサービスの設定

ディレクトリサービスを設定するには、`cfgLdap` および `cfgLdapRoleGroup` RACADM グループにあるオブジェクトを使用します。

LDAP ログインの設定には、数多くのオプションがあります。大半の場合、デフォルト設定とともにいくつかのオプションを使います。

メモ: 初めてのセットアップで LDAP 設定をテストするには、`testfeature -f LDAP` コマンドを使用することをお勧めします。この機能は、IPv4 と IPv6 を両方サポートします。

必要なプロパティの変更には、LDAP ログインの有効化、サーバー FQDN または IP の設定、LDAP サーバーのベース DN の設定があります。

- ```
  $ racadm config -g cfgLDAP -o cfgLDAPEnable 1
  ```
- ```
  $ racadm config -g cfgLDAP -o cfgLDAPServer 192.168.0.1
  ```
- ```
  $ racadm config -g cfgLDAP -o cfgLDAPBaseDN dc=
  company,dc=com
  ```

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** で入手可能の『Dell Chassis Management Controller for PowerEdge FX2/FX2s 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。
```

11

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 Kerberos レルムとキー配付センター (KDC) の設定。
- クロックドリフトやリバースルックアップに伴う問題を回避するための強固な NTP および DNS インフラストラクチャ。
- 承認済みメンバーのある Active Directory 標準スキーマ役割グループに対する CMC の設定
- スマートカード用には、各 CMC の Active Directory を作成し、事前認証でなく Kerberos DES 暗号化を使用できるように設定します。
- SSO またはスマートカードのログインに使用するブラウザの設定
- Ktpass を使用して CMC ユーザーをキー配付センターに登録します(これにより、CMC にアップロードするキーも出力されます)。

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、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 の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。

```
C:\>ktpass -princ HTTP/cmcname.domain_name.com@REALM_NAME.COM - mapuser dracname -mapOp
set -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 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 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。

スマートカードでログインするためのブラウザの設定

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。

RACADM を使用した Active Directory ユーザー用 CMC SSO ログインまたはスマートカードログインの設定

SSO を有効にするには、Active Directory の設定中に実行する手順への追加として、次のコマンドを実行します。

```
racadm 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

ウェブインタフェースを使用した Active Directory ユーザーの CMC SSO またはスマートカードログインの設定

CMC での Active Directory SSO またはスマートカードログインを設定するには、次の手順を実行します。

メモ: オプションの詳細については、『*CMC for Dell PowerEdge FX2/FX2s オンラインヘルプ*』を参照してください。

1. ユーザーアカウントをセットアップするために Active Directory を設定する際に、次の追加手順を実行します。
   - 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 が 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『*Dell Chassis Management Controller for PowerEdge FX2/FX2s 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 ファイルのアップロードに成功または失敗したかを通知するメッセージが表示されます。

RACADM を使用した Active Directory ユーザー用 CMC SSO ログインまたはスマートカードログインの設定

SSO を有効にするには、Active Directory の設定中に実行する手順への追加として、次のコマンドを実行します。

```
racadm 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

12

コマンドラインコンソールを使用するための CMC の設定

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 FX2/FX2s 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 21. 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、『Dell Chassis Management Controller for PowerEdge FX2/FX2s 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 IO 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置を実行し、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。

管理ステーションで Microsoft Windows XP または Microsoft Windows Server 2003 を実行している場合は、CMC の telnet セッションで文字の不具合が発生する可能性があります。リターンキーが応答しなかったり、パスワードプロンプトが表示されないログインのフリーズ状態として発生することがあります。

この問題を解決するには、**support.microsoft.com** からホットフィックス 824810 をダウンロードします。詳細については、Microsoft サポート技術情報の記事 824810 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備えたコマンドラインセッションですが、セキュリティ強化のためのセッションネゴシエーションと暗号化を備えています。CMC は、パスワード認証付きの SSH バージョン 2 をサポートしており、デフォルトで SSH が有効になっています。

メモ: CMC は SSH バージョン 1 をサポートしていません。

CMC ログイン中にエラーが発生した場合は、SSH クライアントがエラーメッセージを発行します。メッセージのテキストはクライアントによって異なり、CMC では制御されません。エラーの原因を特定するには、RACLog メッセージを確認してください。

メモ: `OpenSSH` は Windows の VT100 または ANSI ターミナルエミュレータから実行する必要があります。また、`Putty.exe` を使用して `OpenSSH` を実行することもできます。Windows のコマンドプロンプトでの `OpenSSH` の実行は、完全に機能しません (一部のキーが応答せず、グラフィックが表示されません)。Linux を実行するサーバーでは、SSH クライアントサービスを実行し、いずれかのシェルで CMC に接続します。

SSH は 4 セッションの同時実行がサポートされています。セッションタイムアウトは、`cfgSsnMgtSshIdleTimeout` プロパティによって制御されます。RACADM コマンドの詳細については、dell.com/support/Manuals で入手可能の『Dell 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 では、SSH 経由の公開キー認証 (PKA) もサポートされています。この認証方法は、ユーザー ID/ パスワードの組み込みや入力を排除することで SSH スクリプトの自動化を改善します。

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。

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 22. 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 • 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 インターフェイス経由でサービス ユーザー名と併用できる公開キーは、最大 6 個まで設定できます。意図しないキーの上書きや削除を防止するため、公開キーを追加または削除する際は、事前に `view` コマンドを用い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、キーの追加先インデックスに、既存のキーが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の確認は行われません。SSH インターフェイ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、RACADM `getssninfo` コマンド使用時における SSH ユーザーの識別に、CMC では公開キー コメントが使用されます。

たとえば、コメント PC1 およびコメント PC2 を持つ 2 つの公開キーが設定されている場合は、次のようになります。

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

`sshpkauth` の詳細については、『*Chassis Management Controller for PowerEdge FX2/FX2s 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。

ターミナルエミュレーションソフトウェアの設定

CMC は、どのターミナルエミュレーションソフトウェアによっても起動可能なシリアルテキストコンソールをサポートしてます。CMC への接続に使用できるターミナルエミュレーションソフトウェアの例は次のとおりです。

1. Linux Minicom
2. Hilgraveve's HyperTerminal for Windows

シリアル Null モデムケーブル (両端に存在) の一方をシャーシ背面のシリアルコネクタに接続し、ケーブルのもう一方を管理ステーションのシリアルポートに接続します。ケーブル接続についての詳細は、「シャーシ概要」の項でシャーシ背面パネルを参照してください。

次のパラメータを使用してターミナルエミュレーションソフトウェアを設定します。

- **ボーレート** : 115200
- **ポート** : COM 1
- **データ** : 8 ビット
- **パリティ** : なし
- **停止** : 1 ビット
- **ハードウェアフロー制御** : はい
- **ソフトウェアフロー制御** : いいえ

connect コマンドを使用したサーバ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 FX2/FX2s 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、サーバまたは I/O モジュールへのシリアル接続を確立するために、CMC で `connect` コマンドがサポートされています。サーバシリアルコンソールには、BIOS の起動画面とセットアップ画面の両方、および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を利用できます。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` オプションが接続されたままとなります。この接続はセキュリティリスクとなる可能性があります。

メモ: `connect` コマンドには、`-b`（バイナリ）オプションがあります。`-b` オプションはバイナリのローデータを渡し、`cfgSerialConsoleQuitKey` は使用しません。さらに、CMC シリアルコンソールを使用してサーバに接続した場合、DTR 信号が遷移しても（デバッガを接続するためにシリアルケーブルを取り外した場合など）、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ていない場合、`connect` コマンドは空のコンソールを表示します。その場合、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の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 23. 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
A2	switch-a2 または switch- 2

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（PowerEdge FM120x4 の場合）または 1~8（PowerEdge FC630 の場合）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` コマンドにより、ユーザーによるサーバ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、サーバの BIOS セットアップでシリアルリダイレクトが有効化されている必要があります。また、ターミナルエミュレータウィンドウを 80 x 25 に設定しておく必要もあります。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、どのキーも動作しません。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のための管理下サーバー BIOS の設定

iDRAC7 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『Dell Integrated Dell Remote Access Controller（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

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
```

iDRAC RACADM プロキシを使用した CMC の管理

CMC がネットワーク上にない場合、iDRAC RACADM プロキシを使用して CMC を管理することができます。次の表は、プロキシの操作のための、iDRAC 権限への CMC 権限のマッピングを示しています。

表 24. CMC-iDRAC 特権のマッピング

CMC 特権	プロキシの操作に必要な iDRAC 特権
CMC ログインユーザー	iDRAC ログイン
シャーシ設定システム管理者	iDRAC の設定
ユーザー設定システム管理者	iDRAC でのユーザー設定
ログのクリアシステム管理者	ログ
シャーシ制御システム管理者	システム制御
Server Administrator	システム制御

表 24. CMC-iDRAC 特権のマッピング（続き）

CMC 特権	プロキシの操作に必要な iDRAC 特権
テストアラートユーザー	システム操作
デバッグコマンドシステム管理者	デバッグ
Fabric x Administrator（x は A、B、または C）	システム制御

詳細については、『*Dell Chassis Management Controller Version 2.0 for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*』（PowerEdge FX2/FX2s 向け Dell Chassis Management Controller バージョン 2.0 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。

13

FlexAdress および FlexAddress Plus カードの使用

本項は、FlexAddress についての情報、および FlexAddress Plus カードを使用した FlexAddress の設定方法について説明します。

メモ: FlexAddress はライセンス対象機能です。この機能ライセンスは、Enterprise ライセンスに含まれています。

トピック：

FlexAddress について

FlexAddress では、CMC が WWN/MAC ID を特定のスロットに割り当て、工場出荷時の ID を上書きすることが可能になります。従って、サーバーモジュールが交換されてもスロットベースの WWN/MAC ID は変わりません。この機能によって、新規サーバーモジュールのために各種ファブリックのイーサネットネットワーク管理ツール、SAN リソース、DHCP サーバー、およびルーターを再設定する必要がなくなります。

すべてのサーバーモジュールには製造プロセスの一環として固有の WWN および / または MAC ID が割り当てられます。FlexAddress 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 ID が変更され、新規サーバーモジュールを識別するためにはイーサネット管理ツールおよび SAN リソースを再設定する必要がありました。

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、そのサーバーで新しいスロットに対する FlexAddress 機能が有効になっていない限り、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、サーバー割り当てのアドレスに戻ります。

さらに、*上書き*処置は、FlexAddress が有効になったシャーシにサーバーモジュールを挿入した場合にのみ行われるため、サーバーモジュールに恒久的な変更は行われません。サーバーモジュールを FlexAddress 非対応のシャーシに移動した場合は、工場出荷時に割り当てられた WWN/MAC ID が使用されます。

CMC FX2/FX2S シャーシは、FlexAddress、FlexAddress Plus、および拡張ストレージ機能をサポートする FlexAddress Plus SD カードと共に出荷されています。

メモ: FlexAddress Plus 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。

メモ: FlexAddress Plus 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 FlexAddress Plus SD カードを使用することはできません。

FlexAddress Plus について

各 FlexAddress Plus 機能カードには、シャーシがワールドワイド名 / メディアアクセスコントロール (WWN/MAC) アドレスをファイバチャネルおよび Ethernet デバイスに割り当てることを可能にする、固有の WWN/MAC のプールが含まれています。シャーシが割り当てた WWN/MAC アドレスは、グローバルに固有のアドレスで、サーバースロットに特有のものです。

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 範囲の合計を特定するには、次の式を使用します。

```
<mac_start> + <mac_count> - 1 = <mac_end>
```

たとえば、次のとおりです。

```
(starting_mac)00:18:8B:FF:DC:FA + (mac_count)0xCF – 1 = (ending_mac)00:18:8B:FF:DD:C8
```

メモ: USB メモリカードリーダーに SD カードを挿入する際、SD カードの内容が誤って変更されないように事前にロックしてください。CMC に挿入する前に SD カードのロックを*解除する必要*があります。

FlexAddress 有効化の検証

FlexAddress 機能のアクティブ化状態を表示するには、次の RACADM コマンドを実行します。

```
racadm featurecard -s
```

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

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

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

シャーシ上にアクティブな機能が存在しない場合、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

```
racadm feature -s
No features active on the chassis
```

SD カード情報を表示するには、次のコマンドを使用します。

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

表 25. 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.	SD カードが正しく挿入されていること CMC で確認してください。
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。

表 25. 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
`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。

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、『*Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM コマンドラインリファレンスガイド*』を参照してください。

FlexAddress の非アクティブ化

RACADM コマンドを使用して、FlexAddress 機能を非アクティブ化し、SD カードを取り付け前の状態に戻すことができます。ウェブインタフェースには、非アクティブ化機能はありません。非アクティブ化すると、SD カードは別のシャーシ内に装着し、アクティブ化することが可能な元の状態に戻ります。この文脈では、用語 FlexAddress は FlexAddress と FlexAddressPlus の両方を意味します。

メモ: SD カードは、物理的に CMC に取り付ける必要があります。また、非アクティブ化コマンドを実行する前に、シャーシの電源をオフにする必要があります。

SD カードが取り付けられていない状態、または異なるシャーシからのカードが取り付けられている状態で非アクティブ化コマンドを実行すると、この機能は非アクティブ化されますが、そのカードに対して変更は行われません。

FlexAddress 機能を非アクティブ化し、SD カードを復元するには、次の RACADM コマンドを使用します。

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

正常に非アクティブ化されると、コマンドが次の状態メッセージを返します。

```
feature FlexAddress is deactivated on the chassis successfully.
```

シャーシの電源がオフになっていない状態でコマンドを実行すると、コマンドが次のエラーを返します。

```
ERROR: Unable to deactivate the feature because the chassis is powered ON
```

メモ: FlexAddress 機能を再度有効にするには、CMC を再起動します。

このコマンドの詳細については、『*Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM コマンドラインリファレンスガイド*』の **機能** コマンドの項を参照してください。

FlexAddress の設定

FlexAddress はオプションのアップグレードで、工場出荷時にサーバーモジュールに割り当てられた WWN/MAC ID を、シャーシ提供の WWN/MAC ID に置き換えることを可能にします。

メモ: `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についてのデータは、**dell.com/cmcmanuals** から入手可能の『*Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM コマンドラインリファレンスガイド*』を参照して下さい。

設定を始める前に、サーバーの電源を切る必要があります。FlexAddress はファブリック単位で有効化または無効化できます。さらに、この機能はスロット単位でも有効化または無効化が可能です。ファブリック単位で機能を有効化した後、有効化するスロットを選択できます。例えば、ファブリック A が有効化されていると、有効化されたスロットではいずれもファブリック A でのみ FlexAddress が有効になります。その他すべてのファブリックは、サーバーで工場出荷時割り当ての WWN/MAC を使用します。

メモ: FlexAddress 機能が特定のサーバーモジュール上に初めて導入されたときは、FlexAddress を有効にするために電源切断および投入シーケンスが必要です。イーサネットデバイスの FlexAddress はサーバーモジュール BIOS によってプログラムされます。サーバーモジュール BIOS がアドレスをプログラムするには、サーバーモジュール BIOS が動作可能である必要があり、これにはサーバーモジュールに電源投入する必要があります。電源切断および投入シーケンスが完了すると、シャーシ割り当ての MAC ID が Wake-On-LAN (WOL) 機能用に使用できるようになります。

シャーシレベルのファブリックおよびスロット用 FlexAddress の設定

FlexAddress 機能は、ファブリックおよびスロット用にシャーシレベルで有効化または無効化することができます。FlexAddress は、ファブリックごとに有効化され、次に機能に参加させるスロットが選択されます。FlexAddress を正常に設定するには、ファブリックおよびスロットの両方が有効化されている必要があります。

ワールド ワイド名またはメディア アクセス コントロール ID 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 コントロール (MAC) アドレスを確認します。

コマンドメッセージ

次の表に、RACADM コマンドと、一般的な FlexAddress 状況における出力をリストします。

表 26. FlexAddress コマンドと出力

状況	コマンド	出力
CMC モジュール内の SD カードが別のサービスタグにバインドされている。	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)` `FlexAddress: bound to another chassis, svctag = <Service tag Number> SD card SN = <Valid flex address serial number>`
同じサービスタグにバインドされている CMC モジュール内の SD カード。	`$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 CMC モジュール内の SD カード。	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)` `FlexAddress:not bound`
何らかの理由でシャーシに FlexAddress 機能がない (シャーシ上 SD カードが挿入されていない / SD カードが破損している / 機能の非アクティブ化後 / SD カードが異なるシャーシにバインドされている)。	`$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>]`	`ERROR: Insufficient user privileges to perform operation`

表 26. FlexAddress コマンドと出力（続き）

状況	コマンド	出力
	`$racadm setflexaddr [-i <slot#> <slotstate>]`	
シャーシの電源がオンの状態での FlexAddress 機能の無効化。	`racadm feature -d -c flexaddress`	`ERROR: Unable to deactivate the feature because the chassis is powered ON`
ゲストユーザーがシャーシ上の機能の無効化を試みる。	`racadm feature -d -c flexaddress`	`ERROR: Insufficient user privileges to perform operation`
サーバーモジュールの電源がオンの状態で、スロット / ファブリックの FlexAddress 設定を変更する。	`$racadm setflexaddr -i 1 1`	`ERROR: Unable to perform the set operation because it affects a powered ON server`
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。	`$racadm setflexaddr -i<slotnum> <status>` `$racadm setflexaddr -f<FabricName> <status>`	`ERROR: SWC0242 : A required license is missing or expired. Obtain an appropriate license and try again, or contact your service provider for additional details.` **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。

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管理ファブリックの一部とみなされ、残りのファブリックと共に表示されます。
- コンポーネントに対するチェックマークは、ファブリックで FlexAddress または FlexAddressPlus が有効になっ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、iSCSI、FCoE など。
- シャーシ内スロットのファイバチャネルワールドワイド名 (WWN) 設定および MAC (メディアアクセスコントロール) 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)。緑のチェック 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応じて MAC アドレスをフィルタリングし、そ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用いると、特定スロットの WWN/MAC アドレス情報を [**FlexAddress**] ページに表示することができます (**[サーバー概要]** > **[スロット<x>]** > **[セットアップ]** > **[FlexAddress]** の順にクリック)。すべてのスロットおよびサーバーの WWN/MAC アドレス情報は、[**WWN/MAC サマリー**] ページを用いて表示することができます (**[サーバー概要]** > **[プロパティ]** > **[WWN/MAC]** の順にクリック)。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、パーティション状態を表示することができます。WWN/MAC アドレスのフィールドには、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フィルタリングできます。
- **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できます。

基本モードと詳細モードの両方で、WWN/MAC アドレス情報は、折りたたまれた状態で表示されます。スロットに対する ⊞ をクリックするか、[**すべてを展開/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。

各フィールドの詳細については、*CMC for Dell PowerEdge FX2/FX2s のオンライン 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. 特定スロットに対する ⊞ または [**すべて展開/折りたたむ**] をクリックして、WWN/MAC アドレス表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**] フィールドで、特定の MAC アドレスに関連付けられたスロットをフィルタリングするには、MAC アドレスをそのまま正確に入力してください。または、関連するスロットを表示するには、MAC アドレス エントリーを部分的に入力します。たとえば、`4A` 含む MAC アドレスを持つスロットを表示するには、`4A` を入力します。
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、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。

各フィールドの詳細については、*CMC for Dell PowerEdge FX2/FX2s のオンライン 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 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 アドレスのテーブルには、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、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、およびパーティションの状態) が表示されます。緑のチェック 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。サーバーで FlexAddress または I/O アイデンティティーが有効になっていない場合、[**FlexAddress (シャーシ割り当て)**] または [**I/O アイデンティティー (リモート割り当て)**] は [**無効**] と表示されます。
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. 特定スロットに対する + または [**すべて展開/折りたたむ**] をクリックして、WWN/MAC アドレス表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。または、関連するスロットを表示するには、MAC アドレス エントリーを部分的に入力します。たとえば、`4A` 含む MAC アドレスを持つスロットを表示するには、`4A` を入力します。
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。

各フィールドの詳細については、*CMC for Dell PowerEdge FX2/FX2s のオンライン ヘルプ*を参照してください。

RACADM を使用した WWN/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 iSCSI MACS 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
```

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
```

`getflexaddr` および `getmacaddress` サブコマンドの詳細については、『Dell Chassis Management Controller for PowerEdge FX2/FX2s 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。

14

ファブリックの管理

シャーシは、ファブリック A1 とファブリック A2 の 2 つのファブリックタイプをサポートしています。これらのファブリックは 2 台の I/O モジュールによって使用され、サーバーのオンボードイーサネットアダプタに常に接続されています。

メモ: PowerEdge FX2s シャーシでは、ファブリック B および C が PCIe 拡張カードへの PCIe 接続です。

次の I/O モジュールがサポートされています。

- 1GbE パススルー
- 10GbE パススルー
- I/O アグリゲータ

どちらのファブリックもイーサネットのみをサポートしています。サーバー I/O アダプタ (LOM) には、それぞれ機能に応じて 2 個または 4 個のポートがあります。メザニンカードスロットには、PCIe カード (I/O モジュールではなく) に接続された PCIe 拡張カードが装着されます。

メモ: CMC CLI では、IOM は規則に従って「switch」とされます。

トピック：

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**]、[**I/O モジュール概要**]、[**セットアップ**] の順にクリックします。あるいは、**A1** および **A2** として使用可能な I/O モジュールのネットワークを設定するには、[**A1 ギガビット イーサネット**] または [**A2 ギガビット イーサネット**] をクリックしてから [**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、*オンライン ヘルプ*を参照してください。

   メモ: CMC から IOM に設定された IP アドレスは、スイッチの恒久的な起動設定には保存されません。IP アドレスを恒久的に保存するには、`connect switch` コマンド、または `racadm connect switch` RACADM コマンドを実行するか、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。『*Dell Chassis Management Controller for PowerEdge FX2/FX2s 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 <username> -p <password>
```

```
racadm deploy -m switch -u -p <password> -v SNMPv2 <snmpCommunityString> ro
```

```
racadm deploy -a [server|switch] -u <username> -p <password>
```

Web インターフェイスを使用した入出力モジュールのアップリンクおよびダウンリンク状態の表示

メモ: この機能を使用できるのは、PowerEdge FX2/FX2s のみです。

CMC Web インターフェイスを使用して Dell PowerEdge M I/O アグリゲーターのアップリンクおよびダウンリンクの状態を表示することができます。この操作を行うには、次の手順を実行します。

1. **シャーシ概要** > **I/O モジュール概要** に移動します。
   展開されたリストに、すべての IOM (1~2) が表示されます。
2. 表示する IOM (スロット) をクリックします。

   当該 IOM スロットに固有の I/O モジュールのステータス ページが表示されます。I/O モジュール アップリンク状態および I/O モジュール ダウンリンク状態のテーブルが表示されます。これらのテーブルには、ダウンリンク ポート (1~8) およびアップリンク ポート (9~12) に関する情報が表示されます。詳細については、*CMC for Dell PowerEdge FX2/FX2s のオンライン 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入出力モジュール FCoE セッション情報の表示

CMC Web インターフェイスを使用して Dell PowerEdge M I/O アグリゲーターの FCoE セッション情報を表示することができます。この操作を行うには、次の手順を実行します。

1. **シャーシ概要** > **I/O モジュール概要** に移動します。

展開されたリストに、すべての IOM (2) が表示されます。

2. 表示する IOM (スロット) をクリックします。**[プロパティ]** > **[FCoE]** をクリックします。
その IOM スロットに固有の **FCoE I/O モジュール** ページが表示されます。
3. **ポートの選択** ドロップダウンメニューで、選択された IOM に必要なポート番号を選択し、**セッションの表示** をクリックします。
選択したオプションに応じてスイッチの FCoE セッション情報が取得され、それをテーブル形式にしたものがユーザーに提示されます。
FCoE セッション情報 セクションには、スイッチの FCoE セッション情報が表示されます。

メモ: スイッチがプロトコルを使用しているときは、I/O アグリゲータもアクティブな FCoE セッションを表示します。

工場出荷時のデフォルト設定への IMO のリセット

IOM は、**I/O モジュールの展開** ページを使用して工場出荷時のデフォルト設定にリセットすることができます。

メモ: 本機能は PowerEdge M I/O Aggregator IOM でのみサポートされています。MXL 10/40GbE を含むその他の IOM はサポートされていません。

CMC ウェブインタフェースを使用して、選択した IOM を工場出荷時のデフォルト設定にリセットするには、次の手順を実行します。

1. システムツリーで **I/O モジュール概要** に進んで **セットアップ** をクリックするか、システムツリーで **I/O モジュール概要** を展開して IOM を選択し、**セットアップ** をクリックします。
I/O モジュールの展開 ページに、電源投入された IOM が表示されます。
2. 必要な IOM で **リセット** をクリックします。
警告メッセージが表示されます。
3. **OK** をクリックして続行します。

CMC ウェブインタフェースを使用した IOM ソフトウェアのアップデート

IOM ソフトウェアは、指定された場所から必要なソフトウェアイメージを選択することでアップデートできます。また、以前のソフトウェアバージョンにロールバックすることもできます。

メモ: この機能がサポートされるのは **Dell PowerEdge I/O アグリゲータ** のみです。

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

1. **シャーシ概要** > **I/O モジュール概要** > **アップデート** の順に移動します。
IOM ファームウェアアップデートページが表示されます。または、次のいずれかに移動します。
   - **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**。

   IOM ファームウェアとソフトウェア ページへのリンクが記載されたファームウェアアップデート ページが表示されます。
2. IOM ファームウェアアップデート ページの ファームウェア セクションで、ソフトウェアをアップデートする IOM の アップデート 列のチェックボックスを選択し、**ファームウェアアップデートの適用** をクリックします。または、ソフトウェアの以前のバージョンにロールバックするには、ロールバック 列のチェックボックスを選択します。
3. 参照オプションを使用してソフトウェアアップデート用のソフトウェアイメージを選択します。ソフトウェアイメージの名前が IOM ソフトウェアの場所フィールドに表示されます。
アップデート状態 セクションでは、ソフトウェアアップデートまたはロールバックの状態情報を提供します。イメージファイルがアップロードされる間、ページにステータスインジケータが表示されます。ファイルの転送時間は、接続速度によって異なります。内部アップデート処理が始まると、ページは自動的に更新され、ファームウェアアップデートのタイマーが表示されます。

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

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

   メモ: FTOS または IOM のソフトウェアバージョンは、X-Y (A-B) の形式で表示されます。たとえば、8-3 (1-4) などです。FTOS イメージのロールバックバージョンが、8-3-1-4 などの古いバージョン文字列形式を使用している古いイメージである場合は、現在のバージョンは 8-3 (1-4) と表示されます。

IOA または MXL GUI

CMC から IOA/MXL GUI を起動して IOA/MXL 設定を管理することができます。CMC から IOA/MXL GUI を起動するには、IOM が MXL または IOA に設定されていること、ユーザーがファブリック A の管理者権限を持っていることが必要です。

Dell PowerEdge FX2 MXL GUI は、MXL から IOA へのスイッチモードの変更をサポートしており、PowerEdge FX2 IOA GUI は、IOA から MXL へのスイッチモードの変更をサポートしています。

シャーシの概要、**I/O モジュールの概要**、**I/O モジュールのステータス** ページから MXL/IOA GUI を起動することができます。

メモ: MXL に初めてログインする際には、パスワードの変更を求めるメッセージが表示されます。

シャーシの概要ページからの IOA/MXL GUI の起動

[シャーシの概要] > **[クイック リンク]** > **[I/O モジュール GUI の起動]** の順に移動します。IOA/MXL ログインページが表示されます。

I/O モジュールの概要ページからの IOA/MXL GUI の起動

ディレクトリツリーで **I/O モジュールの概要** に移動します。**I/O モジュールのステータス** のページで、**I/O モジュール GUI の起動** をクリックします。IOA/MXL ログインページが表示されます。

I/O モジュールのステータスページからの IOA/MXL GUI の起動

ディレクトリーツリーの [**I/O モジュールの概要**] で、IOA/MXL スイッチをクリックします。**I/O モジュールのステータス** のページで、**I/O モジュール GUI の起動** をクリックします。IOA/MXL ログインページが表示されます。

入出力アグリゲータモジュール

IOM の詳細は、RACADM インタフェース、シャーシ正常性、IOM 概要、IOM ステータスの各ページで表示できます。また、この情報は CMC RACADM で表示することもできます。

IOM のモードは、次のとおりです。

- スタンドアロン
- Stacking
- PMux
- フルスイッチ

シャーシの正常性、**I/O モジュールのステータス**、**I/O モジュールの概要** ページで IOM を選択すると、IOM のモードをツールチップとして表示することができます。

静的 IP のある IOA のモードをスタッキングからスタンドアロンに変更する際は、IOA のネットワークが DHCP に変更されているようにしてください。変更されていない場合、静的 IP がすべての IOA で重複することになります。

IOM がスタッキングモードの場合、スタック ID は初期電源投入中に MAC に設定されたマスター IOM のものと同じになります。IOM のモードを変更しても、スタック ID は変更されません。たとえば、初期電源投入時に switch-1 がマスターだった場合、スタックの MAC アドレスは、MAC アドレスに設定された switch-1 のものと同じになります。後で switch-3 がマスターになっても、switch-1 の MAC アドレスがスタック ID として保持されます。

RACADM コマンドの `getmacaddress` により、MAC アドレス + 2 に設定された I/F MAC が表示されます。

15

VLAN Manager の使用

VLAN Manager オプションを使用して、IOM での VLAN 設定の割り当てまたは表示を行うことができます。

メモ: この機能がサポートされるのは Dell PowerEdge I/O アグリゲータ のみです。

I/O Aggregator のモードをスタッキングからスタンドアロンに変更した後に、スタートアップ構成を削除し、I/O Aggregator をリロードします。I/O Aggregator をリロードしている間、システム設定を保存する必要はありません。

トピック：

IOM への VLAN の割り当て

IOM 用仮想 LAN (VLAN) は、セキュリティおよびその他の理由のために、ユーザーを個々のネットワークセグメントに分けることを可能にします。VLAN を使用することにより、32 個のポートスイッチで、個々のユーザーのためのネットワークを隔離することができます。スイッチ上の選択されたポートを選択した VLAN と関連付け、これらのポートを別個のスイッチとして扱うこともできます。

CMC ウェブインタフェースでは、IOM に帯域内管理ポート (VLAN) を設定することが可能になります。

IOM に VLAN を割り当てるには、**シャーシ概要** > **I/O モジュール概要** > **セットアップ** > **VLAN Manager** の順に移動します。

VLAN の割り当て セクションで、I/O モジュールを選択してから設定タイプを選びます。またポートの範囲とスロットの指定も行います。

ドロップダウンメニューのリストから VLAN を選択して、VLAN を変更または編集します。

CMC ウェブインタフェースを使用した VLAN の設定

CMC ウェブインタフェースを使用して VLAN 設定を行うには、次の手順を実行します。

1. **I/O モジュール概要** に移動し、**セットアップ**、**VLAN Manager** をクリックします。
   VLAN Manager ページに、電源投入された IOM と利用可能なポートが表示されます。
2. **I/O モジュールの選択** セクションで、ドロップダウンリストから設定タイプを選択し、次に必要な IOM を選択します。
3. **ポート範囲の指定** セクションで、選択した IOM に割り当てられるファブリックポートの範囲を選択します。
4. **選択またはすべて選択解除** オプションを選択して、すべての IOM に変更を適用、またはどの IOM にも変更を適用しません。
   または
   特定のスロットに対するチェックボックスを選択し、必要な IOM を選択します。
5. **VLAN の編集** セクションで、IOM の VLAN ID を入力します。VLAN ID は 1~4094 の範囲内で入力します。VLAN ID は範囲として、またはカンマで区切って入力することもできます。
6. ドロップダウンメニューから、必要に応じて次のオプションのいずれかを選択します。
   - タグ付き VLAN の追加
   - VLAN の削除
   - タグ無し VLAN のアップデート
   - 全 VLAN のリセット

- VLAN の表示

7. **保存** をクリックして **VLAN Manager** ページで行った新規設定を保存します。

   メモ: 全ポートの VLAN の概要セクションには、シャーシに存在する IOM と割り当て済み VLAN についての情報が表示されます。現在の VLAN 設定サマリの csv ファイルを保存するには、**保存** をクリックします。

   メモ: CMC 管理下 VLAN セクションに、IOM に割り当てられた全 VLAN のサマリが表示されます。

8. **適用** をクリックします。
   ネットワーク設定が IOM 用に設定されました。

CMC ウェブインタフェースを使用した VLAN の表示

CMC ウェブインタフェースを使用して VLAN を表示するには、次の手順を実行します。

1. **I/O モジュール概要** に移動し、**セットアップ** > **VLAN Manager** をクリックします。
   VLAN Manager ページが表示されます。全ポートの VLAN サマリセクションに、IOM の現在の VLAN の設定に関する情報が表示されます。
2. **保存**をクリックして、VLAN 設定をファイルに保存します。

CMC ウェブインタフェースを使用した IOM の現在の VLAN 設定の表示

CMC ウェブインタフェースを使用して IOM の現在の VLAN 設定を表示するには、次の手順を実行します。

1. **I/O モジュール概要** に移動し、**セットアップ** > **VLAN Manager** をクリックします。
   VLAN Manager ページが表示されます。
2. **VLAN の編集** セクションで、ドロップダウンリストから **VLAN の表示** を選択し、**適用** をクリックします。
   操作成功メッセージが表示されます。IOM に割り当てられた現在の VLAN 設定が **VLAN 割り当て概要** フィールドに表示されます。

CMC ウェブインタフェースを使用した IOM 用 VLAN の削除

CMC ウェブインタフェースを使用して IOM から VLAN を削除するには、次の手順を実行します。

1. **I/O モジュール概要** に移動し、**セットアップ** > **VLAN Manager** をクリックします。
   VLAN Manager ページが表示されます。
2. **I/O モジュールの選択** セクションで、必要な IOM を選択します。
3. **VLAN の編集** セクションで、ドロップダウンリストから **VLAN の削除** を選択し、**適用** をクリックします。
   選択した IOM に割り当てられた VLAN が削除されます。

   操作成功メッセージが表示されます。IOM に割り当てられた現在の VLAN 設定が **VLAN 割り当て概要** フィールドに表示されます。

CMC ウェブインタフェースを使用した IOM 用のタグ無し VLAN のアップデート

CMC ウェブインタフェースを使用して IOM 用のタグ無し VLAN をアップデートするには、次の手順を実行します。

メモ: タグ無し VLAN は、すでにタグ付けされている VLAN ID に設定することはできません。

1. **I/O モジュール概要** に移動し、**セットアップ** > **VLAN Manager** をクリックします。
   VLAN Manager ページが表示されます。

2. **I/O モジュールの選択** セクションで、必要な IOM を選択します。
3. **ポート範囲の指定** セクションで、選択した IOM に割り当てられるファブリックポートの範囲を選択します。
4. **選択またはすべて選択解除** オプションを選択して、すべての IOM に変更を適用、またはどの IOM にも変更を適用しません。

   または

   特定のスロットに対するチェックボックスを選択し、必要な IOM を選択します。
5. **VLAN の編集** セクションで、ドロップダウンリストから **タグ無し VLAN のアップデート** を選択し、**適用** をクリックします。
   既存のタグ無し VLAN の設定が、新しく割り当てられたタグ無し VLAN の設定で上書きされるという警告メッセージが表示されます。
6. **OK** をクリックして確定します。
   タグ無し VLAN が、新しく割り当てられたタグ無し VLAN の設定でアップデートされます。

   操作成功メッセージが表示されます。IOM に割り当てられた現在の VLAN 設定が VLAN 割り当て概要 フィールドに表示されます。

CMC ウェブインタフェースを使用した IOM 用 VLAN のリセット

CMC ウェブインタフェースを使用して IOM 用 VLAN をデフォルト設定にリセットするには、次の手順を実行します。

1. **I/O モジュール概要**に移動し、**セットアップ** > **v VLAN Manager** をクリックします。
   VLAN Manager ページが表示されます。
2. **I/O モジュールの選択** セクションで、必要な IOM を選択します。
3. **VLAN の編集** セクションで、ドロップダウンリストから **VLAN のリセット** を選択し、**適用** をクリックします。
   既存 VLAN の設定がデフォルト設定で上書きされることを示す警告メッセージが表示されます。
4. **OK** をクリックして確認します。
   デフォルト設定に従って VLAN が選択した IOM に割り当てられます。

   操作成功メッセージが表示されます。IOM に割り当てられた現在の VLAN 設定が VLAN 割り当て概要 フィールドに表示されます。

メモ: すべての VLAN へリセットオプションは Virtual Link Trunking (VTL) モードの IOA でサポートされません。

16

電力の管理と監視

Dell PowerEdge FX2/FX2s 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。これには、効率性の高い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 FX2/FX2s における電力管理は、PowerEdge VRTX とはやや異なっています。電力管理テクノロジで大きく異なる点は、閉回路システムスロットル (CLST) の使用による希望のシャーシ電力上限の維持です。この技術を使用する目的は、より優れた制御、およびシャーシが使用できる PSU を最大限に活用できるようにすることです。

PowerEdge FX2/FX2s 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 FX2/FX2s エンクロージャは AC 電力を利用し、その負荷をアクティブな電源装置ユニット (PSU) に分散します。システムは、最大 3371 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 FX2/FX2s エンクロージャは、PSU の動作に影響を与え、システム管理者に対するシャーシ冗長性状況の報告方法を決定する 3 つの冗長性ポリシーのいずれかに設定することできます。

電源管理は **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

OMPC は次を管理します。

- サーバー電源
- システム入力電力容量

メモ: 実際の電力供給は、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、PSU のステータスを表示します。
- 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の設定が可能です。

- グリッド冗長性
- 冗長性なし
- 冗長性警告のみ

グリッド冗長性ポリシー

グリッド冗長性ポリシーは、1+1 のポリシーとも呼ばれ 1 つのアクティブ PSU と 1 つのスペア PSU を備えています。

グリッド冗長性ポリシーの目的は、エンクロージャが AC 電源障害に耐えるモードでエンクロージャシステムを動作させることにあります。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、または電源装置（PSU）自体が原因となる場合があります。システムをグリッド冗長性用に構成する際には、PSU 1 と PSU 2 を別々の電源グリッドに接続してください。

このモードでは、グリッドまたは 1 台の PSU で障害が発生した場合でも、CMC がシステムを劣化させることなく継続して動作するように電力の使用を確実に維持します。サーバーの電源投入で使用できる電力は、1 台の PSU で使用できる電力に制限されます。冗長性が維持できなくなる場合（PSU が故障した、または取り外されたなど）は、常にアラートがトリガされ、シャーシの正常性が **重要** になります。

冗長性なしポリシー

冗長性なしポリシーは 2+0 ポリシーとも呼ばれます。

このモードでは、両方の PSU の電力がすべて使用可能ですが、PSU またはグリッドに障害が発生した場合に、システムの動作が影響を受けないという保証はありません。

冗長性アラートのみポリシー

冗長性アラートのみポリシーにより、サーバの電源を投入して両方の PSU の容量を使用できます。また、PSU の取り外しや障害、あるいは実際の電力消費量が 1 台の PSU の能力を超える場合など、実際の状態についてアラートを送信します。これはデフォルトのポリシーです。

フォールトトレラント冗長性

このポリシーでは、グリッド冗長性ポリシーと同様に、単一の電源装置ユニット（PSU）の電源容量制限を使用します。このモードでは、CPU のサブシステムピーク電力は新しい IccMax 制限に置き換えられます。このポリシーは、デルの第 14 世代ブレードサーバのみに該当します。

PSU 障害

選択した冗長性ポリシーに関わらず、PSU 障害はどのタイプでも常に警告されます。

メモ: エンクロージャの電源をオフにしている間のモジュラーエンクロージャの冗長性ポリシーを変更します。

デフォルトの冗長性設定

シャーシおよび 2 台の PSU のデフォルトの冗長性設定は **冗長性警告のみ** です。

マルチノードスレッドの導入

PowerEdge FM120x4 はマルチノードのハーフワイドサーバーで、独立したプロセッサを持つ関連 iDRAC を搭載したサーバー 4 台を収容することができます。このサーバーは、最適の電力効率のために設計されており、プロセッサを取り外すことはできません。PowerEdge FM120 内のプロセッサは、例えばスレッド全体に大して 1 つの電力センサーと温度センサーを持つなど、同じ電源構成を共有します。

シャーシ電力制限の監視

Open Manage Power Center（OMPC）は、データセンター内のマシンの電力消費の監視および制御を行うために使用することができます。PowerEdge FX2/FX2s では、シャーシの電力制限を設定するためのプロビジョニング、および電力制限の設定基準となる

上下限を提供することによって OMPC を有効にします。電力制限の上下限は CMC によって設定されているため、手動で設定することはできません。

メモ: 下限とは、現在の構成を前提とした、シャーシの稼動に必要な最低限の電力です。上限は現在の冗長ポリシーの範囲で使用可能な最大電力を表します。

メモ: 最大電力カンバセーションモード (MPCM) がシャーシ上で有効になっている場合は、ブレードサーバーからすべての電源要求は拒否されます。ホストでの電源の入れなおしを必要とするアクションが iDRAC またはブレードサーバーで行われている場合は、ブレードサーバーの電源は入りません。

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
```

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** > **バジェットステータス** の順にクリックします。 **電力バジェットステータス** ページは、**システム入力電力上限**、**冗長性ポリシー** 属性値を持つシステム電力バジェット詳細、**システム入力最大電力容量**、**入力冗長予約**、**サーバー電源投入に使用できる電力** 、および電源装置ユニット詳細が記載されたシャーシ電源装置を表示します。詳細については、『*CMC for Dell PowerEdge FX2/FX2s Online Help*』(CMC for Dell PowerEdge FX2/FX2s 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
```

出力の詳細を含む **getpbinfo** の詳細 ni ついては、『*Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*』(Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM コマンドラインリファレンスガイド) の **getpbinfo** コマンドの項を参照してください。

冗長性状態と全体的な電源正常性

冗長性の状態は、全体的な電源正常性を判断するための要因です。例えば、電源冗長性ポリシーがグリッド冗長性に設定されていて、システムが冗長性で動作していることを冗長性ステータスが示している場合、全体的な電源状態は通常 [**OK**] です。シャーシに取り付けられている PSU が何らかの理由により失敗した場合は、シャーシの全体的な電力正常性状態が [**非重要**] として表示さ

れます。ただし、グリッド冗長性を使用するための条件を満たすことができない場合、冗長性のステータスは [**いいえ**] で、全体的な電力正常性は [**重要**] です。これは、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 から正常性状態をポーリングして、シャーシが冗長であるかどうかを判断します。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。また、スタンバイ CMC がアクティブになっています。ネットワークが停止すると、最初のアクティブ CMC は約 3 分後に起動し、スタンバイ CMC になります。スタンバイ CMC の正常性監視タスクが 5 分後に再開されます。スタンバイが安定した場合にのみ、スタンバイ上の稼働状態の変更が処理されます。アクティブ CMC は、冗長性があるかどうかを判断するために、8 分半待つ必要があります。正常性の変更に対してフェールオーバーを開始する前に、冗長性状態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するか、グリッド冗長性から変更したとき、CMC はこれらの条件の事前チェックを実行しません。そのため、冗長性ポリシーを構成すると、冗長性が失われるか、または回復した状態になる場合があります。

PSU 障害発生後の電力管理

PSU に障害が発生した、または PSU が取り外された場合、サーバーに提供される電力が減少する可能性があります。極端な例では、操作を維持しようとするためにサーバーの電源がオフになることもあります。グリッド冗長性を設定して維持することで、単一の PSU 障害によるサーバーへの影響を回避することができます。

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

電源装置の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) にエントリー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 27. 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 にエントリー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**冗長性警告のみ**電源ポリシーに設定されたエンクロージャにおける冗長性の喪失と回復です。次の表は、電源冗長性ポリシーの変更に関連した SEL エントリーの一覧です。

表 28. 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	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

シャーシ全体 (シャーシ、サーバー、I/O モジュール、CMC、PCIe、シャーシインフラストラクチャ) の電力バジェット、冗長性、および動的電力を設定することができます。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の再割り当てを行います。

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
- 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
- AC 電源リカバリを無効にする

節電と電力バジェット

電力使用量がシステム入力電力上限を超えると、公称レベルを維持するため、PSU によってサーバーに供給される電力が削減されます。

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。
   - **冗長性ポリシー**
   - **シャーシ電源ボタンの無効化**
   - **最大電力節減モード**
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>
     ```

     ここでの *<value>* は 0 (冗長性なし)、1 (グリッド冗長性)、および 3 (冗長性警告のみ) です。デフォルトは 3 です。

     例えば、次のコマンドは冗長性ポリシーを 1 に設定します。

     ```
     racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy 1
     ```
   - 電力バジェット値を設定するには、次を入力します。

     ```
     racadm config -g cfgChassisPower -o cfgChassisPowerCap <value>
     ```

     ここで、*<value>* は現在のランタイムシャーシ負荷および 3371 であり、最大電力制限をワット単位で表しています。デフォルトは 3371 です。

     たとえば、次のコマンドは最大電力バジェットを 3371 ワットに設定します。

     ```
     racadm config -g cfgChassisPower -o cfgChassisPowerCap 3371
     ```
   - 下限と上限を表示するには、次を入力します。

     ```
     racadm getconfig -g cfgchassispower -o cfgchassispowercap <lower,upper> bound
     ```

ここで *<lower,upper>* が下限と上限になります。

```
racadm config -g cfgChassisPower -o cfgChassisPowerCap 3000
```

- 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。

- 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、『Dell 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。

Web インターフェイスを使用したシャーシでの電源制御操作の実行

CMC Web インターフェイ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]** > **[電力]** > **[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 <action>
```

ここでの <*action*> は、powerup、powerdown、powercycle、nongraceshutdown、または reset になります。

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**
   - **正常なシャットダウン**
   - **サーバーの電源を入れる**
   - **サーバーの電源を切る**
   - **サーバーをリセットする (ウォームブート)**
   - **サーバーの電源を入れなおす (コールドブート)**

   オプションの詳細については、*CMC for Dell PowerEdge FX2/FX2s のオンライン 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。

   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。

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: 電源管理アクションを実行するには、**シャーシ制御システム管理者**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 <action>
```

ここで、*<action>* は実行する操作（パワーサイクル）を示します。

RACADM コマンドについての情報は、dell.com/support/manuals で入手可能の『*Dell Chassis Management Controller for PowerEdge FX2/FX2s 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。

スレッド電源ボタンの設定

スレッドの電源ボタンを押しても何も起こらないように、スレッドの電源ボタンを無効に設定することができます。スレッドの電源ボタンを設定するには、**シャーシ概要** > **サーバー概要** > **電源** > **制御**と移動します。

プロパティ セクションで、無効化するチェックボックスにチェックを入れる、またはチェックを外して有効化します。

メモ: この設定は、シャーシ内に存在するマルチノードスレッドのみに適用されます。他のスレッドには影響しません。

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。

17

PCIe スロットの設定

PowerEdge FX2/FX2s シャーシには、オプションで 8 個の PCIe スロットを搭載されており、各 PCIe スロットは特定のスレッドに割り当てられています。デフォルトでは、すべての PCIe スロットがマップされています。サーバーへの PCIe スロットの割り当ては、CMC Web インターフェイスまたは RACADM を用いて有効化および無効化できます。

次の表は、フル幅、ハーフ幅、クォーター幅のコンピュートスレッドへの PCIe のマッピングを示しています。

表 29. フル幅コンピュートスレッドへの PCIe のマッピング

PCIe スロット	フル幅スレッド (PowerEdge FC830) へのマッピング
PCIe スロット 1	3
PCIe スロット 2	3
PCIe スロット 3	1
PCIe スロット 4	1
PCIe スロット 5	3
PCIe スロット 6	3
PCIe スロット 7	1
PCIe スロット 8	1

表 30. ハーフ幅コンピュートスレッドへの PCIe のマッピング

PCIe スロット	ハーフ幅スレッド (PowerEdge FC630) へのマッピング
PCIe スロット 1	4
PCIe スロット 2	4
PCIe スロット 3	2
PCIe スロット 4	2
PCIe スロット 5	3
PCIe スロット 6	3
PCIe スロット 7	1
PCIe スロット 8	1

表 31. クォーター幅コンピュートスレッドへの PCIe のマッピング

PCIe スロット	クォーター幅スレッド (PowerEdge FC430) へのマッピング
PCIe スロット 1	3d
PCIe スロット 2	3c
PCIe スロット 3	1d
PCIe スロット 4	1c
PCIe スロット 5	3b
PCIe スロット 6	3a
PCIe スロット 7	1b
PCIe スロット 8	1a

メモ: PCIe 管理は PowerEdge FX2s でのみサポートされており、PowerEdge FX2 ではサポートされていません。

PCIe スロットのマッピングの詳細については、『*Dell PowerEdge FD332 オーナーズ マニュアル*』を参照してください。

PCIe スロットの管理の詳細については、*CMC for Dell PowerEdge FX2/FX2s のオンライン ヘルプ*を参照してください。

メモ: エージェント フリー モニタリング機能は、シャーシ PCIe スロット内の PCIe PERC およびネットワーク カードでは利用できません。エージェント フリー モニタリングは、デルの第 12 世代 PowerEdge サーバー用のシステム管理ソリューションです。この機能は一切のオペレーティング システム エージェントに依存せず、帯域外となっています。エージェント フリー モニタリングを用いることで、サーバー (PERC、ハード ディスク、エンクロージャなど) ネットワーク デバイスに接続されたストレージのモニタリングを、iDRAC を使用して実行でき、管理対象システムや管理ステーションへのエージェントのインストールは不要です。エージェント フリー モニタリングの詳細については、**Dell TechCenter** にあるホワイト ペーパー『*Dell PowerEdge 第 12 世代サーバーのストレージおよびネットワーク デバイス用エージェント フリー インベントリーとモニタリング*』を参照してください。

トピック :

- CMC Web インターフェイスを使用した PCIe スロット プロパティの表示
- RACADM を使用した PCIe スロットプロパティの表示

CMC Web インターフェイスを使用した 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。
- 単一の PCIe スロットに関する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。

RACADM を使用した PCIe スロットプロパティの表示

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を表示することができ、それらのコマンドの一部をここで説明します。RACADM コマンドの詳細については、**dell.com/support/manuals** で入手可能な『*Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide*』(Dell Chassis Management Controller for PowerEdge FX2/FX2s 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: PCIe カードの名前は、BIOS が関連するスレッドで `POST` を完了した後でしか表示されません。それまでは、デバイス名は **不明** として表示されます。

- 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 getpciecfg -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
```

- 既存の PCIe 設定を表示するには、次のコマンドを実行します。

```
racadm getconfig-g cfgPCIe
```

メモ: メザニンカードが関連スレッドに存在しない場合、PCIe カードの電源はオンになりません。

PCIe の再割り当て

PCIe の再割り当て機能を使用すると、下部ベイのコンピュートスレッドに割り当てられている PCIe スロットを上部ベイのコンピュートスレッドにマップすることができます。

CMC ウェブインタフェース、CMC WSMan または RACADM を使用して PCIe の再割り当てオプションを有効化または無効化することができます。再割り当ての設定を設定または変更するには、シャーシ構成権限が必要です。再割り当ての設定を変更する前に、シャーシ内のコンピュートスレッドのすべての電源を切ります。再割り当てが変更された後に、コンピュートスレッドの電源がオンになると、下段のベイのコンピュートスレッドに以前に割り当てられていたスロットが、上段のベイのコンピュートスレッドに対応してマップされます。以下に PCIe の再割り当ての例を示します。

- **フル幅 (FW) FC830 での PCIe 再割り当て。**
  - FW スレッド -3 (PCIe スロット 1~4) にマップされた PCIe スロットが、スレッド –1 に再割り当てられました。スレッド –1 は PCIe スロット 1~8 にマップされるようになりました。
- **ハーフ幅 (HW) FC630 での PCIe 再割り当て。**
  - HW スレッド -3 (PCIe スロット 5~6) にマップされた PCIe スロットが、スレッド –1 に再割り当てされました。スレッド -1 は PCIe スロット 5~8 にマップされるようになりました。
  - HW スレッド -4 (PCIe スロット 1~2) にマップされた PCIe スロットが、スレッド -2 に再割り当てされました。スレッド -2 は PCIe スロット 1~4 にマップされるようになりました。
- **クオーター幅 (QW) FC430 での PCIe 再割り当て。**
  - QW スレッド -3a (PCIe スロット 6) にマップされた PCIe スロットが、スレッド -1 に再割り当てされました。スレッド -1a は PCIe スロット 6~8 にマップされるようになりました。
  - QW スレッド -3b (PCIe スロット 5) にマップされた PCIe スロットが、スレッド -1b に再割り当てされました。スレッド -1b は PCIe スロット 5 と 7 にマップされるようになりました。
  - QW スレッド -3c (PCIe スロット 2) にマップされた PCIe スロットが、スレッド -1c に再割り当てされました。スレッド -1c は PCIe スロット 2 と 4 にマップされるようになりました。
  - QW スレッド -3d (PCIe スロット 1) にマップされた PCIe スロットが、スレッド -1d に再割り当てされました。スレッド -1d は PCIe スロット 1 と 3 にマップされるようになりました。

詳細については、『*Dell PowerEdge FX2 and FX2s Enclosure Owner's Manual*』(Dell PowerEdge FX2 および FX2s エンクロージャオーナーズマニュアル) 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 再割り当ての有効化または無効化

1. 左ペインで **サーバー概要** をクリックします。
   PCIe ステータス ページが表示されます。
2. **セットアップ** をクリックします。
   マッピング：PCIe スロットの再割り当て ページが表示されます。
3. **PCIe スロットの再割り当ての有効化** チェックボックスを選択またはクリアしてから、**適用** をクリックします。

RACADM を使用した PCIe 再割り当ての有効化または無効化

PCIe のスロットへの再割り当てを有効化または無効化するための入力値は、以下のとおりです。

- 1 - 有効
- 0 - 無効

PCIe の再割り当てを有効化するには、次のコマンドを実行します。

```
racadm config -g cfgPCIe -o cfgPCIeReassignmentEnable 1
```

PCIe の再割り当てを無効化するには、次のコマンドを実行します。

```
racadm config -g cfgPCIe -o cfgPCIeReassignmentEnable 0
```

詳細については、**dell.com/support/manuals** にある『*Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM コマンド ライン リファレンス ガイド*』を参照してください。

18

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。

トピック：

RACDUMP を使用した設定情報、シャーシステータス、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 RADCAM コマンドを集約します。racdump の詳細については、『Dell Chassis Management Controller for PowerEdge FX2/FX2s 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 32. 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

表 32. サブシステム用 Racadm コマンド（続き）

サブシステム	RACADM コマンド
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
NIC 情報（CMC モジュール）	getniccfg
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 により、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ができます。

CMC ウェブインタフェースを使用して CMC の SNMP Management Information Base（MIB）ファイルをダウンロードするには、次の手順を実行します。

1. 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：** この設定では、サイド 1（左側のスロット）の電源装置とサイド 2（右側のスロット）の電源装置がエンクロージャ内に存在し、機能している必要があります。さらに、各電源装置の容量は、シャーシが **グリッド冗長性** を維持するための電力割り当て総量をサポートするために十分である必要があります。
  - **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 の電源装置がひとつの AC グリッドに、サイド 2 の電源装置がもう一方の 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**：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。
- **問題：** エンクロージャの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：** 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。各電子メール、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: 特定のイベントが発生したときに電子メールまたは SNMP トラップを送信するよう CMC を設定することができます。

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
```

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。

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。

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、『Online Help』(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

CMC をリセット、またはサーバーを仮想的にリセットして、サーバーが取り外されて再度挿入されたかのように動作させることができます。

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。

メモ: PowerEdge FM120x4 の個々のノードでは、仮想再装着は使用できません。

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. CMC をリセットするには、**CMC ステータス** セクションで **CMC のリセット** をクリックします。使用可能な CMC が再起動されます。

詳細については、『Dell PowerEdge FX2/FX2s 向け CMC オンラインヘルプ』を参照してください。

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。

メモ: Flexaddress 情報、サーバープロファイル、および拡張ストレージが、シャーシ設定と共に保存または復元されることはありません。重要なサーバープロファイルは、リモートファイル共有またはローカルワークステーションに保存されたコピーを使用して、シャーシとは別に保存することが推奨されます。これらの操作の実行方法については、「プロファイルの追加または保存」を参照してください。

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。

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

ネットワークを介してリモートタイムサーバと時計を同期するよう CMC を設定してから、日付と時刻が変更されるまで数分かかる場合があります。数分たっても変更されない場合は、問題をトラブルシューティングする必要がある場合があります。CMC が時計を同期できないのは、次の理由による可能性があります。

- ネットワークタイププロトコル (NTP) サーバ 1、NTP サーバ 2、NTP サーバ 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 関連の問題をトラブルシューティングするには、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 サーバとも同期できない場合、CMC の時刻はローカルシステムの時計と同期され、トレースログには次のようなエントリが記録されます。

```
Jan 8 20:02:40 cmc ntpd[1423]: synchronized to LOCAL(0), stratum 10
```

次の racadm コマンドを入力することで、ntpd 状態を確認することもできます。

```
racadm getractime -n
```

「*」が設定済みサーバのいずれか 1 つに付いているのでない場合、設定が正しく行われていない可能性があります。このコマンドの出力には、問題のデバッグに有用となる詳細な NTP 統計が含まれています。

Windows ベースの NTP サーバを設定しようとしている場合は、ntpd の MaxDist パラメータを大きくするのが有効な場合があります。大部分の NTP サーバと連携できるよう、デフォルトの設定には十分に大きな値であることが必要となるため、このパラメータを変更する前に、この変更によるすべての影響を把握してください。

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に gettracelog コマンドを入力する方法についての情報は、「診断コンソールの使用」を参照してください。

LED の色と点滅パターンの解釈

シャーシ上の LED は、コンポーネントの次の状態を示します。

- 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。
- 青色の点滅 LED はユーザーによって構成可能であり、識別のために使用されます。設定の詳細については、『シャーシのコンポーネントを識別するための CMC_Stmp_Configuring LED』を参照してください。

表 33. 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		電源オン
		電源オフ
	青色、点灯	ファームウェアのアップロード中

表 33. 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
		ファームウェア アップデートが正常に行われた
	電源オフ	ファームウェア アップデートの進行中
	青色、点灯	アクティブ
	青色、点滅	ユーザーによって有効化されたモジュール識別
	橙色、点灯	不使用
	橙色、点滅	障害
サーバー		電源オン
		ファームウェアのアップロード中
		電源オフ
	青色、点灯	KVM でサーバーが選択されている
	青色、点滅	ユーザーによって有効化されたモジュール識別
	橙色、点灯	不使用
	橙色、点滅	障害
	青色、消灯	障害なし
IOM（共通）	緑色、点灯	電源オン
	緑色、点滅	ファームウェアのアップロード中
	緑色、消灯	電源オフ
	青色、点灯	正常 / スタックマスター
	青色、点滅	ユーザーによって有効化されたモジュール識別
	橙色、点灯	不使用
	橙色、点滅	障害
	青色、消灯	障害なし / スタックスレーブ
IOM（パススルー）	緑色、点灯	電源オン
	緑色、点滅	不使用
	緑色、消灯	電源オフ
	青色、点灯	正常
	青色、点滅	ユーザーによって有効化されたモジュール識別
	橙色、点灯	不使用
	橙色、点滅	障害
	青色、消灯	障害なし
ファン	緑色、点灯	ファン作動中
	緑色、点滅	不使用
	緑色、消灯	電源オフ
	橙色、点灯	ファンタイプを認識できない、CMC ファームウェアのアップデート
	橙色、点滅	ファン障害。タコメーターが範囲外
	橙色、消灯	不使用

表 33. 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
PSU	（楕円）緑色、点灯	AC OK
	（楕円）緑色、点滅	不使用
	（楕円）緑色、消灯	AC OK 外
	橙色、点灯	不使用
	橙色、点滅	障害
	橙色、消灯	障害なし
	（円）緑色、点灯	DC OK
	（円）緑色、無灯	DC OK 外
PCI	青色、消灯	電源オン
	青色、点滅	PCI 識別が進行中です。
	橙色、点滅	障害
ストレージスレッド	橙色、点滅	障害
	青色に点灯	障害なし

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。

問題特定のための LED の観察

CMC には、次の状態を示すために色が変化する LED が搭載されています。

表 34. LED のカラーインジケータ

色	説明
青色	通常の動作
青色、点滅	ID（0.5 秒点灯、0.5 秒消灯）
橙色	シャーシ障害のサマリ
橙色、点滅	並列 ID を伴うシャーシ障害

ネットワーク問題のトラブルシューティング

内部 CMC トレースログでは、CMC アラートとネットワークのデバッグを行うことが可能です。トレースログには CMC ウェブインタフェースまたは RACADM を使ってアクセスできます。『*iDRAC および CMC 向けコマンドラインリファレンスガイド*』の `gettracelog` の項を参照してください。

トレースログは次の情報を追跡します。

- DHCP — DHCP サーバーから送受信されたパケットをトレースします。
- DDNS — 動的 DNS アップデート要求と応答をトレースします。
- ネットワークインタフェースへの設定変更。

トレースログには、管理下システムのオペレーティングシステムではなく、CMC の内部ファームウェアに関連する CMC ファームウェア固有のエラーコードが含まれている場合もあります。

一般的なトラブルシューティング

操作（サーバープロファイルの保存など）完了後に成功メッセージが表示されても、処置が行われない場合があります。

この問題を解決するには、SSH、Telnet、HTTP、または HTTPS の CMC サービスポートが、111 などの OS サービスによって一般的に使用されるポートを使用していないかどうかをチェックします。CMC サービスポートによって使用されている場合は、設定を未予約ポートに変更します。予約済みポートの詳細については、http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml を参照してください。

FX2 シャーシのストレージモジュールのトラブルシューティング

次の情報は、FX2 シャーシ内のストレージスレッドに関連する問題のトラブルシューティングに役立ちます。

- **問題：**ストレージモジュールが挿入時に検出されません。挿入されたストレージモジュールと、電源がオンの関連付けられたサーバーが検出されません。

  対応処置：ストレージモジュールを挿入した後、必ず関連付けられたサーバーに電源を入れ直してください。

- **問題：**ストレージモジュールを挿入し、関連付けられたサーバーの電源を入れ直しましたが、ストレージモジュールが認識されません。

  対応処置：エラーについての詳しい情報については、シャーシログをチェックしてください。ケーブルスプールまたは RAID が検出されないなどのハードウェア障害があるか確認します。

- **問題：**ストレージの橙色の LED が点滅します。

  対応処置：ストレージモジュールが正しく挿入されていることを確認し、シャーシにログに警告メッセージがないかチェックします。このエラーは、元になる障害が解決され、スレッドの削除またはスレッドの仮想抜き差しによって関連付けられているホストの電源が入れ直されたときにのみ、クリアされます。

  問題：ストレージモジュール RAID ファームウェアのアップデートが無効になっています。

  対応処置：スプリットデュアルホストモードでは、RAID ファームウェアを有効にするには、ストレージスレッド RAID に接続された各ホストの電源を入れ直す必要があります。

- **問題：**GUI で PCIe スロットの再割り当てオプションが無効になっています。

  対応処置：シャーシ内のすべてのホストの電源が入っていることを確認します。ホストの電源投入時に RACADM からこの設定を変更しようとすると、エラーメッセージが表示されます。この設定を変更するには、シャーシ設定管理者の権限が必要です。

- **問題：**PCIe スロットの再割り当てが有効で、ホストの電源がオンですが、PCIe スロットの電源が入りません。

  対応処置：古い BIOS、iDRAC、またはサポートされていないホストに関連する警告メッセージがないか、シャーシログを確認してください。

- **問題：**ストレージモジュールのライセンスをインポート、エクスポート、削除できません。

  対応処置：ストレージモジュールのライセンスをインポート、エクスポート、削除するには、シャーシ構成の権限が必要です。

システム管理者パスワードを忘れた場合のリセット

注意: 修理作業の多くは、認定されたサービス技術者のみが行うことができます。製品マニュアルで許可されている範囲、またはオンライン サービスもしくはテレホン サービスおよびサポート チームの指示範囲で、トラブルシューティングや簡単な修理を行うことができます。Dell の許可を受けていない保守による損傷は、保証の対象となりません。製品に付属しているマニュアルの「安全にお使いいただくために」をお読みになり、指示に従ってください。

管理動作を行う場合は、**管理者**の権限が必要になります。CMC ソフトウェアには、ユーザー アカウントのパスワード保護セキュリティ機能があります。管理者アカウントのパスワードを忘れた場合には、この機能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、次の図で示すように 2 ピンのパスワード 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は、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、デフォルト値の「username: root」と「password: calvin」に設定されます。管理者アカウントは、アカウントが削除された、またはパスワードが変更されたかどうかにかかわらず、リセットされます。

メモ: 作業を開始する前に、CMC モジュールがパッシブ状態にあることを確認してください。

管理動作を行う場合は、**管理者**の権限が必要になります。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リセットできます。

J_PWORD ジャンパは、次の図で示されるように 2 ピンコネクタを使用します。

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
```

システム管理者アカウントは、アカウントが削除された、またはパスワードが変更されたかどうかにかかわらず、一時的にリセットされます。

メモ: 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
```

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: 静電気の放電 (ESD) により CMC が損傷する可能性があります。特定の条件下では、ESD は身体や物体に蓄積し、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. 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 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 ジャンパーの位置を確認するには、次の図を参照してください。

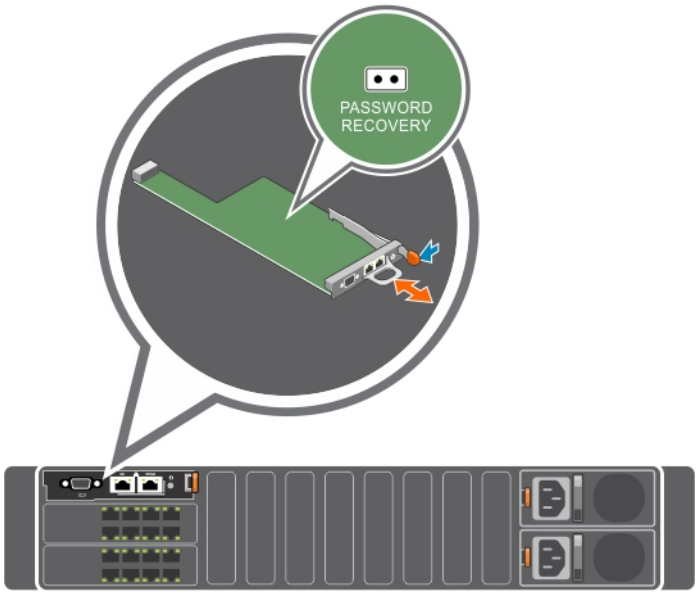


表 35. CMC パスワードジャンパの設定

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 35. 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。

3. 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。

4. 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。
5. 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にならず、アクティブなままです。
6. 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。
7. 2 ピン J_PWORD ジャンパを取り外し、ジャンパプラグを元に戻します。
   a. ハンドルの CMC リリース ラッチを押し、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。
   b. 2 ピンジャンパを取り外し、ジャンパプラグを元に戻します。
   c. CMC モジュールをエンクロージャに挿入します。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、ジャンパーを取り外した CMC モジュールをアクティブな CMC にします。

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
- 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 が処置を実行できない場合の問題です。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。

$ プロンプトに戻すには、<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

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 機能のため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 サーバー証明書が備わっています。この証明書が使用される時、CMC のホスト名（たとえば IP アドレス）に一致しないデフォルト証明書が CMC デフォルト証明書に発行されるため、ウェブブラウザがセキュリティ警告を表示します。

このセキュリティ問題に対処するには、CMC の IP アドレスに発行された CMC サーバー証明書をアップロードします。証明書の発行のために使用される証明書署名要求（CSR）を生成するときは、CSR のコモンネーム（CN）が CMC の IP アドレス（例えば 192.168.0.120）または登録済み DNS CMC 名に一致することを確認してください。

CSR を登録済み DNS CMC 名と一致させるには、次の手順を実行します。

1. 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。

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。

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}
```

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。

イベントおよびエラーメッセージ

CMC ファームウェアの最新バージョンを以前のバージョンにダウングレードすると、シャーシログが一部のログに対して次のメッセージを表示するのはなぜですか?

```
USR8513 - MessageID missing from message registry.
```

これは、最新ファームウェアに導入された、古いバージョンのファームウェアでは解釈できない新しいメッセージです。メッセージ ID の詳細については、**www.dell.com/openmanagemanuals** の OpenManage ソフトウェアにある『*イベントおよびエラーメッセージリファレンスガイド*』を参照してください。