




**Chassis Management Controller for Dell PowerEdge
VRTX バージョン 1.0
ユーザーズガイド**



メモ、注意、警告

-  **メモ:** コンピュータを使いやすくするための重要な情報を説明しています。
-  **注意:** ハードウェアの損傷やデータの損失の可能性を示し、その問題を回避するための方法を説明しています。
-  **警告:** 物的損害、けが、または死亡の原因となる可能性があることを示しています。

© 2013 Dell Inc.

本書に使用されている商標 : Dell™、Dell のロゴ、Dell Boomi™、Dell Precision™、OptiPlex™、Latitude™、PowerEdge™、PowerVault™、PowerConnect™、OpenManage™、EqualLogic™、Compellent™、KACE™、FlexAddress™、Force10™ および Vostro™ は Dell Inc. の商標です。Intel®、Pentium®、Xeon®、Core® および Celeron® は米国およびその他の国における Intel Corporation の登録商標です。AMD® は Advanced Micro Devices, Inc. の登録商標、AMD Opteron™、AMD Phenom™ および AMD Sempron™ は同社の商標です。Microsoft®、Windows®、Windows Server®、Internet Explorer®、MS-DOS®、Windows Vista® および Active Directory® は米国および/またはその他の国における Microsoft Corporation の商標または登録商標です。Red Hat® および Red Hat® Enterprise Linux® は米国および/またはその他の国における Red Hat, Inc. の登録商標です。Novell® および SUSE® は米国およびその他の国における Novell, Inc. の登録商標です。Oracle® は Oracle Corporation またはその関連会社、もしくはその両者の登録商標です。Citrix®、Xen®、XenServer® および XenMotion® は米国および/またはその他の国における Citrix Systems, Inc. の登録商標または商標です。VMware®、vMotion®、vCenter®、vCenter SRM™ および vSphere® は米国またはその他の国における VMware, Inc. の登録商標または商標です。IBM® は International Business Machines Corporation の登録商標です。

2013 - 06

Rev. A00

目次

1 概要	13
主な機能.....	14
管理機能.....	14
セキュリティ機能.....	15
シャーシの概要.....	15
対応リモートアクセス接続.....	18
対応プラットフォーム.....	18
対応ウェブブラウザ.....	19
ライセンスの管理.....	19
ライセンスのタイプ.....	19
ライセンスの取得.....	19
ライセンス操作.....	19
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.....	20
CMC ウェブインタフェースを使用したライセンスの管理.....	20
RACADM を使用したライセンスの管理.....	20
CMC におけるライセンス取得可能な機能.....	21
他言語の CMC ウェブインタフェースの表示.....	22
対応管理コンソールアプリケーション.....	22
本ユーザーズガイドの使用方法.....	22
その他の必要マニュアル.....	22
デルサポートサイトからの文書へのアクセス.....	23
2 CMC のインストールと設定	25
作業を開始する前に.....	25
CMC ハードウェアの取り付け.....	25
シャーシ設定のチェックリスト.....	25
CMC の基本的なネットワーク接続.....	26
管理ステーションへのリモートアクセスソフトウェアのインストール.....	26
RACADM の Linux 管理ステーションへのインストール.....	26
Linux 管理ステーションから RACADM のアンインストール.....	27
ウェブブラウザの設定.....	27
プロキシサーバー.....	27
Microsoft フィッシングフィルタ.....	28
証明書失効リスト (CRL) のフェッチ.....	28
Internet Explorer を使用した CMC からのファイルのダウンロード.....	28
Internet Explorer でのアニメーションの有効化.....	29
CMC への初期アクセスのセットアップ.....	29
初期 CMC ネットワークの設定.....	29

CMC にアクセスするためのインターフェースおよびプロトコル.....	32
その他のシステム管理ツールを使用した CMC の起動.....	34
CMC ファームウェアのダウンロードとアップデート.....	34
シャーシの物理的な場所とシャーシ名の設定.....	34
ウェブインター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.....	34
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.....	35
CMC の日付と時刻の設定.....	35
CMC ウェブインターフェースを使用した CMC の日付と時刻の設定.....	35
RACADM を使用した CMC の日付と時刻の設定.....	35
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.....	35
CMC ウェブインターフェースを使用した LED 点滅の設定.....	35
RACADM を使用した LED の点滅の設定.....	36
CMC プロパティの設定.....	36
冗長 CMC 環境について.....	36
スタンバイ CMC について.....	37
CMC フェイルセーフモード.....	37
アクティブ CMC の選択プロセス.....	37
冗長 CMC の正常性状態の取得.....	38
前面パネルの設定.....	38
電源ボタンの設定.....	38
LCD の設定.....	38
KVM を使用したサーバーへのアクセス.....	38
3 CMC へのログイン.....	41
CMC ウェブインターフェースへのアクセス.....	41
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.....	41
スマートカードを使用した CMC へのログイン.....	42
シングルサインオンを使用した CMC へのログイン.....	43
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.....	43
RACADM を使用した CMC へのアクセス.....	43
公開キー認証を使用した CMC へのログイン.....	44
複数の CMC セッション.....	44
4 ファームウェアのアップデート.....	47
CMC ファームウェアのダウンロード.....	47
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.....	47
CMC ウェブインター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.....	47
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.....	48
CMC ファームウェアのアップデート.....	48
RACADM を使用した CMC ファームウェアのアップデート.....	49
ウェブインターフェースを使用した CMC ファームウェアのアップデート.....	49

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.....	49
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.....	50
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.....	50
サーバー iDRAC ファームウェアのアップデート.....	50
RACADM を使用したサーバー iDRAC ファームウェアのアップデート.....	50
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.....	51
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.....	51
Lifecycle Controller の有効化.....	52
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.....	53
ファームウェアインベントリの表示.....	54
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.....	54
RACADM を使用したファームウェアインベントリの表示.....	55
Lifecycle Controller のジョブ操作.....	56
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.....	56
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.....	57
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.....	57
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.....	57
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.....	58
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.....	58
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.....	59
CMC ウェブインタフェースを使用したストレージコンポーネントのアップデート.....	59
CMC を使用した iDRAC ファームウェアのリカバリ.....	59

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..... 61

シャーシとコンポーネント概要の表示.....	61
シャーシの図解.....	62
選択したコンポーネントの情報.....	62
サーバーモデル名とサービスタグの表示.....	63
シャーシ概要の表示.....	63
シャーシコントローラ情報と状態の表示.....	63
すべてのサーバーの情報および正常性状態の表示.....	63
IOM の情報および正常性状態の表示.....	63
ファンの情報と正常性状態の表示.....	64
ファンの設定.....	64
前面パネルプロパティの表示.....	65
KVM の情報および正常性状態の表示.....	66
LCD の情報と正常性の表示.....	66
温度センサーの情報と正常性状態の表示.....	66

6 CMC の設定	67
CMC ネットワーク LAN 設定の表示と変更.....	67
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.....	68
RACADM を使用した CMC ネットワーク LAN 設定の表示と変更.....	68
CMC ネットワークインタフェースの有効化.....	68
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.....	69
DHCP を使用した DNS IP アドレスの取得機能の有効 / 無効化.....	69
DNS の静的 IP アドレスの設定.....	69
DNS 設定のセットアップ (IPv4 と IPv6)	69
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)	70
最大転送単位 (MTU) の設定 (IPv4 と IPv6)	70
ネットワークセキュリティの設定.....	70
CMC ウェブインタフェースによるネットワークセキュリティの設定.....	70
RACADM を使用した CMC ネットワークセキュリティの設定.....	71
CMC の仮想 LAN タグプロパティ.....	71
RACADM を使用した CMC 用 VLAN タグプロパティの設定.....	71
ウェブインタフェースを使用した CMC の仮想 LAN タグプロパティの設定.....	72
サービスの設定.....	72
CMC ウェブインタフェースを使用したサービスの設定.....	73
RACADM を使用したサービスの設定.....	73
CMC 拡張ストレージカードの設定.....	73
シャールグループのセットアップ.....	74
シャールグループへのメンバーの追加.....	75
リーダーからのメンバーの削除.....	75
シャールグループの無効化.....	75
メンバーシャーシでの個別のメンバーの無効化.....	76
メンバーシャーシまたはサーバーのウェブページの起動.....	76
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.....	76
MCM グループのサーバーインベントリ	77
サーバーインベントリレポートの保存.....	77
RACADM を使用した複数の CMC の設定.....	78
CMC 設定ファイルの作成.....	79
構文解析規則.....	80
CMC IP アドレスの変更.....	81
7 サーバーの設定	83
スロット名の設定.....	83
iDRAC ネットワークの設定.....	84
iDRAC QuickDeploy ネットワーク設定.....	84
個々のサーバー iDRAC の iDRAC ネットワーク設定の変更.....	86
RACADM を使用した iDRAC ネットワーク設定の変更.....	87

iDRAC VLAN タグの設定.....	87
RACADM を使用した iDRAC VLAN タグの設定.....	87
ウェブインタフェースを使用した iDRAC VLAN タグの設定.....	88
最初の起動デバイスの設定.....	88
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.....	89
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.....	89
RACADM を使用した最初の起動デバイスの設定.....	89
サーバー FlexAddress の設定.....	90
リモートファイル共有の設定.....	90
サーバークローンを使用した BIOS の設定.....	90
BIOS プロファイルページへのアクセス.....	91
プロファイルの追加.....	91
保存プロファイルの管理.....	91
プロファイルの適用.....	91
BIOS 設定の表示.....	92
プロファイルログの表示.....	92
完了状態とトラブルシューティング.....	92
シングルサインオンを使った iDRAC の起動.....	92
リモートコンソールの起動.....	93
8 アラートを送信するための CMC の設定.....	95
アラートの有効化または無効化.....	95
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.....	95
RACADM を使用したアラートの有効化または無効化.....	95
アラートのフィルタ.....	95
アラートの宛先設定.....	96
SNMP トラップアラート送信先の設定.....	96
E-メールアラートの設定.....	98
9 ユーザーアカウントと権限の設定.....	101
ユーザーのタイプ.....	101
ルートユーザー管理者アカウント設定の変更.....	105
ローカルユーザーの設定.....	105
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.....	105
RACADM を使用したローカルユーザーの設定.....	105
Active Directory ユーザーの設定.....	107
サポートされている Active Directory の認証機構.....	107
標準スキーマ Active Directory の概要.....	107
標準スキーマ Active Directory の設定.....	108
拡張スキーマ Active Directory 概要.....	111
拡張スキーマ Active Directory の設定.....	112
汎用 LDAP ユーザーの設定.....	120

汎用 LDAP ディレクトリを設定した CMC へのアクセス.....	121
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.....	121
RACADM を使用した汎用 LDAP ディレクトリサービスの設定.....	122
10 シングルサインオンまたはスマートカードログイン用 CMC の設定.....	123
システム要件.....	123
クライアントシステム.....	124
CMC.....	124
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.....	124
Kerberos Keytab ファイルの生成.....	124
Active Directory スキーマ用の CMC の設定.....	125
SSO ログイン用のブラウザの設定.....	125
Internet Explorer	125
Mozilla Firefox	125
スマートカードのログインに使用するブラウザの設定.....	125
Active Directory ユーザーに対する CMC SSO またはスマートカードログインの設定.....	126
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.....	126
Keytab ファイルのアップロード.....	126
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.....	127
11 CMC にコマンドラインコンソールの使用を設定する方法.....	129
CMC コマンドラインコンソールの特徴.....	129
CMC コマンドラインインタフェースコマンド.....	129
CMC での Telnet コンソールの使用.....	130
CMC での SSH の使用.....	130
サポート対象の SSH 暗号スキーム.....	130
SSH 経由の公開キー認証の設定.....	131
ターミナルエミュレーションソフトウェアの設定.....	133
Linux Minicom の設定.....	133
connect コマンドを使用したサーバーまたは I/O モジュールの接続.....	134
シリアルコンソールリダイレクト用に管理されたサーバー BIOS の設定.....	135
シリアルコンソールリダイレクトのための Windows の設定.....	136
起動中における Linux のシリアルコンソールリダイレクトのための設定.....	136
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.....	136
12 FlexAddress および FlexAddress Plus カードの使用.....	139
FlexAddress について.....	139
FlexAddress Plus について.....	140
FlexAddress のアクティブ化.....	140
FlexAddress Plus のアクティブ化.....	141

FlexAddress 有効化の検証.....	141
FlexAddress の非アクティブ化.....	142
FlexAddress 情報の表示.....	143
シャーシの FlexAddress 情報の表示.....	143
全サーバーの FlexAddress 情報の表示.....	143
個別サーバーの FlexAddress 情報の表示.....	144
FlexAddress の設定.....	144
FlexAddress を利用した Wake-On-LAN の使用.....	145
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.....	145
ワールドワイド名 / メディアアクセスコントロール (WWN/MAC) ID の表示.....	146
コマンドメッセージ.....	146
FlexAddress DELL ソフトウェア製品ライセンス契約.....	147
13 ファブリックの管理.....	151
無効な構成.....	151
初回電源投入シナリオ.....	151
IOM 正常性の監視.....	152
IOM 用ネットワークの設定.....	152
CMC ウェブインタフェースを使用した IOM 用ネットワークの設定.....	152
RACADM を使用した IOM 用ネットワークの設定.....	152
14 電力の管理と監視.....	155
冗長性ポリシー.....	155
AC 冗長性ポリシー.....	156
電源装置の冗長性ポリシー.....	156
動的電源供給.....	156
デフォルトの冗長性設定.....	157
AC 冗長性.....	157
電源装置冗長性.....	158
ハードウェアモジュールの電力バジェット.....	158
サーバースロットの電力優先順位の設定.....	159
サーバーへの優先度レベルの割り当て.....	160
CMC ウェブインタフェースを使用したサーバーへの優先度レベルの割り当て.....	160
RACADM を使用したサーバーへの優先度レベルの割り当て.....	160
電力消費量状態の表示.....	160
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.....	160
RACADM を使用した電力消費状態の表示.....	160
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.....	161
RACADM を使用した電力バジェット状態の表示.....	161
冗長性状態と全体的な電源正常性.....	161
PSU 障害発生後の電力管理.....	161
PSU を取り外した後の電力の管理.....	161

新規サーバーの電源供給ポリシー.....	162
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.....	163
電力バジェットと冗長性の設定.....	163
節電と電力バジェット.....	163
最大節電モード.....	164
電源バジェットを維持するためのサーバー電力の低減.....	164
110V PSU AC 操作.....	164
リモートロギング.....	164
外部電源管理.....	164
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.....	165
RACADM を使用した電力バジェットと冗長性の設定.....	166
電源制御操作の実行.....	167
シャーシに対する電源制御操作の実行.....	167
ウェブインタフェースを使用したシャーシでの電源制御操作の実行.....	167
RACADM を使用したシャーシでの電源制御操作の実行.....	167
サーバーに対する電源制御操作の実行.....	168
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.....	168
IOM での電源制御操作の実行.....	168
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.....	168
RACADM を使用した IOM での電源制御操作の実行.....	168
15 シャーシストレージの管理.....	171
ストレージコンポーネントの状態の表示.....	171
ストレージトポロジの表示.....	171
スロットへの仮想アダプタの割り当て.....	171
CMC ウェブインタフェースを使用したコントローラプロパティの表示.....	172
RACADM を使用したコントローラプロパティの表示.....	172
外部設定のインポートまたはクリア.....	172
CMC ウェブインタフェースを使用した物理ディスクプロパティの表示.....	173
RACADM を使用した物理ディスクドライブプロパティの表示.....	173
物理ディスクと仮想ディスクの識別.....	173
CMC ウェブインタフェースを使用したグローバルホットスペアの割り当て.....	173
RACADM を使用したグローバルホットスペアの割り当て.....	173
CMC ウェブインタフェースを使用した仮想ディスクプロパティの表示.....	174
RACADM を使用した仮想ディスクプロパティの表示.....	174
CMC ウェブインタフェースを使用した仮想ディスクの作成.....	174
仮想ディスクへの仮想アダプタアクセスポリシーの適用.....	174
CMC ウェブインタフェースを使用した仮想ディスクプロパティの変更.....	175
CMC ウェブインタフェースを使用したエンクロージャプロパティの表示.....	175
16 PCIe スロットの管理.....	177
CMC ウェブインタフェースを使用した PCIe スロットプロパティの表示.....	177

CMC ウェブインタフェースを使用したサーバーへの PCIe スロットの割り当て.....	177
RACADM を使用した PCIe スロットの管理.....	178
17 トラブルシューティングとリカバリ.....	179
RACDUMP を使用した設定情報、シャーシ状態、およびログの収集.....	179
対応インタフェース.....	179
SNMP Management Information Base (MIB) ファイルのダウンロード.....	180
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.....	180
電源のトラブルシューティング.....	180
アラートのトラブルシューティング.....	182
イベントログの表示.....	182
ハードウェアログの表示.....	182
シャーシログの表示.....	183
診断コンソールの使用.....	183
コンポーネントのリセット.....	184
シャーシ設定の保存と復元.....	184
ネットワークタイムプロトコル (NTP) エラーのトラブルシューティング.....	185
LED の色と点滅パターンの解釈.....	186
無応答 CMC のトラブルシューティング.....	187
問題特定のための LED の観察.....	187
DB-9 シリアルポートからのリカバリ情報の入手.....	188
ファームウェアイメージのリカバリ.....	188
ネットワーク問題のトラブルシューティング.....	189
コントローラのトラブルシューティング.....	189
18 LCD パネルインタフェースの使用.....	191
LCD のナビゲーション.....	191
メインメニュー.....	192
KVM マッピングメニュー.....	192
DVD マッピング.....	192
エンクロージャメニュー.....	193
IP 概要メニュー.....	193
設定.....	193
設定.....	193
診断.....	194
前面パネル LCD メッセージ.....	194
LCD モジュールとサーバー状態情報.....	195
19 よくあるお問い合わせ (FAQ)	199
RACADM.....	199
リモートシステムの管理と復元.....	199
Active Directory.....	201

FlexAddress と FlexAddressPlus.....	201
IOM.....	203

概要

Dell Chassis Management Controller (CMC) for Dell PowerEdge VRTX は、PowerEdge VRTX シャーシを管理するためのシステム管理ハードウェアおよびソフトウェアソリューションです。CMC には独自のマイクロプロセッサとメモリがあり、差し込まれたモジュラシャーシによって電源供給されます。

CMC により、IT 管理者は以下を行うことが可能になります。

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

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

CMC は、サーバーのために複数のシステム管理機能を提供します。電源および温度の管理が CMC の基本的な機能です。それら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 はシステムの電力要件を監視し、オプションの動的電源供給 (DPSE) モードをサポートします。このモードは、サーバーがスタンバイモードである間に電源装置を設定し、負荷および冗長性要件を動的に管理することによって、CMC が電力効率を改善することを可能にします。
 - CMC はリアルタイムの消費電力を報告します (タイムスタンプ付きの高低ポイントも記録されます)。
 - CMC は、オプションのエンクロージャ最大電力制限 (システム入力電力上限) をサポートしています。この機能は警告を行い、エンクロージャが定義された最大電力制限値未満を維持するように、サーバーの電力消費量を制限したり、新しいサーバーの電源投入を妨げるなどの処置を実行します。
 - CMC は冷却ファンと送風装置を監視し、それらの動作を実際の周囲温度と内部温度の測定値に基づいて自動的に制御します。
 - CMC は総合的なエンクロージャのインベントリ、および状態またはエラーレポートを提供します。
- CMC は、次に対する一元的な設定のためのメカニズムを提供します。
 - Dell PowerEdge VRTX エンクロージャのネットワークおよびセキュリティ設定。
 - 電源冗長性と電力上限値設定。
 - I/O スイッチおよび iDRAC ネットワーク設定。
 - サーバーモジュールにおける最初の起動デバイス。
 - I/O モジュールとサーバー間の I/O ファブリック整合性チェック。CMC はシステムハードウェアを保護するために、必要に応じてコンポーネントの無効化も行います。
 - ユーザーアクセスセキュリティ。

- ストレージコンポーネント。
- PCIe スロット。

温度、ハードウェアの誤った構成、停電、ファン速度、送風装置などの警告やエラーについて E-メールアラートや SNMP トラップアラートを送信するように CMC を設定することができます。

主な機能

CMC の機能は、管理とセキュリティ機能のグループに分けられます。

管理機能


CMC は次の管理機能を提供します。

- 冗長 CMC 環境。
- IPv4 および IPv6 のダイナミック DNS (DDNS) 登録。
- ローカルユーザー、Active Directory、および LDAP のログイン管理と設定。
- ECM (拡張冷却モード) やファンオフセットなどの高度な冷却オプションを有効にして冷却効果を高め、パフォーマンスを改善。
- SNMP、ウェブインタフェース、KVM、Telnet または SSH 接続を利用したリモートシステム管理と監視。
- 監視 — システム情報やコンポーネントのステータスへのアクセスを提供。
- システムイベントログへのアクセス — ハードウェアログとシャーシログへのアクセスを提供。
- 各種シャーシコンポーネントのファームウェアアップデート — CMC、サーバー上の iDRAC、シャーシインフラストラクチャ、およびシャーシストレージのファームウェアアップデートが可能。
- Lifecycle Controller を使用したシャーシ内の複数サーバーにおける、BIOS、ネットワークコントローラ、ストレージコントローラなどのサーバーコンポーネントのファームウェアアップデート。
- Dell OpenManage ソフトウェア統合 — Dell OpenManage Server Administrator または OpenManage Essentials (OME) 1.2 からの CMC ウェブインタフェースの起動が可能。
- CMC アラート — リモート Syslog E-メールメッセージまたは SNMP トラップを使って管理下ノードに関する潜在的な問題を通知。
- リモート電源管理 — 管理コンソールからのシャーシコンポーネントの電源オフやリセットなどのリモート電源管理機能を提供。
- 電源使用率の報告。
- Secure Sockets Layer (SSL) 暗号化 — ウェブインタフェースを介したセキュアリモートシステム管理を提供。
- Integrated Dell Remote Access Controller (iDRAC) ウェブインタフェースの起動ポイント。
- WS-Management のサポート。
- FlexAddress 機能 — 特定のスロットに対して、工場で割り当てられたワールドワイドネーム / メディアアクセスコントロール (WWN/MAC) ID のシャーシに割り当てられた WWN/MAC ID への置き換え
- シャーシのコンポーネントステータスおよび状態のグラフィック表示。
- 単一およびマルチスロットサーバーのサポート。
- LCD iDRAC 設定ウィザードによる iDRAC ネットワーク設定のサポート。
- iDRAC シングルサインオン。
- ネットワークタイムプロトコル (NTP) 対応。
- サーバーサマリ、電力レポート、電力制御ページの強化。
- 強制 CMC フェールオーバー、およびサーバーの仮想再装着。
- 最大 8 つまでのシャーシをリードシャーシから監視できるマルチシャーシ管理。
- シャーシ上のストレージコンポーネントの設定。

- サーバーおよびそれらの識別情報への PCIe スロットのマッピング。

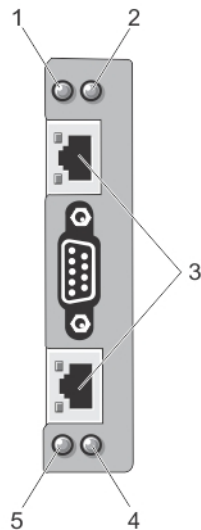
セキュリティ機能

CMC は次のセキュリティ機能を提供しています。

- パスワードレベルのセキュリティ管理 — リモートシステムへの無許可のアクセスを防止。
 - 次による一元ユーザー認証：
 - 標準スキーマまたは拡張スキーマ（オプション）を使用する **Active Directory**。
 - ハードウェアに保存されたユーザー ID とパスワード。
 - 役割ベースの権限 — システム管理者が各ユーザーに特定の権限を設定可能。
 - ウェブインタフェースを介したユーザー ID およびパスワードの設定。ウェブインタフェースは、128 ビット SSL 3.0 暗号化と 40 ビット SSL 3.0 暗号化（128 ビットが使用できない国向け）をサポート。
-  **メモ:** Telnet は SSL 暗号化をサポートしていません。
- 設定可能な IP ポート（該当する場合）。
 - IP アドレスごとのログイン失敗数の制限による、制限を超えた IP アドレスのログインの阻止。
 - 設定可能なセッション自動タイムアウトおよび複数の同時セッション数。
 - CMC に接続するクライアントの IP アドレス範囲を限定。
 - 暗号化層を使用してセキュリティを強化するセキュアシェル（SSH）。
 - シングルサインオン、二要素認証、公開キー認証。

シャーシの概要

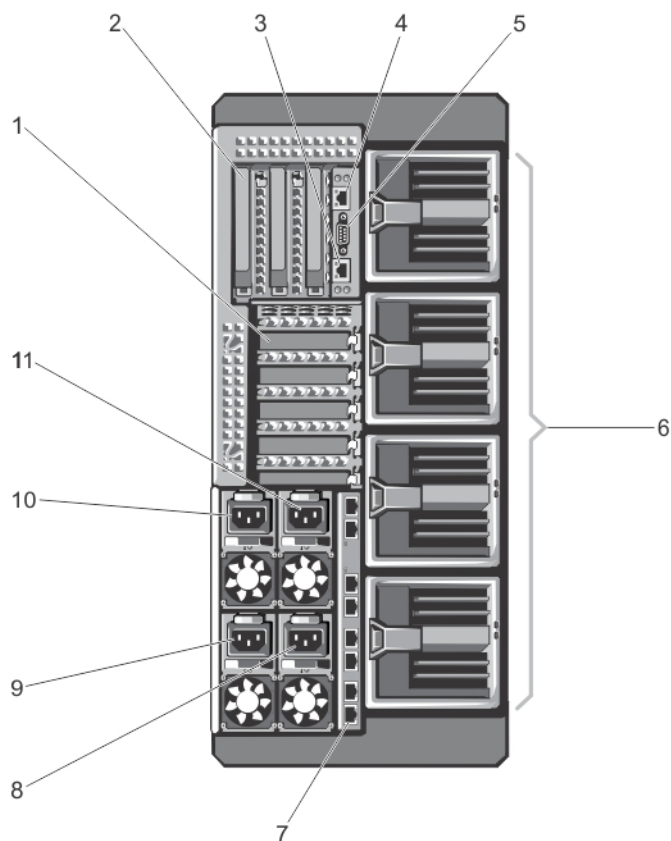
この図は、CMC コネクタを示しています。



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

項目	インジケータ、ボタン、またはコネクタ
4	電源インジケータ (CMC 2)
5	ステータス/識別インジケータ (CMC 2)

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



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

項目	インジケータ、ボタン、またはコネクタ
11	PSU 2

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

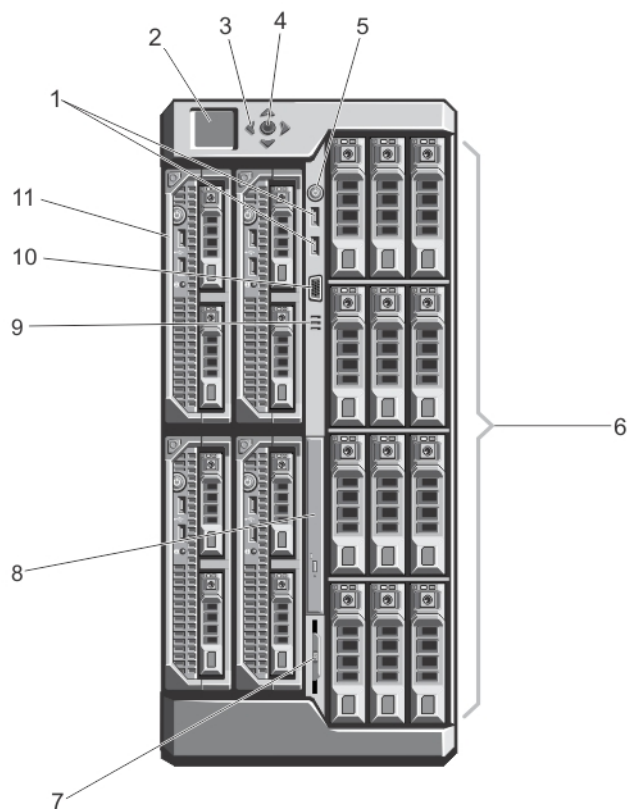



図 1. 前面パネルの機能とインジケータ - 3.5 インチハードディスクドライブシャーシ

項目	インジケータ、ボタン、またはコネクタ	説明
1	USB コネクタ (2)	キーボードとマウスをシステムに接続することができます。
2	LCD パネル	システムが正常に動作しているとき、またはシステムに注意が必要なときを示すシステム情報、状態、およびエラーメッセージが表示されます。
3	LCD メニュースクロールボタン (4)	カーソルを 1 段ずつ移動させます。
4	選択 (「チェック」) ボタン	LCD 画面上的のアイテムを選択して保存し、次の画面に移動します。
5	エンクロージャ電源インジケータ、電源ボタン	電源インジケータは、エンクロージャの電源が入っている時に点灯します。電源ボタンによってシステムへの PSU の供給を制御します。
6	ハードディスクドライブ (HDD)	2.5 インチハードドライブエンクロージャ 最大 25 台のホットスワップ対応 2.5 インチハードディスクドライブ。

項目	インジケータ、ボタン、またはコネクタ	説明
		3.5 インチハードディスクドライブエンクロージャ 最大 12 台のホットスワップ対応 3.5 インチハードディスクドライブ。
7	情報タグ	サービスタグ、NIC、MAC アドレス、システムの電力定格、および世界各国の規制機関マークなどのシステム情報を記録することができる、引き出し式のラベルパネル。
8	光学ドライブ (オプション)	オプションの SATA DVD-ROM ドライブまたは DVD+/-RW ドライブ 1 台。
9	通気孔	温度センサーの通気孔。  メモ: 適切な冷却を確保するため、通気孔がふさがれていないことを確認してください。
10	ビデオコネクタ	モニターをシステムに接続することができます。
11	サーバーモジュール	最大 4 台のエンクロージャ用に特別に構成された PowerEdge M520 または M620 サーバーモジュール。

対応リモートアクセス接続

次の表で、サポートされているリモートアクセスコントローラを示します。

表 1. 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	<ul style="list-style-type: none"> GB ポート: CMC ウェブインタフェースの専用ネットワークインタフェース。 DHCP サポート。 SNMP トラップおよび E-メールイベント通知。 iDRAC および I/O モジュール (IOM) 用のネットワークインタフェース。 システム起動、リセット、電源投入、シャットダウンコマンドを含む Telnet/SSH コマンドコンソールおよび RACADM CLI コマンドのサポート。
シリアルポート	<ul style="list-style-type: none"> 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。 アクティブ CMC のみへのアクセスを提供。

対応プラットフォーム

CMC は、PowerEdge VRTX プラットフォーム用に設計されたモジュラーサーバーをサポートします。CMC との互換性の詳細については、デバイスのマニュアルを参照してください。

最新の対応プラットフォームについては、dell.com/support/manualsにある『Dell Chassis Management Controller (CMC) for Dell PowerEdge VRTX バージョン 1.00 リリースノート』を参照してください。

対応ウェブブラウザ

対応ウェブブラウザの最新情報については、dell.com/support/manualsにある『Dell Chassis Management Controller (CMC) for Dell PowerEdge VRTX バージョン 1.00 リリースノート』を参照してください。

ライセンスの管理

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

ライセンスのタイプ

提供されるライセンスには次のタイプがあります。

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


ライセンスの取得

次のいずれかの方法を使用して、ライセンスを取得できます。

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


ライセンス操作

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


 **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。

一対一のライセンス管理には CMC、RACADM、および WS-MAN を使用し、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。

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

 **メモ:** 一部の機能では、機能の有効化に CMC の再起動が必要になります。

- エクスポート — バックアップ目的、またはサービス部品交換後の再インストールのために、インストールされているライセンスを外部ストレージデバイスにエクスポートします。エクスポートされたライセンスのファイル名と形式は <EntitlementID>.xml になります。
- 削除 — コンポーネントが欠落している場合に、そのコンポーネントに割り当てられているライセンスを削除します。ライセンスが削除されると、そのライセンスは CMC に保存されず、基本的な製品機能が有効になります。
- 置き換え — 評価ライセンスの有効期限を延長したり、評価ライセンスなどのライセンスタイプを購入ライセンスに変更したり、有効期限の切れたライセンスを延長するために、ライセンスを置換します。
- 評価ライセンスは、アップグレードされた評価ライセンスまたは購入したライセンスと置換できません。
- 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せん。
- 詳細表示 — インストールされているライセンス、またはサーバーにインストールされているコンポーネントに使用可能なライセンスの詳細を表示します。

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

ライセンスコンポーネントの状態または状況と使用可能な操作

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

表 1. 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	はい	いいえ	いいえ	いいえ	はい
アクティブなライセンス	はい	はい	はい	はい	はい
期限切れのライセンス	いいえ	はい	はい	はい	はい
ライ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	いいえ	はい	はい	いいえ	はい

CMC ウェブインタフェースを使用したライセンスの管理

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

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

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

RACADM を使用したライセンスの管理

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

racadm license <ライセンスコマンドタイプ>

RACADM コマンドの詳細については、dell.com/support/Manualsにある『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。

CMC におけるライセンス取得可能な機能

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

機能	Express	Enterprise	メモ
CMC ネットワーク	はい	はい	
CMC シリアルポート	はい	はい	
Active Directory と LDAP	いいえ	はい	
スロットおよび機能割り当て (PCIe と仮想アダプタ)	いいえ	はい	
RACADM (SSH、ローカル、およびリモート)	はい	はい	
WS-MAN	はい	はい	
snmp	はい	はい	
Telnet	はい	はい	
SSH	はい	はい	
ウェブベースのインタフェース	はい	はい	
E-メールアラート	はい	はい	
LCD 導入	はい	はい	
拡張 iDRAC 管理	はい	はい	
エンクロージャの復元とバックアップ	いいえ	はい	
サーバーモジュールファームウェアのアップデート	いいえ	はい	
リモート Syslog	いいえ	はい	
ディレクトリサービス	なし*	はい	*デフォルト以外のディレクトリサービス設定の場合、Express ライセンスで許可されるのはディレクトリサービスのリセットのみです。ディレクトリサービスのリセットは、ディレクトリサービスを工場出荷時のデフォルトに設定します。
iDRAC シングルサインオン	いいえ	はい	
2 要素認証	いいえ	はい	
PK 認証	いいえ	はい	
リモートファイル共有	はい	はい	
スロットリソース管理	いいえ	はい	
エンクロージャレベルの電力制限	なし*	はい	*デフォルト以外の電力制限設定の場合、Express ライセンスで許可されるのは電力制限の復元のみです。電力制限の復元は、電力制限設定を工場出荷時のデフォルトにリセットします。

動的電源供給	なし*	はい	*デフォルト以外の DPSE 設定の場合、Express ライセンスで許可されるのは DPSE の復元のみです。DPSE の復元は、DPSE を工場出荷時のデフォルトにリセットします。
マルチシャーシ管理	いいえ	はい	
詳細設定	いいえ	はい	
FlexAddress の有効化	なし*	はい	*デフォルト以外の FlexAddress 設定の場合、Express ライセンスで許可されるのはデフォルトの復元のみです。デフォルトの復元は、FlexAddress 設定を工場出荷時のデフォルトにリセットします。
PCIe アダプタマッピング	はい	はい	*Express ライセンスでは、サーバー 1 台につき最大 2 台の PCIe アダプタを割り当てることができます。
仮想アダプタからスロットへのマッピング	なし*	はい	*デフォルト以外の仮想アダプタマッピングの場合、Express ライセンスで許可されるのはデフォルトマッピングのみです。デフォルトの復元は、仮想アダプタのマッピングを工場出荷時のデフォルトに変更します。
仮想アダプタとスロットのマッピング解除	はい	はい	
サーバークローニング	いいえ	はい	
1 対多のサーバーファームウェアアップデート	いいえ	はい	
iDRAC の 1 対多設定	いいえ	はい	

他言語の CMC ウェブインタフェースの表示

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

対応管理コンソールアプリケーション

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

本ユーザーズガイドの使用方法

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。

- ウェブインタフェース：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、ウェブインタフェースから開くことができる『CMC for Dell PowerEdge VRTX 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/support/manuals にある『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。

その他の必要マニュアル

デルサポートサイトからマニュアルにアクセスします。dell.com/support/manuals では、本リファレンスガイドに加え、以下のガイドにアクセスできます。

- 『VRTX CMC オンラインヘルプ』には、ウェブインタフェースの使用に関する情報が記載されています。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ヘルプをクリックします。

- 『Chassis Management Controller for Dell PowerEdge VRTX RACADM バージョン 1.0 コマンドラインリファレンスガイド』には、VRTX 関連の RACADM 機能の使用に関する情報が記載されています。
- 『Dell Chassis Management Controller (CMC) for Dell PowerEdge VRTX バージョン 1.00 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 7 (iDRAC7) ユーザーズガイド』には、管理下システムでの iDRAC 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 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 Shared PowerEdge RAID Controller (PERC) 8 ユーザーズガイド』には、共有 PERC 8 カードの展開とストレージサブシステムの管理に関する情報が記載されています。このマニュアルは、dell.com/storagecontrollermanuals からオンラインで使用できます。
- Dell システム管理アプリケーションのマニュアルでは、システム管理ソフトウェアのインストール方法と使い方を説明しています。

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

- システムに付属している「安全にお使いいただくために」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。
- システムに同梱されている『Dell PowerEdge VRTX はじめに』には、システム機能の概要、システムの設定、および技術仕様が記載されています。
- システムに同梱のセットアッププレースマットには、初期のシステムセットアップおよび設定の情報が記載されています。
- サーバーモジュールの『オーナーズマニュアル』には、サーバーモジュールの機能に関する情報が記載されており、サーバーモジュールのトラブルシューティング方法およびサーバーモジュールのコンポーネントの取り付けまたは交換方法が説明されています。このマニュアルは、dell.com/poweredgemanuals からオンラインで使用できます。
- ラックソリューションに付属のマニュアルでは、システムをラックに取り付ける方法について説明しています（必要な場合）。
- 本書で使用されている略語や頭字語の正式名については、dell.com/support/manuals で『用語集』を参照してください。
- システム管理ソフトウェアのマニュアルでは、システム管理ソフトウェアの機能、動作要件、インストール、および基本操作について説明しています。
- 別途購入されたコンポーネントのマニュアルでは、これらのオプション装置の取り付けや設定について説明しています。
- システムに同梱のメディアには、システムと一緒に購入したオペレーティングシステム、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に関するマニュアルおよびツールが収録されています。システムの詳細については、システム上、およびシステムに同梱のシステムセットアッププレースマットにあるクイックリソースローケーター (QRL) をスキャンしてください。QRL アプリケーションをモバイルデバイスで有効にするには、モバイルプラットフォームからこのアプリケーションをダウンロードします。

システム、ソフトウェア、またはマニュアルの変更を説明するために、アップデート情報がシステムに付属していることがあります。このアップデート情報はしばしば他の文書の差し替となることから、常に最初にお読みください。

デルサポートサイトからの文書へのアクセス

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。

1. dell.com/support/manuals にアクセスします。

2. サービスタグまたはエクスプレスサービスコードをお持ちですか? セクションの **いいえ** ですべてのデル製品のリストから **選択する** を選択し、**続行** をクリックします。
3. **お使いの製品タイプ**を選択してください セクションで、**ソフトウェアとセキュリティ** をクリックします。
4. **お使いのデル製システム**を選択してください - **Software** セクションで、次の中から必要なリンクをクリックします。
 - クライアントシステム管理
 - エンタープライズシステム管理
 - リモートエンタープライズシステム管理
 - **Serviceability Tools**
5. マニュアルを表示するには、必要な製品バージョンをクリックします。



メモ: または、次のリンクを使用してマニュアルに直接アクセスすることもできます。

- エンタープライズシステム管理マニュアル — dell.com/openmanagemanuals
- リモートエンタープライズシステム管理マニュアル — dell.com/esmmanuals
- Serviceability Tools マニュアル — dell.com/serviceabilitytools
- クライアントシステム管理マニュアル — dell.com/OMConnectionsClient
- OpenManage Connections エンタープライズシステム管理マニュアル — dell.com/OMConnectionsEnterpriseSystemsManagement
- OpenManage Connections クライアントシステム管理マニュアル — dell.com/OMConnectionsClient

CMC のインストールと設定

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

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

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

作業を開始する前に

CMC 環境をセットアップする前に、PowerEdge VRTX 用の最新バージョンの CMC ファームウェアを [dell.com/support/](#) からダウンロードしてください。


また、システム付属の『*Dell Systems Management Tools およびマニュアル*』DVD があることを確認してください。


CMC ハードウェアの取り付け

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

シャーシ設定のチェックリスト

次のタスクによって、シャーシを正確に設定することができます。

1. 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必要があります。Ethernet ネットワークケーブルを、CMC アクティブポートから管理ネットワークに接続します。
2. シャーシに I/O モジュールを取り付け、ネットワークケーブルをシャーシに接続します。
3. シャーシにサーバーを挿入します。
4. シャーシを電源に接続します。
5. 手順 7 のタスクが完了したら、電源ボタンを押すか、CMC ウェブインターフェースからシャーシの電源をオンにします。
 **メモ:** サーバーの電源は入れないでください。
6. LCD パネルを使用して IP 概要に移動し、チェック ボタンをクリックして選択します。管理システムブラウザ (IE、Chrome、または Mozilla) で CMC の IP アドレスを使用します。CMC 向けに DHCP をセットアップするには、LCD パネルを使用して **メインメニュー** → **設定** → **ネットワーク設定** をクリックします。
7. ウェブブラウザを使用してデフォルトのユーザー名 (root) とパスワード (calvin) を入力することで、CMC IP アドレスに接続します。
8. CMC ウェブインターフェースで各 iDRAC に IP アドレスを指定し、LAN と IPMI インタフェースを有効にします。

 **メモ:** サーバーによっては、デフォルトで iDRAC LAN インタフェースが無効になっています。この情報は、CMC ウェブインタフェースの **サーバー概要** → **セットアップ** で確認できます。これは、高度なライセンスオプションである可能性があり、その場合は、サーバーごとに **セットアップ** 機能を使用する必要があります。

9. CMC ウェブインタフェースで、I/O モジュールを IP アドレスで入力します。IP アドレスは、**I/O モジュール概要** をクリックしてから、**セットアップ** をクリックすることで取得できます。
10. ウェブブラウザを介して各 iDRAC に接続し、iDRAC の最終設定を行います。デフォルトユーザー名は root、パスワードは calvin です。
11. ウェブブラウザを使用して I/O モジュールに接続し、I/O モジュールの最終設定を行います。
12. サーバーの電源を入れ、オペレーティングシステムをインストールします。

CMC の基本的なネットワーク接続

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

管理ステーションへのリモートアクセスソフトウェアのインストール

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


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

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

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

RACADM の Linux 管理ステーションへのインストール


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

 **メモ:** Red Hat Enterprise Linux 5 オペレーティングシステムでは、DVD が `-noexec mount` オプションで自動的にマウントされます。このオプションは DVD からの実行ファイルの実行を許可しません。DVD-ROM を手動でマウントしてから、コマンドを実行する必要があります。

4. **SYSMGMT/ManagementStation/linux/rac** ディレクトリに移動します。RAC ソフトウェアをインストールするには、次のコマンドを入力します。

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

5. RACADM コマンドについてのヘルプは、前のコマンドを実行した後で `racadm help` と入力します。RACADM の詳細については、『Chassis Management Controller for Dell PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。

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


Linux 管理ステーションから RACADM のアンインストール

1. 管理ステーション機能をアンインストールするシステムに、`root` でログインします。
2. 次の `rpm` クエリコマンドを使用して、インストールされている DRAC ツールのバージョンを確認します。
`rpm -qa | grep mgmtst-racadm`
3. アンインストールするパッケージバージョンを確認してから、`-e rpm -qa | grep mgmtst-racadm` コマンドを使って機能をアンインストールします。


ウェブブラウザの設定

シャーシに取り付けられている CMC、サーバー、モジュールはウェブブラウザを使って設定、管理することができます。dell.com/support/manuals にある『Dell Systems ソフトウェアサポートマトリックス』で「対応ブラウザ」の項を参照してください。

CMC と、ブラウザを使用する管理ステーションは、管理ネットワークと呼ばれる同じネットワーク上にある必要があります。セキュリティ要件に基づいて、管理ネットワークは隔離された非常に安全性の高いネットワークにすることができます。

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

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

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

プロキシサーバー

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

Internet Explorer

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

1. Internet Explorer を起動します。
2. ツール → インターネットオプション → 接続 をクリックします。
3. ローカルエリア ネットワーク (LAN) 設定 セクションで、LAN の設定 をクリックします。
4. プロキシサーバー セクションで、LAN にプロキシサーバーを使用する (これらの設定はダイヤルアップまたは VPN 接続には適用されません) オプションを選択し、詳細設定 をクリックします。

5. **例外** セクションのリストに管理ネットワーク上の **CMC** と **iDRAC** のアドレスをセミコロンで区切って追加します。エントリに **DNS** 名やワイルドカードを使用できます。

Mozilla Firefox

Mozilla Firefox バージョン 19.0 で例外リストを編集するには、次の手順を実行します。

1. Mozilla Firefox を起動します。
2. ツール → オプション をクリックするか (Windows で動作するシステムの場合)、または **編集** → **プリファレンス** (Linux で動作するシステムの場合) をクリックします。
3. **詳細設定**、**ネットワーク** タブの順にクリックします。
4. **設定** をクリックします。
5. **手動プロキシ設定** を選択します。
6. **プロキシなしの接続** フィールドに、管理ネットワーク上の **CMC** と **iDRAC** のアドレスをカンマで区切って追加します。エントリに **DNS** 名やワイルドカードを使用できます。

Microsoft フィッシングフィルタ

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

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

証明書失効リスト (CRL) のフェッチ

CMC にインターネットへのアクセスがない場合は、**Internet Explorer** の **証明書失効リスト (CRL)** のフェッチ機能を無効にしてください。この機能では、**CMC** ウェブサーバーなどのサーバーが、インターネットから取得する無効な証明書リストにある証明書を使用しているかどうかをテストします。インターネットにアクセスできない場合、ブラウザまたはリモート **RACADM** などのコマンドラインインタフェースを使って **CMC** にアクセスするときに、この機能が数秒の遅延の原因となる可能性があります。

CRL フェッチングを無効にするには、次の手順を実行します。

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

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

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

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

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

Internet Explorer でのアニメーションの有効化

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

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

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

CMC への初期アクセスのセットアップ

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



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

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

各サーバーとスイッチ I/O モジュールのネットワーク管理ポートにある CMC と iDRAC は、PowerEdge VRTX シェアード内の共通の内部ネットワークに接続されます。これにより、管理ネットワークをサーバーデータネットワークから分離することができます。中断のないシェアード管理へのアクセスには、このトラフィックを分離することが重要です。

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

シェアード管理はデータネットワークから分離することが推奨されます。データネットワーク上における潜在的なトラフィックのため、内部管理ネットワーク上の管理インタフェースがサーバー向けのトラフィックによって飽和状態になる可能性があります。このため、CMC と iDRAC 間の通信に遅延が発生します。これらの遅延は、iDRAC が稼動中であっても CMC が iDRAC をオフライン状態と見なしたりするなどの予期しないシェアード動作が発生し、他の不要な動作が発生する原因になります。管理ネットワークを物理的に分離することができない場合は、CMC および iDRAC トラフィックをそれぞれ異なる VLAN に分離するというオプションもあります。CMC と個々の iDRAC ネットワークインタフェースは、VLAN を使用するように設定することができます。

初期 CMC ネットワークの設定



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

CMC の初期ネットワーク設定は、CMC に IP アドレスが与えられる前でも後でも行うことができます。IP アドレスが与えられる前に CMC の初期ネットワーク設定を行う場合は、次のいずれかのインタフェースを使用できます。

- シェアードの前面にある LCD パネル
- Dell CMC シリアルコンソール

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


- シリアルコンソール、Telnet、SSH、Dell CMC コンソールなどのコマンドラインインタフェース (CLI)。

- リモート RACADM
- CMC ウェブインタフェース
- LCD パネルインタフェース

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

LCD パネルインタフェースを使用した CMC ネットワークの設定

クイックセットアップを使用した CMC の設定 (DHCP)

 **メモ:** LCD 表示の向きをカスタマイズするには (ラックモードまたはタワーモード)、上下のボタンを 2 秒間押し続けます。または、左右のボタンを使用することもできます。CMC LCD パネルで利用できるボタンの詳細については、「[LCD のナビゲーション](#)」を参照してください。

LCD パネルインタフェースを使用してネットワークを設定するには、次の手順を実行します。

1. シャーシの電源ボタンを押してシャーシに電源を入れます。電源投入されると、LCD パネルに一連の初期画面が表示されます。
2. メインメニューパネルで、**設定** を選択します。
3. **LCD 言語** パネルで、矢印ボタンを使用して言語を選択し、中央のボタンを押します。メインメニューパネルが表示されます。
4. **設定** を選択してから、**ネットワーク設定** を選択します。ネットワーク設定パネルで、DHCP を使用した CMC のクイックセットアップ、または詳細セットアップモードによるセットアップのいずれかを選択するように求められたら、矢印キーを使用して次のいずれかを選択します。

- クイックセットアップ (DHCP)
- 詳細セットアップ

5. **クイックセットアップ (DHCP)** を選択する場合、パネルには次のメッセージが表示されます。

DHCP アドレスを取得しようとしています。CMC ネットワークケーブルが接続されていることを確認してください。

中央のボタンを押して、数分待機します。パネルには、**お待ちください** メッセージが表示され、**IP 概要** パネルに **CMC IP 番号** が表示されます。

CMC IP4: <IP 番号>

中央のボタンを押し、再度中央のボタンを押します。メインメニューパネルが表示されます。

詳細セットアップを使用した CMC の設定

1. **ネットワーク設定** パネルで **詳細セットアップ** を選択した場合は、CMC を設定するかどうかをたずねる次のメッセージが表示されます。

CMC を設定しますか?


2. 詳細セットアッププロパティを使用して CMC を設定するには、中央のボタンをクリックし、手順 4 に進みます。使用しない場合は、iDRAC を設定するため、手順 14 に進みます。

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

効果的なネットワークスループットを得るために、ネットワーク速度の設定をネットワーク設定に一致させる必要があります。ネットワーク速度をネットワーク設定の速度より遅くすると、帯域幅の消費が増えてネットワーク通信が遅くなります。使用しているネットワークがネットワーク速度を超える速度をサポートしているかどうかを判断し、それに従って設定してください。ネットワーク設定がこれらの値のいずれにも一致しない場合は、**自動 (1 Gb)** オプションを選択するか、ネットワーク装置メーカーのユーザーマニュアルを参照してください。

4. **自動 (1 Gb)** を選択するには、中央のボタンを押し、再度中央のボタンを押します。手順 7 に進みます。**10 Mb** または **100 Mb** を選択した場合は、手順 5 に進みます。

5. **二重化** パネルで、ネットワーク環境に一致する二重モード (**全二重** または **半二重**) を選択するには、中央のボタンを押し、再度中央のボタンを押します。

 **メモ:** オートネゴシエーションが **オン** か、または **1000 Mb (1 Gbps)** が選択されている場合にはネットワーク速度および二重モードの設定は使用できません。オートネゴシエーションが **1** 台のデバイスで **オン** になっており、別の **1** 台では **オフ** である場合、オートネゴシエーションはもう **1** つのデバイスのネットワーク速度を判別できますが、二重モードは判別できません。この場合、オートネゴシエーション中に二重モードとして半二重モードが選択されます。このような二重モードの不一致は、ネットワーク接続を低速化します。

6. **プロトコル** パネルで、**CMC** に使用するインターネットプロトコル (**IPv4** のみ、**IPv6** のみ、または **両方**) を選択し、中央のボタンを押した後、再度中央ボタンを押します。
7. **IPv4** または **両方** を選択する場合は、**DHCP** モードを選択するか **静的** モードを選択するかに基づいて、手順 **9** または **10** に進みます。**IPv6** を選択する場合は、この手順の後半にある手順 **11** に進みます。
8. **モード** パネルで、**CMC** が **NIC** IP アドレスを取得する必要があるモードを選択します。**DHCP** を選択すると、**CMC** がお使いのネットワーク上の **DHCP** サーバーから自動的に **IP** 設定 (**IP** アドレス、マスク、およびゲートウェイ) を取得します。**CMC** には、ネットワーク上で割り振られた固有の **IP** アドレスが割り当てられます。**DHCP** を選択した場合は、中央のボタンを押し、再度中央のボタンを押します。**iDRAC** の **設定** パネルが表示されます。この手順後半の手順 **12** に進みます。
9. **静的** を選択した場合は、**LCD** パネルの指示にしたがって **IP** アドレス、ゲートウェイ、およびサブネットマスクを入力します。

入力した **IP** 情報が表示されます。中央のボタンを押し、再度中央のボタンを押します。**CMC** 設定画面に、入力した **静的 IP アドレス**、**サブネットマスク**、および **ゲートウェイ** の設定が表示されます。設定に誤りがないことを確認します。設定を修正するには、適切なボタンを押します。中央のボタンを押し、再び中央のボタンを押します。**DNS** を登録しますか? パネルが表示されます。

10. 登録するには、**DNS** **IP** アドレスを入力し、中央のボタンを押します。手順 **12** に進み、**iDRAC** を設定するかどうかを選択します。

11. 登録を選択しない場合は、手順 **12** に進みます。

12. **iDRAC** を設定するかどうかを指定します。

- いいえ：この手順の手順 **17** に進みます。
- はい：中央のボタンを押します。

また、**CMC** ウェブインタフェースから **iDRAC** を設定することもできます。

13. **プロトコル** パネルで、サーバーに使用する **IP** タイプ (**IPv4**、**IPv6**、または **両方**) を選択します。**IPv4** または **両方** を選択した場合、**DHCP** または **静的** を選択して手順 **14** に進みます。**IPv6** を選択した場合は、この手順の手順 **17** に進みます。

動的ホスト構成プロトコル (DHCP)

iDRAC がネットワーク上の **DHCP** サーバーから **IP** 設定 (**IP** アドレス、マスク、ゲートウェイ) を自動的に取得します。**iDRAC** には、ネットワーク上で割り振られた固有の **IP** アドレスが割り当てられます。中央のボタンを押し、この手順の手順 **16** に進みます。

静的

静的 を選択した場合は、**LCD** 画面の指示にしたがって **IP** アドレス、ゲートウェイ、およびサブネットマスクを手動で入力します。

静的 オプションを選択した場合は、中央のボタンを押し、次を行います。

- a. スロット **1** の **IP** を使用して自動的に増分するかどうかを尋ねる、次のメッセージが表示されます。

IP はスロット番号によって自動で増分します。

中央のボタンをクリックします。スロット **1** の **IP** 番号を入力するように求める、次のメッセージが表示されます。

スロット **1** (開始) **IP** を入力してください

スロット **1** の **IP** 番号を入力し、中央のボタンを押します。

- b. サブネットマスクを設定してから中央のボタンを押します。

- c. サブネットマスクを設定してから中央のボタンを押します。
 - d. ネットワーク概要画面に、入力した静的IPアドレス、サブネットマスク、およびゲートウェイの設定が表示されます。設定に誤りがないことを確認します。設定を修正するには、適切なボタンを押してから、中央のボタンを押します。
 - e. 入力した設定が正確であることを確認したら、手順 10 に進みます。
14. 有効または無効を選択して、IPMI over LAN を有効にするかどうかを指定します。中央のボタンを押して続行します。
15. iDRAC 設定 パネルに、次のメッセージが表示されます。
- 取り付けられているサーバーに設定を適用しますか？
- 取り付けられているサーバーにすべての iDRAC ネットワーク設定を適用するには、はいを選択して中央ボタンを押します。または、いいえを選択して中央ボタンを押し、この手順後半の手順 17 に進みます。
16. 次の iDRAC 設定 パネルに、以下のメッセージが表示されます。
- 新しく挿入されたサーバーに設定を自動適用しますか？
- 新しく取り付けられたサーバーにすべての iDRAC ネットワーク設定を適用するには、はいを選択して中央ボタンを押します。新しいサーバーがシャーシに挿入されると、以前に設定したネットワーク設定ポリシーを使用してサーバーを自動的に展開するかどうかを尋ねるメッセージが LCD に表示されます。新しく取り付けられたサーバーに iDRAC ネットワーク設定を適用しない場合は、いいえを選択して中央のボタンを押します。新しいサーバーがシャーシに挿入されても、iDRAC ネットワーク設定は設定されません。
17. iDRAC 設定 パネルに、次のメッセージが表示されます。
- すべてのエンクロージャ設定を適用しますか？
- すべてのエンクロージャ設定を適用するには、はいを選択して中央のボタンを押します。または、いいえを選択して中央のボタンを押します。
18. IP 概要 パネルで、指定した IP アドレスを見直して間違いがないことを確認します。設定を修正するには、戻る ボタンを押してから中央のキーを押して、その設定の画面に戻ります。IP アドレスを修正したら、中央のボタンを押します。
- 入力した設定が正確であることを確認したら、中央のボタンを押し、再度中央のボタンを押します。メニューパネルが表示されます。
- これで CMC と iDRAC は、ネットワークでも利用できるようになりました。ウェブインタフェース、シリアルコンソール、Telnet、SSH などの CLI を使用して、割り当てられた IP アドレスの CMC にアクセスできます。

CMC にアクセスするためのインタフェースおよびプロトコル

CMC ネットワークの設定後、さまざまなインタフェースを使って CMC にリモートアクセスすることができます。次の表は、リモートで CMC にアクセスするために使用できるインタフェースを示しています。





-  **メモ:** Telnet は他のインタフェースほどセキュアではないため、デフォルトでは無効です。Telnet は、ウェブ、ssh またはリモート RACADM を使用して有効化します。
-  **メモ:** 複数のインタフェースを同時に使用すると、予期しない結果が生じることがあります。

表 2. CMC インタフェース

インタフェース	説明
ウェブインタフェース	グラフィカルユーザーインタフェースを使って CMC へのリモートアクセスを提供します。ウェブインタフェースは CMC のファームウェア内蔵で、

インタフェース	説明
	<p>管理ステーションにある対応ウェブブラウザから NIC インタフェースを介してアクセスします。</p> <p>対応するウェブブラウザのリストは、デルサポートサイト dell.com/support/manuals にある『Dell Systems ソフトウェアサポートマトリック』で「対応ブラウザ」の項を参照してください。</p>
リモート RACADM コマンドラインインタフェース	<p>このコマンドラインユーティリティを使用して、CMC とそのコンポーネントを管理します。リモートまたはファームウェア RACADM を使用できません。</p> <ul style="list-style-type: none"> リモート RACADM は、管理ステーションで実行されるクライアントユーティリティです。これは、管理下システムで RACADM コマンドを使用するために帯域外ネットワークインタフェースを使用し、HTTP チャンネルも使用します。-e オプションは、ネットワークで RACADM コマンドを実行します。 ファームウェア RACADM には、SSH または telnet を使用して CMC にログインすることでアクセスできます。CMC IP、ユーザー名、またはパスワードを指定しなくても、ファームウェア RACADM コマンドを実行できます。RACADM プロンプトが開いたら、racadm プレフィックスなしで直接コマンドを実行できます。
シャーシ LCD パネル	<p>前面パネルの LCD を使用して、次の操作を行うことができます。</p> <ul style="list-style-type: none"> アラート、CMC IP または MAC アドレス、ユーザーによるプログラムが可能な文字列の表示 DHCP の設定 CMC 静的 IP の設定
Telnet	<p>ネットワーク経由で CMC へのコマンドラインアクセスを提供します。CMC コマンドラインからは、RACADM コマンドラインインタフェース、およびサーバーまたは IO モジュールのシリアルコンソールの接続に使われる connect コマンドを実行できます。</p> <p> メモ: Telnet は、セキュアなプロトコルではなく、デフォルトで無効になっています。Telnet は、パスワードのプレーンテキストでの送信を含む、すべてのデータを伝送します。機密情報を伝送する場合は、SSH インタフェースを使用してください。</p>
SSH	<p>SSH を使用して RACADM コマンドを実行します。高度なセキュリティを実現するために暗号化されたトランスポート層を使用して、Telnet コンソールと同じ機能を提供します。デフォルトで SSH サービスは CMC で有効になっており、無効にすることができます。</p>
WS-MAN	<p>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。LC-Remote Services 機能を使用するには、WinRM クライアント (Windows) や OpenWSMAN クライアント (Linux) などの WS-MAN クライアントを使用する必要があります。WS-MAN インタフェースのスクリプトには Power Shell および Python を使用することもできます。</p> <p>WSMAN は、システム管理用に使用される SOAP (Simple Object Access Protocol) ベースのプロトコルです。CMC は、Distributed Management Task Force (DMTF) の Common Information Model (CIM) ベースの管理情報の伝達に WS-Management を使用します。CIM 情報は、管理下システムで変更できるセマンティックタイプや情報タイプを定義します。</p>

インタフェース	説明
	<p>CMC WS-MAN の実装は、トランスポートセキュリティに対してポート 443 の SSL を使用し、基本認証をサポートしています。WS-Management で使用できるデータは、DMTF プロファイルおよび拡張プロファイルにマップされている、CMC 計装インタフェースによって提供されます。</p> <p>詳細については、次を参照してください。</p> <ul style="list-style-type: none"> • MOF およびプロファイル — delltechcenter.com/page/DCIM.Library • DMTF ウェブサイト — dmtof.org/standards/profiles/ • WS-MAN リリースノートファイル。 • www.wbem solutions.com/ws_management.html • DMTF WS-Management 仕様 : www.dmtf.org/standards/wbem/wsman <p>ウェブサービスインタフェースは、Windows WinRM や Powershell CLI、WSMANCLI などのオープンソースユーティリティ、Microsoft .NET などのアプリケーションプログラミング環境といったクライアントインフラストラクチャを活用することで、使用できます。</p> <p>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。</p>

 **メモ:** CMC ユーザー名およびパスワードのデフォルト値は、それぞれ root および calvin です。

その他のシステム管理ツールを使用した CMC の起動

CMC は、Dell Server Administrator または Dell OpenManage Essentials を使って起動することもできます。Dell Server Administrator を使って CMC インタフェースにアクセスするには、管理ステーションで Server Administrator を起動します。Server Administrator ホームページの左ペインで、システム → メインシステムシャーシ → リモートアクセスコントローラ の順にクリックします。詳細については、dell.com/support/manuals にある『Dell Server Administrator ユーザーズガイド』を参照してください。

CMC ファームウェアのダウンロードとアップデート

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

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


シャーシの物理的な場所とシャーシ名の設定

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

ウェブインタフェースを使用したシャーシの物理的な場所とシャーシ名の設定

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

1. 左ペインで、**シャーシ概要** に移動し、**セットアップ** をクリックします。
2. **一般シャーシ設定** ページで、場所のプロパティとシャーシ名を入力します。シャーシプロパティの設定の詳細については、『CMC オンラインヘルプ』を参照してください。

 **メモ:** シャーシの場所フィールドはオプションです。データセンター、通路、ラック、およびラックスロットフィールドを使用して、シャーシの物理的な場所を示すことを推奨します。

3. **適用** をクリックします。設定が保存されます。

RACADM を使用したシャーシの物理的な場所とシャーシ名の設定

コマンドラインインターフェースを使用してシャーシ名、場所、日付、および時刻を設定するには、**setsysinfo** コマンドおよび **setchassisname** コマンドを参照してください。詳細については、『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。

CMC の日付と時刻の設定

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

CMC ウェブインター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ースを使用して日付と時刻を設定するには、dell.com/support/manuals にある『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』で、**config** コマンドおよび **cfgRemoteHosts** データベースプロパティグループの項を参照してください。


シャーシ上のコンポーネントを識別するための LED の設定

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

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

CMC ウェブインター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 → **トラブルシューティング**。
 - シャーシ概要 → シャーシコントローラ → **トラブルシューティング**。
 - シャーシ概要 → **サーバー概要** → **トラブルシューティング**。
-  **メモ:** このページではサーバーのみを選択できます。
- シャーシ概要 → **I/O モジュール概要** → **トラブルシューティング**。

- ストレージ → トラブルシューティング。



メモ: このページでは、物理ディスクドライブおよび仮想ディスクのみを選択できます。

コンポーネント LED を点滅させるには、物理ディスクドライブまたは仮想ドライブに対応する **すべて選択/選択解除** オプションを選択し、**点滅** をクリックします。コンポーネント LED の点滅を無効にするには、その LED に対応する **すべて選択/選択解除** オプションをクリアして、**点滅解除** をクリックします。

RACADM を使用した LED の点滅の設定

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

`racadm setled -m <module> [-l <ledState>]`。ここで <module> には、設定する LED が存在するモジュールを指定します。設定オプションは次のとおりです。

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

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

- 0 — 点滅なし (デフォルト)
- 1 — 点滅

`racadm raid <operation> <component FQDD>`。ここで **動作値** は blink または unblink であり、FQDD はコンポーネントの物理ディスクドライブおよび仮想ディスクのものです。

CMC プロパティの設定


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

冗長 CMC 環境について

アクティブ CMC の機能が停止した場合にそれを引き継ぐスタンバイ CMC をインストールできます。冗長 CMC は事前にインストールされている場合がありますが、あとからインストールすることもできます。完全な冗長性または最良のパフォーマンスを得るには、CMC ネットワークが適切にケーブル配線されていることが重要です。

フェイルオーバーは、次のような場合に行われます。


- RACADM `cmcchangeover` コマンドを実行。dell.com/support/manuals にある『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』で `cmcchangeover` コマンドの項を参照してください。
- アクティブ CMC で RACADM `racreset` コマンドを実行。dell.com/support/manuals にある『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』で、`racreset` コマンドの項を参照してください。
- ウェブインタフェースからアクティブ CMC をリセット。「[電力制御操作の実行](#)」で説明されている **電力制御操作** の `Reset CMC` オプションを参照してください。
- アクティブ CMC からネットワークケーブルを外した場合。
- シャーシからアクティブ CMC を取り外した場合。
- アクティブ CMC で CMC ファームウェアフラッシュアップデートを行った場合。
- アクティブ CMC が機能していない場合

 **メモ:** CMC フェールオーバーが発生すると、すべての iDRAC 接続およびすべてのアクティブな CMC セッションがログオフされます。セッションからログオフしたユーザーは、新しいアクティブ CMC に再接続する必要があります。

スタンバイ CMC について

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

スタンバイ CMC はアクティブ CMC と同じ設定とプロパティを引き継ぎます。両方の CMC のファームウェアリビジョンは同じである必要がありますが、スタンバイ CMC に設定を全く同じにする必要はありません。

 **メモ:** CMC の取り付けについては、『VRTX オーナーズマニュアル』を参照してください。スタンバイ CMC への CMC ファームウェアのインストール手順については、「[ファームウェアのアップデート](#)」を参照してください。

CMC フェイルセーフモード

冗長 CMC によるフェールオーバー保護と同じく、PowerEdge VRTX エンクロージャでもサーバーと I/O モジュールを機能停止から保護するフェイルセーフモードを有効化します。フェイルセーフモードは、CMC がシャーシを制御していないときに有効になります。CMC フェールオーバー時間中、または単一の CMC 管理が失われている間は、次の状態が発生します。

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

CMC 管理の喪失につながる状況のいくつかを以下に示します。

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

 **メモ:** エンクロージャは、単一、または冗長 CMC で構成することができます。冗長 CMC 構成では、プライマリ CMC がエンクロージャまたは管理ネットワークとの通信を失うと、スタンバイ CMC がシャーシ管理をそれを引き継ぎます。

アクティブ CMC の選択プロセス

2 つの CMC スロットには違いはありません。つまり、スロットは優先順位を示しているわけではなく、最初に取り付けた、または起動した CMC がアクティブ CMC の役割を担います。CMC が 2 つ取り付けられている状態で AC 電源を入れると、CMC シャーシスロット 1 に取り付けられている CMC が通常アクティブ CMC の役割を担います。アクティブ CMC は青色 LED で示されます。

既に電源が入っているシャーシに2台の CMC を挿入する場合、自動アクティブまたはスタンバイネゴシエーションに最大2分間かかることがあります。通常のシャーシの動作は、ネゴシエーション完了時に再開されます。

冗長 CMC の正常性状態の取得

ウェブインタフェースでスタンバイ CMC の正常性状態を表示できます。ウェブインタフェースでの CMC の正常性状態へのアクセスについての詳細は、「[シャーシ情報の表示とシャーシとコンポーネントの正常性状態の監視](#)」を参照してください。

前面パネルの設定

次を設定することができます。

- 電源ボタン
- LCD
- DVD ドライブ


電源ボタンの設定

シャーシの電源ボタンを設定するには、次の手順を実行します。

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

LCD の設定

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

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

KVM を使用したサーバーへのアクセス

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

CMC ウェブインタフェースを使用したサーバーの KVM へのマッピング

KVM コンソールがシャーシに接続されていることを確認してください。

KVM にサーバーをマップするには、次の手順を実行します。

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

LCD を使用した KVM へのサーバーのマッピング

KVM コンソールがシャーシに接続されていることを確認してください。

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

DVD ドライブへのサーバーのマッピング

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


1. 左ペインで、**シャーシ概要** → **前面パネル** → **セットアップ** をクリックします。
2. **前面パネル設定** ページの **DVD ドライブの設定** セクションで、次を行います。
DVD マップ済み ドロップダウンメニューから、サーバーのひとつを選択します。シャーシ DVD ドライブアクセスを必要とするサーバーを選択します。
3. **適用** をクリックします。

CMC へのログイン

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


CMC ウェブインタフェースへのアクセス

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

 **メモ:** Microsoft Internet Explorer を使用しており、プロキシで接続して、エラーメッセージ The XML page cannot be displayed が表示された場合、続行するためにはプロキシを無効にする必要があります。


CMC ウェブインタフェースにアクセスするには、次の手順を実行します。

1. システムでサポートされるウェブブラウザを開きます。
対応ウェブブラウザの最新情報については、dell.com/support/manuals にある『Dell Systems ソフトウェア サポートマトリックス』を参照してください。
2. アドレス フィールドに次の URL を入力し、<Enter> を押します。
 - IPv4 アドレスを使用して CMC にアクセスするには : `https://<CMC IP address>`
デフォルトの HTTPS ポート番号 (ポート 443) が変更されている場合は、次のように入力します : `https://<CMC IP address>:<port number>`
 - IPv6 アドレスを使用して CMC にアクセスするには : `https://[<CMC IP address>]`
デフォルトの HTTPS ポート番号 (ポート 443) が変更された場合、`https://[<CMC IP address>]:<port number>` を入力します。ここで、<CMC IP address> は CMC の IP アドレスであり、<port number> は HTTPS ポート番号です。
CMC のログインページが表示されます。

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

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

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


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

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


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

1. **ユーザー名** フィールドにユーザー名を入力します。

- CMC ユーザー名: <ユーザー名>
- Active Directory ユーザー名: <ドメイン><ユーザー名>、<ドメイン>/<ユーザー名> または <ユーザー名>@<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. 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。

4. **OK** をクリックします。

必要なユーザー権限で CMC にログインしました。


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。

スマートカードを使用した CMC へのログイン

この機能を使用するには、Enterprise ライセンスが必要です。スマートカードを使用して CMC にログインできます。スマートカードでは、次の2層構造のセキュリティを実現する2要素認証 (TFA) が提供されます。

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

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


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

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

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

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

1. 次のリンクを使用して CMC にログインします。 <https://<cmcname.domain-name>>
スマートカードの挿入を求める **CMC ログイン** ページが表示されます。

 **メモ:** デフォルトの HTTPS ポート番号 (ポート 80) を変更した場合は、<cmcname.domain-name>:<port number> を使って CMC ウェブページにアクセスします。ここで、cmcname は CMC の CMC ホスト名、domain-name はドメイン名、port number は HTTPS のポート番号をそれぞれ表します。

2. スマートカードを挿入し、**ログイン** をクリックします。

PIN ダイアログボックスが表示されます。


3. PIN を入力し、送信 をクリックします。

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

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

シングルサインオンを使用した CMC へのログイン

シングルサインオン (SSO) が有効になっている場合は、ユーザー名やパスワードなどのドメインユーザー認証資格情報を入力しないで CMC にログインできます。この機能を使用するには、Enterprise ライセンスが必要です。


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

SSO を使用して CMC にログインする前に、次の点を確認してください。


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

SSO を使用して CMC にログインするには、次の手順を実行します。

1. ネットワークアカウントを使ってクライアントシステムにログインします。
2. `https://<cmcname.domain-name>` を使用して CMC ウェブインター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 ウェブインターフェースにアクセスします。ここで、**cmcname** は CMC の CMC ホスト名、**domain-name** はドメイン名、**port number** は HTTPS のポート番号をそれぞれ表します。

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

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

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

シリアル、Telnet、または SSH 接続を介して CMC にログインできます。

管理ステーションのターミナルエミュレータソフトウェアおよび管理下ノード BIOS を設定した後、次のタスクを実行して CMC にログインします。

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

RACADM を使用した CMC へのアクセス

RACADM は、テキストベースのインターフェースを通して CMC の設定と管理を行えるコマンド群を提供します。RACADM には、Telnet/SSH またはシリアル接続の使用、KVM 上での Dell CMC コンソールの使用、あるいは

は管理ステーションにインストールされた RACADM コマンドラインインタフェースのリモート使用によってアクセスできます。

RACADM インタフェースは、次のように分類されます。

- リモート RACADM オプションと CMC の DNS 名または IP アドレスを使って、管理ステーション上で RACADM コマンドを実行できます。
 - **メモ:** リモート RACADM は、『Dell Systems Management Tools and Documentation DVD』に含まれており、管理ステーションにインストールされます。
- ファームウェア RACADM - Telnet、SSH、またはシリアル接続を使って CMC にログインすることを可能にします。ファームウェア RACADM では、CMC ファームウェアの一部である RACADM 実装を実行できます。

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

RACADM の詳細については、『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。

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

公開キー認証を使用した CMC へのログイン

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

SSH 経由で CMC にログインする前に、公開キーがアップロードされていることを確認します。この機能を使用するには、Enterprise ライセンスが必要です。

たとえば、次のとおりです。

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

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

複数の CMC セッション

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

表 3. 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

インタフェース	セッション数
SSH	4

ファームウェアのアップデート

以下のファームウェアをアップデートできます。

- CMC - アクティブとスタンバイ
- シャーシインフラストラクチャ
- I/O モジュール
- iDRAC7

以下のサーバーコンポーネントのファームウェアをアップデートできます。

- iDRAC
- BIOS
- 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

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。

現在インストールされているファームウェアのバージョンの表示

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

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

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

- シャーシ概要 → アップデート
- シャーシ概要 → シャーシコントローラ → アップデート
- シャーシ概要 → サーバー概要 → サーバーコンポーネントアップデート
- シャーシ概要 → I/O モジュール概要 → アップデート
- シャーシ概要 → ストレージ → ストレージコンポーネントアップデート

ファームウェアアップデート ページに、リストされた各コンポーネントに対するファームウェアの現行バージョンが表示され、ファームウェアを最新バージョンにアップデートすることを可能にします。

シャーシに iDRAC がリカバリモードにある前世代のサーバーが存在する場合、または iDRAC のファームウェアが破損していることを CMC が検出した場合には、これらの前世代 iDRAC も **ファームウェアアップデート** ページにリストされます。

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

RACADM を使用して iDRAC と CMC の IP 情報、および CMC サービスタグまたは資産タグを表示するには、`racadm getsysinfo` サブコマンドを実行します。その他の RACADM コマンドの詳細については、『**Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド**』を参照してください。

CMC ファームウェアのアップデート

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



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

システムコンポーネントファームウェアのアップデートにウェブユーザーインタフェースのセッションを利用する場合、ファイル転送時間を許容できるように **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、場合によっては最大 30 分かかることがあります。アイドルタイムアウト値を設定するには、「[サービスの設定](#)」を参照してください。

CMC ファームウェアのアップデート中における、シャーシ内の冷却ファンの一部または全部の 100% 速度での回転は、通常の動作です。

シャーシに冗長 CMC を取り付けた場合、両方の CMC を一度の操作で同時に同じファームウェアバージョンにアップデートすることをお勧めします。ファームウェアのバージョンが異なるときにフェールオーバーが発生した場合、不測の結果が生じることがあります。

ファームウェアが正常にアップロードされた後、アクティブ CMC がリセットされ、一時的に使用不可になります。スタンバイ CMC が存在する場合、スタンバイとアクティブの役割が入れ替わり、スタンバイ CMC がアクティブ CMC になります。アクティブ CMC のみにアップデートが適用される場合、リセット完了後、アクティブ CMC はアップデートされたイメージを実行せず、スタンバイ CMC だけがそのイメージを持つことになります。概して、アクティブおよびスタンバイ CMC には同一ファームウェアバージョンを維持することを強くお勧めします。

スタンバイ CMC がアップデートされたら、新しくアップデートした CMC がアクティブ CMC になり、以前のバージョンのファームウェアを持つ CMC がスタンバイ CMC になるように、CMC の役割を交代させます。役割の交代については、『**Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド**』の `cmcchangeover` コマンドの項を参照してください。このコマンドの実行は、2 番目の CMC のファームウェアをアップデートする前に、アップデートが正常に完了し、新しいファームウェアが正しく機能していることを確認するために役立ちます。両方の CMC をアップデートしたら、`cmcchangeover` コマンドを使用して CMC をそれぞれ元の役割に戻すことができます。CMC ファームウェアバージョン 2.x は、`cmcchangeover` コマンドを実行することなく、プライマリ CMC と冗長 CMC の両方をアップデートします。


リセット中に他のユーザーが切断されないように、CMC にログインできる認定ユーザーに通知し、**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、左ペインから **シャーシ概要** を選択し、**ネットワーク** をクリックしてから、**セッション** をクリックします。

CMC 間でファイル転送を行う場合、転送中にファイル転送アイコンが回転します。アイコンが動かない場合は、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ます。ブラウザでのアニメーションの許可については、「[Internet Explorer でのアニメーションの再生](#)」を参照してください。

RACADM を使用した CMC ファームウェアのアップデート


RACADM を使用して CMC ファームウェアをアップデートするには、fwupdate サブコマンドを使用します。RACADM コマンドの詳細については、『Chassis Management Controller for PowerEdge VRTX RACADM コントローラコマンドラインリファレンスガイド』を参照してください。

ウェブインタフェースを使用した CMC ファームウェアのアップデート

 **メモ:** CMC ファームウェアをアップデートする前に、シャーシをオンになっている場合でも、シャーシ内のサーバーはすべてオフになっ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 (スタンバイ CMC が存在する場合は複数になります) の **ターゲットのアップデート** 列に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 vrtx_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。
5. スタンバイ CMC の場合、アップデートが完了すると **アップデート状態** フィールドに **完了** が表示されます。アクティブ CMC の場合、ファームウェアのアップデート処理の最終段階でブラウザセッションおよび CMC との接続が一時的に失われますが、これはアクティブ CMC がネットワークに接続されていないためです。アクティブ CMC の再起動時は、数分待ってからログインする必要があります。CMC のリセット後、新しいファームウェアが **ファームウェアアップデート** ページに表示されます。

 **メモ:** ファームウェアのアップデート後、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。

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。
- 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。
- **アップデート状況** フィールドにはファームウェアのアップデート状態が表示されます。

 **メモ:** CMC のアップデートプロセスには数分かかる場合があります。

シャーシインフラストラクチャファームウェアのアップデート

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



メモ: シャーシインフラストラクチャファームウェアをアップデートする場合は、シャーシの電源がオンで、サーバーの電源がオフになっていることを確認してください。

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

1. 次のいずれかのページに移動します。
 - シャーシ概要 → アップデート。
 - シャーシ概要 → シャーシコントローラ → アップデート。
2. ファームウェアアップデート ページの シャーシインフラストラクチャファームウェア セクションにある **ターゲットのアップデート** 列でオプションを選択し、シャーシインフラストラクチャファームウェアの **適用** をクリックします。
3. ファームウェアアップデート ページで **参照** をクリックし、適切なシャーシインフラストラクチャファームウェアを選択します。
4. **ファームウェアアップデートを開始する** をクリックし、**はい** をクリックします。
ファームウェアアップデートの **進行状況** セクションに、ファームウェアアップデートの状態情報が表示されます。状態インジケータは、イメージファイルのアップロード中表示されます。ファイルの転送時間は接続速度によって異なります。内部アップデート処理が始まると、ページが自動的に更新され、ファームウェアアップデートタイマーが表示されます。

追加手順：

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

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

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

RACADM を使用してシャーシインフラストラクチャをアップデートするには、fwupdate サブコマンドを使用します。RACADM コマンドの使用の詳細については、『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。

サーバー iDRAC ファームウェアのアップデート

iDRAC7 以降のファームウェアをアップデートできます。この機能を使用するには、Enterprise ライセンスが必要です。

iDRAC 搭載のサーバーの場合、iDRAC ファームウェアバージョンは 1.40.40 以降である必要があります。ファームウェアアップデート後は、iDRAC (サーバー上) がリセットされ、一時的に使用不可になります。



メモ: iDRAC ファームウェアをアップデートするには、CMC に SD カードが装備されている必要があります。

RACADM を使用したサーバー iDRAC ファームウェアのアップデート

iDRAC7 のファームウェアは fwupdate コマンドを実行してアップデートすることができます。これには、Enterprise ライセンスが必要です。iDRAC7 バージョンは 1.40.40 以降である必要があります。コマンドの詳細については、『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。

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。
 - シャーシ概要 → I/O モジュールの概要 → アップデート。

ファームウェアアップデート ページが表示されます。



メモ:

サーバー iDRAC ファームウェアは、[シャーシ概要 → サーバー概要 → アップデート](#) を使用してアップデートすることもできます。詳細については、「[サーバーコンポーネントファームウェアのアップデート](#)」を参照してください。

2. iDRAC7 ファームウェアをアップデートするには、**iDRAC7 ファームウェア** セクションで、ファームウェアをアップデートするサーバーの **アップデート** リンクをクリックします。
サーバーコンポーネントアップデート ページが表示されます。続行するには、「[サーバーコンポーネントファームウェアのアップデート](#)」を参照してください。
3. **ファームウェアイメージ** フィールドに、管理ステーションまたは共有ネットワーク上のファームウェアのイメージファイルへのパスを入力するか、**参照** をクリックし、ファイルの保存場所にナビゲートします。デフォルトの iDRAC ファームウェアイメージ名は **firring.imc** です。
4. **ファームウェアアップデートを開始する** をクリックし、**はい** をクリックします。
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。進捗バーがアップロードプロセス状態を示します。ファイル転送時間は、接続速度に応じて変化します。内部アップデート処理が始まると、ページが自動的に更新され、ファームウェアアップデートタイマーが表示されます。



メモ: 追加手順:

- ファイル転送時に、**更新** アイコンをクリックしたり、他のページへ移動しないでください。
- アップデートプロセスをキャンセルするには、**ファイル転送およびアップデートのキャンセル** をクリックします。このオプションは、ファイル転送時にのみ、利用可能です。
- **アップデート状況** フィールドにはファームウェアのアップデート状態が表示されます。

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

サーバーコンポーネントファームウェアのアップデート

Lifecycle Controller サービスは各サーバー上で利用することができ、iDRAC によって円滑化されます。Lifecycle Controller サービスを使って、サーバー上のコンポートおよびデバイスのファームウェアの管理を行うことができます。Lifecycle Controller はファームウェアのアップデートに最適化アルゴリズムを使用して再起動の数を効率的に削減します。

Dell Update Packages (DUP) は Lifecycle Controller を使ったファームウェアのアップデートを行うために使用します。オペレーティングシステムドライバパックコンポーネントの DUP はこの制限を超えており、拡張ストレージ機能を使用して別途アップデートする必要があります。

Lifecycle Controller は、iDRAC6 以降のサーバー向けの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 以降になっている必要があります。



メモ: Lifecycle Controller ベースのアップデート機能を使用する前に、サーバー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必要もあります。

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

- BIOS
- Lifecycle Controller
- iDRAC

CMC ウェブインタフェースを使用してサーバーコンポーネントファームウェアをアップデートするには、**シヤリ概要 → 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。

サーバーが Lifecycle Controller サービスをサポートしない場合、**コンポーネント/デバイスのファームウェア インベントリ** セクションでは **未対応** と表示されます。最新世代のサーバーには、Lifecycle Controller ファームウェアをインストールして iDRAC ファームウェアをアップデートし、サーバーで Lifecycle Controller サービスが有効になるようにします。古い世代のサーバーの場合は、このアップグレードができません。

通常、Lifecycle Controller 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によってインストールされます。対応するサーバーでは、**.usc** ファイル拡張子を持つ特別な修復パッケージまたはインストールパッケージを利用できます。このファイルによって、ネイティブの iDRAC ウェブブラウザインタフェースで利用できるファームウェアアップデート機能から Lifecycle Controller ファームウェアをインストールすることが可能になります。

また、サーバー OS で実行された適切なインストールパッケージを介して、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 が有効化されていない可能性があります。

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。

- iDRAC6 サーバーの場合、起動コンソールで次のメッセージが表示されたら、<Ctrl><E>を押します。リモートアクセスセットアップには 5 秒内に <CTRL-E> を押ししてください。
次に、セットアップ画面で **システムサービス** 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。
- iDRAC7 サーバーの場合、起動コンソールで **セットアップユーティリティ** にアクセスするには、<F2> キーを押します。
- **セットアップユーティリティ** メインメニュー ページで **iDRAC 設定 → Lifecycle Controller** に移動し、**有効** をクリックします。**セットアップユーティリティ** メインメニュー ページに移動し、**終了** をクリックして設定を保存します。

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

Lifecycle Controller と対応サーバーコンポーネント、およびデバイスファームウェアの管理についての詳細は、

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


サーバーコンポーネントアップデート ページでは、サーバーにあるさまざまなファームウェアコンポーネントをアップデートすることができます。このページの機能を使用するには次の権限が必要です。

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

権限が不十分である場合には、サーバー上のコンポーネントおよびデバイスのファームウェアインベントリの表示のみが可能となります。そのサーバーでは、どのタイプの Lifecycle Controller 操作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。


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。

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ーを絞り込むための、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。

場合によっては、1つの BIOS ファームウェアアップデートイメージが複数のサーバーモデルと互換性を持つことがあります。この互換性が将来失われる場合に備え、このような最適化は無視されます。

- 自動フィルタリングは、ネットワークインタフェースコントローラ (NIC) や RAID コントローラのファームウェアアップデートにおいて重要です。これらのデバイスカテゴリには、種々のタイプやモデルが存在します。同様に、ファームウェアアップデートイメージ (DUP) が最適化された形式 (ある特定のカテゴリ内の複数のタイプまたはモデルのデバイスをアップデートできるように DUP がプログラムされている) で利用できる場合もあります。

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

デバイスをフィルタするには、次の手順を実行します。

1. 左ペインで **サーバー概要** に移動し、**アップデート** をクリックします。
2. **サーバーコンポーネントアップデート ページの コンポーネント/デバイスアップデートフィルタ** セクションで、次の1つまたは複数を選択します。
 - BIOS
 - iDRAC
 - Lifecycle Controller
 - 32 ビット診断
 - オペレーティングシステムのドライバパック
 - ネットワーク I/F コントローラ

- RAID コントローラ

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

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

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

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


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

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

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

ファームウェアインベントリの表示

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

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

CMC ウェブインタフェースを使用したファームウェアインベントリの表示

ファームウェアインベントリを表示するには、次の手順を実行します。

1. 左ペインで **サーバー概要** をクリックし、**アップデート** をクリックします。
2. **サーバーコンポーネントアップデート** ページの **コンポーネント/デバイスファームウェアインベントリ** セクションで、ファームウェアインベントリの詳細を確認します。このページでは、次の情報を表示できます。
 - 現在 Lifecycle Controller サービスをサポートしないサーバーは、**未対応** としてリストされます。iDRAC ファームウェアのみを直接アップデートすることができる代替ページへのハイパーリンクが表示されます。このページは iDRAC ファームウェアアップデートのみをサポートし、サーバー上の他のコンポーネントおよびデバイスはサポートしません。iDRAC ファームウェアアップデートは Lifecycle Controller サービスには依存しません。
 - サーバーが **準備中** と表示されている場合は、ファームウェアインベントリを取得した時点でサーバー上の iDRAC がまだ初期化中であったことを示します。iDRAC が完全に動作可能になるまで待ってから、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。
 - 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。

この処置を自動化する、または iDRAC 設定ユーティリティ (iDRAC7 用) が起動コンソールからアクセスできるオプションを提供するには、次の手順を実行します。

1. iDRAC7 サーバーの場合、起動コンソールで **セットアップユーティリティ** にアクセスするには、<F2> を押します。
 2. **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。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 4. コンポーネントおよびデバイス情報


フィールド	説明
スロット	シャーシ内でサーバーが装着されているスロットを表示します。スロット番号は 1~4 (シャーシ内の使用可能な 4 個のスロット用) の連番 ID で、シャーシ内におけるサーバーの場所の識別に役立ちます。スロットに装着されているサーバーが 4 台未満の場合は、サーバーが装着されているスロットのスロット番号のみが表示されます。
名前	各スロット内のサーバーの名前を表示します。
モデル	サーバーのモデルを表示します。
コンポーネント/デバイス	サーバー上のコンポーネントおよびデバイスの情報を表示します。列幅が狭すぎる場合、マウスオーバーツールで説明が表示されます。
現在のバージョン	サーバー上のコンポーネントとデバイスの現在のバージョンを表示します。
ロールバックバージョン	サーバー上のコンポーネントとデバイスのロールバックバージョンを表示します。
ジョブ状態	そのサーバー上でスケジュールされているすべての操作のジョブ状態を表示します。ジョブ状態は継続的に動的にアップデートされます。状態が完了となっているジョブの完了が検出されると、コンポーネントまたはデバイスのいずれかでファームウェアバージョンが変更された場合に備えて、サーバー上のコンポーネントおよびデバイスのファームウェアバージョンが自動的に更新されます。現在の状況の隣には情報アイコンも表示され、現在のジョブ状態に関する追加情報を提供します。この情報は、アイコンをクリックする、またはカーソルを置くことで表示できます。
アップデート	サーバー上のファームウェアをアップデートするコンポーネントまたはデバイスをクリックして選択します。

RACADM を使用したファームウェアインベントリの表示

RACADM を使用してファームウェアインベントリを表示するには、getversion コマンドを使用します。
`racadm getversion -l [-m <module>] [-f <filter>]`

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

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。Lifecycle Controller 操作を許可しないでください。

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

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

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

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

スケジュールのために操作を送信した後は、他のページに移動しないでください。他のページに移動しようとすると、ページ移動をキャンセルするための確認のメッセージが表示されます。キャンセルしない場合は、操作が中断されます。操作の中断（特にアップデート操作中の中断）は、ファームウェアイメージファイルのアップロードが正しく完了せず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. **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. **ロールバックバージョン** 列で、ファームウェアをロールバックするコンポーネントまたはデバイスのオプションを選択します。
4. 次のオプションのいずれかを選択します。
 - **今すぐ再起動** - サーバーをただちに再起動します。
 - **次の起動時** - サーバーを後ほど手動で再起動します。
5. **ロールバック** をクリックします。以前インストールされたファームウェアのバージョンが、選択されたコンポーネントまたはデバイスに再インストールされます。

サーバーコンポーネントファームウェアのアップデート

1つ、または複数のサーバー全体で、選択されたコンポーネントまたはデバイスにファームウェアイメージの後続バージョンをインストールすることができます。ファームウェアイメージは、ロールバック操作のために **Lifecycle Controller** 内で使用可能になっています。この機能を使用するには、**Enterprise** ライセンスが必要です。

 **メモ:** iDRAC およびオペレーティングシステムドライバパックファームウェアのアップデートでは、**拡張ストレージ** 機能が有効になっていることを確認してください。

サーバーコンポーネントファームウェアのアップデートを初期化する前に、ジョブキューをクリアすることをお勧めします。サーバー上のすべてのジョブのリストは、**Lifecycle Controller** **ジョブ** ページで使用できます。このページでは、単一または複数のジョブの削除、またはサーバー上の全ジョブのパージが可能です。**BIOS** アップデートはサーバーのモデル固有です。場合によっては、サーバー上でのファームウェアアップデート用に単一のネットワークインタフェースコントローラ (NIC) デバイスが選択されていたとしても、そのサーバーにあるすべての NIC デバイスにアップデートが適用されることがあります。この動作は **Lifecycle Controller** の機能性、とりわけ **Dell Update Package (DUP)** に含まれるプログラミングに固有です。現時点では、サイズが **48MB** 未満の **Dell Update Package (DUP)** がサポートされています。

アップデートファイルのイメージサイズがこれより大きい場合、ジョブ状態にはダウンロードの失敗が示されます。サーバーで複数のサーバーコンポーネントのアップデートが試行された場合、すべてのファームウェアアップデートファイルの合計サイズが **48 M** を超えることがあります。このような場合には、それらのコ


ンポーネントアップデートのうちの1つのアップデートが、アップデートファイルの切り捨てによって失敗します。1つのサーバー上で複数のコンポーネントをアップデートするには、最初に Lifecycle Controller および 32 ビット診断のコンポーネントをまとめてアップデートすることをお勧めします。これにはサーバーの再起動が不要で、比較的短時間で完了します。その後、その他のコンポーネントをまとめてアップデートすることができます。

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

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


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

1. 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. **アップデート** 列で、ファームウェアを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オプションを選択します。


 **メモ:** <Ctrl> キーを使用して、適用可能なすべてのサーバーにわたってアップデート対象のコンポーネントまたはデバイスのタイプを選択します。<Ctrl> キーを押し続けると、すべてのコンポーネントが黄色でハイライトされます。<Ctrl> キーを押したまま、**アップデート** 列内の対応するオプションを選択することにより、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イメージファイルのセレクトラをリストした別の表が表示されます。各コンポーネントタイプに対してファームウェアイメージファイル用に1つのセレクトラが表示されます。

ネットワークインタフェースコントローラ (NIC) および RAID コントローラといった一部のデバイスには、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。この自動フィルタ動作の第一の理由は、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、または組み合わせられた 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。

4. 選択されたコンポーネントまたはデバイスに対する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 用の Dell Update Package (DUP) ファイルです。
5. 次のオプションのいずれかを選択します。
 - **今すぐ再起動** - 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。

 **メモ:** このタスクは、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に対しては無効です。これらのデバイスに対しては、サーバーの再起動操作はただちに実行されます。

6. **アップデート** をクリックします。選択されたコンポーネントまたはデバイスのファームウェアバージョンがアップデートされます。

スケジュールされたサーバーコンポーネントファームウェアジョブの削除

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

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

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

スケジュール済みサーバーコンポーネントファームウェアジョブを削除するには：

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

CMC ウェブインタフェースを使用したストレージコンポーネントのアップデート

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

ストレージコンポーネントをアップデートするには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** → **ストレージ** → **アップデート** をクリックします。
2. **ストレージコンポーネントアップデート** ページで、**参照** をクリックし、先にダウンロードした DUP を選択し、**アップロード** をクリックします。
DUP が CMC にアップロードされ、**ファームウェアアップデート状態** ページが次の情報と共に表示されます。
 - 経過時間
 - ターゲットコンポーネント
 - 現在のファームウェアバージョン
 - アップデート状況

CMC を使用した iDRAC ファームウェアのリカバリ

iDRAC ファームウェアは通常、iDRAC ウェブインタフェースなどの iDRAC インタフェース、SM-CLP コマンドラインインタフェース、または support.dell.com からダウンロードしたオペレーティングシステム固有のアップデートパッケージを使ってアップデートされます。詳細については、『iDRAC7 ユーザーズガイド』を参照してください。

早い世代のサーバーでは、新しい iDRAC ファームウェアアップデート処理を使用して破損したファームウェアを回復することができます。CMC が iDRAC ファームウェアの破損を検知すると、**ファームウェアアップデート** ページにそのサーバーがリストされます。「[サーバー iDRAC ファームウェアのアップデート](#)」に記載されているタスクを完了してください。

シャーシ情報の表示とシャーシとコンポーネントの正常性状態の監視

次に関する情報の表示と正常性の監視を行うことができます。

- アクティブとスタンバイの CMC
- すべてのサーバーと個々のサーバー
- IO モジュール
- ファン
- 電源装置ユニット (PSU)
- 温度センサー
- ハードディスクドライブ
- LCD アセンブリ
- ストレージコントローラ
- PCIe デバイス

シャーシとコンポーネント概要の表示

CMC ウェブインタフェースにログインすると、**シャーシ正常性** ページにシャーシの正常性とそのコンポーネントが表示されます。そこでは、シャーシとそのコンポーネントがグラフィカルに表示されます。表示は動的にアップデートされ、現在の状況を反映するようにコンポーネントのサブグラフィックオーバーレイおよび



テキストヒントも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、**シャーシ概要** をクリックします。システムがシャーシ、アクティブとスタンバイの CMC、サーバーモジュール、IO モジュール (IOM)、ファン、送風装置、電源装置ユニット (PSU)、LCD アセンブリ、ストレージコントローラ、および PCIe デバイスの総合的な正常性ステータスを表示します。各コンポーネントをクリックすると、そのコンポーネントの詳細情報が表示されます。さらに、CMC ハードウェアログ内の最新のイベントも表示されます。詳細については『オンラインヘルプ』を参照してください。

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

シャーシの図解

シャーシは正面図と背面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）。サーバー、DVD、HDD、KVM、およびLCD 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。コンポーネントを選択すると青色で表示され、必要なコンポーネントイメージをクリックする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、そのコンポーネントの追加情報を示すツールチップが表示されます。

表 5. サーバーアイコン状況

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

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 — 最も頻繁にアクセスするページと最も頻繁に実行される操作へ移動できるリンクが提供されます。選択したコンポーネントに適用されるリンクのみが、この項に表示されます。

サーバーモデル名とサービスタグの表示

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

1. 左ペインで、**サーバー概要** をクリックします。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。

シャーシ概要の表示

シャーシ概要の情報を表示するには、左ペインで、**シャーシ概要** → **プロパティ** → **概要** をクリックします。

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

シャーシコントローラ情報と状態の表示

シャーシコントローラ情報と状態を表示するには、CMC ウェブインタフェースで、**シャーシ概要** → **シャーシコントローラ** をクリックします。

シャーシコントローラ状態 ページが表示されます。詳細については『オンラインヘルプ』を参照してください。

すべてのサーバーの情報および正常性状態の表示

すべてのサーバーの正常性状態を表示するには、次のいずれかを実行します。

- **シャーシ概要** をクリックします。**シャーシ正常性** ページに、シャーシに取り付けられているすべてのサーバーの概要がグラフィック表示されます。サーバーの正常性状態は、サーバーサブグラフィックのオーバーレイによって示されます。シャーシ正常性の詳細については、『オンラインヘルプ』を参照してください。
- **シャーシ概要** → **サーバー概要** をクリックします。**サーバー状態** ページに、シャーシ内のサーバーの概要が示されます。詳細については『オンラインヘルプ』を参照してください。

IOM の情報および正常性状態の表示

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

1. **シャーシ概要** をクリックします。
シャーシ正常性 ページが表示されます。左ペインのグラフィックは、シャーシの背面図、正面図、および側面図を表示し、IOM の正常性状態も含まれています。IOM 正常性状態は、IOM サブグラフィックのオーバーレイによって示されます。テキストヒントはその IOM の追加情報を示します。右ペインに IOM の情報を表示するには、IOM サブグラフィックをクリックします。
2. **シャーシ概要** → **I/O モジュール概要** に移動します。


I/O モジュール状態 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『オンラインヘルプ』を参照してください。

ファンの情報と正常性状態の表示

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

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


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

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

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

次のイベントが発生した場合、CMC はアラートを生成し、ファン速度を上げます。

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

 **メモ:** サーバーにおける CMC または iDRAC ファームウェアのアップデート中は、シャーシ内のファンの一部またはすべてが 100 パーセントの速度で回転します。これは正常な動作です。


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


1. シャーシ概要 に移動します。

シャーシ正常性 ページが表示されます。シャーシ図の下部にはシャーシの左側が表示され、これにはファンの正常性状態が含まれています。ファンの正常性状態は、ファンのサブグラフィックのオーバーレイで示されます。カーソルをファンのサブグラフィック上に移動します。テキストヒントがファンに関する追加情報を提供します。ファン情報を右ペインに表示するには、ファンのサブグラフィックをクリックします。

2. シャーシ概要 → ファン に移動します。

ファン状態 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。

ファン <番号> が重要な下限しきい値の下回っています。

詳細については『オンラインヘルプ』を参照してください。

ファンの設定

ファンオフセット — シャーシのストレージおよび PCIe 領域により高い冷却機能を提供する機能です。この機能によって、HDD、共有 PERC コントローラ、および PCIe カードスロットへの送風量を増やすことができます。ファンオフセットは、たとえば、通常よりも高い冷却能力を必要とするハイパワーまたはカスタム PCIe

カードを使用するときに使用します。ファンオフセット機能には、オフ、低、中、高のオプションがあります。これらの設定は、それぞれ最大速度の 20%、50%、および 100% のファン速度オフセット（上昇）に対応します。また、オプションごとに最小速度設定もあり、低は 35%、中は 65%、および高は 100% となります。

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

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

オフセット機能を設定するには、**シャーシ概要** → **ファン** → **セットアップ** 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** ドロップダウンメニューから適切な値を選択します。

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

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

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

ファンオフセット関連の RACADM コマンドの詳細については、dell.com/support/Manuals にある『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。

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

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

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

ECM モードを設定するには、**シャーシ概要** → **ファン** → **セットアップ** に移動します。**詳細ファン設定** ページで、**拡張冷却モード** に対応する **値** ドロップダウンメニューから適切な値を選択します。

ECM 機能の詳細については、『オンラインヘルプ』を参照してください。

前面パネルプロパティの表示

前面パネルプロパティを表示するには、次の手順を実行します。

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

KVM の情報および正常性状態の表示

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

1. **シャーシ概要** をクリックします。

シャーシ正常性 ページが表示されます。左ペインに、シャーシの正面図と、KVM の正常性状態が表示されます。KVM の正常性状態は、KVM サブグラフィックのレイオーバーで示されます。ポインタを KVM サブグラフィック上に移動すると、対応するテキストヒントまたは画面ヒントが表示されます。テキストヒントは KVM に関する追加情報を提供します。KVM サブグラフィックをクリックすると、KVM 情報が右ペインに表示されます。

2. または、**シャーシ概要** → **前面パネル** をクリックします。

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

LCD の情報と正常性の表示

LCD の正常性状態を表示するには、次の手順を実行します。

1. 左ペインで **シャーシ概要** をクリックします。

シャーシ正常性 ページが表示されます。左ペインには、シャーシの正面図が表示されます。LCD の正常性状態は、LCD サブグラフィックのオーバーレイで示されます。

2. カーソルを LCD のサブグラフィックに移動します。対応するテキストのヒントまたはスクリーンのヒントに、LCD の追加情報が表示されます。

3. LCD サブグラフィックをクリックして、右ペインに LCD 情報を表示します。詳細については『オンラインヘルプ』を参照してください。


または、**シャーシ概要** → **前面パネル** → **プロパティ** → **状態** に移動します。**状態** ページの **LCD のプロパティ** で、シャーシ上で使用可能な LCD の状態を表示できます。詳細については『オンラインヘルプ』を参照してください。

温度センサーの情報と正常性状態の表示

温度センサーの正常性状態を表示するには、次の手順を実行します。

左ペインで、**シャーシ概要** → **温度センサー** をクリックします。

温度センサー状態 ページには、シャーシ全体（シャーシおよびサーバー）の温度プローブの状態と読み取り値が表示されます。詳細については『オンラインヘルプ』を参照してください。


 **メモ:** 温度プローブの値を編集することはできません。しきい値を超える変化にはアラートが生成され、ファン速度が変化します。たとえば、CMC 環境温度プローブがしきい値を超えると、シャーシ内のファンの速度が上昇します。

CMC の設定

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

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

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

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

CMC のセットアップおよび基本的な設定の終了後、以下を実行できます。

- 必要に応じてネットワーク設定を変更。
- CMC にアクセスするインタフェースを設定。
- LCD ディスプレイを設定。
- 必要に応じてシャーシグループを設定。
- 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。
- CMC ユーザーを追加し、権限を設定。
- E-メールアラートおよび SNMP トラップを設定して有効化。
- 必要に応じて電力制限ポリシーを設定。

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


- &#
- < と > の同時使用
- ; (セミコロン)


CMC ネットワーク LAN 設定の表示と変更

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

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

IPv6 が起動時に有効化されると、3 つのルータ要請がその後 4 秒ごとに送信されます。外部ネットワークのスイッチがスパニングツリープロトコル (SPT) を実行している場合、外部スイッチポートが 13 秒以上ブロックされ、IPv6 ルータ要請が送信されます。このような場合、IPv6 ルータによってルータ広告が不要に送信されるまで、IPv6 接続性が制限される期間が生じる場合があります。

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

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

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

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

1. 左ペインで、**シャーシ概要**をクリックし、**ネットワーク**をクリックします。**ネットワーク設定**ページに現在のネットワーク設定が表示されます。
2. 必要に応じて、**全般**、**IPv4**、または **IPv6** の設定を変更します。詳細については『オンラインヘルプ』を参照してください。
3. 各セクションで **変更の適用** をクリックして、設定を適用します。

RACADM を使用した CMC ネットワーク LAN 設定の表示と変更

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

- getniccfg
- getconfig
- cfgCurrentLanNetworking

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

- getconfig
- cfgIPv6LanNetworking


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

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

CMC ネットワークインタフェースの有効化


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

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

 **メモ:** CMC NIC はデフォルトで有効になっています。


CMC IPv4 アドレス指定を有効または無効にするには、次を入力します。

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

 **メモ:** CMC IPv4 アドレス設定はデフォルトで有効になっています。

CMC IPv6 アドレス指定を有効または無効にするには、次を入力します。

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

 **メモ:** CMC IPv6 アドレス指定はデフォルトで無効になっています。

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

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

```
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0 racadm config -g  
cfgLanNetworking -o cfgNicIpAddress <静的 IP アドレス> racadm config -g
```

```
cfgLanNetworking -o cfgNicGateway <静的ゲートウェイ> racadm config -g
cfgLanNetworking -o cfgNicNetmask <静的サブネットマスク>
```

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

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

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

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

DHCP を使用した DNS IP アドレスの取得機能の有効/無効化

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


DNS アドレス用 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 0
```

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 0
```

DNS の静的 IP アドレスの設定

 **メモ:** 静的 DNS IP アドレス設定は、DNS アドレス機能向けの DHCP が無効化されない限り、有効ではありません。

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

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


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

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

DNS 設定のセットアップ (IPv4 と IPv6)

- **CMC 登録**—DNS サーバーで CMC を登録するには、次を入力します。
racadm config -g cfgLanNetworking -o cfgDNSRegisterRac 1

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

 **メモ:** 次の設定は、`cfgDNSRegisterRac` を 1 に設定することで DNS サーバー上に CMC を登録した場合にのみ有効です。

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

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

ここで、<name> は 63 文字以内の英数字とハイフンを使って指定します。例えば、次のようになります。e: `cmc-1, d-345`

- **DNS ドメイン名** — デフォルトの DNS ドメイン名は空白文字 1 文字です。DNS ドメイン名を設定するには、次を入力します。

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

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

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

オートネゴシエーション機能を有効にすると、この機能は最も近いルーターまたはスイッチと通信することによって、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。デフォルトでは、オートネゴシエーション機能が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。

最大転送単位 (MTU) の設定 (IPv4 と IPv6)

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

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


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

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

ネットワークセキュリティの設定

ネットワークセキュリティの設定は IPv4 のみで可能です。

CMC ウェブインタフェースによるネットワークセキュリティの設定

 **メモ:** 次のタスクを実行するには、`シャシ設定システム管理者` 権限が必要です。

CMC ウェブインタフェースを使用してネットワークセキュリティを設定するには：

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** ページが表示されます。
2. **IPv4 設定** セクションで、**詳細設定** をクリックします。 **ネットワークセキュリティ** ページが表示されます。
3. IP 範囲と IP ブロック値を指定します。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. 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 CMC ネットワークセキュリティの設定

IP フィルタは受信ログインの IP アドレスを、次の **cfgRacTuning** プロパティで指定する IP アドレス範囲と比較します。

- **cfgRacTunelpRangeAddr**
- **cfgRacTunelpRangeMask**

受信 IP アドレスからのログインは、次のアドレスが同一である場合に限り許可されます。

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

CMC の仮想 LAN タグプロパティ

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

RACADM を使用した CMC 用 VLAN タグプロパティの設定

1. 外部シャーシ管理ネットワークの VLAN 機能を有効にします。

```
racadm config -g cfgLanNetworking -o cfgNicVlanEnable 1
```
2. 外部シャーシ管理ネットワークの VLAN ID を指定します。

```
racadm config -g cfgLanNetworking -o cfgNicVlanID <VLAN id>
```

<VLAN id> の有効値は 1~4000、および 4021~4094 の範囲の数値です。デフォルト値は 1 です。
たとえば、次のとおりです。

```
racadm config -g cfgLanNetworking -o cfgNicVlanID 1
```
3. 次に、外部シャーシ管理ネットワークの VLAN 優先順位を指定します。

```
racadm config -g cfgLanNetworking -o cfgNicVlanPriority <VLAN priority>
```

<VLAN priority> の有効値は 0~7 です。デフォルト値は 0 です。
たとえば、次のとおりです。

```
racadm config -g cfgLanNetworking -o cfgNicVlanPriority 7
```

また、1つのコマンドで VLAN ID と VLAN 優先順位を指定できます。

```
racadm setniccfg -v <VLAN id> <VLAN priority>
```

たとえば、次のとおりです。

```
racadm setniccfg -v 1 7
```
4. CMC VLAN を削除するには、外部シャーシ管理ネットワークの VLAN 機能を無効にします。

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

次のコマンドを使用しても、**CMC VLAN** を削除できます。

```
racadm setniccfg -v
```

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

ウェブインタフェースを使用して CMC 用 LAN を設定するには：

1. 次のいずれかのページに移動します。
 - 左ペインで、**シャーシ概要** をクリックし、**ネットワーク** → **VLAN** をクリックします。
 - 左ペインで、**シャーシ概要** → **サーバー概要** をクリックし、**ネットワーク** → **VLAN** をクリックします。
- VLAN タグ設定** ページが表示されます。VLAN タグはシャーシプロパティです。このタグは、コンポーネントを削除した後もシャーシに残ります。
2. **CMC** セクションで **CMC** 用に **VLAN** を有効にし、優先順位を設定して **ID** を割り当てます。各フィールドの詳細については、『**オンラインヘルプ**』を参照してください。
 3. **適用** をクリックします。VLAN のタグ設定が保存されます。
シャーシ概要 → サーバー → セットアップ → **VLAN** から、このページにアクセスすることもできます。

サービスの設定


CMC では、次のサービスの設定と有効化ができます。

- **CMC** シリアルコンソール — シリアルコンソールを使用した **CMC** へのアクセスを有効にします。
- **ウェブサーバー** — **CMC** ウェブインタフェースへのアクセスを有効にします。ウェブサーバーを無効にすると、リモート **RACADM** も無効になります。
- **SSH** — ファームウェア **RACADM** を介した **CMC** へのアクセスを有効にします。
- **Telnet** — ファームウェア **RACADM** を介した **CMC** へのアクセスを有効にします。
- **RACADM** — **RACADM** を使用した **CMC** へのアクセスを有効にします。
- **SNMP** — イベントに対して **SNMP** トラップを送信するよう **CMC** を有効にします。
- **リモート Syslog** — **CMC** によるリモートサーバーへのイベントのログを有効にします。この機能を使用するには、**Enterprise** ライセンスが必要です。

CMC には、クライアント間で暗号化されたデータをインターネット経由で受け入れて転送するための業界標準の **SSL** セキュリティプロトコルを設定したウェブサーバーが含まれています。ウェブサーバーには、デルの自己署名 **SSL** デジタル証明書（サーバー **ID**）があり、クライアントからのセキュア **HTTP** 要求の受け入れと応答を担います。このサービスは、ウェブインタフェースとリモート **RACADM CLI** ツールが **CMC** と通信するために必要です。

ウェブサーバーがリセットされた場合は、サービスが再び利用可能になるまで少なくとも 1 分間お待ちください。ウェブサーバーのリセットは、通常以下のいずれかのイベントの結果として発生します。

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

 **メモ:** サービス設定を変更するには、シャーシ設定管理者権限が必要です。

リモート **Syslog** は、追加の **CMC** ログターゲットです。リモート **Syslog** を設定したら、**CMC** によって生成される新しい各ログエントリが、それぞれの送信先に転送されます。



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

CMC ウェブインタフェースを使用したサービスの設定

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

1. 左ペインで **セッション概要** をクリックし、**ネットワーク** → **サービス** をクリックします。 **サービス管理** ページが表示されます。
2. 必要に応じて次のサービスを設定します。
 - CMC シリアル
 - Web サーバー
 - SSH
 - Telnet
 - リモート RACADM
 - snmp
 - リモート Syslog

各種フィールドについての情報は、『オンラインヘルプ』を参照してください。

3. **適用** をクリックしてから、すべてのデフォルトのタイムアウト値および最大タイムアウト制限値をアップデートします。

RACADM を使用したサービスの設定

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

- `cfgRacTuning`
- `cfgRacTuneRemoteRacadmEnable`

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

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

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

たとえば、次のとおりです。

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

CMC 拡張ストレージカードの設定

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

CMC ウェブインタフェースを使用してリムーバブルフラッシュメディアを有効化または修復するには、次の手順を実行します。

1. 左ペインで **シャーシ概要** に移動し、**シャーシコントローラ → フラッシュメディア** をクリックします。
2. **リムーバブルフラッシュメディア** ページで、ドロップダウンメニューから必要に応じて次のいずれかを選択します。
 - アクティブコントロールメディアを修復する
 - シャーシデータの保存用にフラッシュメディアを使用しない

これらのオプションの詳細については『オンラインヘルプ』を参照してください。

3. **適用** をクリックして選択したオプションを適用します。

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

シャーシグループのセットアップ

CMC では、単一のリードシャーシから複数のシャーシを監視することが可能になります。シャーシグループを有効にした場合、リードシャーシの CMC は、シャーシ内のリードシャーシとすべてのメンバーシャーシの状態のグラフィカル表示を生成します。この機能を使用するには、**Enterprise** ライセンスが必要です。


シャーシグループの機能は以下のとおりです。

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

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

CMC ウェブインタフェースを使用してシャーシグループをセットアップするには、次の手順を実行します。

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


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

シャーシグループが作成されると、GUI が自動的に **シャーシグループ** ページに切り替わります。左ペインにグループ名とリードシャーシでグループが示され、未実装のメンバーシャーシが左ペインに表示されます。

シャーシグループへのメンバーの追加

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

1. リーダーシャーシに、シャーシ管理者権限でログインします。
2. システムツリーでリードシャーシを選択します。
3. **セットアップ** → **グループ管理** とクリックします。
4. **グループ管理** にある **ホスト名/IP アドレス** フィールドで、メンバーの IP アドレスまたは DNS 名を入力します。
5. **ユーザー名** フィールドに、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. **適用** をクリックします。
9. 最大の 8 メンバーを追加するには、手順 4~8 のタスクを完了します。新しいメンバーのシャーシ名が **メンバー** ダイアログボックスに表示されます。

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

リーダーからのメンバーの削除

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

1. リーダーシャーシにシャーシ管理者権限でログインします。
2. 左ペインで、リードシャーシを選択します。
3. **セットアップ** → **グループ管理** とクリックします。
4. **メンバーの削除** リストで、削除対象のメンバーの名前を選択し、**適用** をクリックします。
その後、リードシャーシは、グループから削除されたメンバー（1つまたは複数）との通信を行います。メンバー名が削除されます。ネットワーク上の問題によりリードとメンバー間の通信が妨げられている場合、メンバーシャーシがメッセージを受信しない場合があります。そのような場合には、メンバーシャーシからそのメンバーを無効にして削除を完了させてください。

シャーシグループの無効化

リードシャーシからグループを解除するには、次の手順を実行します。

1. リーダーシャーシに、管理者権限でログインします。
2. 左ペインで、リードシャーシを選択します。
3. **セットアップ** → **グループ管理** とクリックします。
4. **シャーシグループ** ページの **役割** で **なし** を選択し、**適用** をクリックします。
その後、リードシャーシはすべてのメンバーに、グループから削除されたことを伝えます。このリードシャーシは、新しいグループのリーダーまたはメンバーに割り当てることができます。
ネットワーク問題によってリーダーとメンバー間の通信ができない場合、メンバーシャーシがメッセージを受信しない可能性があります。その場合は、メンバーシャーシからメンバーを無効にして、削除プロセスを完了させてください。

メンバーシャーシでの個別のメンバーの無効化

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

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

メンバーシャーシまたはサーバーのウェブページの起動

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ウェブページ、サーバーのリモートコンソール、または iDRAC サーバーのウェブページにアクセスできます。メンバーデバイスにリードシャーシと同じログイン資格情報が設定されている場合は、その資格情報を使用してメンバーデバイスにアクセスできます。メンバーデバイスに移動するには、次の手順を実行します。

1. リードシャーシにログインします。
2. ツリー内で **グループ : 名前** を選択します。
3. 移動先がメンバーの **CMC** の場合には、目的のシャーシの **CMC の起動** を選択します。
シャーシ内のサーバーが移動先の場合には、次の手順を実行します。
 - a) 目的のシャーシの画像を選択します。
 - b) **正常性** セクションに表示されるシャーシイメージで、サーバーを選択します。
 - c) **クイックリンク** という表題のボックスで、移動先デバイスを選択します。移動先ページ、またはログイン画面を表示する新しいウィンドウが開きます。

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 6. 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。

プロパティ	ナビゲーション
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、0~8 個のシャーシグループメンバーを持つリードシャーシです。**シャーシグループ正常性** ページでは、すべてのメンバーシャーシが表示され、標準のブラウザダウンロード機能を使用して、サーバーインベントリレポートをファイルに保存することができます。レポートには以下のデータが含まれています。

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

サーバーインベントリレポートの保存

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

1. 左ペインで、**グループ** を選択します。
2. **シャーシグループ正常性** ページで、**インベントリレポートの保存** をクリックします。ファイルを開くか、または保存するかを尋ねる **ファイルダウンロード** ダイアログボックスが表示されます。
3. **保存** をクリックして、サーバーモジュールインベントリレポートのパスとファイル名を指定します。

 **メモ:** 最も正確なサーバーモジュールインベントリレポートを取得するには、シャーシグループのリーダー、シャーシグループのメンバーシャーシ、および関連シャーシ内のサーバーモジュールがオンになっている必要があります。

エクスポートされたデータ


サーバーインベントリレポートには、シャーシグループリーダーの通常のポーリング（30 秒ごと）中に各シャーシグループメンバーによって最近返されたデータが含まれます。

最も正確なサーバーインベントリレポートを取得するには、以下の条件を満たしている必要があります。

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

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

- **シャーシ電源状況オフ** 状況
- 電源オフ

 **メモ:** シャーシの電源がオフの状態ですらサーバーを挿入した場合、シャーシの電源が再びオンになるまで、モデル番号はウェブインタフェースのどこにも表示されません。

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

表 7. サーバーモジュールインベントリフィールドの説明

データフィールド	例
シャーシ名	データセンターのシャーシリーダー
シャーシ IP アドレス	192.168.0.1

データフィールド	例
スロットの場所	1
スロット名	SLOT-01
ホスト名	企業のウェブサーバー  メモ: サーバー上で Server Administrator エージェントが実行されている必要があります。実行されていない場合は、何も表示されません。
オペレーティングシステム	Windows Server 2008  メモ: サーバー上で Server Administrator エージェントが実行されている必要があります。実行されていない場合は、何も表示されません。
モデル	PowerEdgeM610
サービスタグ	1PB8VF1
総システムメモリ容量	4.0 GB  メモ: メンバー上に VRTX CMC 1.0 (以降) が存在している必要があります。存在しなければ、何も表示されません。
CPU の数	2  メモ: メンバー上に VRTX CMC 1.0 (以降) が存在している必要があります。存在しなければ、何も表示されません。
CPU 情報	Intel (R) Xeon (R) CPU E5502 @1.87GHzn  メモ: メンバー上に VRTX CMC 1.0 (以降) が存在している必要があります。存在しなければ、何も表示されません。


データフォーマット

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

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 getconfig -f myfile.cfg
```

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

```
racadm reset
```

getconfig -f myfile.cfg サブコマンドは、アクティブ CMC の設定を要求し、**myfile.cfg** ファイルを生成します。必要に応じて、ファイル名の変更、または別の場所への保存を行うことができます。

getconfig コマンドを使用して、次の操作を実行できます。


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

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

CMC 設定ファイルの作成

CMC 設定ファイル **<filename>.cfg** は、単純なテキストファイルを作成するために `racadm config -f <filename>.cfg` コマンドと共に使用されます。このコマンドを使うと、（**.ini** ファイルに類似した）設定ファイルを構築し、このファイルから CMC を設定することができます。

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

 **メモ:**getconfig サブコマンドの詳細については、『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。

RACADM は、**.cfg** ファイルが CMC に初めてロードされるときにそのファイルをパースして、有効なグループ名およびオブジェクト名が存在し、シンプルな構文規則に沿っていることを確認します。エラーはエラーを検出した行番号と共に示され、メッセージによりその問題が説明されます。ファイル全体が正確性のためにパースされ、すべてのエラーが表示されます。**.cfg** ファイルにエラーが発見された場合は、CMC に書き込みコマンドは送信されません。設定を行う前に、すべてのエラーを訂正する必要があります。

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

.cfg ファイルを作成するときは、次のガイドラインに従ってください。

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

パーサーは、CMC からそのグループのすべてのインデックスを読み取ります。グループ内のオブジェクトは、CMC が設定されたときに修正されたものです。修正されたオブジェクトが新しいインデックスを表す場合、設定中 CMC にそのインデックスが作成されます。

- ユーザーは .cfg ファイルの必要なインデックスを指定できません。
インデックスは、作成されたり、削除されたりします。時間と共に、使用済みおよび未使用のインデックスでグループがフラグメント化される可能性があります。インデックスが存在する場合は、変更されます。インデックスが存在しない場合は、最初に使用できるインデックスが使用されます。
この方法では、管理されているすべての CMC 間でインデックスを完全に一致させる必要がないので、インデックスエントリを柔軟に追加できます。新しいユーザーは、最初に使用可能なインデックスに追加されます。1つの CMC で正しくパースおよび実行される .cfg ファイルは、すべてのインデックスが一杯で新しいユーザーを追加しなければならない場合に、別の CMC では正しく実行されない場合があります。
- 同等のプロパティを持つ CMC を両方共に設定するには、racresetcfg サブコマンドを使用します。
racresetcfg サブコマンドを使って CMC を初期のデフォルトにリセットした後、racadm config -f <filename>.cfg コマンドを実行します。 .cfg ファイルに、必要なオブジェクト、ユーザー、インデックス、およびその他のパラメータがすべて含まれていることを確認してください。オブジェクトとグループの完全なリストについては、『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。

△ **注意:** racresetcfg サブコマンドを使用して、データベースと CMC ネットワークインタフェース設定を元のデフォルト設定にリセットし、すべてのユーザーとユーザー設定を削除します。
root ユーザーは使用可能ですが、その他のユーザー設定もデフォルト設定にリセットされます。

- racadm getconfig -f <ファイル名> .cfg と入力すると、このコマンドは現在の CMC 設定のために .cfg ファイルを作成します。この設定ファイルは、固有の .cfg ファイルの使用例または開始点として利用できます。

構文解析規則

- ハッシュ文字 (#) で始まる行はコメントとして取り扱われます。
コメント行は一列目から記述する必要があります。その他の列の「#」文字は単に # 文字として扱われます。
モデムパラメータでは文字列に # 文字が含まれている場合があります。エスケープ文字は必要ありません。racadm getconfig -f <filename> .cfg コマンドで .cfg を生成し、エスケープ文字を追加せずに、racadm config -f <filename> .cfg コマンドを異なる CMC 上で実行します。
たとえば、次のとおりです。
This is a comment [cfgUserAdmin] cfgUserAdminPageModemInitString=<Modem init # not a comment>
- グループエントリはすべて大カッコ ([と]) で囲む必要があります。
グループ名を示す右カッコ (]) は一列目にある必要があり、このグループ名は、そのグループ内の他のオブジェクトよりも前に指定する必要があります。関連するグループ名が含まれていないオブジェクトは、エラーを生成します。構成データは、『iDRAC6 および CMC 向け RACADM コマンドラインリファレンスガイド』のデータベースプロパティの章で定義されているようにグループ化されます。次に、グループ名、オブジェクト、およびオブジェクトのプロパティ値の使用例を示します。
[cfgLanNetworking] -{group name} cfgNicIpAddress=143.154.133.121 {object name} {object value}
- すべてのパラメータは、オブジェクト、=、または値の間に空白を入れずに「オブジェクト=値」のペアとして指定されます。値の後にあるスペースは無視されます。値の文字列内にあるスペースは変更されません。= の右側の文字はそのまま使用されます (例: 2つ目の =、#、[,、など)。これらの文字は、有効なモデムチャットスクリプト文字です。
[cfgLanNetworking] -{group name} cfgNicIpAddress=143.154.133.121 {object name} {object value}

- **.cfg** パーサーはインデックスオブジェクトエントリを無視します。
ユーザーは、使用するインデックスを指定できません。索引が既に存在する場合は、それが使用されます。索引がない場合は、そのグループで最初に使用可能な索引に新しいエントリが作成されます。
`racadm getconfig -f <filename>.cfg` コマンドは、インデックスオブジェクトの前にコメントを配置するため、ここでコメントを確認できます。



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

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

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

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

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



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

インデックス付きグループの内容を表示するには、次のコマンドを実行します。

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

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

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

- 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に、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** インデックス化されたすべてのグループに該当します。

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、[] で囲まれた実際の変数グループのラベルのみが残ります。

例:

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

このファイルは次のように更新されます。

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

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

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

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

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

スロット名の設定

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

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

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

ウェブインタフェースでのスロット名の設定は、CMC にしか保存されません。サーバーがシャーシから取り外されると、スロット名の設定はサーバーに残りません。

CMC ウェブインタフェースで設定したスロット名の設定は、iDRAC インタフェースに表示されている名前の変更は常に上書きします。

CMC ウェブインタフェースを使用してスロット名を編集するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** → **サーバー概要** → **セットアップ** → **スロット名** に移動します。
2. **スロット名** ページの **スロット名** フィールドで、スロット名を編集します。
3. サーバーのホスト名をスロット名として使用するには、**ホスト名をスロット名として使用する** オプションを選択します。これにより、サーバーのホスト名（またはシステム名）がある場合は、静的スロット名がこれで上書きされます。この操作には、サーバーに **OMSA** エージェントをインストールする必要があります。OMSA エージェントの詳細については、dell.com/support/manuals にある『Dell OpenManage Server Administrator ユーザーズガイド』を参照してください。
4. 設定を保存するには、**適用** をクリックします。

デフォルトのスロット名（サーバーのスロット位置に基づいた SLOT-01～SLOT-4）をサーバーに復元するには、**デフォルト値に戻す** をクリックします。

iDRAC ネットワークの設定

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

iDRAC の詳細については、dell.com/support/manuals にある『iDRAC7 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、次の表に示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 8. QuickDeploy 設定

設定	説明
QuickDeploy の有効化	このオプションを選択して、このページで設定した iDRAC 設定が新規に挿入されたサーバーに自動的に適用される QuickDeploy 機能を有効化します。自動設定は、LCD パネル上でローカルに確認する必要があります。
サーバー挿入で iDRAC root パスワードを設定	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	サーバー挿入で iDRAC root パスワードを設定 および QuickDeploy 有効 オプションが選択されている場合、シャーシにサーバーが挿入されたときに、このパスワードがサーバーの iDRAC 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。


設定	説明
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 を有効にする	iDRAC LAN チャンネルを有効化または無効化します。デフォルトでは、このオプションは選択されていません。
iDRAC IPv4 を有効にする	iDRAC での IPv4 を有効化または無効化します。このオプションはデフォルトで選択されています。
iDRAC IPMI オーバー LAN を有効にする	シャーシに存在する各 iDRAC の IPMI オーバー LAN チャンネルを有効化または無効化します。デフォルトでは、このオプションは選択されていません。
iDRAC IPv4 DHCP を有効にする	シャーシに存在する各 iDRAC の DHCP を有効化または無効化します。このオプションを有効化すると、 QuickDeploy IP 、 QuickDeploy サブネットマスク 、および QuickDeploy ゲートウェイ フィールドが無効になり、各 iDRAC へのこれらの設定の自動割り当てに DHCP が使用されるため、変更できません。このオプションを選択するには、 iDRAC IPv4 を有効にする オプションを選択しておく必要があります。
iDRAC IPv4 アドレス (スロット 1) をスタート中	<p>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。</p> <p> 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。</p> <p>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 である場合、スロット 15 の QuickDeploy IP アドレスは 192.168.0.265 です。サブネットマスクが 255.255.255.0 のとき、QuickDeploy 設定を保存する または QuickDeploy 設定を使用して自動入力する をクリックすると、QuickDeploy IP address range is not fully within QuickDeploy Subnet というエラーメッセージが表示されます。</p>
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り当てられた 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 を有効にする	IPv6 対応のシャーシ内にある各 iDRAC の IPv6 アドレス設定を有効にします。

設定	説明
iDRAC IPv6 自動設定を有効にする	iDRAC が DHCPv6 サーバーから IPv6 設定 (アドレスおよびプレフィックス長) を取得できるようにします。また、ステートレスなアドレスの自動構成も有効にします。このオプションはデフォルトでは有効になっています。
iDRAC IPv6 ゲートウェイ	デフォルトの IPv6 ゲートウェイが iDRAC に割り当てられるように指定します。デフォルト値は "::" です。
iDRAC IPv6 プレフィックス長	プレフィックス長が iDRAC 上の IPv6 アドレスに対して割り当てられるように指定します。デフォルト値は 64 です。

3. **QuickDeploy 設定を保存する** をクリックして設定を保存します。iDRAC ネットワークの設定を変更した場合は、**iDRAC ネットワーク設定を適用する** をクリックして設定を iDRAC に導入します。QuickDeploy 機能は、有効化されており、サーバーがシャーシに挿入されているときにのみ実行されます。サーバー挿入で iDRAC ルートパスワードを設定 および QuickDeploy 有効 が有効になっている場合、ユーザーに LCD インタフェースを使用してパスワードの変更を許可または許可しないようにするプロンプトが表示されます。現在の iDRAC 設定と異なるネットワーク構成設定が存在する場合、それらの変更を受け入れるか拒否するかどうかを尋ねるプロンプトが表示されます。

 **メモ:** LAN または IPMI オーバー LAN の違いが存在する場合は、ユーザーに QuickDeploy IP アドレス設定を受け入れるためのプロンプトがメッセージが表示されます。その違いが DHCP である場合は、ユーザーに DHCP QuickDeploy 設定を受け入れるためのプロンプトが表示されます。


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

 **メモ:** QuickDeploy フィールドの変更はただちに適用されますが、1 つ、または複数の iDRAC サーバー ネットワーク構成設定を変更した場合は、CMC から iDRAC に反映されるまで数分かかる場合があります。更新を早くクリックしすぎると、1 つ、または複数の iDRAC サーバーのデータが部分的にしか正しく表示されない場合があります。


個々のサーバー iDRAC の iDRAC ネットワーク設定の変更

この機能を使用して、取り付けられている各サーバーの iDRAC ネットワーク設定を設定できます。それぞれの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、取り付けられているすべてのサーバーの iDRAC IPv4 および IPv6 ネットワーク設定がリストされます。
2. サーバーの必要に応じて、iDRAC ネットワーク設定を変更します。
 **メモ:** IPv4 または IPv6 設定を指定するには、**LAN を有効にする** オプションを選択する必要があります。各フィールドの詳細については、『オンラインヘルプ』を参照してください。
3. iDRAC に設定を適用するには、**iDRAC ネットワーク設定を適用する** をクリックします。QuickDeploy 設定 に対して行った変更も保存されます。
iDRAC ネットワーク設定 表は、将来のネットワーク構成を反映するため、インストールされているサーバーに対して表示されている値は、現在インストールされている iDRAC ネットワーク構成と一致しない

場合もあります。**更新** をクリックして変更後の iDRAC ネットワーク構成で **iDRAC の導入** ページを更新します。

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

RACADM を使用した iDRAC ネットワーク設定の変更

RACADM config または getconfig コマンドでは、次の設定グループに対する `-m <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『iDRAC7 および CMC 向け RACADM コマンドラインリファレンスガイド』を参照してください。

iDRAC VLAN タグの設定

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

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
```

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。各フィールドの詳細については、『オンラインヘルプ』を参照してください。
3. 設定を保存するには、**適用** をクリックします。

最初の起動デバイスの設定

各サーバーについて、**CMC** の最初の起動デバイスを指定できます。これはサーバーの実際の最初の起動デバイスでなくてもよく、またそのサーバー上に存在するデバイスを示すものでなくともかまいません。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。


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 9. 起動デバイス

起動デバイス	説明
PXE	ネットワークインタフェースカードの PXE (プレブート実行環境) プロトコルから起動します。
ハードドライブ	サーバーのハードディスクドライブから起動します。
ローカル CD/DVD	サーバー上の CD または DVD ドライブから起動します。
仮想フロッピー	仮想フロッピードライブから起動します。フロッピードライブ (またはフロッピーディスクイメージ) は管理ネットワーク上の別のコンピュータ上にあり、 iDRAC GUI コンソールビューアで接続されます。
仮想 CD/DVD	仮想 CD/DVD ドライブ、または CD/DVD ISO イメージから起動します。この光学ドライブまたは ISO イメージファイルは管理ネットワーク上の別のコンピュータまたは起動ディスク上にあり、 iDRAC GUI コンソールビューアで連結されます。
iSCSI	iSCSI (インターネット小型コンピュータシステムインタフェース) デバイスから起動します。
ローカル SD カード	ローカル SD カードから起動します (iDRAC 6 および iDRAC 7 システムをサポートするサーバーのみで可能)。

起動デバイス	説明
ローカルフロッピー	ローカルフロッピーディスクドライブにあるフロッピーディスクから起動します。
リモートファイル共有	リモートファイル共有 (RFS) イメージから起動します。イメージファイルは iDRAC GUI コンソールビューアで接続されます。


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

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

複数のサーバーに最初の起動デバイスを設定するには、次の手順を実行します。

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

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

 **メモ:** サーバーの最初の起動デバイスを設定するには、**サーバー管理者** 特権、または **シャーシ設定システム管理者** 特権、および **iDRAC ログイン** 特権が必要です。

個々のサーバーに最初の起動デバイスを設定するには、次の手順を実行します。

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

RACADM を使用した最初の起動デバイスの設定

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

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

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

サーバー FlexAddress の設定

サーバーの FlexAddress の設定については、「[CMC ウェブインタフェースを使用したシャードレベルファブリックおよびスロット用 FlexAddress の設定](#)」を参照してください。この機能を使用するには、Enterprise ライセンスが必要です。

リモートファイル共有の設定

リモート仮想メディアファイル共有機能は、オペレーティングシステムを導入またはアップデートするために、ネットワーク上の共有ドライブのファイルを CMC を介して 1 つまたは複数のサーバーにマップします。接続されると、リモートファイルがローカルサーバー上でアクセス可能なファイルと同様にアクセス可能になります。サポートされているメディアはフロッピードライブと CD/DVD ドライブの 2 種類です。


リモートファイル共有操作（接続、切断、または導入）を実行するには、**シャード設定システム管理者** 権限または **サーバー管理者** 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。各フィールドの詳細な説明については、『オンラインヘルプ』を参照してください。
3. 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への接続には、パス、ユーザー名、パスワードを指定する必要があります。操作が正常に行われると、メディアへのアクセスが可能になります。

接続解除 をクリックして、以前接続したリモートファイル共有を接続解除します。

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ーが再起動されるため、その前に、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。

サーバークローンを使用した BIOS の設定

サーバークローニング機能では、指定されたサーバーからの BIOS 設定のすべてを 1 つ、または複数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 BIOS 設定のみがクローン可能です。この機能を使用するには、Enterprise ライセンスが必要です。

サーバークローニング機能は iDRAC7 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。

サーバークローニング機能を使用するには、以下の条件を満たしている必要があります。

- 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 1.40.40 が必要です。
- サーバーにサポートされている世代の iDRAC がある。
- サーバーの電源がオンになっている。

ソースサーバーとターゲットサーバーが同じ世代に属している必要はありません。利用できるクローン可能な設定のみが、1 つのサーバープロファイルから他のサーバーに適用されます。

次の操作が可能です。

- BIOS 設定を別のサーバーにコピーする。
- 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。
- サーバーまたは保存したプロファイルから BIOS 設定を表示する。
- 最近の BIOS プロファイルタスクのログアクティビティを表示する。

BIOS プロファイルページへのアクセス

BIOS プロファイル ページを使用して、BIOS プロファイルを 1 つまたは複数のサーバーに追加、管理、および導入できます。

CMC ウェブインタフェースを使用して BIOS 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。BIOS プロファイル ページが表示されます。

プロファイルの追加

サーバーの BIOS プロパティをルートクローニングする前に、まず最初に保存プロファイルにプロパティを取得する必要があります。

保存プロファイルを作成するときに、各プロファイルに名前と任意の説明を指定する必要があります。CMC 不揮発性拡張ストレージメディアに最大 16 個の保存プロファイルを保存できます。

不揮発性ストレージメディアを取り外すか無効にすると、保存プロファイルにアクセスできなくなり、サーバークローニング機能が無効になります。

プロファイルを追加するには、次の手順を実行します。

1. BIOS プロファイル ページで、**プロファイルの追加** をクリックします。
2. BIOS プロファイルの追加 ページで、プロファイル名と説明 (オプション) を入力し、プロファイルをクローンする必要がある元のサーバーを選択して **保存** をクリックします。CMC は、Lifecycle Controller と通信して利用可能な BIOS 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。

保存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. BIOS 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、『オンラインヘルプ』を参照してください。

プロファイルの適用

CMC 上の不揮発性メディアに保存プロファイルがあるときにサーバークローニング操作を開始するには、保存プロファイルを 1 つまたは複数のサーバーに適用してください。

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. 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. **BIOS 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。
3. **ターゲットサーバーの選択** セクションから、プロファイルを適用するサーバーに対応するオプションを選択します。このページのフィールドの説明に関する詳細は、『**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。選択したプロファイルがサーバーに適用され、サーバーが自動的に再起動します。

BIOS 設定の表示

選択したサーバーの BIOS 設定を表示するには、**BIOS 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、BIOS 設定列にある **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。

プロファイル (クローン可能な設定) を適用することによって変更できる、サーバー上の BIOS 設定のみが表示されます。設定は、**iDRAC BIOS セットアップ** ページでの表示と同じ方法でグループ分けされています。

 **メモ:** Control System Inventory on Restart (CSIOR) オプションが有効の場合にのみ、CMC サーバークローニングアプリケーションが、特定のサーバーの正しい BIOS および起動設定を取得して表示します。

CSIOR を有効にするには、次の手順を実行します。

- 第 12 世代サーバー — サーバーを再起動した後、**F2** を押し、**iDRAC 設定** → **Lifecycle Controller** を選択して **CSIOR** を有効にし、変更を保存します。

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、**BIOS プロファイル** ページで、最新の 10 プロファイルログエントリがサーバークローニング操作から直接リストされる、**最新のプロファイルログ** セクションを見ます。各最新のプロファイルログには、重大度、サーバークローニング操作が実行された日時、クローニングログメッセージの説明が表示されます。ログエントリも **RAC** ログで利用できます。その他の閲覧可能なエントリを表示するには、**プロファイルログを表示** 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。

完了状態とトラブルシューティング

適用済みの BIOS プロファイルの完了状態をチェックするには、次の手順を実行します。


1. 左ペインで、**シャーシ概要** → **サーバー概要** → **セットアップ** → **プロファイル** をクリックします。
2. **BIOS プロファイル** ページで、**最近のプロファイルログ** セクションから実行済みジョブのジョブ ID (JID) を書き取ります。
3. 左ペインで、**サーバー概要** → **トラブルシューティング** → **Lifecycle Controller ジョブ** をクリックします。**ジョブ** 表内で同じ JID を検索します。CMC を使用した Lifecycle Controller ジョブの実行の詳細については、「[Lifecycle Controller ジョブ操作](#)」を参照してください。


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 (iDRAC) のウェブベースインタフェースの起動ポイントを提供します。

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せずに iDRAC ウェブインタフェースを起動することができます。シングルサインオンポリシーは次の通りです。

- サーバー管理者の権限を持つ CMC のユーザーは、シングルサインオンで自動的に iDRAC にログインされます。iDRAC のサイトが表示されたら、そのユーザーに管理者権限が自動的に許可されます。これは、iDRAC のアカウントを持たない同じユーザーや、アカウントに管理者権限のない場合でも同様です。
- サーバー管理者の権限を **持たない** CMC ユーザーでも、iDRAC に同じアカウントがある場合は、シングルサインオンで iDRAC に自動ログインできます。iDRAC のサイトが表示されたら、iDRAC アカウントに対して作られた権限が許可されます。
- サーバー管理者の権限、または iDRAC に同じアカウントを持たない CMC ユーザーは、シングルサインオンで iDRAC に自動ログイン **されません**。このユーザーが **iDRAC GUI の起動** をクリックすると、iDRAC ログインページが表示されます。

 **メモ:** ここで言う「同じアカウント」とは、ユーザーが CMC および iDRAC にパスワードが一致する同じログイン名を持っているということです。同じログイン名で、パスワードが一致しないユーザーは、同じアカウントを持つと見なされます。

 **メモ:** その場合、ユーザーは、iDRAC のログインページが表示されます（前述のシングルサインオンの 3 つ目の項目参照）。

 **メモ:** iDRAC ネットワーク LAN が無効（LAN 無効=オフ）の場合は、シングルサインオンは利用できません。

サーバーがシャーンから取り外された、iDRAC IP アドレスを変更した、または iDRAC ネットワーク接続にエラーが発生した場合、iDRAC GUI の起動をクリックするとエラーページが表示されることがあります。

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 ウェブインタフェースが表示されます。フィールドの説明については、『オンラインヘルプ』を参照してください。

サーバー状態ページからの iDRAC の起動

サーバー状態 ページから iDRAC 管理コンソールを起動するには、次の手順を実行します。

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

リモートコンソールの起動

サーバーでキーボード - ビデオ - マウス (KVM) セッションを直接起動できます。リモートコンソール機能は、次の条件がすべて満たされた場合のみサポートされます。

- シャーンに電源が入っている。
- iDRAC 7 をサポートするサーバー。
- サーバーの LAN インタフェースが有効である
- ホストシステムに JRE (Java Runtime Environment) 6 アップデート 16 以降がインストールされている
- ホストシステム上のブラウザで、ポップアップウィンドウが許可されている（ポップアップブロッキングが無効）

リモートコンソールは、iDRAC ウェブインタフェースから起動することもできます。詳細については、dell.com/support/manuals にある『iDRAC ユーザーズガイド』を参照してください。

シャーシ正常性ページからのリモートコンソールの起動

CMC ウェブインタフェースからリモートコンソールを起動するには、次の手順を実行します。

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

サーバー状態ページからのリモートコンソールの起動

個別にサーバーのリモートコンソールを起動するには、次の手順を実行します。

1. 左ペインで **サーバー概要** を展開します。展開されたサーバーのリストに 4 つのサーバーがすべて表示されます。
2. リモートコンソールを起動するサーバーをクリックします。
3. **サーバー状態** ページで、**リモートコンソールの起動** をクリックします。

サーバー状態ページからのリモートコンソールの起動

サーバー状態 ページからサーバーリモートコンソールを起動するには、次の手順を実行します。

1. 左ペインで、**サーバー概要** に移動し、**プロパティ** → **状態** をクリックします。**サーバー状態** ページが表示されます。
2. 必要なサーバーの **リモートコンソールの起動** をクリックします。

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。

アラートの有効化または無効化

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

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

CMC ウェブインタフェースを使用したアラートの有効化または無効化

アラートの生成を有効化または無効化するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** → **アラート** をクリックします。
2. シャーシイベント ページの **シャーシアラート有効化** セクションで、**シャーシイベントアラートの有効化** オプションを選択して有効化するか、オプションの選択を外してアラートを無効化します。
3. 設定を保存するには、**適用** をクリックします。

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、`cfglpmiLanAlertEnable` RACADM オブジェクトを使用します。詳細については、『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。

アラートのフィルタ

カテゴリと重要度に基づいて、アラートをフィルタすることができます。

CMC ウェブインタフェースを使用したアラートのフィルタ

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



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

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

監視対象アラート セクションには、選択したカテゴリと重要度に基づいた結果が表示されます。このページのフィールドの説明については、『オンラインヘルプ』を参照してください。

RACADM を使用したイベントアラートの設定

イベントアラートを設定するには、`eventfilters` コマンドを実行します。詳細については、dell.com/support/manuals にある『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。

アラートの宛先設定

管理ステーションは、シンプル ネットワーク 管理プロトコル (SNMP) を使用して CMC からデータを受信します。

IPv4 および IPv6 アラートの宛先設定、E-メール設定、SMTP サーバー設定を行い、これらの設定をテストすることができます。

E-メールアラートまたは SNMP トラップ設定を設定する前に、シャーシ設定システム管理者権限があることを確認してください。

SNMP トラップアラート送信先の設定

SNMP トラップを受信する IPv6 または IPv4 アドレスを設定できます。

CMC ウェブインタフェースを使用した SNMP トラップアラート送信先の設定

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

1. 左ペインで、**シャーシ概要** → **アラート** → **トラップの設定** をクリックします。
2. シャーシイベントアラート送信先 ページで、次の値を入力します。
 - **送信先** フィールドに有効な IP アドレスを入力します。ドットで4つに区切られた IPv4 フォーマット、標準 IPv6 アドレス表記、または FQDN を使用します。例: **123.123.123.123**、**2001:db8:85a3::8a2e:370:7334**、**dell.com**。


ネットワーキング技術またはインフラストラクチャと一貫性のあるフォーマットを選択します。テストトラップ機能では、現在のネットワーク設定に不適当な選択項目は検出されません (IPv4専用の環境で IPv6 送信先を使用する場合など)。

- **コミュニティ文字列** フィールドに、送信先管理ステーションが属する有効なコミュニティ名を入力します。
このコミュニティ文字列は、**シャーシ概要** → **ネットワーク** → **サービス** ページにあるコミュニティ文字列とは異なります。**SNMP** トラップのコミュニティ文字列は、**CMC** が管理ステーション宛のアウトバウンドトラップのために使用するものです。**シャーシ概要** → **ネットワーク** → **サービス** ページのコミュニティ文字列は、管理ステーションが **CMC** の **SNMP** デーモンをクエリするために使用します。
- **有効** で、送信先 IP に対応するオプションを選択して、トラップを受け取る IP アドレスを有効化します。IP アドレスは最大 4 つまで指定できます。

3. 設定を保存するには、**適用** をクリックします。
4. IP アドレスが **SNMP** トラップを受信しているかどうかを確認するには、**SNMP トラップのテスト列の送信** をクリックします。
IP アラート送信先が設定されます。

RACADM を使用した SNMP トラップアラート送信先の設定

RACADM を使用して IP アラート送信先を設定するには、次の手順を実行します。

1. シリアル/Telnet/SSH テキストコンソールを開いて **CMC** に進み、ログインします。
 **メモ:** SNMP と E-メールアラートのいずれも、設定できるフィルタマスクは 1 つだけです。フィルタマスクをすでに選択している場合は、**タスク 2** を実行せずに **手順 3** に進みます。
2. アラートの生成を有効にします。

```
racadm config -g cfgAlerting -o cfgAlertingEnable 1
```
3. `racadm eventfilters set` コマンドを実行することによって、イベントフィルタを指定します。
 - a) 使用可能なアラート設定をすべてクリアするには、次のコマンドを実行します。`racadm eventfilters set -c cmc.alert.all -n none`
 - b) 重要度をパラメータとして使用して設定します。たとえば次の場合、ストレージカテゴリのすべての情報イベントには処置として電源オフ、および通知として E-メールと **SNMP** が割り当てられます。
`racadm eventfilters set -c cmc.alert.storage.info -n email,snmp`
 - c) サブカテゴリをパラメータとして使用して設定します。たとえば次の場合、監査カテゴリ内のライセンスサブカテゴリ下にあるすべての設定には処置として電源オフが割り当てられ、すべての通知が有効化されます。`racadm eventfilters set -c cmc.alert.audit.lic -n all`
 - d) サブカテゴリおよび重要度をパラメータとして使用して設定します。たとえば次の場合、監査カテゴリ内のライセンスサブカテゴリ下にあるすべての情報イベントには処置として電源オフが割り当てられ、すべての通知が無効化されます。`racadm eventfilters set -c cmc.alert.audit.lic.info -n none`
4. トラップアラートを有効にします。

```
racadm config -g cfgTraps -o cfgTrapsEnable 1 -i <index>
```

ここで、<index> は 1~4 の値です。**CMC** はインデックス番号を使用して、トラップアラート用の設定可能送信先を最大 4 つまで識別します。送信先は適切にフォーマットされた数値アドレス (IPv6 または IPv4)、または完全修飾ドメイン名 (FQDN) で指定できます。
5. トラップアラートの送信先 IP アドレスを指定します。


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

ここで、<IP address> は有効な IP アドレスで、<index> は手順 4 で指定したインデックス値です。
6. コミュニティ名を指定します。

```
racadm config -g cfgTraps -o cfgTrapsCommunityName <community name> -i <index>
```

ここで <community name> はシャーシが属する SNMP コミュニティの名前で、<index> は手順 4 および 5 で指定したインデックス値です。

トラップアラートの送信先 IP アドレスを 4 つまで設定できます。送信先をさらに追加するには、手順 2 ~6 のタスクを実行します。

 **メモ:** 手順 2~6 のコマンドは、指定するインデックス (1~4) の既存の設定をすべて上書きします。インデックスに既に値が設定されているかを調べるには、`racadm getconfig -g cfgTraps -i <インデックス>` を入力します。インデックスが設定されていると、`cfgTrapsAlertDestIPAddr` オブジェクトおよび `cfgTrapsCommunityName` オブジェクトに値が表示されます。

7. アラート送信先へのイベントトラップをテストするには、次を入力します。

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

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

インデックス番号が不明な場合は、次のコマンドを実行します。


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

E-メールアラートの設定

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

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

 **メモ:** メールサーバーが Microsoft Exchange Server 2007 である場合、iDRAC7 から E-メールアラートを受信するには、そのメールサーバー用に iDRAC7 ドメイン名が設定されていることを確認してください。

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

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

CMC ウェブインタフェースを使用した E-メールアラートの設定

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


1. 左ペインで、**シャーシ概要** → **アラート** → **E-メールアラートの設定** をクリックします。
2. SMTP E-メールサーバー設定と、アラートを受信する E-メールアドレスを指定します。フィールドの説明については『オンラインヘルプ』を参照してください。
3. 設定を保存するには、**適用** をクリックします。
4. **E-メールのテスト** で **送信** をクリックして、指定した E-メールアラートの宛先にテスト E-メールを送信します。

RACADM を使用した E-メールアラートの設定

RACADM を使用して E-メールアラートの送信先にテスト E-メールを送信するには、次の手順を実行します。

1. シリアル/Telnet/SSH テキストコンソールを開いて CMC に進み、ログインします。
2. アラートの生成を有効にします。

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

 **メモ:** SNMP と E-メールアラートの両方も、設定できるフィルタマスクは 1 つだけです。フィルタマスクをすでに設定した場合は、手順 3 のタスクは実行しないでください。

- アラートが生成されるべきイベントを指定します。

```
racadm config -g cfgAlerting -o cfgAlertingFilterMask <mask value>
```

ここで、<mask value>は0x0~0xffffffffの16進数値で、0xで始まる形式である必要があります。イベントトラップのフィルタマスク表は、各イベントタイプ向けのフィルタマスクを提供します。有効にするフィルタマスクの16進値の計算方法は、「[RACADMを使用したSNMPトラップアラート送信先の設定](#)」の手順3を参照してください。

- E-メールアラートの生成を有効化します。

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable 1 -i <index>
```

ここで、<index>は1~4の範囲の値です。CMCではインデックス番号を使用して、設定可能な最大4つの送信先E-メールアドレスを区別します。

- アラートを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。

- 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 cfgEmailAlertAddress <email name> -i <index>
```

ここで、<email name>は、E-メールアラートを受信する人またはグループの名前で、<index>は手順4と5で指定したインデックス値です。E-メール名は、32文字以内の英数字、ハイフン、下線、ピリオドで指定します。スペースは使用できません。

- 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-メールアドレスを追加するには、手順2~6のタスクを実行します。

 **メモ:** 手順2~6のコマンドは、指定するインデックス(1~4)に設定されている既存設定をすべて上書きします。インデックスに既に値が設定されているかを調べるには、`racadm getconfig -g cfgEmailAlert -I <index>`を入力します。インデックスが設定されていると、**cfgEmailAlertAddress** オブジェクトおよび **cfgEmailAlertEmailName** オブジェクトに値が表示されます。

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

ユーザーアカウントと権限の設定

CMC を使用したシステムの管理、およびシステムセキュリティの維持を行うために、特定の権限（役割ベースの権限）を持つユーザーアカウントをセットアップすることができます。デフォルトで、CMC はローカル管理者アカウントで設定されています。デフォルトユーザー名は root で、パスワードは calvin です。管理者として、他のユーザーが CMC にアクセスすることを許可するためのユーザーアカウントをセットアップできます。

最高 16 のローカルユーザーをセットアップしたり、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。

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resh ユーザー
- iDRAC ユーザーまたはサーバーユーザー（iDRAC がサーバーにあるため）

CMC および iDRAC ユーザーは、ローカルユーザーまたはディレクトリサービスユーザーにすることができます。

サーバーユーザーは CMC ユーザーとは独立して作成されるため、CMC ユーザーが **サーバー管理者** 権限を持つ場合を除き、CMC ユーザーに与えられる権限はサーバー上の同じユーザーに自動的に転送されるわけではありません。つまり、CMC Active Directory ユーザーと iDRAC Active Directory ユーザーは、Active Directory ツリーの異なるブランチに位置することになります。ローカルサーバーユーザーを作成するには、ユーザー設定システム管理者は直接サーバーにログインする必要があります。ユーザー設定システム管理者は、CMC からサーバーユーザーまたはその逆を作成できません。このルールにより、サーバーのセキュリティと整合性は保護されます。

表 10. ユーザータイプ

権限	説明
CMC ログインユーザー	<p>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。</p> <p>ユーザーは、CMC ログインユーザー権限を持たずに他の権限を持つこともできます。この機能は、ユーザーが一時的にログインを禁止されている場合に便利です。そのユーザーの CMC ログインユーザー権限が復元した場合にも、その前に与えられていたその他のすべての権限を保持できます。</p>
シャresh設定システム管理者	<p>ユーザーは、次のデータの追加や変更ができます。</p> <ul style="list-style-type: none"> • シャreshを識別する（シャresh名やシャreshの位置など）。 • シャresh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）。

権限	説明
	<ul style="list-style-type: none"> • シャーシにサービスを提供する（日時、ファームウェアアップデート、CMC リセットなど）。 • シャーシに関連している（スロット名やスロットの優先順位など）。これらのプロパティはサーバーに適用されますが、正確にはサーバーそのものでなくスロットに関連付けられるシャーププロパティです。このため、スロット名とスロットの優先順位は、サーバーがスロットにあるなしに関係なく、追加または変更することができます。 <p>サーバーが異なるシャーシに移動されると、サーバーは新しいシャーシで使用するスロットに割り当てられたスロット名と優先順位を継承します。前のスロット名と優先順位はそのまま前のシャーシに残ります。</p> <p> メモ: シャーシ設定システム管理者 権限を持つ CMC ユーザーが電源設定を行うことができます。ただし、シャーシの電源オン、電源オフ、パワーサイクルなどのシャーシ電源操作を行うには、シャーシ制御システム管理者 権限が必要です。</p>
ユーザー設定システム管理者	<p>ユーザーは次の操作ができます。</p> <ul style="list-style-type: none"> • 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	<p>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。</p>
シャーシ制御システム管理者（電源コマンド）	<p>シャーシ電源システム管理者 の権限を持つ CMC ユーザーは、電源関連の操作をすべて行うことができます。電源オン、電源オフ、パワーサイクルなどのシャーシ電力操作を制御できます。</p> <p> 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。</p>
サーバーシステム管理者	<p>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。</p> <p>サーバーシステム管理者 権限を持つユーザーがサーバー上で実行する処置を発行すると、CMC ファームウェアはサーバー上のユーザーの権限を確認せずに、コマンドを対象のサーバーに送信します。つまり、サーバーシステム管理者 権限は、サーバーにおけるシステム管理者権限の欠如を無視します。</p> <p>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。</p> <ul style="list-style-type: none"> • 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 <p>サーバーシステム管理者 権限のない CMC ユーザーがサーバー上で実行する処置を出す場合、CMC はユーザーのログイン名とパスワードを入力して、対象のサーバーにコマンドを送信します。ユーザーがサーバー上に存在しない、またはパスワードが一致しない場合は、ユーザーは処置を実行することができません。</p> <p>ユーザーが対象のサーバーに存在し、パスワードが一致する場合は、サーバーはユーザーがサーバー上で与えられた権限を使って応答し</p>

権限	説明
	<p>ます。CMC ファームウェアはサーバーから返された権限に基づいてユーザーに処置を実行する権利があるかどうかを決定します。</p> <p>以下のリストに、サーバーシステム管理者が持っているサーバー上の権限と処置を示します。これらの権利は、シャreshユーザーがシャresh上でサーバーシステム管理者権限を持っていない場合にのみ適用されます。</p> <p>サーバー設定システム管理者：</p> <ul style="list-style-type: none"> • 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 <p>ユーザーの設定：</p> <ul style="list-style-type: none"> • iDRAC ルートパスワードの設定 • iDRAC のリセット <p>サーバー制御システム管理者：</p> <ul style="list-style-type: none"> • 電源オン • 電源オフ • 電源の入れ直し • 正常なシャットダウン • サーバーの再起動
テストアラートユーザー	ユーザーはテストアラートメッセージを送信できます。
デバッグコマンドシステム管理者	ユーザーはシステム診断コマンドを実行できます。
ファブリック A システム管理者	ユーザーは、ファブリック A IOM をセットアップし、設定できます。
ファブリック B システム管理者	ユーザーはファブリック B をセットアップし、設定できます。これは、サーバー内の最初のメザニンカードに対応し、メインボードの共有 PCIe サブシステム内のファブリック B 回路に接続されます。
ファブリック C システム管理者	ユーザーはファブリック C をセットアップし、設定できます。これは、サーバー内の 2 番目のメザニンカードに対応し、メインボードの共有 PCIe サブシステム内のファブリック C 回路に接続されます。

CMC ユーザーグループは、あらかじめ割り当てられたユーザー権限を持つ一連のユーザーグループを提供します。


 **メモ:** システム管理者、パワーユーザー、またはゲストユーザーを選択し、事前に定義された設定から権限を追加または削除した場合、CMC グループは自動的にカスタムに変更されます。

表 11. CMC グループ権限

ユーザーグループ	特権
システム管理者	<ul style="list-style-type: none"> • CMC ログインユーザー • シャresh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 • サーバーシステム管理者


ユーザーグループ	特権
	<ul style="list-style-type: none"> 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
パワーユーザー	<ul style="list-style-type: none"> ログイン ログのクリアシステム管理者 シャージ制御システム管理者（電源コマンド） サーバーシステム管理者 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	<p>次の権限を任意の組み合わせで選択します。</p> <ul style="list-style-type: none"> CMC ログインユーザー シャージ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 シャージ制御システム管理者（電源コマンド） サーバーシステム管理者 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 12. 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	はい	はい	はい
シャージ設定システム管理者	はい	いいえ	いいえ
ユーザー設定システム管理者	はい	いいえ	いいえ
ログのクリアシステム管理者	はい	はい	いいえ
シャージ制御システム管理者（電源コマンド）	はい	はい	いいえ
サーバーシステム管理者	はい	はい	いいえ
テストアラートユーザー	はい	はい	いいえ
デバッグコマンドシステム管理者	はい	いいえ	いいえ
ファブリック A システム管理者	はい	はい	いいえ

ルートユーザー管理者アカウント設定の変更


セキュリティを強化するため、ルート（ユーザー 1）アカウントのデフォルトパスワードを変更することを強くお勧めします。ルートアカウントは、CMC に組み込まれているデフォルトの管理アカウントです。ルートアカウントのデフォルトパスワードを変更するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** をクリックし、次に **ユーザー認証** をクリックします。
2. **ユーザー** ページの **ユーザー ID** 列で、**1** をクリックします。
 **メモ:** ユーザー ID 1 は CMC にデフォルトで組み込まれているルートユーザーアカウントです。これを変更することはできません。
3. **ユーザー設定** ページで、**パスワードの変更** オプションを選択します。
4. **パスワード** フィールドに新しいパスワードを入力し、同じパスワードを **パスワードの確認** に入力します。
5. **適用** をクリックします。ユーザー ID 1 のパスワードが変更されます。


ローカルユーザーの設定

CMC では、特定のアクセス権限を持つローカルユーザーを最大 16 人設定できます。CMC ローカルユーザーを作成する前に、現行のユーザーが存在するかどうかを確認してください。これらのユーザーには、ユーザー名、パスワード、および権限付きの役割を設定できます。ユーザー名とパスワードは、ウェブインタフェース、RACADM、WS-MAN などの CMC でセキュア化された任意のインタフェースを使用して変更できます。


CMC ウェブインタフェースを使用したローカルユーザーの設定

 **メモ:** CMC ユーザーを作成するには、**ユーザーの設定** 権限が必要です。


ローカル CMC ユーザーを追加し、設定するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** をクリックし、次に **ユーザー認証** をクリックします。
2. **ローカルユーザー** ページの **ユーザー ID** 列で、ユーザー ID 番号をクリックします。**ユーザー設定** ページが表示されます。
 **メモ:** ユーザー ID 1 は CMC にデフォルトで組み込まれているルートユーザーアカウントです。これを変更することはできません。
3. **ユーザー ID** を有効にして、そのユーザーのユーザー名、パスワード、およびアクセス権限を指定します。オプションの詳細については、『オンラインヘルプ』を参照してください。
4. **適用** をクリックします。適切な権限を持つユーザーが作成されます。

RACADM を使用したローカルユーザーの設定


 **メモ:** リモート Linux システム上で RACADM コマンドを実行するには、root ユーザーとしてログインする必要があります。

CMC のプロパティデータベースには 16 のユーザーを設定できます。CMC ユーザーを手動で有効にする前に、現在のユーザーが存在するか確認します。新しい CMC を設定する場合、または RACADM の `racresetcfg` コマンドを使用した場合、現在のユーザーのみがパスワードが `calvin` を持つ root となります。`racresetcfg` サブコマンドは、すべての設定パラメータをデフォルト値にリセットします。それまでに行った変更はすべて失われます。

 **メモ:** ユーザーをいつでも有効および無効に切り替えられますが、ユーザーを無効にしてもそのユーザーはデータベースから削除されません。

ユーザーが存在するかどうかを確認するには、CMC への Telnet/SSH テキストコンソールを開き、ログインしてから、1~16 のインデックスごとに、次のコマンドを一度入力します。

```
racadm getconfig -g cfgUserAdmin -i <インデックス>
```

 **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一名によって使用されています。

racadm config サブコマンドを使用してユーザーを手動で有効または無効化する場合は、-i オプションでインデックスを指定する必要があります。

コマンドオブジェクト内の「#」文字は、それが読み取り専用オブジェクトであることを示しています。また、racadm config -f racadm.cfg コマンドを使用して、書き込み用に任意の数のグループ/オブジェクトを指定する場合、インデックスは指定できません。新規ユーザーは最初の使用可能なインデックスに追加されます。この動作は、メイン CMC と同じ設定での第 2 の CMC の設定におけるより優れた柔軟性を可能にします。


RACADM を使用した CMC ユーザーの追加

CMC 設定に新しいユーザーを追加するには、次の手順を実行します。

1. ユーザー名を設定します。
2. パスワードを設定します。
3. ユーザー権限を設定します。ユーザー権限の詳細については、「[ユーザーのタイプ](#)」を参照してください。
4. ユーザーを有効にします。

例：

次の例は、パスワードが「123456」で CMC へのログイン権限のある「John」という新しいユーザーを追加する方法を示しています。

 **メモ:** 特定のユーザー権限に対する有効なビットマスク値のリストについては、『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。デフォルトの権限値は 0 で、これはユーザーの権限が有効化されていないことを示します。

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 john racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456 racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminPrivilege 0x00000001 racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminEnable 1
```

正しい権限を持つユーザーが追加されたことを確認するには、次のコマンドを実行します。

```
racadm getconfig -g cfgUserAdmin -i 2
```

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

CMC ユーザーの無効化

RACADM を使用しているときは、各ユーザーを手動で個別に無効化する必要があります。設定ファイルを使用してユーザーを削除することはできません。

CMC ユーザーを削除するためのコマンド構文は、次のとおりです。

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <インデックス>" " racadm  
config -g cfgUserAdmin -i 2 -o cfgUserAdminPrivilege 0x0
```

二重引用符のヌル文字列 ("") は、指定したインデックスのユーザー設定を削除し、そのユーザー設定を工場出荷時のデフォルト値にリセットするように CMC に指示します。

許可を持つ iDRAC7 ユーザーの有効化


特定の管理許可（役割ベースの権限）を持つユーザーを有効にするには、次の手順を実行します。

1. 次のコマンド構文を使用して使用可能なユーザーインデックスを見つけます。

```
racadm getconfig -g cfgUserAdmin -i <インデックス>
```


2. 新しいユーザー名とパスワードで次のコマンドを入力します。

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <インデックス> <ユーザー権限ビットマスク値>
```

 **メモ:** 特定のユーザー権限に対して有効なビットマスク値のリストについては、dell.com/support/manuals にある『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。デフォルトの権限値は 0 で、これはユーザーの権限が有効化されていないことを示します。

Active Directory ユーザーの設定

会社で Microsoft Active Directory ソフトウェアを使用している場合、CMC にアクセス権を付与するようにソフトウェアを設定することができます。これにより、ディレクトリサービスの既存ユーザーに CMC ユーザー権限を追加し、制御することが可能になります。これはライセンスが必要な機能です。

 **メモ:** 次のオペレーティングシステムでは、Active Directory を使用してユーザーを認識できます。

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

CMC にログインするために、Active Directory を介してユーザー認証を設定できます。また、管理者が各ユーザーに特定の権限を設定できるようにする、役割ベースの権限を提供することもできます。

サポートされている Active Directory の認証機構

Active Directory を使用して、次の 2 つの方法を使用する CMC ユーザーアクセスを定義できます。

- Microsoft のデフォルトの Active Directory グループオブジェクトのみを使用する標準スキーマソリューション。
- デル提供のカスタマイズされた Active Directory オブジェクトを持つ拡張スキーマソリューション。アクセスコントロールオブジェクトはすべて Active Directory で管理されます。これにより、異なる CMC 上でさまざまな権限レベルを持つユーザーアクセスを設定するための最大限の柔軟性が実現します。

標準スキーマ Active Directory の概要


次の図に示すように、標準スキーマを使用して Active Directory を統合する場合は、Active Directory と CMC の両方での設定が必要となります。


標準グループオブジェクトは、Active Directory では役割グループとして使用されます。CMC アクセスを持つユーザーは、役割グループのメンバーです。このユーザーに特定の CMC へのアクセスを与えるには、その特定 CMC に役割グループ名およびドメイン名を設定する必要があります。役割および権限のレベルは、Active

Directory ではなく、各 CMC で定義されます。各 CMC には最大 5 つまで役割グループを設定できます。次の表は、デフォルトの役割グループの権限を示します。

表 13. : 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • CMC ログインユーザー • ログのクリアシステム管理者 • シャーシ制御システム管理者 (電源コマンド) • Server Administrator • テストアラートユーザー • ファブリック A システム管理者 	0x00000ed9
3	なし	CMC ログインユーザー	0x00000001
4	なし	権限の割り当てなし	0x00000000
5	なし	権限の割り当てなし	0x00000000

 **メモ:** ビットマスク値は、RACADM で標準スキーマを設定する場合に限り使用されます。

 **メモ:** ユーザー権限の詳細については、「[ユーザーのタイプ](#)」を参照してください。


標準スキーマ Active Directory の設定

Active Directory ログインアクセスのために CMC を設定するには、次の手順を実行します。


1. Active Directory サーバー (ドメインコントローラ) で、**Active Directory ユーザーとコンピュータ**スナップインを開きます。
2. CMC ウェブインタフェースまたは RACADM の使用 :

- a) グループを作成するか、既存のグループを選択します。
 - b) 役割権限を設定します。
3. CMC にアクセスするには、Active Directory ユーザーを Active Directory グループのメンバーとして追加します。


CMC ウェブインタフェースを使用した標準スキーマでの Active Directory の設定

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

1. 左ペインで、**シャージ概要** に移動し、**ユーザー認証 → ディレクトリサービス** をクリックします。**ディレクトリサービス** ページが表示されます。
2. **Microsoft Active Directory (標準スキーマ)** を選択します。標準スキーマ用に設定される設定が同じページに表示されます。
3. 以下を指定します。
 - Active Directory の有効化、ルートドメイン名、およびタイムアウト値の入力。
 - ドメインコントローラとグローバルカタログの検索を直接呼び出す場合は、**検索する AD サーバーの検索 (オプション)** オプションを選択して、ドメインコントローラとグローバルカタログの詳細を指定します。
4. 設定を保存するには、**適用** をクリックします。

 **メモ:** 先に進む前に、設定を適用する必要があります。設定を適用しない場合、次のページへ移動したときに設定が失われます。

5. **標準スキーマの設定** セクションで、**役割グループ** をクリックします。**役割グループの設定** ページが表示されます。
6. 役割グループのグループ名、ドメイン、および権限を指定します。
7. **適用** をクリックして役割グループ設定を保存し、**ユーザー設定ページに戻る** をクリックします。
8. 証明書の検証を有効にした場合、ドメインフォレストのルート認証局の署名付き証明書を CMC にアップロードする必要があります。**証明書を管理** セクションで、証明書のファイルパスを入力するか、参照をクリックして証明書ファイルを選択します。**アップロード** をクリックしてファイルを CMC にアップロードします。

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

ドメインコントローラの SSL 証明書は、ルート認証局の署名付き証明書で署名されていなければなりません。CMC にアクセスする管理ステーションで、ルート認証局の署名付き証明書が使用可能である必要があります。

9. シングルサインオン (SSO) を有効にした場合、**Kerberos Keytab** セクションで **参照** をクリックして keytab ファイルを指定し、**アップロード** をクリックします。アップロードを完了したら、アップロードに成功または失敗したかを通知するメッセージが表示されます。
10. **適用** をクリックします。**適用** をクリックした後、CMC ウェブサーバーが自動的に再起動します。
11. CMC Active Directory の設定を完了するには、ログアウトしてから CMC にログインします。
12. システムツリーで、**シャージ** を選択し、**ネットワーク** タブへ移動します。**ネットワークの設定** ページが表示されます。
13. **ネットワーク設定** で **DHCP を使用 (CMC ネットワークインターフェース IP アドレス用)** が選択されている場合、**DHCP を使用して DNS サーバーアドレスを取得** を選択します。
DNS サーバーの IP アドレスを手動で入力するには、**DHCP を使用して DNS サーバーアドレスを取得する** チェックボックスをオフにし、プライマリおよび代替 DNS サーバーの IP アドレスを入力します。
14. **変更の適用** をクリックします。

これで、CMC 標準スキーマ Active Directory 機能の設定が完了します。


RACADM を使用した標準スキーマの Active Directory の設定


RACADM コマンドプロンプトで、次のコマンドを実行します。

- **config** コマンドを使用 :


```
racadm config -g cfgActiveDirectory -o cfgADEnable 1 racadm config -g
cfgActiveDirectory -o cfgADType 2 racadm config -g cfgStandardSchema -
i <インデックス> -o cfgSSADRoleGroupName <役割グループの共通名> racadm
config -g cfgStandardSchema -i <インデックス> -o cfgSSADRoleGroupDomain <
完全修飾ドメイン名> racadm config -g cfgStandardSchema -i <インデックス> -o
cfgSSADRoleGroupPrivilege <特定の役割グループ許可のためのビットマスク値>
```


```
racadm config -g cfgActiveDirectory -o cfgADDomainController1 <ドメインコ
ントローラの完全修飾ドメイン名または IP アドレス> racadm config -g
cfgActiveDirectory -o cfgADDomainController2 <ドメインコントローラの完全修飾
ドメイン名または IP アドレス> racadm config -g cfgActiveDirectory -o
cfgADDomainController3 <ドメインコントローラの完全修飾ドメイン名または IP アド
レス>
```

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

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

```
racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog1 <ドメインコン
トローラの完全修飾ドメイン名または IP アドレス> racadm config -g
cfgActiveDirectory -o cfgADGlobalCatalog2 <ドメインコントローラの完全修飾ドメ
イン名または IP アドレス> racadm config -g cfgActiveDirectory -o
cfgADGlobalCatalog3 <ドメインコントローラの完全修飾ドメイン名または IP アドレス>
```

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

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

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

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


この場合、認証局 (CA) 証明書をアップロードする必要はありません。

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

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

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

```
racadm sslcertupload -t 0x2 -f <ADS ルート CA 証明書>
```

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

拡張スキーマ Active Directory 概要

拡張スキーマソリューションを使用する場合は、Active Directory スキーマの拡張が必要です。

Active Directory スキーマ拡張

Active Directory データは、属性とクラスの分散データベースです。Active Directory スキーマには、データベースに追加、または含めるデータのタイプを決定する規則があります。データベースに格納されるクラスの一例として、ユーザークラスがあります。ユーザークラス属性の一例として、ユーザーの姓、名、電話番号などがあります。

特定の要件を満たす属性およびクラスを追加して、データベースを拡張できます。デルでは、スキーマを拡張して、Active Directory を使用したリモート管理の認証と許可をサポートするために必要な変更を含めました。

既存の Active Directory スキーマに追加される各属性またはクラスは、固有の ID で定義される必要があります。業界全体で固有の ID を保持するため、Microsoft では Active Directory オブジェクト識別子 (OID) のデータベースを維持しており、企業がスキーマに拡張を追加したときに、それらが固有であり、お互いに競合しないことを保証できるようにしています。Microsoft の Active Directory におけるスキーマの拡張のため、Dell はディレクトリサービスに追加される属性およびクラス用に固有の OID、固有の名前拡張子、および固有にリンクされた属性 ID を取得しました。

- デルの拡張子 : dell
- デルのベース OID : 1.2.840.113556.1.8000.1280
- RAC LinkID の範囲 : 12070 ~ 12079


スキーマ拡張の概要

デルでは、関連、デバイス、および権限プロパティを取り入れるためにスキーマを拡張しました。関連プロパティは、特定の権限セットを持つユーザーまたはグループと、1つ、または複数の RAC デバイスとをリンクするために使用されます。このモデルは、複雑な操作をほとんど行うことなく、ネットワーク上のユーザー、RAC 権限、および RAC デバイスの様々な組み合わせにおける最大の柔軟性をシステム管理者に提供します。

認証と承認を Active Directory と統合したい CMC が 2 つネットワーク上にある場合は、各 CMC につき少なくとも 1 つの関連オブジェクトと 1 つの RAC デバイスオブジェクトを作成する必要があります。関連オブジェクトは必要なだけいくつでも作成でき、各関連オブジェクトにリンクできるユーザー、ユーザーグループ、RAC デバイスオブジェクトの数にも制限はありません。ユーザーと RAC デバイスオブジェクトは、企業内のどのドメインのメンバでもかまいません。

ただし、各関連オブジェクト（または、ユーザー、ユーザーグループ、あるいは RAC デバイスオブジェクト）は、1 つの権限オブジェクトにしかリンクすることができません。この例では、システム管理者が、特定の CMC で各ユーザーの権限をコントロールすることができます。

RAC デバイスオブジェクトは、Active Directory に照会して認証と許可を実行するための RAC ファームウェアへのリンクです。RAC をネットワークに追加した場合、システム管理者は RAC とそのデバイスオブジェクトをその Active Directory 名で設定して、ユーザーが Active Directory で認証と認可を実行できるようにする必要があります。さらに、ユーザーが認証できるように、RAC を少なくとも 1 つの関連オブジェクトに追加する必要があります。

 **メモ:** RAC 権限オブジェクトは CMC に適用されます。

関連オブジェクトは、必要に応じて多くも少なくも作成できます。ただし、少なくとも 1 つの関連オブジェクトを作成する必要があり、Active Directory を統合するネットワーク上の RAC (CMC) ごとに、1 つの RAC デバイスオブジェクトが必要です。

関連オブジェクトは、必要な数だけのユーザーおよび/またはグループの他、RAC デバイスオブジェクトにも対応できます。ただし、関連オブジェクトには、関連オブジェクトにつき1つの権限オブジェクトしか含めることができません。関連オブジェクトは、RAC (CMC) に対して権限を持つユーザーを連結します。

また、Active Directory オブジェクトは、単一ドメイン、または複数ドメインで設定することができます。たとえば、CMC が2つ (RAC1、RAC2) と、既存の Active Directory ユーザーが3つ (ユーザー1、ユーザー2、ユーザー3) あるとし、ユーザー1とユーザー2に両方の CMC へのシステム管理者権限を与え、ユーザー3に RAC2 カードへのログイン権限を与えるなどです。

別のドメインからユニバーサルグループを追加するときは、ユニバーサルスコープを持つ関連オブジェクトを作成します。Dell Schema Extender ユーティリティによって作成されるデフォルトの関連オブジェクトは、ドメインローカルグループであり、他のドメインのユニバーサルグループとは連携しません。

単一ドメインのシナリオでオブジェクトを設定するには、次の手順を実行します。

1. 関連オブジェクトを2つ作成します。
2. 2つの CMC を表す2つの RAC デバイスオブジェクト、RAC1 と RAC2 を作成します。
3. 2つの特権オブジェクト、特権1と特権2を作成します。特権1にはすべての特権 (システム管理者)、特権2にはログイン特権を与えます。
4. ユーザー1とユーザー2をグループ1にグループ化します。
5. グループ1を関連オブジェクト1 (A01) のメンバ、特権1を A01 の特権オブジェクトとして、RAC1 と RAC2 を A01 の RAC デバイスとして追加します。
6. ユーザー3を関連オブジェクト2 (A02) のメンバ、特権2を A02 の特権オブジェクト、RAC2 を A02 の RAC デバイスとして追加します。

複数ドメインのシナリオでオブジェクトを設定するには

1. ドメインのフォレスト機能がネイティブまたは Windows 2003 モードになっていることを確認します。
2. 2つの関連オブジェクト A01 (ユニバーサルスコープの) と A02 を任意のドメインに作成します。複数ドメインに Active Directory オブジェクトを設定している図では、オブジェクトがドメイン2に示されています。
3. 2つの CMC を表す2つの RAC デバイスオブジェクト、RAC1 と RAC2 を作成します。
4. 2つの特権オブジェクト、特権1と特権2を作成します。特権1にはすべての特権 (システム管理者)、特権2にはログイン特権を与えます。
5. ユーザー1とユーザー2をグループ1にグループ化します。グループ1のグループスコープはユニバーサルである必要があります。
6. グループ1を関連オブジェクト1 (A01) のメンバ、特権1を A01 の特権オブジェクトとして、RAC1 と RAC2 を A01 の RAC デバイスとして追加します。
7. ユーザー3を関連オブジェクト2 (A02) のメンバ、特権2を A02 の特権オブジェクト、RAC2 を A02 の RAC デバイスとして追加します。

拡張スキーマ Active Directory の設定

Active Directory を設定して CMC にアクセスするには、次の手順を実行します。

1. Active Directory スキーマを拡張します。
2. Active Directory ユーザーとコンピュータスナップインを拡張します。
3. Active Directory に CMC ユーザーと権限を追加します。
4. 各ドメインコントローラ上で SSL を有効にします。
5. CMC ウェブインタフェースまたは RACADM を使用して、CMC Active Directory のプロパティを設定します。

Active Directory スキーマの拡張

Active Directory スキーマを拡張すると、Active Directory スキーマに Dell の組織単位、スキーマクラスと属性、および権限例と関連オブジェクトが追加されます。スキーマを拡張する前に、ドメインフォレストのスキーマ

マスタ Flexible Single Master Operation (FSMO) 役割所有者におけるスキーマ管理者権限を所持していることを確認してください。

スキーマは、次のいずれかの方法を使用して拡張できます

- Dell Schema Extender ユーティリティ
- LDIF スクリプトファイル

LDIF スクリプトファイルを使用すると、Dell の組織単位はスキーマに追加されません。


LDIF ファイルと Dell Schema Extender はそれぞれ『*Dell Systems Management Tools およびマニュアル*』DVD の次のディレクトリに収録されています。

- DVD ドライブ:\SYSTEMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files
- <DVD ドライブ>:\SYSTEMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema_Extender

LDIF ファイルを使用するには、**LDIF_Files** ディレクトリにあるリリースノートの説明を参照してください。

Schema Extender または LDIF ファイルは、任意の場所にコピーして実行することができます。

Dell Schema Extender の使用

 **注意:** Dell Schema Extender では、**SchemaExtenderOem.ini** ファイルを使用します。Dell Schema Extender ユーティリティが正常に機能することを確認するため、このファイルの名前は変更しないでください。

1. ようこそ画面で、**次へ** をクリックします。
2. 警告を読み、理解した上で、もう一度 **次へ** をクリックします。
3. **現在のログイン資格情報を使用** を選択するか、スキーマ管理者権限でユーザー名とパスワードを入力します。
4. **次へ** をクリックして、Dell Schema Extender を実行します。
5. **終了** をクリックします。

スキーマが拡張されます。スキーマ拡張子を確認するには、MMC と Active Directory スキーマスナップインを使用して、クラスと属性があることを確認します。クラスと属性に関する詳細は、「[クラスと属性](#)」を参照してください。MMC および Active Directory スキーマスナップインの使い方は、Microsoft のマニュアルを参照してください。

クラスと属性

表 14. Active Directory スキーマに追加されたクラスのクラス定義

クラス名	割り当てられたオブジェクト識別番号 (OID)
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

表 15. dellRacDevice クラス

OID	1.2.840.113556.1.8000.1280.1.7.1.1
説明	Dell RAC7 デバイスを表します。Active Directory では、RAC7 は delliDRACDevice として設定される必要があ

OID	1.2.840.113556.1.8000.1280.1.7.1.1
	ります。この設定によって、CMC から Active Directory に Lightweight Directory Access Protocol (LDAP) クエリを送信できるようになります。
クラスの種類	構造体クラス
SuperClasses	dellProduct
属性	dellSchemaVersion dellRacType

表 16. dellDRACAssociationObject クラス

OID	1.2.840.113556.1.8000.1280.1.7.1.2
説明	Dell 関連オブジェクトを表します。関連オブジェクトは、ユーザーとデバイス間の連結を可能にします。
クラスの種類	構造体クラス
SuperClasses	グループ
属性	dellProductMembers dellPrivilegeMember

表 17. dellRAC4Privileges クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.3
説明	CMC デバイスの権限（承認権限）を定義します。
クラスの種類	補助クラス
SuperClasses	なし
属性	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsTestAlertUser dellIsDebugCommandAdmin dellPermissionMask1 dellPermissionMask2

表 18. dellPrivileges クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.4
説明	デルの権限（許可権限）のコンテナクラスとして使用されます。
クラスの種類	構造体クラス
SuperClasses	ユーザー

OID	1.2.840.113556.1.8000.1280.1.1.1.4
属性	dellRAC4Privileges

表 19. dellProduct クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.5
説明	すべての Dell 製品が派生するメインクラス。
クラスの種類	構造体クラス
SuperClasses	コンピュータ
属性	dellAssociationMembers

表 20. Active Directory スキーマに追加された属性のリスト

割り当てられた OID/ 構文オブジェクト識別子	単一値
属性 : dellPrivilegeMember 説明 : この属性に属する dellPrivilege オブジェクトのリスト。 OID : 1.2.840.113556.1.8000.1280.1.1.2.1 識別名 : (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
属性 : dellProductMembers 説明 : この役割に属する dellRacDevices オブジェクトのリスト。この属性は、dellAssociationMembers バックワードリンクへのフォワードリンクです。 リンク ID : 12070 OID : 1.2.840.113556.1.8000.1280.1.1.2.2 識別名 : (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
属性 : dellIsCardConfigAdmin 説明 : ユーザーがデバイスの設定権限がある場合には TRUE。 OID : 1.2.840.113556.1.8000.1280.1.1.2.4 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
属性 : dellIsLoginUser 説明 : ユーザーがデバイスでログイン権限がある場合には TRUE。 OID : 1.2.840.113556.1.8000.1280.1.1.2.3 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
属性 : dellIsUserConfigAdmin 説明 : ユーザーがデバイスのユーザー設定システム管理者権限がある場合には TRUE。 OID : 1.2.840.113556.1.8000.1280.1.1.2.5 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
属性 : delIsLogClearAdmin	TRUE

割り当てられた OID/ 構文オブジェクト識別子	単一値
<p>説明: ユーザーがデバイスのログのクリアシステム管理者権限がある場合には TRUE。</p> <p>OID : 1.2.840.113556.1.8000.1280.1.1.2.6</p> <p>ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)</p>	
<p>属性: dellIsServerResetUser</p> <p>説明: ユーザーがデバイスのサーバーリセット権限がある場合には TRUE。</p> <p>OID : 1.2.840.113556.1.8000.1280.1.1.2.7</p> <p>ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)</p>	TRUE
<p>属性: dellIsTestAlertUser</p> <p>説明: ユーザーがデバイスのテスト警告ユーザー権限がある場合には TRUE。</p> <p>OID : 1.2.840.113556.1.8000.1280.1.1.2.10</p> <p>ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)</p>	TRUE
<p>属性: dellIsDebugCommandAdmin</p> <p>説明: ユーザーがデバイスのデバッグコマンドシステム管理者権限がある場合には TRUE。</p> <p>OID : 1.2.840.113556.1.8000.1280.1.1.2.11</p> <p>ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)</p>	TRUE
<p>属性: dellSchemaVersion</p> <p>説明: 現在のスキーマバージョンを使用してスキーマをアップデートします。</p> <p>OID : 1.2.840.113556.1.8000.1280.1.1.2.12</p> <p>大文字小文字を区別しない文字列 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)</p>	TRUE
<p>属性: dellRacType</p> <p>説明: この属性は dellRacDevice オブジェクトの現在の RAC タイプで、dellAssociationObjectMembers フォワードリンクへのバックワードリンクです。</p> <p>OID : 1.2.840.113556.1.8000.1280.1.1.2.13</p> <p>大文字小文字を区別しない文字列 (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)</p>	TRUE
<p>属性: dellAssociationMembers</p> <p>説明: この製品に属する dellAssociationObjectMembers のリスト。この属性は、dellProductMembers にリンクされた属性へのバックワードリンクです。</p> <p>リンク ID : 12071</p> <p>OID : 1.2.840.113556.1.8000.1280.1.1.2.14</p> <p>識別名 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)</p>	FALSE
<p>属性: dellPermissionsMask1</p> <p>OID : 1.2.840.113556.1.8000.1280.1.6.2.1 整数 (LDAPTYPE_INTEGER)</p>	

割り当てられた OID/ 構文オブジェクト識別子	単一値
--------------------------	-----

属性 : dellPermissionsMask2

OID : 1.2.840.113556.1.8000.1280.1.6.2.2 整数 (LDAPTYPE_INTEGER)

Active Directory ユーザーとコンピュータスナップインへの Dell 拡張のインストール

Active Directory でスキーマを拡張する場合は、RAC (CMC) デバイス、ユーザーとユーザーグループ、RAC 関連、RAC 特権などを管理できるように、Active Directory ユーザーとコンピュータスナップインも拡張する必要があります。

『Dell Systems Management Tools and Documentation』DVD を使用してシステム管理ソフトウェアをインストールする場合、インストール手順の実行中に **Active Directory ユーザーとコンピュータスナップイン** オプションを選択して、スナップインを拡張できます。システム管理ソフトウェアのインストールに関する追加手順については、『Dell OpenManage ソフトウェアクイックインストールガイド』を参照してください。64 ビットの Windows オペレーティングシステムの場合、スナップインのインストーラは <DVDdrive>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64 にあります。

Active Directory ユーザーとコンピュータスナップインの詳細については、Microsoft のマニュアルを参照してください。

Active Directory への CMC ユーザーと権限の追加

Dell 拡張 Active Directory ユーザーとコンピュータスナップインを使用して、RAC デバイスオブジェクト、関連オブジェクト、および権限オブジェクトを作成することにより、CMC ユーザーおよび権限を追加できます。各オブジェクトを追加するには、次の操作を行います。

- RAC デバイスオブジェクトの作成
- 権限オブジェクトの作成
- 関連オブジェクトの作成
- 関連オブジェクトへのオブジェクトの追加


RAC デバイスオブジェクトの作成

RAC デバイスオブジェクトを作成するには、次の手順を実行します。

1. MMC コンソールルート ウィンドウでコンテナを右クリックします。
2. 新規 → Dell リモート管理オブジェクトの詳細設定 を選択します。
3. 新規オブジェクト ページで、新しいオブジェクトの名前を入力します。この名前は、「[ウェブインタフェースを使用した標準スキーマでの Active Directory の設定](#)」で入力した CMC 名と同じである必要があります。
4. RAC デバイスオブジェクト を選択し、OK をクリックします。

権限オブジェクトの作成

権限オブジェクトを作成するには、次の手順を実行します。

 **メモ:** 権限オブジェクトは、関係のある関連オブジェクトと同じドメイン内に作成する必要があります。

1. MMC コンソールルート ウィンドウでコンテナを右クリックします。
2. 新規 → Dell リモート管理オブジェクトの詳細設定 を選択します。
3. 新規オブジェクト ページで、新しいオブジェクトの名前を入力します。
4. 権限オブジェクト を選択し、OK をクリックします。
5. 作成した権限オブジェクトを右クリックして **プロパティ** を選択します。
6. RAC 権限 タブをクリックしてユーザーまたはグループの権限を割り当てます。CMC のユーザー権限の詳細については、[ユーザータイプ](#) を参照してください。

関連オブジェクトの作成

関連オブジェクトはグループから派生したもので、グループタイプを含む必要があります。関連スコープは、関連オブジェクトのセキュリティグループタイプを指定します。関連オブジェクトを作成する際は、追加するオブジェクトのタイプに適用する関連スコープを選択してください。たとえば、ユニバーサルを選択すると、Active Directory ドメインがネイティブモードで機能している場合のみ、関連オブジェクトが使用可能になります。

関連オブジェクトを作成するには、次の手順を実行します。

1. **コンソールのルート (MMC)** ウィンドウでコンテナを右クリックします。
2. **新規 → Dell リモート管理オブジェクトの詳細設定** を選択します。
3. **新規オブジェクト** ページで、新しいオブジェクトの名前を入力し、**関連オブジェクト** を選択します。
4. **関連オブジェクト** の範囲を選択し、**OK** をクリックします。

関連オブジェクトへのオブジェクトの追加

関連オブジェクトプロパティ ウィンドウを使用すると、ユーザーまたはユーザーグループ、権限オブジェクト、および RAC デバイスまたは RAC デバイスグループを関連付けることができます。お使いのシステムで Microsoft Windows 2000 以降のバージョンのオペレーティングシステムを実行している場合は、ユニバーサルグループを使って、ユーザーまたは RAC オブジェクトでドメインをスパンします。

ユーザーおよび RAC デバイスのグループを追加できます。

ユーザーまたはユーザーグループの追加

ユーザーまたはユーザーグループを追加するには、次の手順を実行します。

1. **関連オブジェクト** を右クリックし、**プロパティ** を選択します。
2. **ユーザー** タブを選択して、**追加** を選択します。
3. ユーザーまたはユーザーグループの名前を入力し、**OK** をクリックします。

権限の追加

権限を追加するには、次の手順を実行します。

1. **権限オブジェクト** タブを選択し、**追加** をクリックします。
2. 権限オブジェクト名を入力し、**OK** をクリックします。
権限オブジェクト タブをクリックして、RAC7 デバイスに対して認証を行うときにユーザーまたはユーザーグループの権限を定義する関連に、権限オブジェクトを追加します。関連オブジェクトに追加できる権限オブジェクトは、1つだけです。


RAC デバイスまたは RAC デバイスグループの追加






RAC デバイスまたは RAC デバイスグループを追加するには、次の手順に従います。

1. **製品** タブを選択して **追加** をクリックします。
2. RAC デバイスまたは RAC デバイスグループの名前を入力し、**OK** をクリックします。
3. **プロパティ** ウィンドウで、**適用**、**OK** の順にクリックします。
製品 タブをクリックして、1 台または複数台の RAC デバイスを関連に追加します。関連デバイスは、ネットワークに接続している RAC デバイスのうち、定義したユーザーまたはユーザーグループが使用できるものを指定します。関連オブジェクトには複数の RAC デバイスを追加できます。


CMC ウェブインタフェースを使用した拡張スキーマの Active Directory の設定

CMC ウェブインタフェースを使用して Active Directory を拡張スキーマで設定するには、次の手順を実行します。

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

1. 左ペインで、**シャーシ概要** → **ユーザー認証** → **シャーシ概要** → **ディレクトリサービス** をクリックします。
2. **Microsoft Active Directory (拡張スキーマ)** を選択します。
拡張スキーマ用に設定される設定値が同じページに表示されます。
3. 以下を指定します。
 - **Active Directory** を有効化し、ルートドメイン名とタイムアウト値を入力します。
 - ドメインコントローラとグローバルカタログの検索を直接呼び出す場合は、**検索する AD サーバーの検索 (オプション)** オプションを選択して、ドメインコントローラとグローバルカタログの詳細を指定します。
 -  **メモ:** IP アドレスを **0.0.0.0** に設定すると、**CMC** のサーバー検索が無効になります。
 -  **メモ:** コンマ区切りのドメインコントローラまたはグローバルカタログサーバーのリストを指定できます。**CMC** では、最大 **3** 個の IP アドレスまたはホスト名を指定できます。
 -  **メモ:** ドメインコントローラまたはグローバルカタログサーバーが、すべてのドメインとアプリケーションに対して正しく設定されていない場合は、既存のアプリケーション/ドメインの動作中に予期しない結果が生成される可能性があります。
4. 設定を保存するには、**適用** をクリックします。
 -  **メモ:** 先に進む前に、設定を適用する必要があります。設定を適用しない場合、次のページへ移動したときに設定が失われます。
5. **拡張スキーマ設定** セクションで、**CMC** デバイス名およびドメイン名を入力します。
6. 証明書の検証を有効にした場合、ドメインフォレストのルート認証局の署名付き証明書を **CMC** にアップロードする必要があります。**証明書を管理** セクションで、証明書のファイルパスを入力するか、**参照** をクリックして証明書ファイルを選択します。**アップロード** をクリックしてファイルを **CMC** にアップロードします。
 -  **メモ:** アップロードする証明書の相対ファイルパスが **ファイルパス** の値に表示されます。フルパスと正しいファイル名とファイル拡張子を含む絶対ファイルパスを入力する必要があります。

ドメインコントローラの **SSL 証明書** は、ルート認証局の署名付き証明書で署名されていなければなりません。**CMC** にアクセスする管理ステーションで、ルート認証局の署名付き証明書が使用可能である必要があります。

 **注意:** デフォルトでは、**SSL 証明書の検証** が必要です。この証明書を無効にすることは推奨されません。
7. シングルサインオン (SSO) を有効にした場合、**Kerberos Keytab** セクションで **参照** をクリックし、**keytab** ファイルを指定して **アップロード** をクリックします。アップロードを完了したら、アップロードに成功または失敗したかを通知するメッセージが表示されます。
8. **適用** をクリックします。
適用 をクリックした後、**CMC** ウェブサーバーが自動的に再起動します。
9. **CMC** ウェブインターフェースにログインします。
10. システムツリーで、**シャーシ** を選択し、**ネットワーク** タブをクリックして、次に **ネットワーク** サブタブをクリックします。**ネットワーク設定** ページが表示されます。
11. **CMC** ネットワークインターフェースの IP アドレスに **DHCP** を使用 が有効の場合は、次のいずれかを行います。
 - **DHCP** を使用して **DNS サーバーアドレスを取得する** を選択して、DHCP サーバーが DNS サーバーアドレスを自動的に取得できるようにします。
 - **DHCP** を使用して **DNS サーバーアドレスを取得する** チェックボックスをオフにしたままで、フィールドにプライマリおよび代替 DNS サーバーの IP アドレスを入力して DNS サーバーの IP アドレスを手動で設定します。


12. **変更の適用** をクリックします。

拡張スキーマ用の **Active Directory** 設定が設定されます。

RACADM を使用した拡張スキーマの **Active Directory** の設定


RACADM コマンドを使用して **CMC Active Directory** を拡張スキーマで設定するには、コマンドプロンプトを開き、次のコマンドを入力します。

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1 racadm config -g
cfgActiveDirectory -o cfgADType 1 racadm config -g cfgActiveDirectory -o
cfgADRacName <RAC 共通名> racadm config -g cfgActiveDirectory -o cfgADRacDomain
< 完全修飾 rac ドメイン名 > racadm config -g cfgActiveDirectory -o
cfgADDomainController1 < ドメインコントローラの完全修飾ドメイン名または IP アドレス >
racadm config -g cfgActiveDirectory -o cfgADDomainController2 < ドメインコントロー
ラの完全修飾ドメイン名または IP アドレス > racadm config -g cfgActiveDirectory -o
cfgADDomainController3 < ドメインコントローラの完全修飾ドメイン名または IP アドレス >
```

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

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

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


 **メモ:** この場合、CA 証明書をアップロードする必要はありません。

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

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

この場合、CA 証明書をアップロードする必要があります。

```
racadm sslcertupload -t 0x2 -f <ADS ルート CA 証明書>
```

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

次の RACADM コマンドの使用はオプションです。

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

汎用 LDAP ユーザーの設定

CMC は Lightweight Directory Access Protocol (LDAP) ベースの認証をサポートするための汎用ソリューションを提供します。この機能は、ディレクトリサービス上のどのスキーマ拡張にも必要です。

CMC 管理者は、LDAP サーバーのユーザーログインを CMC と統合することが可能です。この統合を行うには、LDAP サーバーと CMC の両方での設定が必要です。Active Directory 側では、標準グループオブジェクトが役割グループとして使用されます。CMC のアクセス権を持つユーザーは、役割グループのメンバーとなります。特権は、Active Directory サポートを伴う標準スキーマセットアップの動作に似た認証のため、CMC に引き続き保存されます。

LDAP ユーザーが特定の CMC カードにアクセスできるようにするには、その CMC カードに役割グループ名とそのドメイン名を設定する必要があります。各 CMC には、5 つまで役割グループを設定できます。ユーザーは、オプションでディレクトリサービス内に複数のグループを追加できます。ユーザーが複数グループのメンバの場合、そのグループのすべての特権を取得します。

役割グループの特権レベルおよびデフォルトの役割グループ設定に関する詳細は、「[ユーザータイプ](#)」を参照してください。

汎用 LDAP ディレクトリを設定した CMC へのアクセス

CMC の汎用 LDAP 実装では、ユーザーにアクセスを許可するためにユーザー認証とユーザー承認の 2 つのフェーズが使用されます。

LDAP ユーザーの認証

一部のディレクトリサーバーでは、特定の LDAP サーバーを検索する前にバインドが必要です。ユーザーを認証するには、次の手順を実行します。

1. オプションでディレクトリサービスにバインドします。デフォルトは匿名バインドです。
2. ユーザーログインに基づいて、ユーザーを検索します。デフォルト属性は uid です。複数のオブジェクトが検出された場合、プロセスはエラーを返します。
3. バインドを解除してから、ユーザーの DN とパスワードを使ってバインドを実行します。バインドできないシステムでは、ログインが失敗します。
4. これらの手順に問題がなければ、ユーザーは認証されています。


LDAP ユーザーの承認

ユーザーを承認するには、次の手順を実行します。


1. 設定された各グループで、member or uniqueMember 属性内のユーザーのドメイン名を検索します。ユーザードメインは管理者が設定できます。
2. ユーザーが所属するユーザーグループごとに、適切なユーザーアクセス権と権限をユーザーに付与します。

CMC ウェブインタフェースを使用した汎用 LDAP ディレクトリサービスの設定


汎用 LDAP ディレクトリサービスを設定するには、次の手順を実行します。

 **メモ:** シャーシ設定システム管理者 権限が必要です。

1. 左ペインで、**シャーシ概要** → **ユーザー認証** → **ディレクトリサービス** をクリックします。
2. **汎用 LDAP** を選択します。
同じページに、標準スキーマ用に設定される設定が表示されます。
3. 以下を指定します。

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


- 共通設定
- LDAP で使用するサーバー：
 - * 静的サーバー — FQDN または IP アドレスおよび LDAP ポート番号を指定します。
 - * DNS サーバー — DNS 内で SRV レコードを検索して、LDAP サーバーのリストを取得するための DNS サーバーを指定します。
次の DNS クエリが SRV レコードに対して実行されます。
`_[Service Name]._tcp.[Search Domain]`
ここで、<Search Domain> は、クエリ内で使用するルートレベルドメインで、<Service Name 名> はクエリ内で使用するサービス名です。
たとえば、次のとおりです。
`_ldap._tcp.dell.com`
ここで、ldap はサービス名、dell.com は検索ドメインです。

4. 設定を保存するには、**適用** をクリックします。
 **メモ:** 先に進む前に、設定を適用する必要があります。設定を適用しない場合、次のページへ移動したときに設定が失われます。
5. **グループ設定** セクションで、**役割グループ** をクリックします。
6. **LDAP 役割グループの設定** ページで、役割グループのグループドメイン名と権限を指定します。
7. **適用** 役割グループの設定を保存し、**ユーザー設定ページに戻る** をクリックして **汎用 LDAP** を選択します。
8. **証明書検証を有効にする** オプションを選択した場合、**証明書を管理** セクションで、**SSL ハンドシェイク** 中に LDAP サーバー証明書を検証する **CA 証明書** を指定し、**アップロード** をクリックします。証明書が **CMC** にアップロードされ、詳細が表示されます。
9. **適用** をクリックします。
汎用 LDAP ディレクトリサービスが設定されました。

RACADM を使用した汎用 LDAP ディレクトリサービスの設定

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

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

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

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

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

CMC は、オプションとして SRV レコードのために DNS サーバーをクエリするように設定することができます。`cfgLDAPSRVLookupEnable` プロパティが有効の場合、`cfgLDAPServer` プロパティは無視されます。SRV レコードのための DNS の検索には、次のクエリが使用されます。

```
_ldap._tcp.domainname.com
```

上記のクエリの `ldap` は、`cfgLDAPSRVLookupServiceName` プロパティです。

`cfgLDAPSRVLookupDomainName` は、**domainname.com** に設定されます。


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

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。

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alm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に、CMC は Windows Kerberos ネットワークをサポートします。ユーザーアカウントへのサービスプリンシパル名 (SPN) バインドの作成、および信頼情報の MIT スタイルの Kerberos keytab ファイルへのエクスポートには、ktpass ツール (サーバーインストール CD/DVD の一部として Microsoft から使用可能) が使用されます。ktpass ユーティリティの詳細については、Microsoft のウェブサイトを参照してください。

keytab ファイルを生成する前に、ktpass コマンドの **-mapuser** オプションで使用する Active Directory ユーザーアカウントを作成する必要があります。この名前は、生成した keytab ファイルのアップロード先となる CMC DNS 名と同じにする必要があります。


ktpass ツールを使用して keytab ファイルを生成するには、次の手順を実行します。

1. **ktpass** ユーティリティを、Active Directory 内のユーザーアカウントに CMC をマップするドメインコントローラ (Active Directory サーバー) 上で実行します。
2. 次の ktpass コマンドを使用して、Kerberos keytab ファイルを作成します。

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

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

CMC にアップロードする必要のある **keytab** ファイルが作成されます。

 **メモ:** keytab には暗号化キーが含まれており、安全な場所に保管する必要があります。ktpass ユーティリティの詳細については、**Microsoft** ウェブサイトを参照してください。

Active Directory スキーマ用の CMC の設定

Active Directory 標準スキーマ用の CMC の設定については、「[標準スキーマ Active Directory の設定](#)」を参照してください。

Active Directory 拡張スキーマ用の CMC の設定については、「[拡張スキーマ Active Directory 概要](#)」を参照してください。

SSO ログイン用のブラウザの設定


シングルサインオン (SSO) は Internet Explorer バージョン 6.0 以降、および Firefox バージョン 3.0 以降でサポートされています。

 **メモ:** 次の手順は、CMC が Kerberos 認証でシングルサインオンを使用する場合にのみ適用されます。


Internet Explorer

Internet Explorer でシングルサインオンの設定を行うには、次の手順を実行します。

1. Internet Explorer で、ツール → インターネットオプション を選択します。
2. セキュリティタブのセキュリティ設定を表示または変更するゾーンを選択する の下で、ローカルイントラネットを選択します。
3. サイト をクリックします。
ローカルイントラネット ダイアログボックスが表示されます。
4. 詳細設定 をクリックします。
ローカルイントラネットの詳細設定 ダイアログボックスが表示されます。
5. このサイトをゾーンに追加する に CMC の名前とそれが属するドメインを入力し、追加 をクリックします。

 **メモ:** 対象ドメインでは、ワイルドカード (*) を使用してすべてのデバイスまたはユーザーを指定できます。

Mozilla Firefox

1. Firefox では、アドレスバーに **about:config** と入力します。
 **メモ:** ブラウザに「保証が無効になる場合があります」という警告が表示された場合は、**注意することをお約束します** をクリックします。
2. フィルタ テキストボックスに、**negotiate** と入力します。
ブラウザには、「negotiate」という単語を含んだプリファレンス名のリストが表示されます。
3. 表示されたリストから、**network.negotiate-auth.trusted-uris** をダブルクリックします。
4. 文字列値の入力ダイアログボックスに、CMC のドメイン名を入力し、**OK** をクリックします。

スマートカードのログインに使用するブラウザの設定


Internet Explorer - インターネットブラウザが Active-X プラグインをダウンロードするように設定されていることを確認してください。

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

CMC ウェブインタフェースまたは RACADM を使用して、CMC SSO またはスマートカードログインを設定することができます。


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

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

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

1. ユーザーアカウント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 <ユーザー>@<ドメイン>
```

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

コマンドが正常に実行されれば、CMC は Kerberos 資格情報を取得することができ、ユーザーの **Active Directory** アカウントにアクセスできることを示します。コマンドが正常に実行されない場合は、エラーを訂正してコマンドを実行し直してください。詳細については、dell.com/support/manuals にある『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。

Keytab ファイルのアップロード

Kerberos keytab ファイルは Kerberos データセンター (KDC) に対する CMC のユーザ名とパスワード資格情報として使用され、これによって **Active Directory** にアクセスすることができます。Kerberos 領域の各 CMC は **Active Directory** を使って登録し、一意の keytab ファイルがあることが必要です。

Active Directory Server 関連で生成される Kerberos Keytab をアップロードできます。 **ktpass.exe** ユーティリティを実行すると、**Active Directory Server** から Kerberos Keytab を生成できます。この keytab は、**Active Directory Server** と CMC の間の信頼関係を確立します。

keytab ファイルをアップロードするには、次の手順を実行します。

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. **Microsoft Active Directory (標準スキーマ)** を選択します。
3. **Kerberos Keytab** セクションで、**参照** をクリックして keytab ファイルを選択し、**アップロード** をクリックします。

アップロードを完了したら、**keytab** ファイルのアップロードに成功または失敗したかを通知するメッセージが表示されます。

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

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

```
racadm -g cfgActiveDirectory -o cfgADSSOEnable 1
```

スマートカードログインを有効にするには、**Active Directory** の設定中に実行する手順への追加として、次のオブジェクトに従います。

- `cfgSmartCardLogonEnable`
- `cfgSmartCardCRLEnable`

CMC にコマンドラインコンソールの使用を設定する方法

本項では、CMC コマンドラインコンソール（またはシリアル/Telnet/セキュアシェルコンソール）の機能について、およびコンソールからシステム管理操作を実行できるようにシステムを設定する方法について説明します。コマンドラインコンソールを介した CMC での RACADM コマンドの使用方法については、『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。

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、『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。
connect	サーバーまたは I/O モジュールのシリアルコンソールに接続します。詳細については、「 connect コマンドを使用したサーバーまたは I/O モジュールの接続 」を参照してください。  メモ: connect RACADM コマンドを使用することもできます。
exit、logout、quit	これらすべてのコマンドは同じ処置を実行し、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 にある『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。

CMC では、SSH 経由の公開キー認証 (PKA) もサポートされています。この認証方法は、ユーザー ID/パスワードの組み込みや入力を排除することで SSH スクリプトの自動化を改善します。詳細については、「[SSH 経由の公開キー認証の設定](#)」を参照してください。

SSH はデフォルトで有効になっています。SSH が無効になっている場合は、サポートされている他のインタフェースを使用して有効にできます。

SSH を設定するには、[サービスの設定](#) を参照してください。

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	<ul style="list-style-type: none">AES256-CBCRIJNDAEL256-CBC

スキームの種類	スキーム
	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
認証	パスワード

SSH 経由の公開キー認証の設定

SSH インタフェース経由のサービスユーザー名と共に使用できる公開キーは、最大 **6** 個まで設定できます。キーを誤って上書きしたり削除したりするのを防ぐため、公開キーを追加または削除する前に `view` コマンドを使って設定済みのキーを確認してください。サービスユーザー名は、SSH 経由で **CMC** にアクセスするときに使用できる特殊なユーザーアカウントです。SSH 経由の **PKA** を正しく設定し、使用すれば、**CMC** へのログインにユーザー名やパスワードを入力する必要がなくなります。この機能は、各種機能を実行するための自動化されたスクリプトのセットアップに大変便利です。

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

新しい公開キーを追加するときは、そのキーを追加するインデックスに既存のキーが存在していないことを確認してください。**CMC** では、新しいキーを追加する前に、前のキーが削除されているかどうかの確認作業は行われません。SSH インタフェースが有効化されている限り、新しいキーは追加されてすぐに自動で有効化されます。

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

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

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


`sshpkauth` の詳細については、『**Chassis Management Controller for PowerEdge VRTX RACADM** コマンドラインリファレンスガイド』を参照してください。

Windows を実行するシステム用の公開キーの生成

アカウントを追加する前に、SSH 経由で **CMC** にアクセスするシステムからの公開キーが必要になります。公開 / 秘密キーペアを生成する方法には、Windows を実行しているクライアントの **PuTTY Key Generator** アプリケーションを使用する方法と Linux を実行しているクライアントの `ssh-keygen` を使用する方法の **2** 通りあります。

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

PuTTY Key Generator を使用して、Windows を実行しているクライアント用の基本キーを作成するには、次の手順を実行します。

1. アプリケーションを起動し、生成するキーの種類として、SSH-2 RSA または SSH-2 DSA を選択します (SSH-1 はサポートされていません)。
2. キーのビット数を入力します。数字は 768~4096 の間で指定します。
 **メモ:** 768 未満、または 4096 を超えるキーを追加しても CMC がメッセージを表示しない場合がありますが、ログインしようとするときこれらのキーは失敗します。
3. **生成** をクリックし、指示に従ってマウスポインタをウィンドウ内で移動させます。
キーを作成したら、キーコメントフィールドを変更できます。
パスフレーズを入力すると、キーをセキュリティ保護することもできます。秘密キーを保存したことを確認します。
4. 公開キーの使用方法には 2 つのオプションがあります。
 - 公開キーをファイルに保存し後でアップロードします。
 - テキストオプションを使用してアカウントを追加する場合に、**公開キーの貼り付け** ウィンドウからテキストをコピーして貼り付けます。

Linux を実行するシステム用の公開キーの生成

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

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

ここで、

-t は、dsa または rsa である必要があります。

-b は 768~4096 で、ビット暗号化サイズを指定します。

-c を使用すると、公開キーコメントを変更できます。これはオプションです。

<passphrase> はオプションです。コマンドを完了したら、パブリックファイルを使用してファイルをアップロードするために RACADM に渡します。

CMC の RACADM 構文メモ

racadm sshpkauth コマンドを使用する場合、次を確認します。

- -i オプションを使用する場合は、パラメータが svcacct である必要があります。CMC では、-i へのそれ以外のパラメータの使用は失敗します。svcacct は、CMC で SSH 経由の公開キー認証を行うための特殊なアカウントです。
- CMC にログインするには、ユーザーはサービスである必要があります。他のカテゴリのユーザーは、sshpkauth コマンドを使用して入力した公開キーにアクセスできません。

公開キーの表示

CMC に追加した公開キーを表示するには、次を入力します。

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

キーを一度に 1 つずつ表示するには、all を数字の 1~6 に置き換えます。たとえば、キー 2 を表示するには、次を入力します。

```
racadm sshpkauth -i svcacct -k 2 -v
```

公開キーの追加

ファイルのアップロードオプション -f を使用して、CMC に公開キーを追加するには、コマンドラインインタフェースコンソールで次を入力します。

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

 **メモ:** リモート RACADM ではファイルのアップロードオプションしか使用できません。詳細については、『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。

テキストのアップロードオプションを使用して公開キーを追加するには、次を入力します。

```
racadm sshpkauth -i svcacct -k 1 -p 0xffff -t "<公開キーテキスト>"
```

公開キーの削除

公開キーを削除するには、次のコマンドを実行します。

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

すべての公開キーを削除するには、次のコマンドを実行します。

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

ターミナルエミュレーションソフトウェアの設定

CMC は、次のいずれかのタイプのターミナルエミュレーションソフトウェアを実行している管理ステーションからのシリアルテキストコンソールをサポートしています。


- Linux Minicom。
- Hilgraeve の HyperTerminal Private Edition (バージョン 6.3)。

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

Linux Minicom の設定

Minicom は Linux 用のシリアルポートアクセスユーティリティです。次の手順は Minicom バージョン 2.0 の設定に有効な手順です。他の Minicom バージョンは多少異なる場合がありますが、同じ基本的な設定が必要です。他のバージョンの Minicom を設定するには、本ユーザーズガイドの「必要な Minicom 設定」の項を参照してください。

Minicom バージョン 2.0 の設定

 **メモ:** 最適な結果を得るには、`cfgSerialConsoleColumns` プロパティをコンソールの列数に一致するように設定します。プロンプトには 2 列分が使用されることに注意してください。たとえば、80 列のターミナルウィンドウでは、次のように設定します。

```
racadm config -g cfgSerial -o cfgSerialConsoleColumns 80
```

1. Minicom 設定ファイルがない場合には、次の手順に進んでください。Minicom 設定ファイルがある場合は、`minicom<Minicom config file name>` を入力し、手順 12 に進みます。
2. Linux コマンドプロンプトで、`minicom -s` と入力します。
3. シリアルポートセットアップを選択し、<Enter> を押します。
4. <a> を押して、適切なシリアルデバイスを選択します (例: /dev/ttyS0)。
5. <e> を押して、**速度/パリティ/ビット** のオプションを **115200 8N1** に設定します。
6. <f> を押して、**ハードウェアフロー制御** をはいに、**ソフトウェアフロー制御** をいいえに設定します。シリアルポートセットアップメニューを終了するには、<Enter> を押します。
7. **モデムとダイヤル** を選択して、<Enter> を押します。
8. **モデムダイヤルとパラメータセットアップ** メニューで、<Backspace> を押して **init**、**reset**、**connect** および **hangup** 設定をクリアして空白にし、次に <Enter> をクリックして各空白値を保存します。
9. 指定のフィールドがすべてクリアされたら、<Enter> を押して **モデムダイヤルとパラメータセットアップ** メニューを終了します。

10. **Minicom** を終了を選択して、<Enter> を押します。
11. コマンドシェルプロンプトで、`minicom <Minicom config file name>` と入力します。
12. **Minicom** を終了するには、<Ctrl><a>、<x>、<Enter> を押します。
Minicom ウィンドウにログインプロンプトが表示されていることを確認します。ログインプロンプトが表示されたら、接続が正常に行われています。これで **CMC** コマンドラインインタフェースにログインし、アクセスする準備が完了しました。

必要な Minicom 設定

Minicom を設定するには、どのバージョンでも表を参照してください。

表 23. Minicom 設定

設定の説明	必要な設定
速度/パリティ/ビット	115200 8N1
ハードウェアフロー制御	はい
ソフトウェアフロー制御	いいえ
ターミナルエミュレーション	ANSI
モデムダイヤルとパラメータ設定	初期化、リセット、接続、切断 設定をクリアして空白にします。

connect コマンドを使用したサーバーまたは I/O 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せん。


サーバーでは、次を使用してシリアルコンソールリダイレクトを実行できます。

- **CMC** コマンドラインインタフェース (CLI) または **RACADM** `connect` コマンド。 **RACADM** コマンドの実行の詳細については、『**Chassis Management Controller for PowerEdge VRTX RACADM** コマンドラインリファレンスガイド』を参照してください。
- **iDRAC** ウェブインタフェースのシリアルコンソールリダイレクト機能。
- **iDRAC** Serial Over LAN (SOL) 機能。

シリアル、Telnet、SSH コンソールでは、**CMC** はサーバーまたは I/O モジュールへのシリアル接続の確立に `connect` コマンドをサポートします。サーバーシリアルコンソールには、**BIOS** の起動画面とセットアップ画面の両方と、オペレーティングシステムシリアルコンソールが備わっています。I/O モジュールでは、スイッチシリアルコンソールを使用できます。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** がリセットするまで `connect -b` オプションが接続されたままとなります。この接続はセキュリティリスクとなる可能性があります。

 **メモ:** `connect` コマンドは、`-b` (バイナリ) オプションを提供します。`-b` オプションはバイナリのローデータを渡し、`cfgSerialConsoleQuitKey` は使用されません。さらに、**CMC** シリアルコンソールを使用してサーバーに接続した場合、**DTR** 信号が遷移しても (たとえば、デバッグを接続するためにシリアルケーブルが取り外される)、アプリケーションは終了しません。

 **メモ:** **IOM** がコンソールリダイレクトをサポートしない場合、`connect` コマンドは空のコンソールを表示します。この場合に **CMC** コンソールに戻るには、エスケープシーケンスを入力します。コンソールのデフォルトエスケープシーケンスは `<Ctrl><I>` 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 24. スイッチへの IO モジュールのマッピング


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


 **メモ:** IOM 接続はシャージごとに同時に 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。

管理下サーバーのシリアルコンソールに接続するには、connect server-n コマンドを実行します (n は 1 ~4)。また、racadm connect server-n コマンドを使用することもできます。-b オプションを使用してサーバーに接続する場合、バイナリ通信が想定され、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、ホストへのルートなしエラーメッセージが表示されます。

connect server-n コマンドでは、ユーザーによるサーバーのシリアルポートへのアクセスが可能になります。この接続が確立されると、ユーザーは CMC のシリアルポート経由でサーバーのコンソールリダイレクトを表示できます。これには、BIOS シリアルコンソールとオペレーティングシステムシリアルコンソールが含まれます。

 **メモ:** BIOS 起動画面を表示するには、サーバーの BIOS セットアップでシリアルリダイレクトが有効になっ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、一部のキーが動作しません。そのため、<Ctrl> <Alt> <Delete> などに対して適切なキーボードショートカットを入力します。必要なキーボードショートカットは、最初のリダイレクト画面に表示されます。


シリアルコンソールリダイレクト用に管理されたサーバー BIOS の設定

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『iDRAC7 ユーザーズガイド』を参照)。

デフォルトでは、BIOS のシリアル通信はオフになっています。ホストテキストコンソールデータをシリアルオーバー LAN にリダイレクトするには、COM1 経由でコンソールリダイレクトを有効化する必要があります。BIOS 設定を変更するには、次の手順を実行します。

1. 管理下サーバーの電源をオンにします。
2. POST 中に <F2> キーを押して BIOS セットアップユーティリティを起動します。
3. シリアル通信に移動し、<Enter> を押します。ダイアログボックス内のシリアル通信リストに次のオプションが表示されます。
 - オフ
 - コンソールリダイレクトなしでオン
 - COM1 経由のコンソールリダイレクトでオン

これらのオプション間を移動するには、矢印キーを押します。

 **メモ:** COM1 経由のコンソールリダイレクトでオン オプションが選択されていることを確認してください。


4. 起動後のリダイレクトを有効化します (デフォルトは無効)。このオプションは次回再起動時に BIOS コンソールリダイレクトを有効化します。
5. 変更を保存して終了します。管理下システムが再起動します。

シリアルコンソールリダイレクトのための Windows の設定

Windows Server 2003 以降の Microsoft Windows Server バージョンを実行しているサーバーには設定は必要ありません。Windows は BIOS から情報を受け取り、COM 1 の Special Administration Console (SAC) コンソールを有効化します。

起動中における Linux のシリアルコンソールリダイレクトのための設定

次の手順は Linux GRand Unified Bootloader (GRUB) に固有の手順です。異なるブートローダーを使用する場合は、類似した変更が必要です。

 **メモ:** クライアント VT100 エミュレーションウィンドウを設定するときは、リダイレクトされたコンソールが表示されるウィンドウまたはアプリケーションを 25 行 x 80 桁に設定して、テキストが正しく表示されるようにします。異なる設定をすると、テキストの一部がずれて表示されます。

/etc/grub.conf ファイルを次のように編集します。

1. ファイル内の一般設定セクションを見つけ、次の 2 行を新たに入力します。
`serial --unit=1 --speed=57600 terminal --timeout=10 serial`
2. カーネル行に次の 2 つにオプションを追加します。
`kernel console=ttyS1,57600`
3. **/etc/grub.conf** に splashimage ディレクティブがある場合は、コメントアウトします。

次の例は、この手順で説明した変更を示しています。

```
# grub.conf generated by anaconda # # Note that you do not have to rerun
grub after making changes # to this file # NOTICE: You do not have a /boot
partition. This means that # all kernel and initrd paths are relative to /,
e.g. # root (hd0,0) # kernel /boot/vmlinuz-version ro root= /dev/sda1 #
initrd /boot/initrd-version.img # #boot=/dev/sda default=0 timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz serial --unit=1 --speed=57600 terminal --timeout=10
serial title Red Hat Linux Advanced Server (2.4.9-e.3smp) root (hd0,0) kernel /
boot/vmlinuz-2.4.9-e.3smp ro root= /dev/sda1 hda=ide-scsi console=ttyS0
console= ttyS1,57600 initrd /boot/initrd-2.4.9-e.3smp.img title Red Hat
Linux Advanced Server-up (2.4.9-e.3) root (hd0,0) 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 10:0:wait:/etc/rc.d/rc 0 11:1:wait:/etc/
rc.d/rc 1 12:2:wait:/etc/rc.d/rc 2 13:3:wait:/etc/rc.d/rc 3 14:4:wait:/etc/
rc.d/rc 4 15:5:wait:/etc/rc.d/rc 5 16:6: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
```


FlexAdress および FlexAddress Plus カードの使用

本項では、FlexAddress、FlexAddress Plus カード、およびそれらのカードの設定と使用について説明します。

 **メモ:** FlexAddress 機能はライセンスされています。この機能を使用するには、Enterprise ライセンスが必要です。

FlexAddress について

FlexAddress 機能は、オプションのアップグレードです。この機能により、工場出荷時にサーバーモジュールに割り当てられたワールドワイドネームおよびメディアアクセスコントロール (WWN/MAC) のネットワーク ID を、シャーシによって提供される WWN/MAC ID に置き換えることが可能となります。

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

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

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

FlexAddress 機能カードには、広範囲の MAC アドレスが含まれています。FlexAddress をインストールする前に、you can determine the range of MAC addresses contained on a feature card by inserting the USB メモリカードリーダーに SD カードを挿入し、`pwwn_mac.xml` ファイルを表示することにより、FlexAddress 機能カードに含まれる MAC アドレスの範囲を判断することができます。これにより、この一意の MAC アドレス範囲のために使用される 16 進数の MAC 開始アドレスである XML タグ `mac_start` が含まれる SD カード上の XML テキストファイルがクリアされます。`mac_count` タグは SD カードが割り当てる MAC アドレスの総数です。割り当てられた MAC 範囲の合計は次の式で求めることができます。


$$\langle \text{mac_start} \rangle + 0 \times \text{CF} (208 - 1) = \text{mac_end}$$

ここで、208 は `mac_count` を表し、次の式で求めることができます。

$$\langle \text{mac_start} \rangle + \langle \text{mac_start} \rangle - 1 = \langle \text{mac_end} \rangle$$

たとえば、次のとおりです。

$$(\text{starting_mac})00188BFFDCFA + 0 \times \text{CF} = (\text{ending_mac})00188BFFDCC9$$

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

FlexAddress Plus について

FlexAddress Plus は、カードバージョン 2.0 に追加された新機能であり、FlexAddress カードバージョン 1.0 のアップグレード版です。FlexAddress Plus には、FlexAddress よりも多くの MAC アドレスが含まれています。どちらの機能も、シャーシによるファイバチャネルおよびイーサネットデバイスへのワールドワイドネーム/メディアアクセスコントロール (WWN/MAC) アドレスの割り当てを可能にします。シャーシによって割り当てられた WWN/MAC アドレスはグローバルレベルで一意であり、サーバースロット固有です。

FlexAddress のアクティブ化

FlexAddress はセキュアデジタル (SD) カードに搭載されており、機能をアクティブ化するには SD カードを CMC に挿入する必要があります。FlexAddress 機能をアクティブ化するには、ソフトウェアのアップデートが必要な場合があります。FlexAddress をアクティブ化しない場合は、これらのアップデートは不要です。次の表にリストされているアップデートには、サーバーモジュール BIOS と CMC ファームウェアが含まれます。これらのアップデートは FlexAddress を有効化する前に適用する必要があります。これらのアップデートが適用されていないと FlexAddress が正しく機能しない場合があります。




 **メモ:** FlexAddress は、DELL モノリシックサーバーではアクティブ化できません。

表 25. FlexAddress をアクティブ化するための前提条件


コンポーネント	必要最低限のバージョン
サーバーモジュール BIOS	<ul style="list-style-type: none">• M620• M520 <p> メモ: M520 および M620 の BIOS バージョンは、1.7.6 以降である必要があります。</p>
PowerEdgeM600/M605 LAN on motherboard (LOM)	<ul style="list-style-type: none">• ブートコードファームウェア 4.4.1 以降• iSCSI ブートファームウェア 2.7.11 以降
iDRAC7	バージョン 1.40.40 以降
LC-USC	バージョン 1.1.5 以降
CMC	バージョン 1.0 以降


FlexAddress 機能の正しい導入を確実にするため、BIOS とファームウェアを次の順序でアップデートしてください。

1. サーバーモジュールの BIOS をアップデートします。
2. サーバーモジュールの iDRAC ファームウェアをアップデートします。
3. シャーシ内の CMC ファームウェアをすべてアップデートします。冗長 CMC がある場合は、両方をアップデートするようにしてください。
4. 冗長 CMC モジュールシステムではパッシブモジュールに、冗長なしのシステムでは CMC モジュール 1 つに SD カードを挿入します。

 **メモ:** FlexAddress をサポートする CMC ファームウェア (バージョン 1.10 以降) がインストールされていない場合、FlexAddress の機能はアクティブ化されません。

SD カードの取り付け手順については、『Chassis Management Controller (CMC) セキュアデジタル (SD) カード技術仕様』文書を参照してください。

 **メモ:** SD カードには FlexAddress 機能が搭載されており、SD カードに格納されているデータは暗号化されています。システム機能を妨げ、システムの誤作動を招く可能性があることから、どのような方法でも複製または改変することはできません。

 **メモ:** SD カードの使用は、1 台のシャーシのみに限定されています。シャーシが複数台ある場合は、必要な台数分の SD カードを別途購入してください。

FlexAddress 機能のアクティブ化は、SD 機能カードが取り付けられている CMC の再起動時に自動的に行われます。これにより、この機能が現在のシャーシにバインドされます。SD カードを冗長 CMC システムに取り付けた場合は、冗長 CMC がアクティブになるまで FlexAddress 機能もアクティブ化されません。冗長 CMC のアクティブ化方法については、『Chassis Management Controller (CMC) セキュアデジタル (SD) カード技術仕様』文書を参照してください。

CMC が再起動したら、アクティブ化プロセスを検証してください。FlexAddress のアクティブ化の詳細については、「[FlexAddress アクティブ化の検証](#)」を参照してください。

FlexAddress Plus のアクティブ化

FlexAddress Plus は、FlexAddress 機能と共に FlexAddress Plus SD カードで提供されます。

 **メモ:** FlexAddress のラベルの付いた SD カードには FlexAddress のみが含まれ、FlexAddress Plus のラベルの付いたカードには FlexAddress と FlexAddress Plus が含まれます。機能をアクティブ化するには、カードを CMC に挿入する必要があります。

一部のサーバーでは、それらの設定方法に応じて、FA が CMC に提供できる数より多くの MAC アドレスを必要とする場合があります。これらのサーバーでは、FlexAddress Plus へのアップグレードにより WWN/MAC 設定の完全な最適化が可能になります。FlexAddress Plus 機能のサポートを受けるには、デルにお問い合わせください。

FlexAddress Plus 機能をアクティブ化するには、サーバー BIOS、サーバー iDRAC、および CMC ファームウェアのソフトウェアアップデートが必要です。これらのアップデートが適用されていない場合は、FlexAddress 機能しか使用できません。これらのコンポーネントの最低必要バージョンについては、dell.com/support/manuals にある『Dell Chassis Management Controller (CMC) for Dell PowerEdge VRTX バージョン 1.00 リリースノート』を参照してください。

FlexAddress 有効化の検証

機能カードには、FlexAddress、FlexAddress Plus、および拡張ストレージ、またはそのいずれかが搭載されています。SD 機能カードとその状態を確認するには、次の RACADM コマンドを実行します。

```
racadm featurecard -s
```

表 26. featurecard -s コマンドによって返される状態メッセージ

状態メッセージ	処置
機能カードが挿入されていません。	CMC をチェックして、SD カードが正しく挿入されていることを確認します。冗長 CMC 構成では、SD 機能カードが取り付けられている CMC がスタンバイ CMC ではなく、アクティブな CMC であることを確認してください。
挿入された機能カードは有効で、次の FlexAddress 機能が含まれています：バインドされています。	処置の必要はありません。
挿入されている機能カードが有効で、次の FlexAddress 機能が含まれています：別のシャー	SD カードを取り外し、現在のシャーシ用の SD カードを取り付けます。

状態メッセージ	処置
---------	----

シ (svctag = ABC1234、SD card SN = 1122334455) にバインドされています。

挿入された機能カードは有効で、次の FlexAddress 機能が含まれています：バインドされていません。

機能カードは、別のシャーシに移動したり、現在のシャーシで再有効化することができます。現在のシャーシで再有効化するには、機能カードが取り付けられている CMC モジュールがアクティブになるまで racadm racreset を入力し続けます。

シャーシ上でアクティブ化された全機能を表示するには、次の RACADM コマンドを使用します。

```
racadm feature -s
```

このコマンドを実行すると、次の状態メッセージが返されます。

機能 = FlexAddress アクティブ化日 = 2008 年 4 月 8 日 - 10:39:40 SD カード SN = 01122334455 からインストールされた機能

シャーシ上にアクティブな機能が存在しない場合は、コマンドは次のメッセージを返します。

```
racadm feature -s このシャーシでアクティブな機能はありません
```


Dell 機能カードには複数の機能が含まれている場合があります。シャーシ上で Dell 機能カードに含まれている機能のいずれかがアクティブ化されると、その Dell 機能カードに含まれているその他の機能は異なるシャーシでアクティブ化できなくなります。この場合、racadm feature -s コマンドは対象機能に関して次のメッセージを表示します。

エラー：SD カード上の 1 つ、または複数の機能が別のアクティブです。

feature コマンドおよび featurecard コマンドの詳細については、『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。

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。

シャーシ上の FlexAddress 機能の非アクティブ化に成功しました。

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。

エラー：シャーシの電源がオンのため、機能を非アクティブ化できません

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

FlexAddress 情報の表示

シャーシ全体または個々のサーバーの状態情報を表示することができます。表示される情報には、次が含まれます。

- ファブリック設定。
- FlexAddress のアクティブ/非アクティブ状況。
- スロットの番号および名前。
- シャーシに割り当てられたアドレスとサーバーに割り当てられたアドレス。
- 使用中のアドレス。

シャーシの FlexAddress 情報の表示

全シャーシの FlexAddress 状態情報を表示することができます。状態情報には、機能がアクティブかどうか、および各サーバーの FlexAddress 状態の概要が含まれます。

CMC ウェブインタフェースを使用してシャーシ FlexAddress 状態を表示するには、**シャーシ概要** → **セットアップ** をクリックします。

シャーシの**一般設定** ページが表示されます。

FlexAddress には **アクティブ** または **非アクティブ** の値があります。**アクティブ** という値は、機能がシャーシにインストール済みであることを示し、**非アクティブ** は機能がシャーシにインストールされておらず、使用されていないことを示します。

シャーシ全体の FlexAddress 状態を表示するには、次の RACADM コマンドを実行します。

```
racadm getflexaddr
```

特定のスロットの FlexAddress 状態を表示するには、次のコマンドを使用します。

```
racadm getflexaddr [-i <スロット番号>]
```

ここで <スロット番号> は 1~4 の値です。

getflexaddr コマンドの詳細については、『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。

全サーバーの FlexAddress 情報の表示


すべてのサーバーに対する FlexAddress 状態を表示するには、**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、次の情報が表示されます。

- WWN 設定
- シャーシ内のすべてのスロットの MAC アドレス

ファブリックの設定 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せん。

iDRAC には、サーバー管理 MAC アドレスが表示されます。


 **メモ:** ファブリック A 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。

WWN/MAC アドレス シャーシ内の各スロットの FlexAddress 設定を表示します。表示される情報は次のとおりです。

- スロット番号および位置。

- FlexAddress のアクティブ / 非アクティブ 状況。
- ファブリックタイプ。
- 使用中のサーバー割り当て、およびシャーシ割り当ての WWN/MAC アドレス。

緑色のチェックマークは、アクティブなアドレスタイプ（サーバー割り当てまたはシャーシ割り当てのいずれか）を示します。

 **メモ:** iDRAC 管理コントローラはファブリックではありませんが、その FlexAddress はファブリックとして扱われます。

各種フィールドについての情報は、『オンラインヘルプ』を参照してください。


個別サーバーの FlexAddress 情報の表示


CMC ウェブインタフェースを使用して特定のサーバーの FlexAddress 情報を表示するには、次の手順を実行します。

1. 左ペインで **サーバー概要** を展開します。
シャーシに挿入されているすべてのサーバーがリストされます。
2. 表示するサーバーをクリックします。
サーバー状態 ページが表示されます。
3. **セットアップタブ** をクリックし、**FlexAddress** をクリックします。
選択したサーバーの WWN 設定と MAC アドレスが記載された **FlexAddress** ページが表示されます。詳細については、『オンラインヘルプ』を参照してください。

FlexAddress の設定

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

 **メモ:** 本項では、FlexAddress という用語は FlexAddress Plus も意味します。

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

```
racadm racresetcfg -c flex
```

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

FlexAddress を設定するには、FlexAddress アップグレードを購入してインストールする必要があります。アップグレードを購入およびインストールしていない場合は、次のテキストがウェブインタフェースに表示されます。

オプション機能はインストールされていません。シャーシベースの WWN および MAC アドレス管理機能についての情報は、『Dell Chassis Management Controller ユーザーズガイド』を参照してください。本機能を購入するには、デル (www.dell.com) にお問い合わせください。

シャーシと共に FlexAddress をご購入いただいた場合、システムの電源投入時に FlexAddress がインストール済みでアクティブです。FlexAddress を別途購入された場合は、dell.com/support/manuals にある『Chassis Management Controller (CMC) セキュアデジタル (SD) カード技術仕様』マニュアルの手順に従って SD 機能カードを取り付ける必要があります。

設定を始める前に、サーバーの電源を切る必要があります。FlexAddress はファブリック単位で有効化または無効化できます。さらに、この機能はスロット単位でも有効化または無効化が可能です。ファブリック単位

で機能を有効化した後、有効化するスロットを選択できます。例えば、ファブリック A が有効化されていると、有効化されたスロットではいずれもファブリック A でのみ FlexAddress が有効になります。その他すべてのファブリックは、サーバーで工場出荷時割り当ての WWN/MAC を使用します。

FlexAddress を利用した Wake-On-LAN の使用

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



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

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

CMC ウェブインタフェースを使用したシャーシレベルファブリックおよびスロット用 FlexAddress の設定

スロットにサーバーがある場合は、そのスロットで FlexAddress 機能を有効化する前にサーバーの電源を切ってください。

CMC ウェブインタフェースを使用して、ファブリックおよびスロットによる FlexAddress 機能の使用を有効化または無効化するには、次の手順を実行します。

1. 左ペインで、**サーバー概要** → **セットアップ** → **FlexAddress** をクリックします。
2. **FlexAddress** の導入 ページの **シャーシ割り当て WWN/MAC のファブリックの選択** 画面で、FlexAddress を有効にするファブリックタイプ (ファブリック A または iDRAC) を選択します。無効にするには、オプションをクリアします。
 **メモ:** ファブリックが選択されていないと、次のメッセージが表示されます。
選択されたスロットに FlexAddress が有効化されていません。
3. **シャーシ割り当て WWN/MAC のスロットの選択** ページで、FlexAddress を有効にするスロットに対して **有効** オプションを選択します。無効にするには、オプションをクリアします。
 **メモ:** スロットが選択されていないと、選択されたファブリックに対して FlexAddress は有効になりません。
4. 設定を保存するには、**適用** をクリックします。

RACADM を使用したシャーシレベルファブリックおよびスロット用 FlexAddress の設定

ファブリックを有効化または無効化するには、次の RACADM コマンドを使用します。

```
racadm setflexaddr [-f <fabricName> <state>]
```

ここで、<fabricName> = A or iDRAC および <state> = 0 or 1 です。

0 は無効、1 は有効を示します。


スロットを有効化または無効化するには、次の RACADM コマンドを使用します。


```
racadm setflexaddr [-i <slot#> <state>]
```

ここで、<slot#> = 1 or 4 および <state> = 0 or 1 です。

0は無効、1は有効を示します。

setflexaddr コマンドの詳細については、『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。

 **メモ:** Dell PowerEdge VRTX と共に FlexAddress または FlexAddressPlus 機能をご購入いただいた場合、これらの機能は事前にインストール済みで、全スロットおよびファブリックで有効化されています。この機能のご購入には、dell.com でデルにお問い合わせください。

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

```
racadm racresetcfg -c flex
```


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

ワールドワイド名 / メディアアクセスコントロール (WWN/MAC) ID の表示

WWN/MAC 概要 ページでは、シャーシ内のスロットの WWN 設定および MAC アドレスを表示することができます。

ファブリック設定

ファブリック設定 セクションには、ファブリック A のために取り付けられた入力 / 出力ファブリックのタイプが表示されます。緑色のチェックマークはファブリックが FlexAddress 用に有効化されていることを示します。FlexAddress 機能は、シャーシ内の各種ファブリックおよびスロットに対してシャーシ割り当て、およびスロット固定の WWN/MAC アドレスを展開するために使用されます。この機能は、ファブリックごと、およびスロットごとに有効化されます。

 **メモ:** FlexAddress 機能の詳細については、「[FlexAddress について](#)」を参照してください。

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 27. FlexAddress コマンドと出力

状況	コマンド	出力
アクティブ CMC モジュールの SD カードが他のサービスタグにバインドされている。	<code>\$racadm featurecard -s</code>	挿入された機能カードは有効で、次の機能が含まれます FlexAddress: 別のシャーシにバインドされています、svctag = <サービスタグ番号> SD カード SN = <有効な FlexAddress シリアル番号>
同じサービスタグにバインドされているアクティブ CMC モジュールの SD カード。	<code>\$racadm featurecard -s</code>	挿入された機能カードは有効で、次の機能が含まれます FlexAddress: バインドされています
どのサービスタグにもバインドされていないアクティブ CMC モジュールの SD カード。	<code>\$racadm featurecard -s</code>	挿入された機能カードは有効で、次の機能が含まれます FlexAddress: バインドされていません

状況	コマンド	出力
何らかの理由（SD カードが挿入されていない、破損した SD カード、機能の非アクティブ化後、SD カードが異なるシャーシにバインドされている）で FlexAddress 機能がシャーシ上でアクティブではない。	<pre>\$racadm setflexaddr [-f < ファブリック名> <スロット状況 >] \$racadm setflexaddr [-i < スロット番号> <スロット状況>]</pre>	エラー: FlexAddress 機能はシャーシ上で有効になっていません
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。	<pre>\$racadm setflexaddr [-f < ファブリック名> <スロット状況 >] \$racadm setflexaddr [-i < スロット番号> <スロット状況>]</pre>	エラー: 操作を実行するための特権が不足しています
シャーシの電源がオンの状態での FlexAddress 機能の無効化。	<pre>racadm feature -d -c flexaddress</pre>	エラー: シャーシの電源がオンのため、機能を非アクティブ化できません
ゲストユーザーによるシャーシ上の機能の無効化試行。	<pre>racadm feature -d -c flexaddress</pre>	エラー: 操作を実行するための特権が不足しています
サーバーモジュールの電源がオンの状態での、スロット / ファブリックの FlexAddress 設定の変更。	<pre>\$racadm setflexaddr -i 1 1</pre>	エラー: 電源がオンになっているサーバーに影響を与えるため、設定した操作を実行することはできません
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。	<pre>\$racadm setflexaddr -i<ス ロット番号> <状況> \$racadm setflexaddr -f<フ ァブリック名> <状況></pre>	エラー: SWC0242 : 必要なライセンスが欠落しているか期限切れです。適切なライセンスを取得して再試行してください。または追加詳細についてサービスプロバイダにお問い合わせください。

 **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み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。お客様は、FlexAddress および FlexAddress 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、責任を負いません。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

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對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。

ファブリックの管理

シャーシはファブリック A というファブリックタイプをサポートしています。ファブリック A は単一の I/O モジュールによって使用され、常にサーバーのオンボードイーサネットアダプタに接続されます。

シャーシに存在する I/O モジュール (IOM) は 1 個だけで、パススルーまたはスイッチモジュールになります。この I/O モジュールはグループ A に分類されます。

シャーシ IOM は **ファブリック** と呼ばれる分散データバスが使用されます。このファブリックには A という名前が付けられており、イーサネットのみをサポートします。各サーバー IO アダプタ (メザニンカードまたは LOM) には、機能に応じて 2 個または 4 個のポートを搭載できます。メザニンカードスロットには、PCIe カード (IO モジュールではなく) に接続される PCIe 拡張カードが装着されます。イーサネット、iSCSI、またはファイバチャネルネットワークを導入するときは、最大の可用性のために、バンク 1 および 2 の間にそれらの冗長リンクをスパンします。分散 IOM はファブリック識別子で識別されます。

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

無効な構成

無効な構成には、次の 3 タイプがあります。

- 無効な MC または LOM 構成では、サーバーの新しく取り付けられたファブリックタイプが既存の IOM ファブリックと異なる、つまり、単一のサーバーの LOM または MC がそれに対応する IOM によってサポートされていません。この場合、シャーシ内の他のサーバーはすべて稼働していますが、不一致 MC カードがあるサーバーの電源はオンにできません。サーバーの電源ボタンが橙色に点滅してファブリックの不一致を警告します。
- 無効な IOM-MC 構成では、I/O モジュールの新しく取り付けられたファブリックタイプと常駐する MC のファブリックタイプが一致しない、またはそれらに互換性がありません。一致しない IOM は電源が切れた状況に維持されます。CMC は無効な構成が記され、IOM 名が指定されているエントリを CMC およびハードウェアログに追加します。CMC は不一致のファブリックタイプを持つ IOM のエラー LED を点滅させます。アラートを送信するように CMC が設定されている場合は、CMC はこのイベントの E-メールおよび/または SNMP アラートを送信します。
- 無効な IOM-IOM 構成では、新しく取り付けられた IOM に、グループ内にすでに取り付けられている IOM と異なる、または互換性のないファブリックタイプが存在します。CMC は新しく取り付けられた IOM を電源が切れた状況に維持し、IOM のエラー LED を点滅させ、CMC およびハードウェアログ不一致についてのエントリをログします。

初回電源投入シナリオ

シャーシが電源に接続され、オンにされたとき、I/O モジュールはサーバーよりも優先されます。IOM は他よりも先に電源がオンになります。このとき、ファブリックタイプの検証は実行されません。

IOM の電源がオンになった後、サーバーの電源がオンにされ、次に CMC によってサーバーのファブリックの整合性が検証されます。

パススルーモジュールとスイッチは、ファブリックが同じである場合、同じグループに属することが可能です。スイッチとパススルーモジュールは、異なるベンダーによって製造されたものである場合でも、同じグループに存在できます。

IOM 正常性の監視


IOM 正常性の監視については、「[IOM の情報および正常性状態の表示](#)」を参照してください。


IOM 用ネットワークの設定

IOM を管理するために使用されるインタフェースのネットワーク設定を指定することができます。イーサネットスイッチには帯域外管理ポート (IP アドレス) が設定されます。帯域内管理ポート (つまり VLAN1) の設定にはこのインタフェースは使用されません。

IOM のネットワーク設定を行う前に、IOM の電源がオンになっている事を確認してください。

グループ A 内の IOM のネットワーク設定を設定するには、ファブリック A システム管理者の権限が必要です。

 **メモ:** イーサネットスイッチの場合、帯域内 (VLAN1) と帯域外の管理 IP アドレスは同じにすることも、同じネットワーク上にすることもできません。同じにすると、帯域外 IP アドレスが設定されなくなります。デフォルトの帯域内管理 IP アドレスについては、IOM のマニュアルを参照してください。

 **メモ:** イーサネットパススルースイッチまたは Infiniband スイッチ用に I/O モジュールのネットワーク設定を行わないでください。

CMC ウェブインタフェースを使用した IOM 用ネットワークの設定

I/O モジュールのネットワーク設定を行うには、次の手順を実行します。

1. 左ペインで **シャーシ概要** をクリックし、**I/O モジュール概要** をクリックして **セットアップ** をクリックします。あるいは、唯一使用可能な I/O モジュールである **A** のネットワーク設定を設定するには **A ギガビットイーサネット** をクリックし、**セットアップ** をクリックします。


I/O モジュールネットワーク設定の実行 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 コミュニティ文字列、および Syslog サーバー IP アドレスを入力します。各フィールドの詳細情報については、『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) を入力するか、IOM GUI へのダイレクトインタフェースを使用して、起動設定ファイルにこのアドレスを保存する必要があります。

3. **適用** をクリックします。

ネットワーク設定が IOM 用に設定されます。

 **メモ:** 許可されている場合は、VLAN、ネットワークプロパティ、および IO ポートをデフォルトの設定値にリセットできます。

RACADM を使用した IOM 用ネットワークの設定

RACADM を使用して、IOM にネットワークを設定するには、日付と時刻を設定します。『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』の deploy コマンドの項を参照してください。

RACADM deploy コマンドを使用して、IOM のユーザー名、パスワード、および SNMP 文字列を設定することができます。

```
racadm deploy -m switch -u <ユーザー名> -p <パスワード>
```

```
racadm deploy -m switch -u -p <パスワード> -v SNMPv2 <snmp コミュニティ文字列> ro
```

```
racadm deploy -a [サーバー|スイッチ] -u <ユーザー名> -p <パスワード>
```


電力の管理と監視

Dell PowerEdge VRTX シャーシは、電力効率が最も優れたモジュラーサーバーエンクロージャです。高効率の電源装置とファンを装備するように設計されており、システム内の通気がより良く行われるように最適化されたレイアウトと、電力最適化されたコンポーネントをエンクロージャ全体に備えています。最適化されたハードウェア設計と、Chassis Management Controller (CMC)、電源装置、および iDRAC 内蔵の高性能電源管理機能が一体となり、電力効率のよいサーバー環境のさらなる強化が可能になります。

PowerEdge VRTX の電源管理機能は、システム管理者が電力消費を削減し、環境固有の必要に合わせて電力を調整するためにエンクロージャの設定を行う際に役立ちます。

PowerEdge VRTX モジュラーエンクロージャは AC 電力を利用し、その負荷をアクティブな内部電源装置ユニット (PSU) すべてに振り分けます。このシステムは、サーバーモジュールおよび関連エンクロージャインフラストラクチャに割り当てられた最大 5000 ワットの AC 電力を供給することが可能です。ただし、この容量は、選択する電源の冗長性ポリシーによって異なります。


PowerEdge VRTX エンクロージャは、PSU の動作に影響を与え、システム管理者に対するシャーシ冗長性状況の報告方法を決定する 2 つの冗長性ポリシーのいずれかに設定することができます。

電源管理は OpenManage Power Center (OMPC) を介して制御することもできます。OMPC が外部から電源を制御するとき、CMC は引き続き次を維持します。

- 冗長性ポリシー
- リモート電力ログ
- 動的電源供給 (DPSE)

OMPC は次を管理します。

- サーバー電源
- サーバーの優先順位
- システム入力電力容量
- 最大節電モード

 **メモ:** 実際の電源供給は、設定と作業負荷に基づきます。

CMC における次の電源制御の管理と設定には、CMC ウェブインタフェースまたは RACADM を使用できます。

- シャーシ、サーバーおよび PSU への電力割り当て、消費量および状態の表示。
- シャーシの電力バジェットおよび冗長性の設定。
- シャーシの電源制御操作 (電源投入、電源切断、システムリセット、パワーサイクル) の実行。

冗長性ポリシー


冗長性ポリシーとは、CMC がシャーシへの電力をどのように管理するかを決定する、設定可能なプロパティの一式です。次の冗長性ポリシーは動的な PSU 電源供給の有無に関わらず、設定可能です。


- AC 冗長性
- 電源装置冗長性

AC 冗長性ポリシー

AC 冗長性ポリシーの目的は、モジュラーエンクロージャシステムを AC 電源障害に耐えるモードで動作できるようにすることです。これらの障害は、AC 電源グリッド、ケーブル配線と電源供給、または PSU 自体に由来することが考えられます。

AC 冗長性のためにシステムを構成する場合、スロット 1 および 2 にある PSU は第 1 グリッド、スロット 3 および 4 にある PSU は第 2 グリッドに振り分けられます。CMC は、グリッドのいずれかが故障した場合、システムが劣化することなく動作を継続するよう電力を管理します。AC 冗長性は個々の PSU の故障にも耐えます。

 **メモ:** AC 冗長性の役割のひとつは、電源グリッド全体に障害が発生してもサーバー動作がシームレスに行えるようにすることですが、AC 冗長性を維持するために使用できる電力は、2つのグリッドの容量がほぼ同等の場合に最大となります。

 **メモ:** AC 冗長性は、負荷要件が最も弱い電源グリッドの容量を超えない場合のみ満たされます。

AC 冗長性レベル

AC 冗長として使用するには、各グリッドにつき 1 台の PSU が必要最低限の構成です。追加の構成は、各グリッドに少なくとも 1 台の PSU があるすべての組み合わせで行うことができます。ただし、最大電力を使用できるようにするには、各レグの PSU の電力合計ができるだけ同じに近くなるようにしてください。AC 冗長性を維持する間の電力上限は、2つのグリッドのうち弱い方で使用可能な電力となります。

冗長性喪失イベントを警告するように設定されている場合には、CMC が AC 冗長性を維持できなくなると、E-メールまたは SNMP（またはその両方）アラートが管理者に送信されます。


この構成で 1 台の PSU が機能しなくなると、その障害の発生したグリッド内にある残りの PSU がオンラインとしてマーク付けされます。この状態では、残りのどの PSU もシステムの動作を中断させることなく機能を停止することができます。1 台の PSU が機能を停止すると、シャーシ正常性が非重要としてマーク付けされます。小さい方のグリッドがシャーシ電力割り当ての合計量をサポートできない場合は、AC 冗長性はなしと報告され、シャーシの正常性は **重要** と表示されます。

電源装置の冗長性ポリシー

電源装置の冗長性ポリシーは、冗長電源グリッドが使用できない場合に便利ですが、モジュラーエンクロージャ内のサーバーをダウンさせる単一 PSU 障害からの保護も推奨されます。この目的のため、最大容量 PSU がオンライン予約に維持されます。これにより、電源装置冗長プールが形成されます。下図は、電源装置の冗長性モードを図解しています。

電力と冗長性のために必要な分を超えた PSU を利用することも可能で、これらは障害時に備えて冗長性プールに追加されます。

AC 冗長性とは異なり、電源冗長性が選択されると、CMC では PSU ユニットを特定の PSU スロットの位置に設置する必要がありません。

 **メモ:** 動的電源供給（DPSE）では、PSU をスタンバイにすることが可能になります。スタンバイ状況は、電力を供給していない PSU の物理的な状況を示します。DPSE を有効化すると、効率性を向上させ、電力を節約するために、追加の PSU がスタンバイモードに設定される場合があります。

動的電源供給


デフォルトでは、動的電源供給（DPSE）モードは無効になっています。DPSE は、シャーシに電力を供給する PSU の電力効率を最適化することにより、電力を節約します。これにより、PSU の寿命も延び、発熱も低減されます。この機能を使用するには、Enterprise ライセンスが必要です。

CMC はエンクロージャの電力割り当て全体を監視し、PSU をスタンバイ状況にして、シャーシの全電力割り当てを少数の PSU で供給するようにします。オンライン PSU は高利用率での動作時に効率が良くなることから、オンライン PSU の効率が向上し、スタンバイ PSU の寿命が延びます。

残りの PSU を最大効率で動作させるには、次の電源冗長性モードを使用します。

- DPSE を使用した **PSU 冗長性** モードは電力効率性を提供します。少なくとも 2 台の PSU がオンラインであり、そのうち 1 台の PSU が構成への電力供給に必要とされ、もう 1 台は PSU 故障時における冗長性を提供します。PSU 冗長性モードは、1 台の PSU 障害に対する保護を提供しますが、AC グリッド喪失発生時での保護は提供しません。
- DPSE を使用した **AC 冗長性** モードでは、少なくとも 2 台の PSU がアクティブであり、各電源グリッドごとに 1 台が存在します。AC 冗長性は、部分的に载荷されたモジュラエンクロージャ構成に対してバランスのとれた効率性と最大可用性も提供します。
- DPSE の無効化は、6 台の PSU すべてがアクティブで負荷を共有し、各電源装置の活用率が下がることになるため、電力効率が最も低くなります。

DPSE は、ここで説明された 2 つ両方の電源装置冗長設定（**電源装置冗長性** および **AC 冗長性**）用に有効化することが可能です。


 **メモ:** 2 台の PSU 構成モードでは、サーバーの負荷によっては、いずれの PSU もスタンバイモードに移行できない場合があります。

- **電源装置冗長性** 設定では、エンクロージャは、エンクロージャへの電源供給に必要な PSU に加え、常にもう 1 台の PSU の電源をオンにして **オンライン** とマークしておきます。電力使用率が監視され、システム全体の負荷に応じて 1 台の PSU をスタンバイ状況に移行することが可能です。4 台の PSU 構成では、少なくとも 2 台の PSU の電源が常にオンになります。

電源装置冗長性 設定のエンクロージャでは追加の PSU が常に起動状態であるため、オンライン PSU 1 台の損失に対応可能であり、取り付けられているサーバーモジュールに対して十分な電力供給を維持できます。オンライン PSU が失われると、スタンバイ PSU がオンラインになります。複数の PSU に障害が同時に発生すると、スタンバイ PSU がオンになるまでの間、一部のサーバーモジュールに対して電力が失われる可能性があります。

- **AC 冗長性** 設定では、シャーシの電源がオンになると、すべての電源装置が起動されます。電力使用率が監視され、システム構成と電力使用率に応じて許容される場合は、PSU が **スタンバイ** 状況になります。グリッド内の PSU の **オンライン** 状態は他のグリッドの状態をミラーするため、エンクロージャは、エンクロージャへの電力を中断することなく、グリッド全体への電力喪失に耐えることができます。

AC 冗長性 設定における電力需要の上昇により、**スタンバイ** 状況の PSU が起動されます。これにより、デュアルグリッド冗長性に必要なミラー設定が維持されます。

 **メモ:** DPSE が有効になっている状況では、電力需要が 2 つの電源冗長性ポリシーモードの両方で上昇した場合、電力を回収するためにスタンバイ PSU が **オンライン** になります。

デフォルトの冗長性設定

次の表に示されているように、シャーシのデフォルトの冗長性設定は、シャーシに取り付けられている PSU の台数によって異なります。

表 28. デフォルトの冗長性設定

PSU 構成	デフォルトの冗長性ポリシー	デフォルトの動的 PSU 電源供給設定
2 台の PSU	DC 冗長性	無効
4 台の PSU	DC 冗長性	無効

AC 冗長性

4 台の PSU による AC 冗長性モードでは、4 台すべての PSU がアクティブです。2 台の PSU は 1 つの AC 電源グリッドに接続し、残り 2 台の PSU をもう 1 つの AC 電源グリッドに接続する必要があります。

△ **注意:** システムエラーを回避し、AC 冗長性を効率的に機能させるには、バランスのとれた台数の PSU セットを個別の AC グリッドに適切にケーブル配線する必要があります。

一方の AC グリッドが故障した場合、機能している AC グリッド上にある PSU がサーバーやインフラストラクチャに中断を生じることなく電力供給を引き継ぎます。

△ **注意:** AC 冗長性モードでは、バランスのとれた台数の PSU セットが必要です（各グリッドに少なくとも 1 台の PSU が必要）。この条件を満たさなければ、AC 冗長性は実現できません。

電源装置冗長性

電源装置の冗長性が有効化されると、シャーシ内の 1 台の PSU がスペアとして維持され、PSU のうちいずれかが故障してもサーバーまたはシャーシの電源がオフにならないことを確実にします。電源装置の冗長性モードには、少なくとも 2 台の PSU が必要です。追加の PSU が存在する場合、これらは DPSE が有効になるときに電力効率向上のために活用されます。冗長性喪失後の障害は、シャーシ内のサーバーの電源がオフになる原因となる場合があります。

ハードウェアモジュールの電力バジェット

CMC は、シャーシの電力バジェット、冗長、動的電源機能を設定する電力バジェットサービスを提供します。

電源管理サービスは、電力消費量の最適化、および需要に応じた異なるモジュールへの電力の再割り当てを可能にします。

CMC は、取り付けられているすべてのサーバーとコンポーネントに必要なワット数を蓄える、エンクロージャ用の電力バジェットを維持します。

CMC はシャーシ内の CMC インフラストラクチャおよびサーバーに電力を割り当てます。CMC インフラストラクチャは、ファン、I/O モジュール、ストレージアダプタ、PCIe カード、物理ディスク、メイン基板などのシャーシ内のコンポーネントで構成されます。シャーシには、iDRAC を介してシャーシと通信するサーバーを最大 4 台装備できます。詳細については、dell.com/support/manuals にある『iDRAC7 ユーザーズガイド』を参照してください。

iDRAC は、サーバーへの電源投入前に CMC にパワーエンベロープ要件を提示します。パワーエンベロープには、サーバーの動作を維持するために必要な最大および最低電力要件が含まれています。iDRAC の初期推定値は、サーバー内のコンポーネントについての当初の理解に基づいています。動作が開始され、コンポーネントがさらに検出されると、iDRAC は初期電力要件を増加または削減する場合があります。


エンクロージャ内でサーバーの電源がオンになると、iDRAC ソフトウェアは電力要件を推定し直して、パワーエンベロープの次回変更を要求します。

CMC は要求された電力をサーバーに供給し、割り当てられたワット数は利用可能バジェットから差し引かれます。サーバーの電力要求が認められた後、サーバーの iDRAC ソフトウェアが実際の電力消費を継続的に監視します。実際の電力要件に基づいて、iDRAC パワーエンベロープは時間の経過と共に変化する場合があります。サーバーが割り当てられた電力を完全に使用していると、iDRAC が電力増加を要求します。

高負荷下では、電力消費がユーザー設定のシステム入力電力上限未満に留まることを確実にするため、サーバー上のプロセッサのパフォーマンスが劣化する場合があります。

PowerEdge VRTX エンクロージャは、ほとんどのサーバー構成のピークパフォーマンスに十分な電力を供給できますが、使用できる多くのサーバー構成では、エンクロージャが供給できる最大電力を消費しません。データセンターでのエンクロージャ用電力の割り当てに役立てるため、PowerEdge VRTX では、シャーシ全体の AC 電力利用が特定のしきい値内に留まることを確実にするシステム入力電力上限を指定することができます。CMC はまず、ファン、I/O モジュール、ストレージアダプタ、物理ディスクドライブ、メイン基板、および CMC そのものを動作させるために十分な電力を確保します。この電力割り当てはシャーシインフラストラクチャに割り当てられた入力電力と呼ばれます。シャーシインフラストラクチャの後、エンクロージャ内のサーバーの電源がオンになります。システム入力電力上限は、「電力負荷」より低く設定することはできません。

せん。電力負荷とは、インフラストラクチャに割り当てられた電力と電源の入ったサーバーに割り当てられた最小電力の合計です。

 **メモ:** 電力上限機能を使用するには、Enterprise ライセンスが必要です。

総電力バジェットをシステム入力電力上限以下に保つために必要な場合、CMC はサーバーに対して要求された最大電力よりも少ない値を割り当てます。サーバーにはサーバー優先順位設定に基づいて電力が割り当てられるので、優先順位の高いサーバーには最大電力が提供され、優先度 2 のサーバーは、優先度 1 のサーバーの後に電力が割り当てられることになります。優先順位の低いサーバーは、システム入力最大電力容量とユーザー設定のシステム入力電力上限設定に基づいて優先度 1 のサーバーより少ない電力が提供される場合があります。

シャーシ内における追加サーバー、共有 HDD、PCIe カードなどの構成の変化には、システム入力電力上限の引き上げが必要な場合があります。温度状態が変化し、ファンをより高速で稼働させる必要がある時にも、追加電力を消費する原因となることから、モジュラーエンクロージャでの電力需要が増加します。I/O モジュール、ストレージアダプタ、PCIe カード、物理ディスク、メイン基板の装着や、PSU の台数、タイプ、構成によっても、モジュラーエンクロージャの電力需要が増加します。管理コントローラを起動させておくためにサーバーの電源が切られる時でさえも、サーバーによってごく少量の電力が消費されます。

追加サーバーは、十分な電力が使用可能である場合にのみ、モジュラーエンクロージャ内での電源投入が可能です。システム入力電力上限は、追加サーバーへの電源投入を行うため、最大値の 5000 ワットまで常時増加させることができます。

電力割り当てを削減するモジュラーエンクロージャの変化には、次が含まれます。

- サーバーの電源オフ
- I/O モジュールの電源オフ
- ストレージアダプタ、PCIe カード、物理ディスクドライブ、およびメイン基板の電源オフ
- シャーシの電源オフ状態への移行


システム入力電力上限は、シャーシの電源がオンであるかオフであるかに関わらず、再設定することができます。

サーバースロットの電力優先順位の設定

CMC では、エンクロージャ内の 4 個のサーバースロットのそれぞれに電力優先順位を設定することができます。優先順位設定は、1 (最高) から 9 (最低) になります。これらの設定はシャーシ内のスロットに割り当てられ、スロットの優先順位はそのスロットに挿入されるサーバーによって引き継がれます。CMC はスロットの優先順位を使用して、エンクロージャ内で優先順位が最も高いサーバーに優先的に電力をバジェットします。


デフォルトのサーバースロット優先順位設定では、電力はすべてのスロットに均等に分配されます。スロットの優先順位を変更することによって、システム管理者は電力割り当ての優先権が与えられたサーバーを優先することができます。より重要なサーバーモジュールをデフォルトのスロット優先順位 1 のままにすると、重要度の低いサーバーモジュールは低い優先値 2 以降に変更され、優先順位 1 サーバーが最初に電源投入されます。これらの優先順位の高いサーバーには最大の電力割り当てが提供されますが、優先順位の低いサーバーには、システム入力電力上限とサーバー電力要件がどれだけ低いかによって最大パフォーマンスで稼働するために十分な電力が割り当てられなかったり、電源投入されない場合もあります。


システム管理者が優先順位の高いサーバーモジュールより先に優先順位の低いサーバーモジュールを手動で起動すると、その優先順位の低いサーバーモジュールが、優先順位の高いサーバーに対応するために最小値まで電力割り当てが削減される最初のモジュールになります。従って、使用できる割り当て電力の全てが消費されると、CMC が、優先順位が低い、または同じサーバーから、それらの最低電力レベルに達するまで電力を回収します。

-  **メモ:** I/O モジュール、ファン、メイン基板、物理ディスクドライブ、ストレージアダプタには、最高の優先順位が与えられます。CMC が優先順位の高いデバイスまたはサーバーの電力需要を満たすために電力を回収するのは、優先順位の低いデバイスからのみです。

サーバーへの優先度レベルの割り当て

追加の電力が必要なとき、サーバー優先度レベルによって CMC がどのサーバーからの電力を利用するかが決定されます。

-  **メモ:** サーバーに割り当てる優先順位は、サーバーそのものではなくサーバーのスロットにリンクされます。サーバーを新しいスロットに移動させる場合は、新しいスロットの場所に優先順位を再設定する必要があります。

-  **メモ:** 電力管理処置を行うには、**シャーシ設定システム管理者** 権限が必要です。

CMC ウェブインタフェースを使用したサーバーへの優先度レベルの割り当て

優先度レベルを割り当てるには、次の手順を実行します。

- 左ペインで、**サーバー概要** → **電源** → **優先度** をクリックします。
サーバー**優先順位** ページに、シャーシ内のすべてのサーバーがリストされます。
- 優先度** ドロップダウンメニューから、1台、複数台、またはすべてのサーバーのために優先度レベル (1~9、ここでは1が最優先) を選択します。デフォルトの値は1です。同じ優先度レベルを複数のサーバーに割り当てることができます。
- 適用** をクリックして変更を保存します。

RACADM を使用したサーバーへの優先度レベルの割り当て

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

```
racadm config -g cfgServerInfo -o cfgServerPriority -i <スロット番号> <優先度レベル>
```

ここで、<スロット番号> (1~4) はサーバーの位置を表し、<優先度レベル> は1~9の数値になります。

たとえば、スロット4のサーバーに優先度レベル1を設定するには、次のコマンドを入力します。


```
racadm config -g cfgServerInfo -o cfgServerPriority -i 4 1
```

電力消費量状態の表示

CMC は、システム全体の実際の入力電力消費量を提供します。

CMC ウェブインタフェースを使用した電力消費状態の表示

左ペインで、**シャーシ概要** → **電源** → **電源監視** をクリックします。電源監視 ページに電源正常性、システム電源状態、リアルタイム電力統計、およびリアルタイムエネルギー統計が表示されます。詳細については『オンラインヘルプ』を参照してください。

-  **メモ:** 電源装置下でも電源情報性状態を確認することができます。

RACADM を使用した電力消費状態の表示

RACADM を使用して電力消費状態を表示するには、次の手順を実行します。

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

```
racadm getpminfo
```

CMC ウェブインタフェースを使用した電力バジェット状態の表示

CMC ウェブインタフェースを使用して電力バジェット状態を表示するには、左ペインで **シャーシ概要** に進み、**電力** → **バジェット状態** とクリックします。**電力バジェット状態** ページには、システムの電源ポリシー設定、電力バジェット詳細、サーバーモジュールに割り当てられたバジェット、およびシャーシ電源装置詳細が表示されます。詳細については『オンラインヘルプ』を参照してください。

RACADM を使用した電力バジェット状態の表示


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

```
racadm getpbinfo
```

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

冗長性状態と全体的な電源正常性

冗長性状態は全体的な電源正常性を決定する要素です。たとえば、電源冗長性ポリシーが **AC 冗長性** などに設定され、冗長性状態がシステムが稼動しているとなっている場合は、全体的な電源状態は通常 **OK** になります。ただし、**AC 冗長性** がある状態で稼動するための条件を満たすことができない場合は、冗長性状態は **いいえ** になり、全体的な電源正常性は **重要** になります。これは、設定されている冗長性ポリシーに従ってシステムを動作できないためです。

 **メモ:** CMC では、冗長性ポリシーを **AC 冗長性** に変更したり、または **AC 冗長性** から他の設定に変更したりする場合に、こうした条件を事前に確認しません。そのため、冗長性ポリシーを設定すると、即時に冗長性喪失または冗長性回復をもたらす可能性があります。

PSU 障害発生後の電力管理

電力不足イベント (PSU 障害など) が発生すると、CMC はサーバーへの電力供給を削減します。電力の削減後、CMC はシャーシの電力需要を再評価します。電力要件が引き続き満たされない場合、CMC は優先順位の低いサーバーの電源をオフにします。ただし、この処理はお使いの CMC で設定した電源冗長性ポリシーに基づいて実行されます。冗長サーバーは、サーバーのパフォーマンスに影響を与えることなく、電力の喪失に対応することができます。

電力必要量が電力バジェット内にとどまると同時に、優先順位の高いサーバーへの電力供給が徐々に回復されていきます。冗長性ポリシーを設定するには、「[電力バジェットと冗長性の設定](#)」を参照してください。

PSU を取り外した後の電力の管理

CMC は、PSU または PSU AC ケーブルを取り外すと、電力の節約を開始する場合があります。CMC は、電力割り当てがシャーシ内の残りの PSU によってサポートされるまで、優先順位の低いサーバーへの電力を削減します。複数の PSU を取り外す場合、CMC は 2 番目の PSU が取り外された時に電力要件を再評価して、ファームウェアの対応を見極めます。電力要件が引き続き満たされない場合は、CMC は優先順位の低いサーバーの電源をオフにする場合があります。

制限

- CMC は、優先順位の高いサーバーの電源をオンにするための優先順位の低いサーバーの **自動電源オフ** をサポートしませんが、ユーザーが電源をオフにすることはできます。

- PSU 冗長性ポリシーの変更は、シャーシ内の PSU の数によって制限されます。PSU 冗長性設定は、「[デフォルトの冗長性設定](#)」にリストされている 2 つの設定のどちらでも選択することができます。

新規サーバーの電源供給ポリシー

電源をオンにした新規サーバーがシャーシに利用できる電力を超えると、CMC は優先順位の低いサーバーに対する電力を減らす可能性があります。これは、システム管理者が、サーバーにフル電力を割り当てるために必要な電力を下回る電力制限をシャーシに設定している場合や、シャーシ内のすべてのサーバーが高い電力を必要とする状況で電力が不足する場合に発生します。優先順位の低いサーバーに割り当てられた電力を削減しても十分な電力を解放できない場合は、新規サーバーの電源をオンにすることができません。

これは、システム管理者が、サーバーに対するフル電源割り当てよりも低い電力制限をシャーシに設定しているか、高電力を必要とするサーバーに利用可能な電力が不十分である場合に発生します。

次の表は、前述したシナリオで新しいサーバーの電源をオンにしたときに CMC が行う処置を説明しています。

表 29. サーバーへの電源投入試行時の CMC の対応

ワーストケース電力が使用可能	CMC の対応	サーバーへの電源投入
はい	節電は不要	許可
いいえ	節電を実施：	許可 拒否
	<ul style="list-style-type: none"> • 新しいサーバーに必要な電力が使用可能 • 新しいサーバーに必要な電力が使用不可 	

PSU の機能が停止すると、非重要な正常性状況が生じ、PSU 障害イベントが生成されます。PSU を取り外すと、PSU 取り外しイベントが生成されます。

どちらか一方のイベントによって冗長性が損失された場合は、電力割り当てに基づいて、冗長性の喪失イベントが生成されます。

その後の電力容量またはユーザーの電力容量がサーバーの割り当てよりも大きい場合、サーバーのパフォーマンスが劣化する、または極端な場合には、サーバーの電源がオフになる可能性があります。これらの状態はどちらも優先順位の逆順に行われます。つまり、優先順位の低いサーバーから電源がオフになります。

次の表では、さまざまな PSU 冗長構成における PSU の電源オフまたは PSU の取り外しに対するファームウェアの対応を示します。

表 30. PSU 障害または取り外しによるシャーシへの影響

PSU 構成	動的 PSU 電源供給	ファームウェアの対応
AC 冗長性	無効	CMC はユーザーに AC 冗長性の喪失を警告します。
電源装置冗長性	無効	CMC はユーザーに電源装置冗長性の喪失を警告します。
AC 冗長性	有効	CMC はユーザーに AC 冗長性の喪失について警告します。PSU 障害または取り外しによって失われた電力バジェットを補うため、スタンバイモードの PSU（存在する場合）の電源がオンになります。
電源装置冗長性	有効	CMC はユーザーに電源装置冗長性の喪失を警告します。PSU 障害または取り外しによって失われた電力バジェットを補うため、スタンバイモードの PSU（存在する場合）の電源がオンになります。

システムイベントログにおける電源装置および冗長性ポリシーの変更

電源装置状況および電源冗長性ポリシーの変更はイベントとして記録されます。システムイベントログ (SEL) にエントリを記録する電源装置関連のイベントは、電源装置の挿入と取り外し、電源装置入力ケーブルの挿入と取り外し、および電源装置の出力アサートとアサート停止です。

次の表には、電源装置の変更に関連する SEL エントリがリストされています。

表 31. 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失われました。
AC 入力喪失	電源装置への電源入力が復元されました。
DC 出力生成	電源装置は正常に動作しています。
DC 出力喪失	電源装置に障害が発生しました。

SEL にエントリを記録する電源冗長性状態の変更に関連するイベントは、**AC 冗長性** 電源ポリシーまたは **電源装置冗長性** 電源ポリシーのいずれかに設定されたモジュラーエンクロージャにおける冗長性の喪失と回復です。次の表には、電源冗長性ポリシーの変更に関連する SEL エントリがリストされています。

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

電力バジェット、冗長性、および 4 台の電源装置ユニット (PSU) を使用するシャーシ全体 (シャーシ、サーバー、I/O モジュール、KVM、CMC、電源装置) の動的電力を設定できます。電源管理サービスは電力消費を最適化し、要件に基づいて異なるモジュールに電力を割り当て直します。


次を設定することができます。

- システム入力電力の上限
- 冗長性ポリシー
- 電源装置の動的制御を有効にする
- シャーシ電源ボタンの無効化
- 最大電力節減モード
- リモート電力ログ
- リモート電力ログの間隔
- サーバーベースの電源管理

節電と電力バジェット

CMC は、ユーザー設定の電力最大制限に到達すると、節電を実行します。電力に対する需要がユーザー設定のシステム入力電力上限を越えると、CMC は優先順位の高いサーバーおよびシャーシ内のその他モジュールのために電力を解放するために、優先順位の低いサーバー順にサーバーへの電力を削減します。

シャーシ内のすべて、または複数のスロットが同じ優先度レベルに設定されている場合、**CMC** はスロット番号の低い順にサーバーの電力を削減します。たとえば、スロット 1 と 2 のサーバーの優先順位が同じである場合、スロット 1 のサーバーの電力が先に削減され、次にスロット 2 のサーバーの電力が削減されます。

 **メモ:** シャーシ内の各サーバーに 1 から 9 の番号を割り当てることによって、それぞれの優先度レベルを割り当てることができます。すべてのサーバーのデフォルト優先度レベルは 1 です。番号が低くなるほど、優先度レベルは高くなります。

電力バジェットは、2 台の PSU セットのうち最も弱い PSU の最大値に制限されます。システム入力電力上限値を越える AC 電力バジェット値を設定しようとする、**CMC** がエラーメッセージを表示します。電力バジェットは 5000 W に制限されています。

最大節電モード

このモードは AC 冗長性が選択されている場合にのみ有効になります。**CMC** は、次の場合に最大節電モードを実行します。

- 最大節電モードが有効化されている。
- UPS デバイスにより発行された自動コマンドラインスクリプトが、最大節電モードを有効化する。

最大節電モードでは、すべてのサーバーが最低限の電力レベルで動作し始め、その後のサーバー電力割り当て要求はすべて拒否されます。このモードでは、電源投入されたサーバーのパフォーマンスが劣化する可能性があります。追加サーバーには、その優先順位にかかわらず、電源を投入することはできません。

最大節電モードがクリアされると、システムがフルパフォーマンス状態に戻ります。

電源バジェットを維持するためのサーバー電力の低減

CMC は、システムの消費電力量をユーザー設定のシステム入力電力制限の範囲内に維持するために追加の電力が必要なとき、優先順位の低いサーバーへの電力割り当てを削減します。たとえば、新しいサーバーが起動すると、**CMC** は新しいサーバーにより多くの電力を供給するため、優先順位が低いサーバーへの電力を削減することがあります。優先順位の低いサーバーへの電力割り当てを削減した後も電力量が不十分である場合は、**CMC** は新しいサーバーへの電力投入に十分な電力が解放されるまで、サーバーのパフォーマンスを低下させます。

CMC は次の 2 つの場合にサーバーの電力割り当てを削減します。

- 合計消費電力量が設定可能なシステム入力電力制限を超える場合。
- 非冗長構成で電力障害が発生した場合。

110V PSU AC 操作

デフォルトで、110V PSU AC 操作機能が使用可能です。ただし、110V と 220V 操作の組み合わせはサポートされません。両方の電圧の入力が **CMC** によって検出されると、一方の電圧値のみが選択され、もう一方の電圧レベルに接続されている電源装置の電源がオフにされて、機能していないと表示されます。

リモートロギング

電力消費のレポートを、リモートのシステムログサーバーに報告することができます。収集期間中のシャーシの電力消費の合計量、最大値、最小値、および平均値をログすることができます。この機能の有効化、および収集/ログ間隔の設定に関する詳細については、「[電力の管理と監視](#)」を参照してください。

外部電源管理

CMC 電源管理は、オプションとして OpenManage Power Center (OMPC) から制御することができます。詳細については、『OMPC ユーザーズガイド』を参照してください。

外部電源管理を有効にすると、OMPC は次を管理します。

- 第 12 世代サーバーのサーバー電力
- 第 12 世代サーバーのサーバー優先順位
- システム入力電力容量
- 最大節電モード

CMC は次の維持または管理を継続します。


- 冗長性ポリシー
- リモート電力ログ
- 電源冗長性よりサーバーパフォーマンスを優先する
- 動的電源供給
- 第 11 世代以前のサーバーのサーバー電力

OPMC は次に、シャーシインフラストラクチャと前世代のサーバーノードへの電力の割り当て後に使用できるバジェットから、第 12 世代サーバーノードの優先順位付けと電力を管理します。リモート電力ログは、外部電源管理には影響を受けません。


サーバーベースの電源管理モードが有効化された後、シャーシが PM3 管理用に準備されます。すべての第 12 世代サーバーの優先順位は 1（高）に設定されています。PM3 はサーバー電力および優先順位を直接管理します。PM3 は互換性のあるサーバー電力割り当てを制御するので、CMC は最大節電モードを制御しなくなります。従って、この選択は無効化されます。

最大節電モードが有効化されると、CMC はシステム入力電力容量を、シャーシが対応できる最大量に設定します。CMC は電力の最大容量の超過を許容しませんが、PM3 は他の電力容量制限のすべてに対応します。

電力の PM3 管理が無効化されると、CMC は外部管理が有効になる前のサーバー優先度設定に戻ります。

 **メモ:** PM3 管理が無効化されても、CMC は最大シャーシ電力の以前の設定には戻りません。設定値を手動で回復するには、以前の設定の **CMC ログ** を参照してください。


CMC ウェブインタフェースを使用した電力バジェットと冗長性の設定

 **メモ:** 電源管理処置を実行するには、シャーシ設定システム管理者 権限が必要です。

電力バジェットを設定するには、次の手順を実行します。

1. 左ペインで、シャーシ概要 → 電源 → 設定 をクリックします。
2. バジェット / 冗長性設定 ページで、次のプロパティのいずれかまたはすべてを必要に応じて選択します。各フィールドの説明については、『オンラインヘルプ』を参照してください。
 - サーバーベースの電源管理の有効化
 - システム入力電力の上限
 - 冗長性ポリシー
 - 電源装置の動的制御を有効にする
 - シャーシ電源ボタンの無効化
 - 最大電力節減モード
 - リモート電力ログを有効にする
 - リモート電力ログの間隔
3. 適用 をクリックして変更を保存します。

RACADM を使用した電力バジェットと冗長性の設定

 **メモ:** 電源管理処置を実行するには、**シャーシ設定システム管理者** 権限が必要です。

冗長性を有効にして冗長性ポリシーを設定するには、次の手順を実行します。

1. シリアル/Telnet/SSH テキストコンソールを開いて **CMC** に進み、ログインします。
2. 必要に応じてプロパティを設定します。
 - 冗長性ポリシーを選択するには、次を入力します。

```
racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy <値>
```

ここで、<値> は **0 (AC 冗長性)** および **1 (PSU 冗長性)** です。デフォルト値は **0** です。
例えば、次のコマンドは冗長性ポリシーを **1** に設定します。

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

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

ここで、<値> は現在のランタイムシャーシ負荷および **5000** 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 **5000** です。
たとえば、次のコマンドは最大電力バジェットを **5000** ワットに設定します。

```
racadm config -g cfgChassisPower -o cfgChassisPowerCap 5000
```
 - **PSU** の動的電源供給を有効または無効にするには、次を入力します。

```
racadm config -g cfgChassisPower -o cfgChassisDynamicPSUEngagementEnable <値>
```

ここで <値> は **0 (無効)**、**1 (有効)** です。デフォルトは **0** です。
例えば、次のコマンドは動的 **PSU** 電源供給を無効化します。

```
racadm config -g cfgChassisPower -o cfgChassisDynamicPSUEngagementEnable 0
```
 - 最大節電モードを有効にするには、次を入力します。

```
racadm config -g cfgChassisPower -o cfgChassisMaxPowerConservationMode 1
```
 - 通常の動作を復元するには、次を入力します。

```
racadm config -g cfgChassisPower -o cfgChassisMaxPowerConservationMode 0
```
 - 電力リモートログ機能を有効にするには、次のコマンドを入力します。

```
racadm config -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingEnabled 1
```
 - 電力リモートログの間隔を指定するには、次のコマンドを入力します。

```
racadm config -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingInterval n
```

ここで *n* は **1~1440** 分になります。
 - 電力リモートログ機能が有効かどうかを判定するには、次のコマンドを入力します。

```
racadm getconfig -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingEnabled
```
 - 電力リモートログの間隔を確認するには、次のコマンドを入力します。

```
racadm getconfig -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingInterval
```

電力リモートログ機能は、以前に設定されたリモート **Syslog** ホストに依存します。1つ、または複数のリモート **Syslog** ホストへのロギングを有効化する必要があり、しなかった場合は電力消費

がログされます。これは、ウェブ GUI または RACADM CLI のいずれかを使用して実行できます。詳細については、リモート Syslog 設定手順を参照してください。

- Open Manage Power Center (OPMC) によるリモート電源管理を有効にするには、次を入力します。


```
racadm config -g cfgChassisPower -o cfgChassisServerBasedPowerMgmtMode 1
```
- CMC 電力管理を復元するには、次を入力します。

```
racadm config -g cfgChassisPower -o cfgChassisServerBasedPowerMgmtMode 0
```

シャーシ電力の RACADM コマンドの詳細については、『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』の **config**、**getconfig**、**getpbinf**、および **cfgChassisPower** の項を参照してください。


電源制御操作の実行

シャーシ、サーバー、および IOM のために次の電源制御操作を実行できます。

 **メモ:** 電源制御操作はシャーシ全体に影響します。

シャーシに対する電源制御操作の実行

CMC は、手順に従ったシャットダウンなど、ユーザーがシャーシ全体（シャーシ、サーバー、IOM、PSU）におけるいくつかの電力管理処置をリモートで実行することを可能にします。

 **メモ:** 電力管理処置を行うには、**シャーシ設定システム管理者** 権限が必要です。

ウェブインタフェースを使用したシャーシでの電源制御操作の実行

CMC ウェブインタフェースを使用してシャーシの電源制御操作を行うには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** → **電源** → **制御** をクリックします。
シャーシの**電源制御** ページが表示されます。
2. 次のいずれかの電源制御操作を選択します。
各オプションの情報は『オンラインヘルプ』を参照してください。
 - システムの電源を入れる
 - システムの電源を切る
 - システムのパワーサイクル（コールドブート）
 - CMC のリセット（ウォームブート）
 - 非正常なシャットダウン

3. **適用** をクリックします。
確認を求めるダイアログボックスが表示されます。

4. **OK** をクリックして、電源管理処置（例えば、システムをリセットするなど）を行います。

RACADM を使用したシャーシでの電源制御操作の実行


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

```
racadm chassisaction -m chassis <処置>
```

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

サーバーに対する電源制御操作の実行

複数のサーバーに対して一度に、またはシャーシ内の個々のサーバーに対して電源管理処置をリモートで行うことができます。

 **メモ:** 電力管理処置を行うには、**シャーシ設定システム管理者** 権限が必要です。

CMC ウェブインタフェースを使用した複数サーバーの電源制御操作

CMC ウェブインタフェースを使用して複数サーバーの電源制御操作を行うには、次の手順を実行します。


1. 左ペインで、**サーバー概要** → **電源** をクリックします。
電源制御 ページが表示されます。
2. **操作** 列のドロップダウンメニューから、必要サーバーのために次の電源制御操作の1つを選択します。
 - 操作なし
 - サーバーの電源を入れる
 - サーバーの電源を切る
 - 正常なシャットダウン
 - サーバーをリセットする (ウォームブート)
 - サーバーの電源を入れなおす (コールドブート)

オプションの詳細については、『オンラインヘルプ』を参照してください。

3. **適用** をクリックします。
確認を求めるダイアログボックスが表示されます。
4. **OK** をクリックして、電源管理処置 (たとえば、サーバーのリセット) を実行します。

IOM での電源制御操作の実行

IOM はリモートでリセットまたは電源投入できます。

 **メモ:** 電力管理処置を行うには、**シャーシ設定システム管理者** 権限が必要です。

CMC ウェブインタフェースを使用した IOM での電源制御操作の実行

I/O モジュールで電源制御操作を実行するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** → **I/O モジュール概要** → **電源** をクリックします。
2. **電源制御** ページで、IOM に対するドロップダウンメニューから実行する操作を選択します (パワーサイクル)。
3. **適用** をクリックします。

RACADM を使用した IOM での電源制御操作の実行

RACADM を使用した IOM での電源制御操作を実行するには、CMC へのシリアル/Telnet/SSH テキストコンソールを開き、ログインして次を入力します。

```
racadm chassisaction -m switch <処置>
```

ここで、<処置>は実行する操作（power cycle）を示します。

シャーシストレージの管理


Dell PowerEdge VRTX 上では、次の操作を実行できます。

- 物理ディスクドライブとストレージコントローラの状態の表示。
- コントローラ、物理ディスクドライブ、仮想ディスク、およびエンクロージャのプロパティの表示。
- コントローラ、物理ディスクドライブ、および仮想ディスクのセットアップ。
- 仮想アダプタの割り当て。
- コントローラ、物理ディスクドライブ、および仮想ディスクのトラブルシューティング。
- ストレージコンポーネントのアップデート。

ストレージコンポーネントの状態の表示

ストレージコンポーネントの状態を表示するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** → **ストレージ** → **プロパティ** → **ストレージ概要** をクリックします。
2. **ストレージ概要** ページでは、次を表示することができます。
 - シャーシに取り付けられている物理ディスクドライブのグラフ概要と、各ドライブの状態。
 - すべてのストレージコンポーネントの概要。各コンポーネントには、それぞれのページにアクセスするためのリンクが付いています。
 - ストレージの使用済み容量と合計容量。
 - コントローラ情報。
 - 最近ログされたストレージイベント。

 **メモ:** 詳細については、『オンラインヘルプ』を参照してください。

ストレージトポロジの表示

ストレージトポロジを表示するには、次の手順を実行します。


1. 左ペインで、**シャーシ概要** → **ストレージ** → **プロパティ** → **トポロジ** をクリックします。
2. **トポロジ** ページで、**<コントローラ名>** をクリックして対応するページを表示します。
3. 取り付けられている各コントローラの下で、**仮想ディスクを表示**、**<エンクロージャ名>**、および **物理ディスクを表示** のリンクをクリックして、それぞれのページを開きます。

スロットへの仮想アダプタの割り当て

サーバースロットへの仮想ディスクのマッピングは、最初に仮想ディスクを仮想アダプタ (VA) にマップし、その後に仮想アダプタ (VA) をサーバースロットにマップすることで実行できます。

- VA をサーバースロットに割り当てる前に、次を確認してください。
 - サーバースロットが空、またはスロット内のサーバーの電源がオフになっている。


- サーバーから VA のマッピングが解除されている。
- 仮想ディスクが作成され、これらは **仮想アダプタ 1**、**仮想アダプタ 2**、**仮想アダプタ 3**、または **仮想アダプタ 4** として割り当てられます。詳細については、「[仮想ディスクへの仮想アダプタアクセスポリシーの適用](#)」を参照してください。

 **メモ:** 1 台のサーバーに対して同時にマップできる仮想アダプタは 1 つだけです。適切なライセンスがなくても、VA をデフォルトサーバーにマップしたり、VA-サーバー間の割り当てのマッピングを解除したりすることができます。デフォルトのマッピングは、VA1-サーバーロット 1、VA2-サーバーロット 2、VA3-サーバーロット 3、および VA4-サーバーロット 4 です。

仮想アダプタ機能を使用して、取り付け済みストレージを 4 台のサーバーで共有することができます。サーバーロットから仮想アダプタのマッピングを解除するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** → **ストレージ** → **セットアップ** → **仮想化** をクリックします。
2. **ストレージ仮想化** ページの **処置** ドロップダウンメニューから、**マップ解除** を選択し、**適用** をクリックします。

選択したサーバーロットから VA のマップが解除されます。

 **メモ:** 仮想アダプタへの仮想ディスクの割り当ては、**単一割り当て** モードまたは **複数割り当て** モードを選択して実行することができます。これらのモー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。

CMC ウェブインタフェースを使用したコントローラプロパティの表示

コントローラプロパティを表示するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** → **コントローラ** をクリックします。
2. **コントローラ** ページの **コントローラ** セクションで、コントローラの基本プロパティを確認できます。ただし、詳細なプロパティを表示するには、**+** をクリックします。コントローラの詳細については、『[オンラインヘルプ](#)』を参照してください。

RACADM を使用したコントローラプロパティの表示

RACADM を使用してコントローラプロパティを表示するには、コマンド `racadm raid get controllers -o` を実行します。

詳細については、『[Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド](#)』を参照してください。

外部設定のインポートまたはクリア

外部ディスクはシャーシに挿入されている必要があります。

外部設定をインポートまたはクリアするには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** → **ストレージ** → **コントローラ** → **セットアップ** をクリックします。
2. **コントローラ設定** ページの **外部設定** セクションで、各コントローラに対して次をクリックします。
 - **外部設定のクリア**。既存のディスク設定をクリアします。
 - **インポート/回復**。外部設定を持つディスクをインポートします。

CMC ウェブインタフェースを使用した物理ディスクプロパティの表示

物理ディスクがシャーシに取り付けられていることを確認してください。

物理ディスクドライブのプロパティを表示するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** → **ストレージ** → **物理ディスク** に移動します。
プロパティ ページが表示されます。
2. すべての物理ディスクドライブのプロパティを表示するには、**物理ディスク** セクションで **+** をクリックします。また、次のフィルタを使用して、特定の物理ディスクドライブのプロパティを表示することもできます。
 - **物理ディスク基本フィルタ** オプションの **グループ基準** ドロップダウンメニューから、**仮想ディスク**、**コントローラ**、または **エンクロージャ** を選択し、**適用** をクリックします。
 - **詳細フィルタ** をクリックし、各種属性の値を選択して、**適用** をクリックします。

RACADM を使用した物理ディスクドライブプロパティの表示

RACADM を使用して物理ディスクドライブのプロパティを表示するには、コマンド `racadm raid get pdisks -o` を実行します。

詳細については、『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。

物理ディスクと仮想ディスクの識別

LED 点滅機能の有効化または無効化についての詳細は、次を参照してください。

- [CMC ウェブインタフェースを使用した LED 点滅の設定](#)
- [RACADM を使用した LED の点滅の設定](#)

CMC ウェブインタフェースを使用したグローバルホットスペアの割り当て

グローバルホットスペアを割り当てまたは割り当て解除するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** → **ストレージ** → **物理ディスク** → **セットアップ** をクリックします。
物理ディスクのセットアップ ページが表示されます。
2. **グローバルホットスペア割り当て** セクションの **ホットスペア処置** ドロップダウンメニューから、各物理ディスクドライブに対して **割り当て解除** または **グローバルホットスペア** を選択し、**適用** をクリックします。あるいは、**ホットスペア処置 - すべてに割り当て** ドロップダウンメニューから、**割り当て解除** または **グローバルホットスペア** を選択し、**適用** をクリックします。

RACADM を使用したグローバルホットスペアの割り当て

RACADM を使用してグローバルホットスペアを割り当てるには、コマンド `racadm raid hotspare: - assign yes -type ghs` を実行します。

RACADM コマンドの使用の詳細については、『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。

CMC ウェブインタフェースを使用した仮想ディスクプロパティの表示

仮想ディスクが作成されていることを確認してください。

仮想ディスクプロパティを表示するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** → **ストレージ** → **仮想ディスク** → **プロパティ** をクリックします。
2. **プロパティ** ページの **仮想ディスク** セクションで、**+** をクリックします。また、次のフィルタを使用して、特定の仮想ディスクプロパティを表示することもできます。
 - **基本仮想ディスクフィルタ** セクションの **コントローラ** ドロップダウンメニューから、コントローラ名を選択し、**適用** をクリックします。
 - **詳細フィルタ** をクリックし、各種属性の値を選択して、**適用** をクリックします。


RACADM を使用した仮想ディスクプロパティの表示

RACADM を使用して仮想ディスクプロパティを表示するには、コマンド `racadm raid get vdisks -o` を実行します。

詳細については、『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。

CMC ウェブインタフェースを使用した仮想ディスクの作成

物理ディスクがシャーシに取り付けられていることを確認してください。

 **メモ:** 仮想ディスクを削除すると、その仮想ディスクはコントローラの設定から削除されます。

仮想ディスクを作成するには次のように入力します。

1. 左ペインで、**シャーシ概要** → **ストレージ** → **仮想ディスク** → **作成** をクリックします。
2. **仮想ディスクの作成** ページの **設定** セクションに適切なデータを入力し、**物理ディスクの選択** セクションから、前に選択した RAID レベルに基づいた台数の物理ディスクドライブを選択して、**仮想ディスクの作成** をクリックします。

仮想ディスクへの仮想アダプタアクセスポリシーの適用

物理ディスクドライブがインストールされており、仮想ディスクが作成されていることを確認します。

仮想アダプタアクセスポリシーを適用するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** → **ストレージ** → **仮想ディスク** → **割り当て** をクリックします。
2. **仮想ディスクの割り当て** ページの **仮想アダプタのアクセスポリシー** セクションで、**仮想アダプタ <番号>** ドロップダウンメニューから各物理ディスクドライブについて **フルアクセス** を選択します。
3. **適用** をクリックします。


これで、仮想アダプタをサーバースロットに割り当てることができます。詳細については、本ユーザーズガイドのスロットへの仮想アダプタの割り当ての項を参照してください。

CMC ウェブインタフェースを使用した仮想ディスクプロパティの変更


仮想ディスクプロパティを変更するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** → **ストレージ** → **仮想ディスク** → **管理** をクリックします。
2. **仮想ディスクの管理** ページの **仮想ディスク処置** ドロップダウンメニューから、次の処置のいずれかを選択し、**適用** をクリックします。

- **名前の変更**
- **削除**

 **メモ:** 削除を選択した場合、仮想ディスクを削除するとその仮想ディスク内で使用可能なデータが恒久的に削除されることを示す次のメッセージが表示されます。

仮想ディスクの削除はコントローラの構成からその仮想ディスクを削除します。仮想ディスクの初期化はその仮想ディスクからデータを恒久的に消去します。


 **メモ:** 削除を選択した場合、仮想ディスクを削除するとその仮想ディスク内で使用可能なデータが恒久的に削除されることを示す次のメッセージが表示されます。

仮想ディスクの削除はコントローラの構成からその仮想ディスクを削除します。仮想ディスクの初期化はその仮想ディスクからデータを恒久的に消去します。

- **ポリシーの編集: 読み取りキャッシュ**
- **ポリシーの編集: 書き込みキャッシュ**
- **ポリシーの編集: ディスクキャッシュ**
- **初期化: 高速**
- **初期化: 完全**

CMC ウェブインタフェースを使用したエンクロージャプロパティの表示

エンクロージャプロパティを表示するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** → **ストレージ** → **エンクロージャ** → **プロパティ** をクリックします。
2. **プロパティ** ページの **エンクロージャ** セクションで、 をクリックして、物理ディスクドライブとそれらの状態、物理ディスクドライブスロットの概要、および詳細プロパティをグラフィカルに表示します。

PCIe スロットの管理

デフォルトでは、すべてのスロットがマップ解除されています。次を実行することができます。

- シヤーン内の全 PCIe スロットの状態の表示。
- サーバーに対する PCIe スロットの割り当てまたは割り当て解除。

PCIe スロットをサーバーに割り当てる前に、次を考慮してください。

- 空の PCIe スロットを電源がオンになっているサーバーに割り当てることはできません。
- サーバーに割り当てられたアダプタがある PCIe スロットは、現在割り当てられているサーバー（ソース）の電源がオンになっている場合、別のサーバーに割り当てることはできません。
- サーバーに割り当てられたアダプタがある PCIe スロットは、電源がオンになっている別のサーバー（ターゲット）に割り当てることはできません。


PCIe スロットをサーバーから割り当て解除する前に、次を考慮してください。

- PCIe スロットが空の場合、サーバーの電源がオンになっていても、スロットをサーバーから割り当て解除できません。
- PCIe スロットにアダプタがあり、その電源がオンになっていない場合、サーバーの電源がオンになっていてもサーバーから割り当て解除できます。このような状況は、スロットが空で割り当てられているサーバーの電源がオンになっている状態でユーザーが空のスロットにアダプタを挿入すると発生することがあります。

PCIe スロットの割り当ておよび割り当て解除の詳細については、『オンラインヘルプ』を参照してください。

 **メモ:** ライセンスがない場合は、最大 2 台の PCIe デバイスをサーバーに割り当てることができます。

CMC ウェブインタフェースを使用した PCIe スロットプロパティの表示

- 8 個の PCIe スロットすべてについての情報を表示するには、左ペインで **シヤーン概要** → **PCIe 概要** をクリックします。必要なスロットに対し、 をクリックしてプロパティをすべて表示します。
- 1 個の PCIe スロットについての情報を表示するには、**シヤーン概要** → **PCIe スロット <番号>** → **プロパティ** → **状態** をクリックします。

CMC ウェブインタフェースを使用したサーバーへの PCIe スロットの割り当て

PCIe スロットをサーバーに割り当てるには、次の手順を実行します。

- 左ペインで、**シヤーン概要** → **PCIe 概要** → **セットアップ** → **マッピング : PCIe スロット** からサーバー スロットをクリックします。**マッピング : PCIe スロット** からサーバー スロット ページの **処置** 列内にある **処置** ドロップダウンメニューから、適切なサーバー名を選択し、**適用** をクリックします。

サーバーへの PCIe デバイスの割り当ての詳細については、『オンラインヘルプ』を参照してください。

RACADM を使用した PCIe スロットの管理

RACADM コマンドを使用してサーバーに対する PCIe スロットの割り当て、または割り当て解除を行うことができます。したりすることができます。ここにコマンドの一部を紹介します。RACADM コマンドの詳細については、dell.com/support/Manuals にある『Chassis Management Controller for PowerEdge VRTX RACADM コマンドラインリファレンスガイド』を参照してください。

- サーバーに対する PCIe デバイスの現在の割り当てを表示するには、次のコマンドを実行します。

```
racadm getpiecfg -a
```

- FQDD を使用して PCIe デバイスのプロパティを表示するには、次のコマンドを実行します。

```
racadm getpciecfg [-c <FQDD>]
```

たとえば、PCIe デバイス 1 のプロパティを表示するには、次のコマンドを実行します。

```
racadm getpciecfg -c pcie.chassisslot.1
```

- サーバースロットに PCIe アダプタスロットを割り当てるには、次のコマンドを実行します。

```
racadm setpciecfg assign [-c <FQDD>] [i <サーバースロット>]
```

- たとえば、サーバースロット 2 に PCIe スロット 5 を割り当てるには、次のコマンドを実行します。

```
racadm setpciecfg assign -c pcie.chassisslot.5 -i 2
```

- サーバーから PCIe スロット 3 の割り当てを解除するには、次のコマンドを実行します。

```
racadm setpciecfg unassign -c pcie.chassisslot.3
```

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、エラー状態、エラーログの収集。
- 診断コンソールの使用。
- リモートシステムの電源管理。
- リモートシステムの Lifecycle Controller ジョブの管理。
- コンポーネントのリセット。
- ネットワークタイムプロトコル (NTP) 問題に関するトラブルシューティング。
- ネットワーク問題に関するトラブルシューティング。
- アラート問題に関するトラブルシューティング。
- システム管理者パスワードを忘れた場合のリセット。
- シャーシ構成設定および証明書の保存と復元。
- エラーコードおよびログの表示。

RACDUMP を使用した設定情報、シャーシ状態、およびログの収集

racdump サブコマンドは、包括的なシャーシ状態、設定状況情報、イベントログの履歴を収集するための単一のコマンドを提供します。

racdump サブコマンドは、次の情報を表示します。

- 一般的なシステム /RAC 情報
- CMC 情報
- シャーシ情報
- セッション情報
- センサー情報
- ファームウェアビルド情報

対応インタフェース

- CLI RACADM
- リモート RACADM
- Telnet RACADM

racdump には次のサブシステムが含まれており、次の RACADM コマンドを集約します。racdump の詳細については、『PowerEdge VRTX の CMC 用 RACADM コマンドラインリファレンスガイド』を参照してください。

サブシステム	RACADM コマンド
システム/RAC の一般情報	getsysinfo
セッション情報	getssninfo
センサー情報	getsensorinfo
スイッチ情報 (IO モジュール)	getioinfo
メザニンカード情報 (ドーターカード)	getdcinfo
全モジュールの情報	getmodinfo
電力バジェット情報	getpbinfo
KVM 情報	getkvminfo
NIC 情報 (CMC モジュール)	getniccfg
冗長性情報	getredundancymode
トレースログ情報	gettracelog
RAC イベントログ	getraclog
システムイベントログ	getsel

SNMP Management Information Base (MIB) ファイルのダウンロード

CMC SNMP MIB ファイルは、シャードタイプ、イベント、およびインジケータを定義します。CMC は、ウェブインタフェースを使用した MIB ファイルのダウンロードを可能にします。

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

1. 左ペインで、**シャード概要** → **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 **AC 冗長性** に設定すると、電源装置の冗長性喪失イベントが生じた。

- **解決策 A:** この設定には、モジュラーエンクロージャのサイド1（左側2つのスロット）に少なくとも1台の電源装置、およびサイド2（右側2つのスロット）に1台の電源装置が存在し、動作可能であることが必要です。さらに、各サイドの容量は、シャーシが**AC冗長性**を維持するための総電力割り当てをサポートするために十分である必要があります。（完全な**AC冗長性**動作のため、4台の電源装置が装備された完全な**PSU**構成が利用可能であるようにしてください。）
- **解決策 B:** すべての電源装置が2つの**AC**グリッドに正しく接続されていることを確認します。サイド1の電源装置は一方の**AC**グリッドに、サイド2の電源装置は他方の**AC**グリッドに接続され、両方の**AC**グリッドが機能していることが必要です。このうちひとつの**AC**グリッドが機能していないと、**AC冗長性**は失われます。
- **問題:** **AC**ケーブルが接続されていて、電力配分装置も良好な**AC**出力を行っているにもかかわらず、**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**の電源が切れ、障害とマーク付けされます。
- **問題:** 動的電源供給が有効化されているのに、どの電源装置も**スタンバイ**状況として表示されない。
 - **解決策 A:** 余剰電力が十分ではありません。1つまたは複数の電源装置がスタンバイ状況に移行するのは、エンクロージャで利用できる余剰電力が、少なくとも1つの電源装置の容量を超えた場合に限られます。
 - **解決策 B:** 動的電源供給が、エンクロージャ内に存在する電源装置ユニットで完全にサポートできません。これが原因であるかを確認するには、ウェブインタフェースを使用して動的電源供給をオフにしてから、再度オンにします。動的電源供給を完全にサポートできない場合は、メッセージが表示されます。
- **問題:** 新しいサーバーを十分な電源装置があるエンクロージャに挿入しましたが、サーバーの電源がオンになりません。
 - **解決策 A:** システム入力電力上限の設定をチェックします。追加サーバーに電源を供給するには低すぎる設定になっている場合があります。
 - **解決策 B:** 最大節電の設定をチェックします。これが設定されていると、この問題が発生します。詳細については、電源設定を参照してください。
 - **解決策 C:** 新しく挿入したサーバーと関連付けられているサーバースロットの電力優先順位を確認し、他のサーバースロットの電力優先順位より低く設定されていないことを確認してください。
- **問題:** モジュラーエンクロージャ構成を変更していないのに、利用可能な電力の表示が頻繁に変わる。
 - **解決策:** **CMC**にはエンクロージャがユーザー設定の電力上限のピーク近くで動作している場合にサーバーへの電力割り当てを一時的に減少させる動的ファン電源管理機能が搭載されています。これによって、電力利用が**システム入力電力上限**を超えないようにするため、サーバーのパフォーマンスを低減することによってファンに電力が割り当てられます。これは通常の動作です。
- **問題:** ピークパフォーマンス時の余剰電力が<数値>Wと報告される。
 - **解決策:** 現行の構成では、エンクロージャに<数値>Wの使用可能な余剰電力があり、**システム入力電力上限**は、サーバーのパフォーマンスに影響を与えることなく、この報告された量まで安全に引き下げることができます。
- **不具合:** シャーシが4台の電源装置での**AC冗長性**構成で稼働していたにもかかわらず、**AC**グリッドに障害が発生した後、サーバーのサブセットが電力を失った。
 - **解決策:** この問題は、**AC**グリッド障害が発生した時に、電源装置が冗長**AC**グリッドに正しく接続されていなかった場合に発生します。**AC冗長性**ポリシーでは、左側2台の電源装置がひとつの**AC**グリッドに接続され、右側2台の電源装置がもう一方の**AC**グリッドに接続されている必要があります。2台の**PSU**が正しく接続されていない場合（例えば、**PSU 2**と**PSU 3**が

誤った AC グリッドに接続されているなど)、AC グリッド障害は優先順位の最も低いサーバーの電力喪失の原因になります。

- **問題：** PSU に障害が発生した後、優先順位の最も低いサーバーが電力を失った。
 - **解決策：** サーバーの電源が切れる原因となる今後の電源装置障害を避けるには、シャーシに少なくとも 3 台の電源装置が装備され、PUS 障害がサーバー動作に影響しないように **電源装置冗長性** ポリシーが設定されているようにしてください。
- **問題：** データセンターの周囲温度が上がるとサーバー全体のパフォーマンスが低下する。
 - **解決策：** この問題は、ファンの電力需要の増加がサーバーへの電力割り当てを削減することによって埋め合わされる結果となる値に **システム入力電力上限** が設定されている場合に発生します。サーバーパフォーマンスに影響することなくファンに追加電力を割り当てる事を可能にするため、ユーザーは **システム入力電力上限** をより大きい値に増やすことができます。

アラートのトラブルシューティング

CMC アラートのトラブルシューティングには、CMC ログとトレースログを使用します。各 E-メール、および/または SNMP トラップの送信試行の成功と失敗は CMC ログに、特定のエラーを説明する追加情報はトレースログにログされます。ただし、SNMP はトラップの送信を確認しないので、ネットワークアナライザ、または Microsoft の snmputil などのツールを使用して、管理下システムのバケットをトレースしてください。

イベントログの表示

管理下システムで発生したシステムにとって重要なイベントの情報には、ハードウェアログおよびシャーシログを表示することができます。

ハードウェアログの表示

CMC はシャーシで発生したイベントのハードウェアログを生成します。ハードウェアログは、ウェブインタフェースおよびリモート RACADM を使用して表示できます。



メモ: ハードウェアログをクリアするには、**ログのクリアシステム管理者** 特権が必要です。



メモ: 特定のイベント発生時に E-メールまたは SNMP トラップを送信するように CMC を設定することができます。アラートを送信するための CMC の設定についての情報は、「[アラートを送信するための CMC の設定](#)」を参照してください。


ハードウェアログエントリの例

重要システムソフトウェアイベント：冗長性損失 2007 年 5 月 9 日水曜日 15:26:28 正常システムソフトウェアイベント：クリアされたログがアサートされました 2007 年 5 月 9 日水曜日 16:06:00 警告システムソフトウェアイベント：予測障害がアサートされました 2007 年 5 月 9 日水曜日 15:26:31 重要ソフトウェアイベント：ログ満杯がアサートされました 2007 年 5 月 9 日水曜日 15:47:23 不明のシステムソフトウェアイベント：不明イベント


CMC ウェブインタフェースを使用したハードウェアログの表示


ハードウェアログは表示、保存、およびクリアすることが可能です。ログは、列の見出しをクリックすることにより、重大度、日付/時刻、または説明を基準に並べ替えることができます。列の見出しを再度クリックして、並び順を逆にします。

CMC ウェブインタフェースを使用してハードウェアログを表示するには、左ペインで **シャーシ概要** → **ログ** をクリックします。**ハードウェアログ** ページが表示されます。管理下ステーションまたはネットワークにハードウェアログのコピーを保存するには、**ログの保存** をクリックしてから、ログのテキストファイルの場所を指定します。

 **メモ:** ログはテキストファイルとして保存されるため、ユーザーインターフェースで重大度を示すために使用されるグラフィックイメージは表示されません。テキストファイルでは、重大度は **OK**、**情報**、**不明**、**警告**、**重大** という単語で示されます。日付/時刻のエントリは昇順で表示されます。日付/時刻列に <システム起動> が表示される場合は、日付または時刻が利用できない、モジュールの電源オンまたは電源オフ中にイベントが発生したことを意味します。

ハードウェアログをクリアするには、**ログのクリア** をクリックします。

 **メモ:** CMC はログがクリアされたことを示す新しいログエントリを作成します。

 **メモ:** ハードウェアログをクリアするには、**ログのクリア管理者** 権限が必要です。

RACADM を使用したハードウェアログの表示

RACADM を使用してハードウェアログを表示するには、CMC へのシリアル/Telnet/SSH テキスト コンソールを開いて CMC へ進み、ログイン後、次を入力します。


```
racadm getsel
```

ハードウェアログをクリアするには、次を入力します。

```
racadm clrsel
```

シャーシログの表示

CMC は、シャーシ関連のイベントのログを生成します。

 **メモ:** シャーシログをクリアするには、**ログのクリア管理者** 権限が必要です。

RACADM を使用したシャーシログの表示

RACADM を使用してシャーシログ情報を表示するには、CMC へのシリアル/Telnet/SSH テキストコンソールを開いてログインし、次を入力します。

```
racadm chassislog view
```

このコマンドにより、最新のシャーシログエントリが 25 件表示されます。

シャーシログの表示に使用可能なオプションを表示するには、次のコマンドを実行します。

```
racadm chassislog help view
```

ウェブインターフェースを使用したシャーシログの表示


シャーシログを表示、保存、クリアすることができます。ログは、ログタイプとフィルタに基づいて絞り込むことができます。また、キーワードによる検索を実行したり、指定した期間のログを表示したりすることも可能です。

左ペインで、**シャーシ概要** → **ログ** → **シャーシログ** をクリックします。**シャーシログ** ページが表示されます。

お使いの管理下ステーションまたはネットワークにシャーシログのコピーを保存するには、**ログの保存** をクリックして、ログファイルを保存する場所を指定します。

診断コンソールの使用

高度な技術を持つユーザーである、またはテクニカルサポートの指示に従っている場合、CLI コマンドを使用してシャーシハードウェア関連の問題を診断することができます。


 **メモ:** これらの設定を変更するには、**デバッグコマンドシステム管理者** 特権が必要です。

診断コンソールにアクセスするには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** → **トラブルシューティング** → **診断** をクリックします。
診断コンソールページが表示されます。
2. コマンドテキストボックスにコマンドを入力し、**送信** をクリックします。
コマンドの詳細については、『オンラインヘルプ』を参照してください。
診断結果ページが表示されます。

コンポーネントのリセット

アクティブな CMC をリセットしたり、サーバーを仮想的に再装着することによって、取り外されて再挿入されたかのようにサーバーを動作させることができます。シャーシにスタンバイ CMC がある場合は、アクティブな CMC のリセットはフェイルオーバーを生じ、スタンバイ CMC がアクティブになります。

 **メモ:** コンポーネントをリセットするには、**デバッグ コマンド管理者** 特権が必要です。


CMC ウェブインタフェースを使用してコンポーネントをリセットするには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** → **トラブルシューティング** → **コンポーネントのリセット** をクリックします。
コンポーネントのリセット ページが表示されます。
2. アクティブ CMC をリセットするには、**CMC 状態** セクションで、**CMC のリセット/フェールオーバー** をクリックします。スタンバイ CMC が存在し、シャーシに完全な冗長性がある場合は、フェールオーバーが生じ、スタンバイ CMC がアクティブになります。ただし、スタンバイ CMC が存在しない場合は、使用可能な CMC が再起動されます。
3. サーバーを仮想的に再装着するには、**サーバーの仮想的な再装着** セクションで、再装着するサーバーを選択し、**選択の適用** をクリックします。
詳細については、『オンラインヘルプ』を参照してください。
この操作を行うと、サーバーを取り外されて再挿入されたかのように動作させることができます。

シャーシ設定の保存と復元

これはライセンスが必要な機能です。CMC ウェブインタフェースを使用してシャーシ設定のバックアップを保存または復元するには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** → **セットアップ** → **シャーシバックアップ** をクリックします。**シャーシバックアップ** ページが表示されます。シャーシ設定を保存するには、**保存** をクリックします。デフォルトのファイルパスを上書きし（オプション）、**OK** をクリックしてファイルを保存します。デフォルトのバックアップファイル名にはシャーシのサービスタグが含まれています。このバックアップファイルは、このシャーシの設定と証明書を復元する場合に限り、後から使用することができます。
2. シャーシ設定を復元するには、「復元」セクションで **参照** をクリックし、バックアップファイルを指定して **復元** をクリックします。

 **メモ:** CMC 自体は設定の復元時にリセットされることはありませんが、CMC サービスに新しい、または変更された設定内容が事実上反映されるまで、しばらく時間がかかる場合があります。反映が正常に完了した後、現行のセッションがすべて閉じられます。

ネットワークタイムプロトコル (NTP) エラーのトラブルシューティング

ネットワーク上のリモートタイムサーバーの時刻と同期化するように CMC のクロックを設定した後は、日付と時刻が変更されるまで数分かかる場合があります。数分後も変更されない場合は、問題をトラブルシューティングする必要がある場合があります。CMC は、次の理由でクロックを同期化できない可能性があります。

- NTP サーバー 1、NTP サーバー 2、および NTP サーバー 3 設定の問題。
- 無効なホスト名または IP アドレスが誤って入力された可能性がある。
- CMC と設定済みの NTP サーバーとの通信を妨げるネットワーク接続問題がある。
- NTP サーバーホスト名が解決されるのを妨げる DNS 問題がある。

NTP 関連問題のトラブルシューティングを行うには、CMC トレースログの情報をチェックしてください。このログには NTP 関連障害のエラーメッセージが含まれています。CMC がどの設定済みリモート NTP サーバーとも同期化できない場合は、CMC 時刻はローカルシステムのクロックと同期化され、トレースログには次のメッセージに類似したエントリが記録されます。

```
1 月 8 日 20:02:40 cmc ntpd[1423]:LOCAL (0) に同期化、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 gettractime -n
```


「*」が設定済みサーバーのいずれかに表示されない場合、設定が正しく行われていない可能性があります。このコマンドの出力には、問題のデバッグに役立つ可能性のある詳しい NTP 統計が含まれています。

Windows ベースの NTP サーバーの設定を試行する場合、`ntpd` の `MaxDist` パラメータの増加が役立つ場合があります。デフォルト設定は大部分の NTP サーバーと連動するために十分な大きさが必要であることから、このパラメータを変更する前に、変更による影響すべてについて理解しておいてください。

パラメータを変更するには、次のコマンドを入力します。

```
racadm config -g cfgRemoteHosts -o cfgRhostsNtpMaxDist 32
```

変更後 NTP を無効化し、5~10 秒間待ってから再度 NTP を有効化します。

 **メモ:** NTP は、再同期化のためにさらに 3 分時間を費やす場合があります。

NTP を無効化するには、次を入力します。

```
racadm config -g cfgRemoteHosts -o cfgRhostsNtpEnable 0
```

NTP を有効化するには、次を入力します。

```
racadm config -g cfgRemoteHosts -o cfgRhostsNtpEnable 1
```

NTP サーバーが正しく設定されているにもかかわらず、このエントリがトレースログに存在する場合は、CMC が設定された NTP サーバーのいずれとも同期できないことが確実になります。

NTP サーバーの IP アドレスが設定されていない場合、次に似たトレースログエントリが記録される場合があります。

```
1 月 8 日 19:59:24 cmc ntpd[1423]: アドレス 1.2.3.4 の既存インタフェースが見つかりません  
ん 1 月 8 日 19:59:24 cmc ntpd[1423]: 1.2.3.4 の設定が失敗しました
```

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。

```
8 月 21 日 14:34:27 cmc ntpd_initres[1298]: ホスト名: blabla が見つかりません 8 月  
21 日 14:34:27 cmc ntpd_initres[1298]: 「blabla」を解決できませんでした。放棄します。
```

CMC ウェブインタフェースを使用してトレースログを確認するための `gettracelog` コマンドを入力する方法についての情報は、「[診断コンソールの使用](#)」を参照してください。

LED の色と点滅パターンの解釈

シャーシ上の LED は、コンポーネントの次の状態を示します。

- 緑色 LED の点灯は、コンポーネントの電源がオンになっていることを示します。緑色 LED が点滅している場合は、ファームウェアアップロードなど、重要ですが日常的に行われるイベントが発生していることを示しており、この間、ユニットを操作することはできません。障害が発生しているわけではありません。
- モジュール上の橙色 LED の点滅は、モジュール上の不具合を示します。
- 青色 LED の点滅は、ユーザーによる設定が可能で、識別に利用されます。設定の詳細については、「[SNMP Management Information Base \(MIB\) ファイルのダウンロード](#)」を参照してください。

表 32. LED の色と点滅パターン

コンポーネント	LED の色、点滅パターン	状態
CMC	緑色、点灯	電源オン
	緑色、点滅	ファームウェアのアップロード中
	緑色、消灯	電源オフ
	青色、点灯	アクティブ
	青色、点滅	ユーザーによって有効化されたモジュール識別
	橙色、点灯	不使用
	橙色、点滅	障害
	青色、消灯	スタンバイ
	青色、消灯	スタンバイ
サーバー	緑色、点灯	電源オン
	緑色、点滅	ファームウェアのアップロード中
	緑色、消灯	電源オフ
	青色、点灯	正常
	青色、点滅	ユーザーによって有効化されたモジュール識別
	橙色、点灯	不使用
	橙色、点滅	障害
	青色、消灯	障害なし
	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

コンポーネント	LEDの色、点滅パターン	状態
IOM (パススルー)	橙色、点滅	障害
	青色、消灯	障害なし/スタックスレープ
	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
送風装置	橙色、点灯	不使用
	橙色、点滅	障害
	青色、消灯	障害なし
	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
PSU	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
	(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、消灯	DC OK 外	

無応答 CMC のトラブルシューティング

いずれのインタフェース（ウェブインタフェース、Telnet、SSH、リモート RACADM、シリアルなど）を使用しても CMC にログインできない場合は、CMC 上の LED の観察、DB-9 シリアルポートを使用したリカバリ情報の取得、または CMC ファームウェアイメージのリカバリなどを行うことにより、CMC が機能しているかどうかを確認できます。




メモ: シリアルコンソールを使ってスタンバイ CMC にログインすることはできません。

問題特定のための LED の観察

カードの左側には LED が 2 個あります。

- 左上の LED - 電源状態を示します。点灯していない場合は、次を確認してください。
 - 少なくとも 1 台の電源装置に AC 電源がある。
 - CMC カードが正しく装着されている。取り出しハンドルを解放、または引いて CMC を取り外し、基板が完全に挿入され、ラッチが正しく閉じることを確認しながら CMC を再度挿入します。
- 左下の LED - この LED には複数の色があります。CMC がアクティブかつ実行中で、問題がない場合は下部 LED が青色になります。橙色になっている場合は、障害が検出されています。障害は次の 3 つのイベントのいずれかによって発生する可能性があります。
 - コアの障害。この場合、CMC 基板を交換する必要があります。
 - セルフテストの失敗。この場合、CMC 基板を交換する必要があります。
 - イメージの破損。この場合、CMC ファームウェアイメージをアップロードして、CMC を回復します。

 **メモ:** 通常の CMC 起動またはリセットは、そのオペレーティングシステムを完全に起動し、ログインできるようになるまでに 1 分以上かかります。アクティブ CMC では青色の LED が点灯します。冗長の 2 つの CMC 構成の場合は、スタンバイ CMC で右上の緑色の LED だけが点灯されます。

DB-9 シリアルポートからのリカバリ情報の入手

下部の LED が橙色の場合、CMC の前面にある DB-9 シリアルポートからリカバリ情報を取得できます。リカバリ情報を取得するには、次の手順を実行します。


1. CMC システムとクライアントシステムの間に NULL モデムケーブルを取り付けます。
2. 任意のターミナルエミュレータ (HyperTerminal や Minicom など) を起動します。プロンプトが表示されたら、8 ビット、パリティ無し、フロー制御無し、ボーレート 115200 の仕様を入力します。5 秒おきにコアメモリ障害がエラーメッセージを表示します。
3. <Enter> キーを押します。
リカバリプロンプトが表示されたら、追加情報を使用できます。プロンプトには、CMC スロット番号と障害タイプが表示されます。
障害の理由と、いくつかのコマンドの構文を表示するには、recover と入力し、<Enter> を押します。
プロンプト例：
recover1 [セルフテスト] CMC 1 セルフテストの失敗
recover2 [FW イメージ不良] CMC2 に破損したイメージがあります
 - プロンプトがセルフテストの失敗を示している場合、CMC にはサービス可能なコンポーネントはありません。CMC が不良であることから、Dell に返品する必要があります。
 - プロンプトが FW イメージ不良を示している場合は、「[ファームウェアイメージのリカバリ](#)」のタスクを完了します。


ファームウェアイメージのリカバリ

正常な CMC OS の起動が不可能な場合、CMC はリカバリモードになります。リカバリモードでは、ファームウェアアップデートファイル **firmitg.cmc** をアップロードすることによってフラッシュデバイスを再プログラムできる、少数のコマンドのサブセットを使用することができます。このファームウェアイメージファイルは、正常なファームウェアアップデートで使用されるものと同じファイルです。リカバリプロセスは現在のアクティビティを表示し、完了時に CMC OS を起動します。

リカバリ プロンプトで recover と入力して <Enter> を押すと、回復理由と使用可能なサブコマンドが表示されます。リカバリシーケンス例は次のとおりです。

```
recover getniccfg recover setniccfg 192.168.0.120 255.255.255.0 192.168.0.1
recover ping 192.168.0.100 recover fwupdate -g -a 192.168.0.100
```

 **メモ:** ネットワークケーブルを左端の RJ45 に接続します。

 **メモ:** リカバリモードでは、アクティブなネットワークスタックがないため、通常の方法で CMC を ping することはできません。recover ping <TFTP server IP> コマンドを使うことで、TFTP サーバーを ping して LAN 接続を確認できます。一部のシステムでは、setniccfg コマンド後に recover reset コマンドを使用する必要がある場合があります。

ネットワーク問題のトラブルシューティング

内部 CMC トレースログでは、CMC アラートとネットワークのデバッグを行うことが可能です。トレースログには CMC ウェブインタフェースまたは RACADM を使ってアクセスできます。『iDRAC7 および CMC 向けコマンドラインリファレンスガイド』の gettracelog の項を参照してください。

トレースログは次の情報を追跡します。


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

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

コントローラのトラブルシューティング

コントローラをトラブルシューティングするには、次の手順を実行します。

1. 左ペインで、**シャーシ概要** → **ストレージ** → **コントローラ** → **トラブルシューティング** をクリックします。
2. **コントローラトラブルシューティング** ページで、各コントローラに対応する **処置** ドロップダウンリストから次のいずれかを選択し、**適用** をクリックします。
 - **設定のリセット** - 仮想ディスクとホットスペアを削除します。ただし、ディスク上のデータは消去されません。
 - **TTY ログのエクスポート** - ストレージコントローラからの TTY デバッグログがローカルシステムにエクスポートされます。

 **メモ:** 固定キャッシュが存在する場合、それをクリアするオプションが存在します。固定キャッシュが存在しない場合は、このオプションは表示されません。

LCD パネルインタフェースの使用

LCD パネルを使用して設定と診断を実行したり、シャーシやそのコンテンツの状態情報を取得することができます。

次の図は、LCD パネルの図解です。LCD 画面には、メニュー、アイコン、画像、およびメッセージが表示されます。

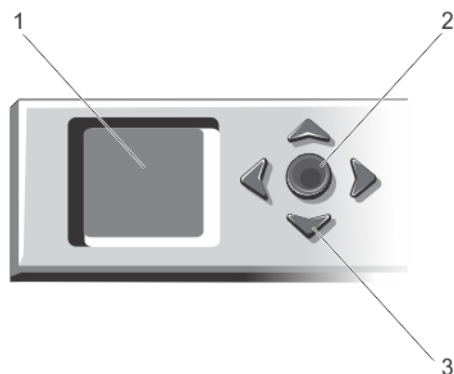


図 2. LCD ディスプレイ

1. LCD 画面
2. 選択（「チェック」）ボタン
3. スクロールボタン（4）

LCD のナビゲーション

LCD パネルの右側には 5 つのボタン（4 つの矢印ボタン（上下左右）と中央ボタン）があります。

- 画面間を移動するには、右（次へ）および左（前へ）矢印ボタンを使用します。パネルの使用中にはいつでも前の画面に戻ることができます。
- 画面上のオプション間を移動するには、上下の矢印ボタンを使用します。
- 画面上の項目を選択して保存し、次の画面へ移動するには、中央ボタンを使用します。

上、下、左、および右矢印ボタンは、画面上で選択されているメニュー項目またはアイコンを変更します。選択された項目は水色の背景、または枠付きで表示されます。

LCD 画面に表示されたメッセージが画面の幅よりも長い場合は、左右の矢印ボタンを使ってテキストを左と右にスクロールします。

次の表で説明するアイコンは、LCD 画面間の移動に使用されます。

表 33. LCD パネルのナビゲーション用アイコン

標準アイコン



ハイライト表示アイコン



アイコン名および説明

戻る — 前の画面に戻るには、中央ボタンをハイライトして押します。




確定/はい — 変更を確定して前の画面に戻るには、中央ボタンをハイライトして押します。

スキップ/次へ — 変更をスキップして次の画面に進むには、中央ボタンをハイライトして押します。

いいえ — 質問に「いいえ」と答え、次の画面に進むには、中央ボタンをハイライトして押します。

コンポーネント識別 — コンポーネントの青色 LED を点滅させます。

 **メモ:** コンポーネント識別が有効になると、このアイコンを囲む青い長方形が点滅します。

LCD パネル上の状態インジケータ LED は、シャーシとそのコンポーネントの全体的な正常性目安を提供します。

- 青色の点灯は、正常性が良好であることを示します。
- 橙色の点滅は、少なくとも 1 つのコンポーネントに障害があることを示します。
- 青色の点滅は、シャーシグループ内の 1 つのシャーシを識別するために使用される ID 信号です。

メインメニュー

メインメニュー から次のいずれかの画面に移動できます。

- **KVM マッピング** - サーバーに対して KVM をマッピングまたはマッピング解除するオプションがあります。
- **DVD マッピング** - このオプションは、DVD ドライブがインストールされている場合のみ **メインメニュー** に表示されます。
- **エンクロージャ** - シャーシの状態情報を表示します。
- **IP サマリ** - CMC IPv4、CMC IPv6、iDRAC IPv4、および iDRAC 4 IPv6 の情報を表示します。
- **設定 - LCD 言語、シャーシの向き、デフォルト LCD 画面、およびネットワーク設定** などのオプションがあります。

KVM マッピングメニュー


このページを使用することにより、KVM からサーバーへのマッピング情報の表示、KVM への別のサーバーのマップ、または既存の接続のマッピング解除を行うことができます。サーバー用に KVM を使用するには、メインメニューから **KVM マッピング** を選択し、適切なサーバーに移動して、中央の **チェック** ボタンを押します。

DVD マッピング

このページを使用することにより、DVD からサーバーへのマッピング情報の表示、別のサーバーのシャーシ上 DVD ドライブへのマップ、または既存の接続のマッピング解除を行うことができます。サーバーが DVD にアクセスできるようにするには、メインメニューから **DVD マッピング** を選択し、必要なサーバーまで移動して、中央の **チェック** ボタンを押します。

DVD ドライブをサーバースロットにマップできるのは、そのサーバースロットに対して DVD が有効になっている場合のみです。DVD ドライブは、いずれのサーバースロットからも使用されないように、マッピングを

解除することもできます。DVD ドライブとメイン基板との間で SATA ケーブルが正しく接続されていないと、DVD ドライブの正常性が重要状態になります。DVD ドライブの正常性が重要状態の場合、サーバーは DVD ドライブにアクセスできません。

 **メモ:** DVD マッピング機能は、DVD ドライブが取り付けられている場合にのみ、LCD のメインメニュー画面に表示されます。

エンクロージャメニュー

この画面から、次の画面に移動できます。

- 前面状態
- 背面
- 側面
- エンクロージャ状態

ナビゲーションボタンを使用して希望のアイテムをハイライト表示し（メインメニューに戻るには戻るアイコンをハイライト表示）、中央ボタンを押します。選択した画面が表示されます。

IP 概要メニュー

IP 概要画面には、CMC (IPv4 および IPv6) と、シャーシに取り付けられている各サーバーの IP 情報が表示されます。

上下矢印ボタンを使ってリスト内をスクロールします。画面に収まりきらない長さの選択済みメッセージをスクロールするには、左右矢印ボタンを使用します。

エンクロージャメニューに戻るには、上下矢印ボタンを使って戻るアイコンを選択し、中央のボタンを押します。

設定

設定メニューには、設定可能アイテムのメニューが表示されます。

- **LCD 言語** - LCD 画面のテキストとメッセージに使用する言語を選択します。
- **シャーシの向き** - シャーシの取り付け方向に基づいて、タワーモードかラックモードを選択します。
- **デフォルト LCD 画面** - LCD パネルにアクティビティがない場合に表示される画面（メインメニュー、前面状態、背面状態、側面状態、またはカスタム）を選択します。
- **ネットワーク設定** - これを選択して CMC のネットワーク設定を行います。この機能の詳細については、[「LCD パネルインタフェースを使用した CMC ネットワークの設定」](#)を参照してください。

上下矢印ボタンを使ってメニュー内のアイテムをハイライト表示するか、メインメニュー画面に戻る場合は戻るアイコンをハイライト表示します。

選択をアクティブにするには、中央のボタンを押します。

設定

設定メニューには、設定可能アイテムのメニューが表示されます。

- **LCD 言語** - LCD 画面のテキストとメッセージに使用する言語を選択します。
- **シャーシの向き** - シャーシの取り付け方向に基づいて、タワーモードかラックモードを選択します。
- **デフォルト LCD 画面** - LCD パネルにアクティビティがない場合に表示される画面（メインメニュー、前面状態、背面状態、側面状態、またはカスタム）を選択します。
- **ネットワーク設定** - これを選択して CMC のネットワーク設定を行います。この機能の詳細については、[「LCD パネルインタフェースを使用した CMC ネットワークの設定」](#)を参照してください。

上下矢印ボタンを使ってメニュー内のアイテムをハイライト表示するか、**メインメニュー** 画面に戻る場合は**戻る** アイコンをハイライト表示します。

選択をアクティブにするには、中央のボタンを押します。

LCD 言語

LCD 言語 画面では、LCD パネルメッセージに使用する言語を選択することができます。現在アクティブな言語が、水色背景でハイライト表示されます。

1. 上下左右の矢印ボタンを使って任意の言語をハイライト表示します。
2. 中央ボタンを押します。**確定** アイコンがハイライト表示されます。
3. 中央ボタンを押して変更を確認します。**LCD セットアップ** メニューが表示されます。

デフォルト画面

デフォルト画面 では、LCD パネルでアクティビティがないときにパネルが表示する画面を変更することができます。工場出荷時のデフォルト画面は**メインメニュー** です。表示する画面は次から選択できます。

- **メインメニュー**
- **前面状態** (シャーシの前面図)
- **背面状態** (シャーシの背面図)
- **側面状態** (シャーシの左側面図)
- **カスタム** (シャーシ名を伴う Dell のロゴ)

現在アクティブなデフォルト画面が水色でハイライト表示されます。

1. 上下の矢印キーを使って、デフォルトに設定する画面をハイライト表示します。
2. 中央ボタンを押します。**確定** アイコンがハイライト表示されます。
3. 中央ボタンを再度押して変更を確認します。**デフォルト画面** が表示されます。

診断

LCD パネルはシャーシ内の任意のサーバーまたはモジュールの問題の診断に役立ちます。シャーシ、またはシャーシ内のサーバーやその他モジュールに問題または障害がある場合、LCD パネルの状態インジケータが橙色に点滅します。**メインメニュー** では、問題のあるサーバーやモジュールを指すメニューアイテム (サーバー または エンクロージャ) の横にアイコンが橙色の背景で表示されます。

LCD メニューシステムで橙色のアイコンをたどっていくことにより、問題のあるアイテムの状態画面とエラーメッセージを表示できます。

LCD パネルのエラーメッセージは、問題の原因となっているモジュールやサーバーの取り外し、またはモジュールやサーバーのハードウェアログのクリアによって削除できます。サーバーエラーでは、iDRAC ウェブインタフェースまたはコマンドラインインタフェースを使用して、サーバーのシステムイベントログ (SEL) をクリアします。シャーシエラーでは、CMC ウェブインタフェースまたはコマンドラインインタフェースを使用して、ハードウェアログをクリアします。

前面パネル LCD メッセージ

このセクションには2つのサブセクションがあり、前面パネル LCD に表示されるエラーと状態情報をリストにします。

LCD の エラーメッセージの形式は、CLI またはウェブインタフェースで表示されるシステムイベントログ (SEL) に似ています。

エラーセクションの表は、各種 LCD 画面に表示されるエラーおよび警告メッセージと、考えられるメッセージの原因をリストします。山括弧 (<>) で囲まれたテキストは、そのテキストが様々であることを示します。

LCD の状態情報には、シャーシ内のモジュールについての記述的信息が含まれます。このセクションの表には、各コンポーネントに対して表示される情報が説明されています。

LCD モジュールとサーバー状態情報

本項の表では、シャーシ内のコンポーネントタイプごとに前面パネル LCD に表示される状態項目について説明します。

表 34. CMC の状態

項目	説明
例：CMC1、CMC2	名前/場所。
エラーなし	何もエラーが発生していない場合は「エラーなし」が表示され、エラーがある場合はエラーメッセージがリストされます。
ファームウェアバージョン	アクティブな CMC についてのみ表示されます。スタンバイ CMC にはスタンバイと表示されます。
IP4 <有効、無効>	アクティブな CMC についてのみ、現在の IPv4 有効化状況を表示します。
IP4 アドレス：<アドレス、取得中>	アクティブな CMC についてのみ、IPv4 が有効化されているかどうかだけを表示します。
IP6 <有効、無効>	アクティブな CMC についてのみ、現在の IPv6 有効化状況を表示します。
IP6 ローカルアドレス：<アドレス>	アクティブな CMC についてのみ、IPv6 が有効化されているかどうかだけを表示します。
IP6 グローバルアドレス：<アドレス>	アクティブな CMC についてのみ、IPv6 が有効化されているかどうかだけを表示します。

表 35. シャーシまたはエンクロージャ状態

項目	説明
ユーザー定義名	例：「Dell Rack System」。これは、CMC CLI またはウェブ GUI で設定可能です。
エラーメッセージ	エラーがない場合は、エラーなしが表示されます。それ以外の場合は、エラーメッセージが重要エラー、警告の順にリストされます。
モデル番号	例：「PowerEdgeM1000」。
電力消費量	現在のワット単位での電力消費量です。
ピーク電力	ワット単位のピーク電力消費量です。
最小電力	ワット単位の最小電力消費量です。
周囲温度	現在の摂氏での周辺温度です。
サービスタグ	工場出荷時に割り当てられたサービスタグです。

項目	説明
CMC 冗長性モード	非冗長または冗長になります。
PSU 冗長性モード	非冗長、AC 冗長、または DC 冗長になります。

表 36. ファン状態

項目	説明
名前 / 場所	例：ファン 1、ファン 2、など。
エラーメッセージ	エラーがない場合は、「エラーなし」表示されます。それ以外の場合は、エラーメッセージが重要エラー、警告の順で表示されます。
RPM	現在のファン速度（RPM）です。

表 37. PSU 状態



項目	説明
名前 / 場所	例：PSU1、PSU2、など。
エラーメッセージ	エラーがない場合は、「エラーなし」表示されます。それ以外の場合は、エラーメッセージが重要エラー、警告の順で表示されます。
状態	オフライン、オンライン、またはスタンバイになります。
最大ワット数	PSU がシステムに供給できる最大ワット数です。

表 38. IOM 状態

項目	説明
名前 / 場所	IOM A
エラーメッセージ	エラーがない場合は、「エラーなし」表示されます。それ以外の場合は、エラーメッセージが重要エラー、警告の順で表示されます。
状態	オフまたはオンになります。
モデル	IOM のモデルです。
ファブリックタイプ	ネットワークタイプです。
IP アドレス	IOM がオンの場合にのみ表示されます。パススルータイプ IOM の値はゼロです。
サービスタグ	工場出荷時に割り当てられたサービスタグです。

表 39. サーバー状態

項目	説明
例：サーバー 1、サーバー 2、など。	名前 / 場所。
エラーなし	エラーがない場合は、エラーなしが表示されます。それ以外の場合は、エラーメッセージが重要エラー、

項目	説明
スロット名	警告の順にリストされます。詳細については、「LCD エラーメッセージ」を参照してください。 シャーシスロット名です。例えば SLOT-01 です。  メモ: この表は、CMC CLI または Web GUI を使用して設定できます。
名前	ユーザーが Dell OpenManage を使用して設定することができるサーバーの名前です。この名前は、iDRAC の起動が完了し、サーバーがこの機能をサポートする場合のみ表示されます。そうでない場合は、iDRAC の起動メッセージが表示されます。
モデル番号	iDRAC の起動が完了すると表示されます。
サービスタグ	iDRAC の起動が完了すると表示されます。
BIOS バージョン	サーバー BIOS ファームウェアのバージョンです。
最終の POST コード	最終のサーバー BIOS POST コードメッセージ文字列を表示します。
iDRAC ファームウェアバージョン	iDRAC の起動が完了すると表示されます。  メモ: iDRAC バージョン 1.01 は 1.1 と表示されません。iDRAC バージョンに 1.10 はありません。
IP4 <有効、無効>	現在の IPv4 の有効化状況を表示します。
IP4 アドレス : <アドレス、取得中>	IPv4 が有効な場合にのみ表示されます。
IP6 <有効、無効>	iDRAC が IPv6 をサポートする場合にのみ表示されます。現在の IPv6 有効化状況を表示します。
IP6 ローカルアドレス : <アドレス>	iDRAC が IPv6 をサポートし、かつ IPv6 が有効な場合にのみ表示されます。
IP6 グローバルアドレス : <アドレス>	iDRAC が IPv6 をサポートし、かつ IPv6 が有効な場合にのみ表示されます。
ファブリック上で有効化された FlexAddress	機能がインストールされている場合にのみ表示されます。このサーバー用に有効化されたファブリックをリストします (つまり、A、B、C)。

表の情報は動的にアップデートされます。サーバーがこの機能をサポートしていない場合は、次の情報は表示されません。サポートしている場合は、サーバー管理者のオプションは次のとおりです。

- オプション「なし」= LCD には一切の文字列を表示しない。
- オプション「デフォルト」= 影響なし。
- オプション「カスタム」= サーバー名の文字列が入力可能。

この情報は、iDRAC の起動が完了している場合にのみ表示されます。この機能の詳細については、『PowerEdge VRTX の CMC 向け RACADM コマンドラインリファレンスガイド』を参照してください。

よくあるお問い合わせ (FAQ)

本項では、次にに関するよくあるお問い合わせをリストします。

- RACADM
- リモートシステムの管理と復元
- Active Directory
- FlexAddress と FlexAddressPlus
- iKVM

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 <サブコマンド> 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 コマンドが失敗しました。
```

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

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?

リモートアクセス : SNMP 認証エラー

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` コミュニティ名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 cfgOobSnmpp
```

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 cfgOobSnmpp -o cfgOobSnmppAgentCommunity <コミュニティ名>
```

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 sslcsrngen [-g] [-f {filename}]
racadm sslcertupload -t 1 -f {web_sslcert}
```

FlexAddress と FlexAddressPlus

機能カードが取り外されるとどうなりますか?

機能カードが取り外されても、特に変化はありません。機能カードは取り外して保管、またはそのままにしておくことができます。

あるシャーシで使用していた機能カードを取り外し、別のシャーシに取り付けるとどうなりますか?

ウェブインタフェースが次のエラーメッセージを表示します。

この機能カードは別のシャーシでアクティブ化されています。FlexAddress 機能にアクセスする前に取り外す必要があります。

現在のシャーシサービスタグ = XXXXXXXX

機能カードのシャーシサービスタグ = YYYYYYYY

CMC ログに次のエントリが追加されます。

```
cmc <日付タイムスタンプ> : feature 'FlexAddress@YYYYYYYY' not activated; chassis ID='XXXXXXXX'
```

機能カードが取り外され、非 FlexAddress カードが取り付けられるとどうなりますか？

カードのアクティブ化や変更はいずれも行われません。カードは CMC によって無視されます。この場合、**\$racadm featurecard -s** コマンドが次のメッセージを返します。

機能カードが挿入されていません。

エラー: ファイルを開くことができません

シャーシのサービスタグが再プログラムされた場合、そのシャーシにバインドされている機能カードはどうなりますか？

- そのシャーシ、または他のシャーシのアクティブな CMC に元の機能カードが存在する場合、ウェブインタフェースが次のエラーメッセージを表示します。
This feature card was activated with a different chassis. It must be removed before accessing the FlexAddress feature.
Current Chassis Service Tag = XXXXXXXX
Feature Card Chassis Service Tag = YYYYYYYY
デルサービスが元のシャーシサービスタグの再プログラムを行ってシャーシに戻し、そのシャーシで元の機能カードを持つ CMC がアクティブ化されない限り、元の機能カードはそのシャーシ、または他のどのシャーシでも非アクティブ化の対象にはなりません。
- FlexAddress 機能は本来バインドされていたシャーシでアクティブ状態が維持されます。そのシャーシ機能のバインディングは、新規サービスタグを反映するようにアップデートされます。

2つの機能カードが冗長 CMC システムに取り付けられた場合、エラーメッセージが表示されますか？

アクティブ CMC の機能カードがアクティブで、シャーシに取り付けられます。2番目のカードは CMC によって無視されます。

SD カードには、書き込み防止ロック機能はありますか？

はい、あります。SD カードを CMC モジュールにインストールする前に、書き込み防止ラッチがアンロックの位置にあることを確認してください。SD カードが書き込み防止されていると、FlexAddress 機能をアクティブ化することはできません。この場合、**\$racadm feature -s** コマンドが次のメッセージを返します。

このシャーシにはアクティブな機能はありません。ERROR: 読み取り専用ファイルシステム

アクティブな CMC モジュールに SD カードが存在しないと、どうなりますか？

\$racadm featurecard -s コマンドを実行すると、次のメッセージが返されます。

機能カードが挿入されていません。

サーバー BIOS のバージョンがバージョン 1.xx から 2.xx にアップデートされると FlexAddress 機能はどうなりますか？

サーバーモジュールは、FlexAddress と併用する前に電源をオフにする必要があります。サーバー BIOS アップデートの完了後、サーバーモジュールはサーバーがパワーサイクルされるまでシャーシ割り当てのアドレスを取得しません。

FlexAddress で deactivation コマンドが実行されたときにシャーシに SD カードがなかった場合、どのように SD カードを回復できますか？


問題は、FlexAddress が無効化されたときに SD カードが CMC になかった場合、別のシャーシに FlexAddress をインストールするためにそのカードを使用できないということです。カードを使用できるように回復するには、バインドされているシャーシの CMC にそのカードを挿入し直し、FlexAddress を再インストールして、その後 FlexAddress を非アクティブ化します。

SD カードが正しく取り付けられ、ファームウェアまたはソフトウェアのアップデートもすべてインストール済みです。FlexAddress がアクティブですが、サーバー導入画面に導入オプションが表示されません。何が間違っていますか？

これは、ブラウザのキャッシュの問題です。ブラウザからログオフし、再起動してください。

RACADM コマンド `racresetcfg` を使用してシャーシ設定をリセットする必要がある場合、FlexAddress はどうなりますか？

FlexAddress 機能は引き続きアクティブ状態で使用可能です。すべてのファブリックとスロットがデフォルトとして選択されています。

 **メモ:** RACADM コマンド `racresetcfg` を実行する前には、シャーシの電源をオフにすることを強くお勧めします。

FlexAddressPlus 機能のみを無効にした後（FlexAddress はアクティブのまま）、まだアクティブな CMC 上で `racadm setflexaddr` コマンドが失敗するのはなぜですか？

FlexAddressPlus 機能カードがカードスロットに入ったままで、後から CMC がアクティブ化されると、FlexAddressPlus 機能が再アクティブ化され、スロットまたはファブリックの FlexAddress 設定の変更を再開できます。

IOM

設定変更後、CMC に IP アドレスが 0.0.0.0 と表示されることがあります。

更新 アイコンをクリックして、IP アドレスがスイッチで正しく設定されているかどうかを確認します。IP/マスク/ゲートウェイの設定でエラーがあった場合、スイッチは IP アドレスを設定せず、すべてのフィールドで 0.0.0.0 を返します。

一般的なエラーには、次が含まれます。

- 帯域外 IP アドレスを帯域内管理 IP アドレスと同じ IP アドレス、または同じネットワーク上のアドレスに設定。
- 無効なサブネットマスクを入力。
- デフォルトゲートウェイを、スイッチに直接接続されているネットワーク上にないアドレスに設定。