Dell™ Chassis Management Controllerファームウェアバージョン 2.10 ユーザーガイド

メモおよび注意

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: 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。

本書の内容は予告なく変更されることがあります。
© 2009 すべての著作権は Dell Inc. にあります。

Dell Inc. の書面による許可のない複製は、いかなる形態においても厳重に禁じられています。

本文書で使用される商標：Dell、DELL ロゴ、FlexAddress、OpenManage、PowerEdge、PowerConnect は、Dell Inc. の商標です。Microsoft、Active Directory、Internet Explorer、Windows、Windows NT、Windows Server、Windows Vista は、米国内および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、米国内および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、米国内およびその他の国における Novell Corporation の登録商標です。Intel は、Intel Corporation の登録商標です。UNIX は、米国内およびその他の国における The Open Group の登録商標です。Avocent は Avocent Corporation の商標であり、OSCAR は Avocent Corporation およびその関連会社の登録商標です。

Copyright 1998-2006 The OpenLDAP Foundation.All rights reserved.ソースおよびバイナリ形式での再配布は、変更の有無を問わず、OpenLDAP の公開ライセンスで承認されている範囲内でのみ許可されます。このライセンスのコピーは、配布パッケージ内の最上位レベルのディレクトリに入っている LICENSE ファイル、または **http://www.OpenLDAP.org/license.html**でご覧いただけます。OpenLDAP はOpenLDAP Foundation の登録商標です。個々のファイルや提供パッケージは、他社が著作権を所有している場合があり、その他の制約を受ける可能性があります。この製品はミシガン大学 LDAP v3.3 配布から派生しています。この製品には、公共ソースから派生した材料も含まれています。OpenLDAP に関する情報は **http://www.openldap.org/** から入手できます。Portions Copyright 1998-2004 Kurt D.Zeilenga.Portions Copyright 1998-2004 Net Boolean Incorporated.Portions Copyright 2001-2004 IBM Corporation.All rights reserved.ソースおよびバイナリ形式での再配布は、変更の有無を問わず、OpenLDAP の公開ライセンスで承認されている範囲内でのみ許可されます。Portions Copyright 1999-2003 Howard Y.H.Chu.Portions Copyright 1999-2003 Symas Corporation.Portions Copyright 1998-2003 Hallvard B.Furuseth.All rights reserved.ソースおよびバイナリ形式での再配布と使用は、変更の有無を問わず、この著作権表示を含めた形式でのみ許可されます。著作権所有者の名前を、書面による事前の許可なく、このソフトウェアの派生製品を推薦または宣伝する目的で使用することはできません。このソフトウェアは、明示または黙示の保証なしに「現状のまま」提供されます。Portions Copyright (c) 1992-1996 Regents of the University of Michigan.All rights reserved.ソースおよびバイナリ形式での再配布と使用は、この著作権表示を含め、米国アン・アーバーのミシガン大学への謝辞を記載した場合にのみ許可されます。この大学名を、書面による事前の許可なく、このソフトウェアの派生製品を推薦または宣伝する目的で使用することはできません。このソフトウェアは、明示または黙示の保証なしに「現状のまま」提供されます。

商標または製品の権利を主張する事業体を表すためにその他の商標および社名が使用されていることがあります。Dell Inc. はデル以外の商標や社名に対する所有権を一切否認します。

2009 年 8 月

目次ページに戻る

CMC と Microsoft Active Directory との併用

Dell™ Chassis Management Controllerファームウェアバージョン 2.10 ユーザーガイド

ディレクトリサービスは、ネットワーク上のユーザー、コンピュータ、プリンタなどを制御するのに必要なすべての情報を格納する共通のデータベースを管理しています。貴社が Microsoft® Active Directory® サービスソフトウェアを使用している場合は、CMC へのアクセスを提供するようにソフトウェアを設定できます。これにより、Active Directory ソフトウェアの既存のユーザーに CMC ユーザー権限を追加して管理できます。

メモ: Microsoft Windows® 2000 および Windows Server® 2003 オペレーティングシステムでは Active Directory を使用して CMC のユーザーを認識できます。IPv6 経由の Active Directory は、Windows 2008 でのみサポートされています。

Active Directory スキーマ拡張

Active Directory で CMC へのユーザーアクセスを定義するには、次の 2 つの方法があります。

- デルによって定義された Active Directory オブジェクトを使用する拡張スキーマソリューション。
- 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。

拡張スキーマと標準スキーマの比較

Active Directory を使って CMC へのアクセス権を設定するには、拡張スキーマまたは標準スキーマソリューションのどちらかを選択する必要があります。

拡張スキーマソリューションの場合

- アクセス制御オブジェクトのすべてを Active Directory で管理できます。
- さまざまな CMC で異なる特権レベルのユーザーアクセスを設定できるため、最大の柔軟性を実現します。

標準スキーマソリューションの場合

- 標準スキーマは Active Directory オブジェクトのみを使用するためスキーマ拡張は不要です。
- Active Directory 側での設定が簡単。

拡張スキーマの概要

拡張スキーマ Active Directory を有効にするには、次の 2 つの方法があります。

- CMC ウェブインタフェースを使用する。 手順については、「拡張スキーマ Active Directory とウェブインタフェースを使用した CMC の設定」を参照してください。
- RACADM CLI ツールを使用する。手順については、「拡張スキーマ Active Directory と RACADM を使用した CMC の設定」を参照してください。

Active Directory スキーマ拡張

Active Directory データは、属性とクラスの分散データベースです。Active Directory スキーマには、データベースに追加または挿入するデータタイプを決定する規則があります。

データベースに格納されるクラスの一例として user class があります。ユーザークラスの属性には、ユーザーの姓、名、電話番号などが含まれます。

貴社の環境の固有なニーズを満たす独自の属性やクラスを追加して、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、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 スキーマに追加した属性やクラスは、それぞれ固有の ID で定義する必要があります。業界全体で一意の ID を維持できるよう、Microsoft は Active Directory オブジェクト識別子(OID)のデータベースを管理しています。Microsoft の Active Directory でスキーマを拡張するために、デルは固有の OID、固有の名前拡張子、デル固有の属性とクラスに一意に関連付けた属性 ID を確立しました。

デルの拡張子:dell

デルのベース OID:1.2.840.113556.1.8000.1280

RAC LinkID 範囲:12070–2079

RAC スキーマ拡張の概要

デルは管理者が設定できるプロパティのグループを提供しています。デルの拡張スキーマには、関連、デバイス、特権などのプロパティが含まれます。

関連プロパティは、特定の特権セットのあるユーザーまたはグループを 1 台または複数台の RAC デバイスに関連付けます。このモデルでは、ユーザー、RAC 権限、およびネットワーク上の RAC デバイスを組み合わせる際に最大限の柔軟性が得られる一方、複雑になり過ぎることはありません。

Active Directory オブジェクトの概要

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ーでもかまいません。

ただし、各関連オブジェクトは 1 つの権限オブジェクトにしかリンクできず、ユーザー、ユーザーグループ、RAC デバイスオブジェクトを 1 つの権限オブジェクトにしかリンクできません。この例では、システム管理者 は特定のCMC で各ユーザーの権限を制御できます。

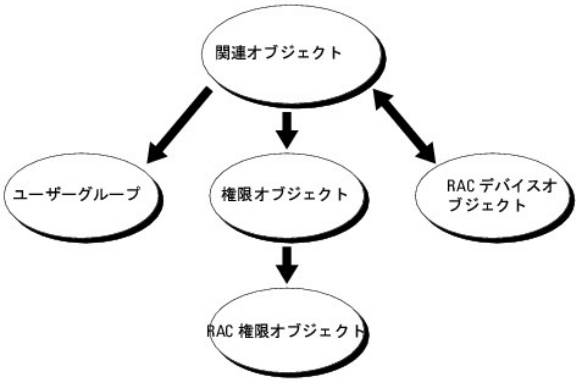
RAC デバイスオブジェクトは、Active Directory に照会して認証と許可を実行するための RAC ファームウェアへのリンクです。RAC をネットワークに追加した場合、システム管理者は RAC とそのデバイスオブジェクトをその Active Directory 名で設定して、ユーザーが Active Directory で認証と認可を実行できるようにする必要があります。さらに、ユーザーが認証できるように、RAC を少なくとも 1 つの関連オブジェクトに追加する必要があります。

図7-1 は、関連オブジェクトがすべての認証と認可に必要な関連付けを提供する仕組みを示しています。

メモ: RAC 特権オブジェクトは DRAC 4、DRAC 5、および CMC に適用します。

作成する関連オブジェクトの数に制限はありません。ただし、関連オブジェクトを少なくとも 1 つ作成する必要があり、Active Directory と統合する各 RAC(CMC)につき 1 つの RAC デバイスオブジェクトが必要です。

図 7-1 Active Directory オブジェクトの典型的なセットアップ

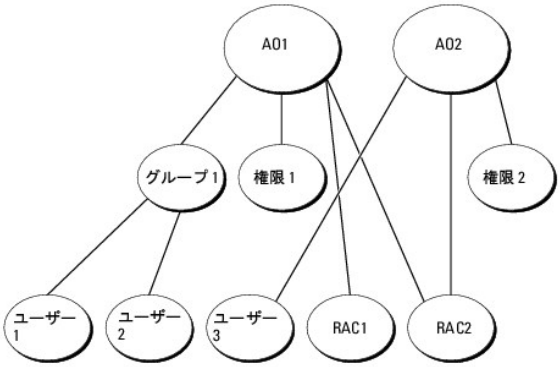


関連オブジェクトに含むことができるユーザー、グループ、RAC デバイスオブジェクトの数に制限はありません。ただし、関連オブジェクトに含むことができる権限オブジェクトは、関連オブジェクト 1 つに 1 つだけです。関連オブジェクトは、RAC(CMC)に「特権」を持つ「ユーザー」を接続します。

また、Active Directory オブジェクトは、単一ドメイン、複数のドメインのいずれに設定することも可能です。たとえば、CMC が 2 つ(RAC1、RAC2)と、既存の Active Directory ユーザーが 3 つ(ユーザー 1、ユーザー 2、ユーザー 3)あるとし、ユーザー 1 とユーザー 2 に 両方の CMC へのシステム管理者権限を与え、ユーザー 3 に RAC2 カードへのログイン特権を与えたいとします。図7-2 に、このシナリオで Active Directory オブジェクトを設定する方法を示します。

別のドメインからユニバーサルグループを追加する場合、ユニバーサルスコープで関連オブジェクトを作成します。Dell Schema Extender Utility で作成された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、他のドメインからのユニバーサルグループとは連動しません。

図 7-2 単一ドメインでの Active Directory オブジェクトの設定



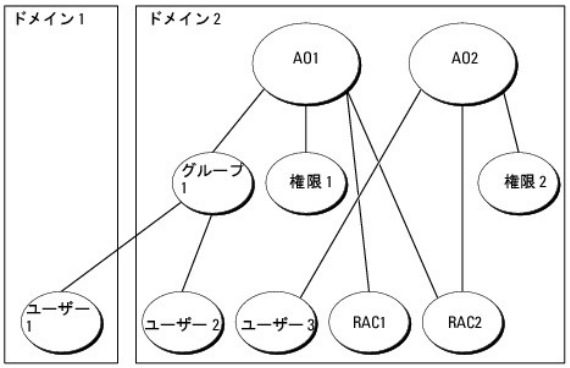
単一ドメインのシナリオでオブジェクトを設定するには

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 をまとめてグループ 1 とします。
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。

詳細な手順については、「Active Directory への CMC ユーザーと特権の追加」を参照してください。

図7-3 に、複数ドメインの Active Directory オブジェクトの例を示します。このシナリオでは、CMC が 2 つ(RAC1 と RAC2)と、既存の Active Directory ユーザーが 3 つ(ユーザー 1、ユーザー 2、ユーザー 3)あるとします。ユーザー 1 はドメイン 1 に存在し、ユーザー 2 とユーザー 3 はドメイン 2 に存在しています。このシナリオでは、ユーザー 1 とユーザー 2 に両方の CMC へのシステム管理者特権を持つように設定し、ユーザー 3 に RAC2 カードへのログイン特権を持つようにします。

図 7-3 複数ドメインでの Active Directory オブジェクトの設定



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。

   図7-3 に、ドメイン 2 のオブジェクトを示します。
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 をまとめてグループ 1 とします。グループ 1 のグループスコープはユニバーサルでなければなりません。
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。

CMC にアクセスするための拡張スキーマ Active Directory の設定

Active Directory を使用して CMC にアクセスする前に、Active Directory ソフトウェアと CMC を設定します。

1. Active Directory スキーマを拡張します。(「Active Directory スキーマの拡張」を参照)
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(「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」を参照)。
3. CMC ユーザーとその権限を Active Directory に追加します(「Active Directory への CMC ユーザーと特権の追加」を参照)。
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 プロパティを設定します(「拡張スキーマ Active Directory とウェブインタフェースを使用した CMC の設定」または「拡張スキーマ Active Directory と RACADM を使用した CMC の設定」を参照)。

Active Directory スキーマの拡張

Active Directory スキーマを拡張すると、Dell の組織単位、スキーマのクラスと属性、サンプル権限、および関連オブジェクトが Active Directory スキーマに追加されます。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ー Flexible Single Master Operation(FSMO)Role Owner にスキーマ管理者特権を持っていることを確認してください。

次のいずれかの方法を使用してスキーマを拡張できます。

- 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 and Documentation DVD』の次のディレクトリに入っています。

- **<DVDdrive>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\<installation type>\LDIF Files**
- **<DVDdrive>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_ Tools\<installation type>\Schema Extender**

LDIF ファイルを使用するには、**LDIF_Files** ディレクトリにある readme の説明を参照してください。Active Directory スキーマを拡張するために Dell Schema Extender を利用する手順については、「Dell Schema Extender の使用」を参照してください。

Schema Extender または LDIF ファイルのコピーと実行はどの場所からでもできます。

Dell Schema Extender の使用

△ **注意: Dell Schema Extender 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しく機能するように、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. 警告を読んでから、もう一度 次へ をクリックします。
3. **資格情報で現在のログの使用** を選択するか、スキーマ Administrator 権限でユーザー名とパスワードを入力します。
4. Dell Schema Extender を実行するには、**次へ**をクリックします。
5. **完了** 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、Microsoft 管理コンソール (MMC) と Active Directory スキーマスナップインを使用して、次のものがあることを確認します。

- クラス― 「表7-1」～「表7-6」を参照
- 属性 ― 「表7-7」を参照

MMC で Active Directory スキーマスナップインを有効にして使用する方法については、Microsoft のマニュアルを参照してください。

表 7-1 Active Directory に追加されるクラスのクラス定義固有の属性

クラス名	割り当てられるオブジェクト識別番号(OID)
dellRacDevice	1.2.840.113556.1.8000.1280.1.1.1.1
dellAssociationObject	1.2.840.113556.1.8000.1280.1.1.1.2
dellRACPrivileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

表 7-2 dellRacDevice クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.1
説明	Dell RAC デバイスを表します。RAC デバイスは Active Directory では dellRacDevice として設定する必要があります。この設定にすると、CMC から Active Directory に Lightweight Directory Access Protocol(LDAP)クエリを送信できます。
クラスの種類	構造体クラス
SuperClasses	dellProduct
属性	**dellSchemaVersion** **dellRacType**

表 7-3 dellAssociationObject クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.2

説明	Dell 関連オブジェクトを表します。この関連オブジェクトはユーザーとデバイスの間の接続を提供します。
クラスの種類	構造体クラス
SuperClasses	グループ
属性	**dellProductMembers** **dellPrivilegeMember**

表 7-4 dellRAC4Privileges クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.3
説明	CMC デバイスの承認権限(特権)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 7-5 dellPrivileges クラス

OID	1.2.840.113556.1.8000.1280.1.1.1.4
説明	Dell の特権(承認権限)のコンテナクラス。
クラスの種類	構造体クラス
SuperClasses	ユーザー
属性	**dellRAC4Privileges**

表 7-6 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 7-7 Active Directory スキーマに追加された属性のリスト

割り当てられる 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:このロールに属する 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: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:dellIsUserConfigAdmin 説明:ユーザーがデバイスのユーザー設定システム管理者権限がある場合には TRUE。	-
OID:1.2.840.113556.1.8000.1280.1.1.2.5 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
属性:dellIsLogClearAdmin 説明:ユーザーがデバイスのログのクリアシステム管理者権限がある場合には TRUE。	-
OID:1.2.840.113556.1.8000.1280.1.1.2.6 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
属性:dellIsServerResetUser 説明:ユーザーがデバイスのサーバーリセット権限がある場合には TRUE。	-
OID:1.2.840.113556.1.8000.1280.1.1.2.7 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
属性:dellIsTestAlertUser 説明:ユーザーがデバイスのテスト警告ユーザー権限がある場合には TRUE。	-
OID:1.2.840.113556.1.8000.1280.1.1.2.10 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
属性:dellIsDebugCommandAdmin 説明:ユーザーがデバイスのデバッグコマンドシステム管理者権限がある場合には TRUE。	-
OID:1.2.840.113556.1.8000.1280.1.1.2.11 ブール (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
属性:dellSchemaVersion 説明:現在のスキーマバージョンを使用してスキーマをアップデートします。	-
OID:1.2.840.113556.1.8000.1280.1.1.2.12 Case Ignore String(LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
属性:dellRacType 説明:この属性は dellRacDevice オブジェクトの現在の RAC タイプで、dellAssociationObjectMembers フォワードリンクへのバックワードリンクです。	-
OID:1.2.840.113556.1.8000.1280.1.1.2.13 Case Ignore String(LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
属性:dellAssociationMembers 説明:この製品に属する dellAssociationObjectMembers のリスト。この属性は dellProductMembers リンク属性へのバックワードリンクです。 リンク ID: 12071	-

OID:1.2.840.113556.1.8000.1280.1.1.2.14 識別名 (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
属性 :dellPermissionsMask1	
OID:1.2.840.113556.1.8000.1280.1.6.2.1 整数(LDAPTYPE_INTEGER)	
属性 :dellPermissionsMask2	
OID:1.2.840.113556.1.8000.1280.1.6.2.2 整数(LDAPTYPE_INTEGER)	

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

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

『Dell Systems Management Tools and Documentation DVD』を使ってシステム管理ソフトウェアをインストールする場合、インストール手順中に **Active Directory ユーザーとコンピュータ スナップインのデル拡張** を選択すると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の手順については、『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。

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。

Administrator Pack のインストール

Active Directory CMC オブジェクトを管理している各システムに、Administrator Pack をインストールする必要があります。Administrator Pack をインストールしないと、コンテナ内の Dell RAC オブジェクトを表示できません。

Active Directory ユーザーとコンピュータスナップインの開始

Active Directory ユーザーとコンピュータスナップインを開くには

1. ドメインコントローラにログインしている場合は、**スタート**→管理ツール→Active Directory ユーザーとコンピュータ の順にクリックします。

   ドメインコントローラにログインしていない場合は、適切な Microsoft Administrator Pack がローカルシステムにインストールされている必要があります。この Administrator Pack をインストールするには、**スタート→ ファイル名を指定して実行** の順にクリックし、MMC と入力して <Enter> を押します。

   Microsoft Management Console (MMC) が表示されます。

2. **コンソール 1** ウィンドウで、ファイル (または Windows 2000 を実行しているシステムではコンソール) をクリックします。
3. **スナップインの追加と削除** をクリックします。
4. Active Directory ユーザーとコンピュータ スナップインを選択し、追加 をクリックします。
5. **閉じる** をクリックして **OK** をクリックします。

Active Directory への CMC ユーザーと特権の追加

Dell の拡張 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、関連、および特権オブジェクトを作成すると、CMC のユーザーと特権を追加できます。各オブジェクトタイプを追加するには

1. RAC デバイスオブジェクトの作成
2. 権限オブジェクトの作成
3. 関連オブジェクトの作成
4. 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

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. Select **新規→ Dell RAC オブジェクト** を選択します。

   新規オブジェクト ウィンドウが表示されます。
3. 新しいオブジェクトの名前を入力します。この名前は、拡張スキーマ Active Directory とウェブインタフェースを使用した CMC の設定 の手順 8a で入力する CMC 名と同一でなければなりません。
4. **RAC デバイスオブジェクト** を選択します。
5. OK をクリックします。

権限オブジェクトの作成

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

1. **コンソールのルート**(MMC)ウィンドウでコンテナを右クリックします。
2. **新規→ Dell RAC オブジェクト** の順に選択します。

   新規オブジェクト ウィンドウが表示されます。
3. 新しいオブジェクトの名前を入力します。
4. **権限オブジェクト** を選択します。
5. OK をクリックします。
6. 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。
7. **RAC 特権** タブをクリックし、ユーザーに与える権限を選択します。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、グループタイプが含まれている必要があります。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の種類を指定します。関連オブジェクトを作成する場合は、追加するオブジェクトの種類に適用される関連スコープを選択します。

たとえば、**ユニバーサル** を選択すると、関連オブジェクトは Active Directory ドメインがネイティブモード以上で機能している場合にのみ使用可能になります。

1. **コンソールのルート**(MMC)ウィンドウでコンテナを右クリックします。
2. **新規→ Dell RAC オブジェクト** の順に選択します。

   新規オブジェクト ウィンドウが開きます。
3. 新しいオブジェクトの名前を入力します。
4. **関連オブジェクト** を選択します。
5. **関連オブジェクト** のスコープを選択します。
6. 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、RAC デバイスまたは RAC デバイスグループ間の関連付けができます。Windows 2000 モード以降のシステムを使用している場合は、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拡張する必要があります。

ユーザーおよび RAC デバイスのグループを追加できます。Dell 関連グループと Dell に関連しないグループを作成する手順は同じです。

ユーザーまたはユーザーグループの追加

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。

権限オブジェクト タブをクリックして、RAC デバイスに認証する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ブジェクトは 1 つだけです。

権限の追加

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。

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。

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。

拡張スキーマ Active Directory とウェブインタフェースを使用した CMC の設定

1. CMC ウェブインタフェースにログインします。
2. システムツリーで **シャーシ**を選択します。
3. **ネットワーク / セキュリティ** タブをクリックして、**Active Directory** サブタブをクリックします。**Active Directory メインメニュー** ページが表示されます。
4. **ラジオボタンの設定** を選択し、**次へ** をクリックします。Active Directory の設定と管理 ページが表示されます。
5. 共通設定 セクションで以下の操作を行います。:
   a. **Active Directory を有効にする** チェックボックスをオンにします。
   b. **ルートドメイン名** を入力します。**ルートドメイン名** はフォレストのルートドメインの完全修飾名です。

   メモ: ルートドメイン名は x.y の命名規則に従う有効なドメイン名でなければなりません。x は 1 ～ 256 文字の ASCII 文字列で文字間にスペースは挿入できません。y は com、edu、gov、int、mil、net、org などの有効なドメイン名の種類です。

   c. **タイムアウト** の時間を秒単位で入力します。設定範囲:15 ～ 300 秒 デフォルト:90 秒
6. オプション: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) チェックボックスをオンにし、以下の操作を行います。
   a. ドメインコントローラ テキストフィールドに、Active Directory サービスがインストールされているサーバーを入力します。
   b. グローバルカタログ テキストフィールドに、Active Directory ドメインコントローラ上のグローバルカタログの場所を入力します。グローバルカタログは Active Directory フォレストを検索するためのリソースを提供します。

   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。
7. Active Directory スキーマの選択 領域で **拡張スキーマの使用** ラジオボタンを選択します。
8. 拡張スキーマの設定 セクションで、以下の操作を行います。
   a. **CMC 名** を入力します。CMC 名 は Active Directory で CMC カードを一意に識別します。CMC 名 は、ドメインコントローラで作成した新しい CMC オブジェクトのコモンネーム(CN)と同じでなければなりません。CMC 名 は 1 ～ 256 文字の ASCII 文字列で、文字間にスペースは挿入できません。

b. **CMC ドメイン名** を入力します（例：cmc.com）。CMC ドメイン名 は、Active Directory CMC オブジェクトがあるドメインの DNS 名（文字列）です。名前は x.y から成る有効なドメイン名にします。x は文字間に空白文字のない 1 ～ 256 の ASCII 文字列で、y は com、edu、gov、int、mil、net、org などの有効なドメインタイプです。

9. 適用 をクリックして設定を保存します。

メモ: 次のステップに進んで別のページへ移動する前に、設定を適用する必要があります。設定を適用しなければ、次のページへ移動したとき、入力した設定が失われます。

10. **Active Directory メインメニューに戻る** をクリックします。
11. AD 証明書のアップロード ラジオボタンを選択し、**次へ** をクリックします。証明書のアップロード ページが表示されます。
12. 証明書のファイルパスをテキストフィールドに入力するか、参照 をクリックして証明書ファイルを選択します。

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 証明書には、ルート認証局による署名が必要です。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なければなりません。

13. 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。
14. CMC ウェブインタフェースに再びログインします。
15. システムツリーで **シャーシ** を選択し、**ネットワーク / セキュリティ** タブをクリックしてから **ネットワーク** サブタブをクリックします。**ネットワーク設定** ページが表示されます。
16. **DHCP を使用（NIC IP アドレスを使用）**が有効（チェックボックスがオン）の場合は、以下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するか、
    - **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。
17. **変更の適用** をクリックします。

CMC 拡張スキーマ Active Directory 機能の設定が完了します。

拡張スキーマ Active Directory と RACADM を使用した CMC の設定

ウェブインタフェースでなく、RACADM CLI ツールを使用した拡張スキーマで CMC Active Directory 機能を設定するには、次のコマンドを使用します。

1. CMC に対応するシリアル/Telnet/SSH テキスト コンソールを開いて、ログイン後、以下を入力します。

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

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

```
racadm config -g cfgActiveDirectory -o cfgADRacDomain <CMC の完全修飾ドメイン名>
```

```
racadm config -g cfgActiveDirectory -o cfgADRootDomain <完全修飾ルードメイン名>
```

```
racadm config -g cfgActiveDirectory -o cfgADRacName <CMC のコモンネーム>
```

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

メモ: このコマンドはリモート RACADM を介してのみ使用できます。

```
racadm sslcertdownload -t 0x1 -f <CMC の SSL 証明書>
```

メモ: このコマンドはリモート RACADM を介してのみ使用できます。

オプション：DNS サーバーから返されたサーバーを使用せずに、LDAP またはグローバルカタログサーバーを指定してユーザー名を検索する場合は、次の サーバーの指定 オプションを有効にします。

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

メモ: サーバーの指定 オプションを使用すると、認証局の署名付き証明書が、指定したサーバーの名前と照合されません。IP アドレスだけでなくホスト名も入力できるため、CMC システム管理者にとっては特に便利です。

サーバーの指定 オプションを有効にした後、サーバーの IP アドレスまたは完全修飾ドメイン名（FQDN）で LDAP サーバーとグローバルカタログを指定できます。FQDN はサーバーのホスト名とドメイン名で構成されます。

LDAP サーバーを指定するには以下のように入力します。

```
racadm config -g cfgActiveDirectory -o cfgADDomainController <AD ドメインコントローラの IP アドレス>
```

グローバルカタログサーバーを指定するには以下のように入力します。

```
racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog <AD グローバルカタログの IP アドレス>
```

メモ: IP アドレスを 0.0.0.0 に設定すると、CMC のサーバー検索が無効になります。

メモ: コンマ区切りの LDAP または グローバルカタログサーバーのリストを 指定できます。CMC では、最大 3 個の IP アドレスまたはホスト名を指定できます。

メモ: すべてのドメインとアプリケーションに LDAP が正しく設定されていないと、既存のアプリケーション / ドメインの機能中に予期せぬ結果を招くことがあります。

2. 次のいずれかのオプションを使用して DNS サーバーを指定します。
   - CMC で DHCP が有効になり、DHCP サーバーによって自動的に取得された DNS アドレスを使用する場合は、次のコマンドを入力します。

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

   - CMC で DHCP が無効になっている場合や、DHCP が有効でも DNS の IP アドレスを手動で指定したい場合は、次のコマンドを入力します。

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

     ```
     racadm config -g cfgLanNetworking -o cfgDNSServer1 <一次 DNS IP アドレス>
     ```

     ```
     racadm config -g cfgLanNetworking -o cfgDNSServer2 <二次 DNS IP アドレス>
     ```

これで、拡張スキーマ機能の設定は完了しました。

標準スキーマの Active Directory の概要

Active Directory の統合に標準スキーマを使用する場合は、Active Directory と CMC の両方で設定が必要になります。

Active Directory 側では、標準グループオブジェクトがロール（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ロールグループのメンバーとなります。

このユーザーに特定の CMC カードへのアクセスを与えるには、ロールグループ名とそのドメイン名を特定の CMC カードで設定する必要があります。拡張スキーマソリューションとは異なり、ロールと特権レベルは Active Directory ではなく各 CMC カードで定義されます。各 CMC につき最大 5 つのロールグループを設定および定義できます。表5-19はロールグループの権限レベルを、表7-8はロールグループのデフォルト設定を示したものです。

図 7-4 Active Directory と標準スキーマによる CMC の設定

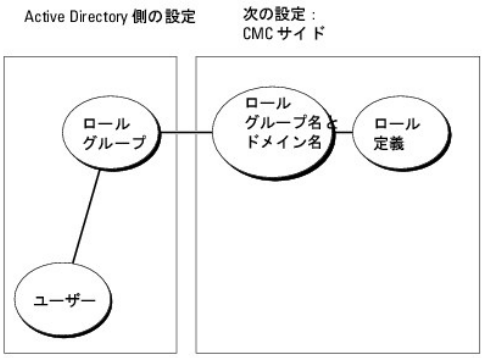


表 7-8 デフォルトのロールグループの権限

ロール（役割）グループ	デフォルトの権限レベル	許可する権限	ビットマスク
1	なし	• CMC ログインユーザー • シャーシ設定システム管理者 • ユーザー設定システム管理者 • ログのクリアシステム管理者 • シャーシ制御システム管理者（電源コマンド） • スーパーユーザー • サーバー管理者 • テスト警告ユーザー • デバッグコマンドユーザー • ファブリック A システム管理者 • ファブリック B システム管理者 • ファブリック C システム管理者	0x00000fff
2	なし	• CMC ログインユーザー • ログのクリアシステム管理者 • シャーシ制御システム管理者（電源コマンド） • サーバー管理者 • テスト警告ユーザー • ファブリック A システム管理者 • ファブリック B システム管理者 • ファブリック C システム管理者	0x000000f9
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のみ使用します。

メモ: 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。

標準スキーマ Active Directory を有効にするには、次の 2 つの方法があります。

- CMC ウェブインタフェースの使用。「標準スキーマ Active Directory とウェブインタフェースを使用した CMC の設定を参照してください。
- RACADM CLI ツールの使用。「標準スキーマ Active Directory と RACADM を使用した CMC の設定を参照してください。

CMC にアクセスするための標準スキーマ Active Directory の設定

Active Directory ユーザーが CMC にアクセスできるようにするには、次の手順を実行して Active Directory を設定する必要があります。

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. グループを作成するか、既存のグループを選択します。CMC でウェブインタフェースまたは RACADM を使用して、グループ名とこのドメインの名前を設定する必要があります。

   詳細については、「標準スキーマ Active Directory とウェブインタフェースを使用した CMC の設定」および「標準スキーマ Active Directory と RACADM を使用した CMC の設定」を参照してください。
3. Active Directory ユーザーを、CMC にアクセスする Active Directory グループのメンバーとして追加します。

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

1. CMC ウェブインタフェースにログインします。
2. システムツリーで シャーシ を選択します。
3. **ネットワーク / セキュリティ** タブをクリックして、**Active Directory** サブタブをクリックします。**Active Directory メインメニュー** ページが表示されます。
4. **設定オプション**を選択し、**次へ** をクリックします。Active Directory の設定と管理 ページが表示されます。
5. 共通設定 セクションで以下の操作を行います。
   a. **Active Directory を有効にする** チェックボックスをオンにします。
   b. **ルードメイン名** を入力します。**ルートドメイン名** はフォレストのルートドメインの完全修飾名です。

      メモ: ルートドメイン名は x.y の命名規則に従う有効なドメイン名でなければなりません。x は 1 ～ 256 文字の ASCII 文字列で文字間にスペースは挿入できません。y は com、edu、gov、int、mil、net、org などの有効なドメイン名の種類です。

   c. **タイムアウト** の時間を秒単位で入力します。設定範囲:15 ～ 300 秒 デフォルト:90 秒
6. オプション:ドメインコントローラとグローバルカタログの検索を呼び出す場合は、検索する AD サーバーの検索(オプション) チェックボックスをオンにし、以下の操作を行います。
   a. ドメインコントローラ テキストフィールドに、Active Directory サービスがインストールされているサーバーを入力します。
   b. グローバルカタログ テキストフィールドに、Active Directory ドメインコントローラ上のグローバルカタログの場所を入力します。グローバルカタログは Active Directory フォレストを検索するためのリソースを提供します。
7. Active Directory スキーマの選択セクションで **標準スキーマの使用** をクリックします。
8. 適用 をクリックして設定を保存します。

   メモ: 次のステップに進んで別のページへ移動する前に、設定を適用する必要があります。設定を適用しなければ、次のページへ移動したとき、入力した設定が失われます。
9. 標準スキーマの設定 セクションで、ロールグループ をクリックします。ロールグループの設定 ページが表示されます。
10. **グループ名** を入力します。グループ名は、CMC カードに関連付けられた Active Directory でロールグループを識別します。
11. **グループドメイン** を入力します。**グループドメイン** はフォレストのルートドメインの完全修飾名です。
12. ロールグループの特権 ページで、グループの特権を選択します。

    特権を変更すると、既存のロールグループの特権(システム管理者、パワーユーザー、ゲストユーザー)がカスタムグループまたは適切なロールグループの特権に変更されます。表5-19を参照してください 。
13. **適用** をクリックして、ロール(役割)グループの設定を保存します。
14. **Active Directory の設定と管理に戻る** をクリックします。
15. **Active Directory メインメニューに戻る** をクリックします。
16. 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 にアップロードします。
    a. **Active Directory CA 証明書をアップロードする** チェックボックスを選択し、**次へ** をクリックします。
    b. **証明書のアップロード** ページで、証明書のファイルパスを入力するか、証明書ファイルの場所まで移動します。

       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なければなりません。

    c. 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。
17. CMC Active Directory 機能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。
18. システムツリーで シャーシ を選択します。
19. **ネットワーク / セキュリティ** タブをクリックします。

20. **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。
21. **ネットワーク設定** で **DHCP を使用(NIC IP アドレス用)**が選択されている場合、**DHCP を使用 を選択して 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、一次および代替 DNS サーバーの IP アドレスを入力します。
22. **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。

標準スキーマ Active Directory と RACADM を使用した CMC の設定

標準スキーマの CMC Active Directory 機能を RACADM CLI を使用して設定するには、次のコマンドを使用します。

1. CMC に対応するシリアル/Telnet/SSH テキスト コンソールを開いて、ログイン後、以下を入力します。

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

racadm config -g cfgActiveDirectory -o cfgADType 2

racadm config -g cfgActiveDirectory -o cfgADRootDomain <完全修飾ルードメイン名>

racadm config -g cfgStandardSchema -i <インデックス> -o cfgSSADRoleGroupName <ロールグループのコモンネーム>

racadm config -g cfgStandardSchema -i <インデックス> -o cfgSSADRoleGroupDomain <完全修飾ドメイン名>

racadm config -g cfgStandardSchema -i <インデックス> -o cfgSSADRoleGroupPrivilege <特定のユーザー権限のビットマスク番号>

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

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

   メモ: ビットマスクの番号については、『Dell Chassis Management Controller 管理者リファレンスガイド』のデータベースプロパティの表 3-1 を参照してください。

2. 次のいずれかのオプションを使用して DNS サーバーを指定します。
   - CMC で DHCP が有効になり、DHCP サーバーによって自動的に取得された DNS アドレスを使用する場合は、次のコマンドを入力します。

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

   - CMC で DHCP が無効になっている場合や、手動で DNS の IP アドレスを入力する場合は、次のコマンドを入力します。

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

     racadm config -g cfgLanNetworking -o cfgDNSServer1 <一次 DNS IP アドレス>

     racadm config -g cfgLanNetworking -o cfgDNSServer2 <セカンダリ DNS IP アドレス>
     ```

よくあるお問い合わせ（FAQ）

表7-9は、CMC で Active Directory を使用する場合によく寄せられる質問とその回答のリストです。

表 7-9 CMC と Active Directory の併用 :よくあるお問い合わせ（FAQ）

質問	回答
複数のツリーで Active Directory を使って CMC にログインできますか?	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。
混合モードで（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、異なるオペレーティングシステムを実行）Active Directory を使って CMC にログインできますか?	はい。混合モードでは、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）が同じドメインになければなりません。 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 の併用では複数のドメイン環境をサポートしていますか?	はい。ドメインフォレストの機能レベルは、ネイティブか Windows 2003 モードであることが必要です。また、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）にあるグループはユニバーサルグループでなければなりません。
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権限オブジェクトは同じドメインの中に置く必要があります。Dell 拡張 Active Directory ユーザーとコンピュータスナップインを使用する場合、これら 2 つのオブジェクトを同じドメインに作成することが強制されます。その他のオブジェクトは別のドメインに作成することができます。
ドメインコントローラの SSL 設定に制限はありますか?	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。
新しい RAC 証明書を作成しアップロードしましたが、ウェブインタフェースが起動しません。	Microsoft 証明書サービスを使用して RAC 証明書を生成した場合、証明書の作成時に **ウェブ証明書** でなく **ユーザー証明書** を誤って選択した可能性があります。 回復するには、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 コマンドを入力してアップロードします。 racadm sslcsrgen [-g] [-f {ファイル名}] racadm sslcertupload -t 1 -f {web_sslcert}
Active Directory 認証を使って CMC にログインできない場合は、どうすればよいですか?この問題はどのようにトラブルシューティングできますか?	1. ログインに NetBIOS 名でなく、正しいユーザードメイン名が使用されていることを確認します。 2. ローカル CMC ユーザーアカウントがある場合は、ローカルの資格情報を使用して CMC にログインします。 ログインした後、次の手順を実行してください。 a. CMC Active Directory 設定ページの **Active Directory を有効にする** チェックボックスがオンになっていることを確認します。 b. CMC ネットワーク設定ページの DNS 設定が正しいことを確認します。 c. Active Directory ルート認証局の署名付き証明書から Active Directory 証明書を CMC にアップロードしたことを確認します。 d. ドメインコントローラの SSL 証明書の有効期限が切れていないことを確認します。 e. **CMC 名**、**ルートドメイン名**、および **CMC ドメイン名** が Active Directory の環境設定と一致することを確認します。 f. CMC のパスワードが 127 文字以内であることを確認します。CMC は最大 256 文字のパスワードをサポートしていますが、Active Directory がサポートしているパスワード長は最大 127 文字です。

シングルサインオンの設定

Microsoft® Windows® 2000、Windows XP、Windows Server® 2003、WindowsVista®、および Windows Server 2008 は、ネットワーク認証プロトコル Kerberos を認証方法に採用しているため、ドメインにサインインしたユーザーは Exchange などの次に使用するアプリケーションに自動的にサインインしたり、シングルサインオンできます。

CMC バージョン 2.10 以降では、CMC は Kerberos を使ってシングルサインオンと Smart Card ログオンという 2 つのログインタイプも使用できるようになりました。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 ActiveDirectory™アカウントにログインした後で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。

メモ: ログイン方法を選択しても、他のログインインタフェース（SSH など）に対してポリシー属性が設定されるわけではありません。他のログインインターフェースに対しては別のポリシー属性を設定する必要があります。すべてのログインインタフェースを無効にするには、**サービス** ページに移動してからすべて（または一部の）ログインインタフェースを無効にします。

システム要件

Kerberos 認証を使用するには、ネットワークには次の項目が必要です。

- DNS サーバー
- Microsoft Active Directory®サーバー

メモ: メモ: Windows 2003 で Active Directory を使用する場合は、クライアントシステムに最新のサービスパックとパッチがインストールされていることを確認してください。Windows 2008 で Active Directory を使用する場合は、SP1 と次のホットフィックスがインストールされていることを確認してください。
KTPASS ユーティリティ用 **Windows6.0-KB951191-x86.msu**。このパッチがないと、ユーティリティで不良な keytab ファイルが生成されます。
LDAP バインド中に GSS_API および SSL トランザクションに使用する **Windows6.0-KB957072-x86.msu**。

- Kerberos キー配付センター(Active Directory サーバーソフトウェアに同梱)
- DHCP サーバー(推奨)
- DNS サーバー用のリバースゾーンには Active Directory サーバーと CMC 用のエントリが必要

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。詳細については、**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と 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 領域の一部でなければなりません。

CMC

- CMC にはファームウェアバージョン 2.10 以降が必要
- 各 CMC には Active Directory アカウントが必要
- CMC は Active Directory ドメインと Kerberos 領域の一部でなければなりません。

設定の実行

必要条件

- Active Directory(AD)の Kerberos 領域とキー配付センター(KDC)が設定済みである(ksetup)。
- クロックドリフトやリバースルックアップの問題を回避するための強力な NTP および DNS インフラストラクチャ
- 認証されたメンバーを含んだ CMC 標準スキーマロールグループ

Active Directory の設定

アカウント オプションの **CMC プロパティ** ダイアログボックスで、以下の設定を行います。

- **アカウントは委任に対して信頼されている** — CMC は、このオプションを選択するときに作成される、転送された資格情報を現在使用していません。このオプションは、他のサービス条件によって、選択できる場合とできない場合があります。
- **アカウントは重要なので委任できない** — このオプションは、他のサービス条件によって、選択できる場合とできない場合があります。
- **このアカウントに Kerberos DES 暗号化を使う** — このオプションを選択します。
- **Kerberos 事前認証を必要としない** — このオプションは選択しません。

Microsoft Windows の一部である ktpass ユーティリティをドメインコントローラ(Active Directory サーバー)上で実行し、ここで CMC を Active Directory 内のユーザーアカウントにマッピングします。例:

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

メモ: cmcname.domainname.com には RFC の要求に従って小文字を使用し、領域名 @REALM_NAME には大文字を使用します。さらに、CMC では Kerberos 認証用の DES-CBC-MD5 タイプの暗号化もサポートされています。

この手順に従うと、CMC にアップロードする必要がある keytab ファイルが生成されます。

メモ: keytab には暗号化キーが含まれているので、安全な場所に保管してください。ktpass ユーティリティの詳細については、Microsoft ウェブサイト **technet2.microsoft.com / windowsserver / en / library / 64042138-9a5a-4981-84e9- d576a8db0d051033.mspx?mfr=true を参照してください。**

CMC の設定

メモ: 本項で説明された設定手順は、CMC のウェブアクセスに対してのみ適用されます。

CMC が Active Directory で設定した標準スキーマロールグループ設定を使用するように設定します。詳細については、「CMC にアクセスするための標準スキーマ Active Directory の設定」を参照してください。

Kerberos 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 ファイルを持つことが必要です。

keytab ファイルをアップロードするには:

1. **リモートアクセス** → **設定** タブ→ **Active Directory** サブタブに移動します。
2. **Kerberos Keytab のアップロード** を選択し、**次へ** をクリックします。
3. **Kerberos Keytab のアップロード** ページで、keytab ファイルの保存先フォルダに移動し、**適用** 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ボックスが表示されます。
4. keytab ファイルを正常にアップロードしたら、**Active Directory メインメニューに戻る** をクリックします。

シングルサインオンの有効化

1. **シャーシ管理コントローラのネットワークセキュリティ** タブ→ **Active Directory** サブタブに移動し、**Active Directory の設定** を選択します。
2. **Active Directory の設定と管理** ページで、次を選択します。
   - シングルサインオン — このオプションでは、Active Directory にログインしたときに取得したキャッシュされた資格情報を使用して、CMC にログインできます。

   メモ: このオプションでは、セキュアシェル(SSH)、Telnet、シリアル、リモート RACADM など、すべてのコマンドライン帯域外インタフェースは変更されません。
3. ページの下までスクロールし、**適用** をクリックします。

CLI コマンドテスト機能を使用すれば、Kerberos 認証によって Active Directory をテストできます。

次のように入力します。

```
testfeature -f adkrb -u <ユーザー>@<ドメイン>
```

ここで、ユーザーは有効な Active Directory ユーザーアカウントを指します。

コマンドが正常に実行されると、CMC は Kerberos 資格情報を取得し、ユーザーの Active Directory アカウントにアクセスできます。コマンドが正常に実行されない場合は、エラーを解決してコマンドをやり直してください。詳細については、**support.dell.com / manuals** の『Chassis Management Controller 管理者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のログインに使用するブラウザの設定

シングルサインオンは、Internet Explorer バージョン 6.0 以降と Firefox バージョン 3.0 以降でサポートされています。

メモ: 次の手順は、CMC が Kerberos 認証でシングルサインオンを使用する場合にのみ適用可能です。

Internet Explorer

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** で、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 / 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、**注意するので大丈夫です** 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。

シングルサインオンを使用した CMC へのログイン

メモ: IP アドレスを使って、シングルサインオンまたはスマートカード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。

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. 以下を使用して CMC ウェブページにアクセスします。

   https:// <cmcname.domain-name>

   例:`cmc-6G2WXF1.cmcad.lab`

   ここで、`cmc-6G2WXF1` は CMC 名を表します。

   `cmcad.lab` はドメイン名を表します。

   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。

   CMC のシングルサインオン ページが表示されます。

3. **ログイン** をクリックします。

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 資格情報を使用すると、CMC にログインできます。ログインに失敗すると、ブラウザは通常の CMC ログインページにリダイレクトされます。

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

スマートカードによる二要素認証の設定

従来の認証方式では、ユーザーの認証にユーザー名とパスワードを使用します。一方、二要素認証ではユーザーがパスワードまたは PIN と秘密キーまたはデジタル証明書を含んだ物理カードを持っている必要があるので、高レベルのセキュリティを実現できます。ネットワーク認証プロトコルの Kerberos では、この二要素認証メカニズムを使用しており、これによってシステムはその信頼性を確認できます。Microsoft Windows2000、Windows XP、Windows Server 2003、Windows Vista、および Windows Server 2008 では、Kerberos を認証方法として優先的に使用します。CMC バージョン 2.10 以降では、CMC は Kerberos を使用してスマートカードログインをサポートできるようになりました。

メモ: ログイン方法を選択しても、他のログインインタフェース(SSH など)に対してポリシー属性が設定されるわけではありません。他のログインインターフェースに対しては別のポリシー属性を設定する必要があります。すべてのログインインタフェースを無効にするには、**サービス** ページに移動してからすべて(または一部の)ログインインタフェースを無効にします。

システム要件

スマートカードの「システム要件」は、シングルサインオンと同じです。

設定の実行

スマートカードの「必要条件」は、シングルサインオンと同じです。

Active Directory の設定

1. Active Dir ectory の Kerberos 領域とキー配付センター(KDC)が設定されていない場合は、設定してください(ksetup)。

   メモ: 強力な NTP および DNS インフラストラクチャによって、クロックドリフトやリバースルックアップの問題を確実に回避します。

2. 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。
3. 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ようにキーも出力されます)。

CMC の設定

メモ: 本項で説明された設定手順は、CMC のウェブアクセスに対してのみ適用されます。

CMC が Active Directory で設定した標準スキーマロールグループ設定を使用するように設定します。詳細については、「CMC にアクセスするための標準スキーマ Active Directory の設定」を参照してください。

Kerberos 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。

keytab ファイルをアップロードするには:

1. **リモートアクセス** → **設定** タブ→ **Active Directory** サブタブに移動します。

2. **Kerberos Keytab のアップロード** を選択し、**次へ** をクリックします。
3. **Kerberos Keytab のアップロード** ページで、keytab ファイルの保存先フォルダに移動し、**適用** 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ボックスが表示されます。
4. keytab ファイルを正常にアップロードしたら、**Active Directory メインメニューに戻る** をクリックします。

スマートカード認証の有効化

1. **シャーシ管理コントローラのネットワークセキュリティ** タブ→ **Active Directory** サブタブに移動し、**Active Directory の設定** を選択します。
2. **Active Directory の設定と管理** ページで、次を選択します。
   - スマートカード — このオプションでは、スマートカードをリーダーに挿入し、PIN 番号を入力する必要があります。

   メモ: このオプションでは、セキュアシェル(SSH)、Telnet、シリアル、リモート RACADM など、すべてのコマンドライン帯域外インタフェースは変更されません。
3. ページの下までスクロールし、**適用** をクリックします。

CLI コマンドテスト機能を使用すれば、Kerberos 認証によって Active Directory をテストできます。

次のように入力します。

```
testfeature -f adkrb -u <ユーザー>@<ドメイン>
```

ここで、ユーザーは有効な Active Directory ユーザーアカウントを指します。

コマンドが正常に実行されると、CMC は Kerberos 資格情報を取得し、ユーザーの Active Directory アカウントにアクセスできます。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、『Chassis Management Controller 管理者リファレンスガイド』を参照してください。

スマートカードのログインに使用するブラウザの設定

Mozilla Firefox

CMC 2.10 では、Firefox ブラウザを使ってスマートカードにログインすることはできません。

Internet Explorer

インターネットブラウザが Active-X プラグインをダウンロードするように設定されていることを確認します。

スマートカードを使用した CMC へのログイン

メモ: IP アドレスを使って、シングルサインオンまたはスマートカード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。

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. 以下を使用して CMC ウェブページにアクセスします。

   https://<cmcname.domain-name>

例：cmc-6G2WXF1.cmcad.lab

ここで、cmc-6G2WXF1 は CMC 名を表します。

cmcad.lab はドメイン名を表します。

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。

CMC のシングルサインオン ページが表示され、スマートカードを挿入を求められます。

3. スマートカードをリーダーに挿入して **OK** をクリックします。

PIN ポップアップダイアログボックスが表示されます。

4. パスワードを入力して、**OK** をクリックします。

スマートカードログイン時のトラブルシューティング

以下は、スマートカードにアクセスできないときのデバッグに役立つヒントです。

ActiveX プラグインがスマートカードリーダーを検出しません

スマートカードが Microsoft Windows オペレーティングシステムでサポートされていることを確認します。Windows がサポートしているスマートカード暗号サービスプロバイダ（CSP）の数は限られています。

ヒント：スマートカード CSP が特定のクライアントに含まれているかどうかを確認する一般的なチェックとして、Windows のログオン（Ctrl-Alt-Del） 画面で、スマートカードをリーダーに挿入し、Windows でスマートカードが検出され、PIN ダイアログボックスが表示されるかどうかを調べます。

不正なスマートカード PIN

間違った PIN でログインを試みた回数が多すぎるためにスマートカードがロックアウトされたかどうかをチェックします。このような場合は、新しいスマートカードを入手方法について、組織のスマートカード発行者に問い合わせてください。

Active Directory ユーザーとして CMC にログインできません

Active Directory ユーザーとして CMC にログインできない場合は、スマートカードログオンを有効にしないで CMC にログインしてみてください。次のコマンドを使用してローカル RACADM からスマートカードログオンを無効にすることもできます。

racadm config -g cfgActiveDirectory -o cfgADSCLEnable 0

racadm config -g cfgActiveDirectory -o cfgADSSOEnable 0

目次ページに戻る

目次ページに戻る

CMC にコマンドラインコンソールの使用を設定する方法

Dell™ Chassis Management Controllerファームウェアバージョン 2.10 ユーザーガイド

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/SSH コンソール）の機能について、およびコンソールからシステム管理操作を実行できるようにシステムを設定する方法について説明します。コマンドラインコンソールを介して CMC で RACADM コマンドを使用する方法については、「RACADM コマンドラインインタフェースの使用」を参照してください。

CMC 上のコマンドラインコンソール 機能

CMC は、以下のシリアル、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 クライアント同時接続が可能
- 最大 4 つの同時セキュアシェル（SSH）クライアント接続
- RACADM コマンドのサポート
- サーバーまたは I/O モジュールのシリアル コンソールに接続する内蔵型**connect** コマンドです。racadm connect としても使えます。
- コマンドラインの編集と履歴
- すべてのコンソールインタフェースでタイムアウト制御

シリアル、Telnet、SSH コンソールの使用

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 3-1 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、**getconfig**、**serveraction**、**getsensorinfo** のようなサブコマンドが続きます。RACADM の使用の詳細については、「RACADM コマンドラインインタフェースの使用」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。**connect** コマンドの使用の詳細については、「接続コマンドでサーバーまたは I/O モジュールに接続する」を参照してください。 **メモ:** racadm connect コマンドも使えます。
exit、logout、quit	これらのコマンドはすべて同じ処置を実行します。現在のセッションを終了してログインプロンプトに戻ります。

CMC での Telnet コンソールの使用

一度に最大 4 台の telnet クライアントシステムと 4 台の SSH クライアントを接続できます。

管理ステーションで Windows XP または Windows 2003 を実行している場合は、CMC Telnet セッションで文字の問題が発生する可能性があります。この問題はログインのフリーズとして表れ、Return キーが応答せず、パスワードプロンプトが表示されません。

この問題を解決するには、Microsoft のサポートウェブサイト **support.microsoft.com** から修正プログラム hotfix 824810 をダウンロードします。詳細については、Microsoft 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、セッションのネゴシエーションと暗号化によってセキュリティが強化されています。CMC は、パスワード認証付きの SSH バージョン 2 をサポートしています。CMC ではデフォルトで SSH が有効になっています。

メモ: CMC は SSH バージョン 1 をサポートしていません。

ログイン中にエラーが発生すると、SSH クライアントからエラーメッセージが発行されます。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 で制御することはできません。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 端末エミュレータから実行してください。Windows のコマンドプロンプトで OpenSSH を実行すると、完全には機能しません(一部のキーが応答せず、グラフィックが表示されません)。Linux の場合は、SSH クライアントサービスを実行して、いずれかのシェルで CMC に接続します。

SSH は 1 度に 4 セッションがサポートされています。セッションのタイムアウトは cfgSsnMgtSshIdleTimeout プロパティ(『Dell Chassis Management Controller 管理者リファレンス ガイド』のデータベースプロパティの章を参照)またはウェブインタフェースの サービス管理 ページ(「サービスの設定」を参照)で制御されています。

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。この認証方法を使用すると、ユーザー ID / パスワードの組み込みや入力を行う必要がないため、SSH スクリプトの自動化が向上します。詳細については、「RACADM による SSH 経由の公開キー認証の設定」を参照してください。

CMC で SSH を有効にする方法

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。

RACADM を使って CMC の SSH 接続を有効にする手順については、『Dell Chassis Management Controller 管理者リファレンス ガイド』の config コマンドの項および cfgSerial データベースプロパティの項を参照してください。ウェブインタフェースを使用して CMC で SSH 接続を有効にする手順については、「サービスの設定」を参照してください。

SSH ポートの変更

SSH ポートを変更するには、次のコマンドを使用します。

```
racadm config -g cfgRacTuning -o cfgRacTuneSshPort <ポート番号>
```

cfgSerialSshEnable および cfgRacTuneSshPort プロパティの詳細については、『Dell Chassis Management Controller 管理者リファレンス ガイド』のデータベースプロパティの章を参照してください。

CCH SSH の実装では、「表3-2」に示すように複数の暗号化スキームがサポートされています。

表 3-2 暗号化スキーム

スキームの種類	スキーム
非対称暗号	Diffie-Hellman DSA/DSS 512-1024(ランダム)ビット(NIST 仕様に準拠)
対称暗号	• AES256-CBC

	• RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
メッセージの整合性	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
認証	パスワード

フロントパネルから iKVM への接続を有効にする方法

iKVM フロントパネルポートの詳細および使用手順については、「フロントパネルの有効または無効」を参照してください。

端末エミュレーションソフトウェアの設定

CMC は、次の種類の端末エミュレーションソフトウェアを実行している管理ステーションからシリアルテキストコンソールをサポートしています。

- Linux Minicom
- Hilgraeve の HyperTerminal Private Edition（バージョン 6.3）

使用するターミナルソフトウェアを設定するには、以下の項の手順に従ってください。

Linux Minicom の設定

Minicom は Linux 用のシリアルポートアクセスユーティリティです。次の手順は、Minicom のバージョン 2.0 の設定に有効です。他のバージョンでは若干異なる場合がありますが、必要な基本設定は同じです。他のバージョンの Minicom の設定については、「必要な Minicom 設定」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カラム数に一致するように設定します。プロンプトは 2 カラム分とることに注意してください。たとえば、80 カラムの端末ウィンドウでは、次を入力します。
`racadm config –g cfgSerial –o cfgSerialConsoleColumns 80`

1. Minicom の設定ファイルがない場合には、次の手順に進んでください。

   Minicom 設定ファイルがある場合は、`minicom <Minicom config ファイル名>` と入力して、手順 14 に進んでください。
2. Linux コマンドプロンプトで、`minicom -s` と入力します。
3. **シリアルポートのセットアップ** を選択し、<Enter> を押します。
4. <a> を押して、該当する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** に設定し、**ソフトウェアフロー制御** を **いいえ** に設定します。

   シリアルポートの設定 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のセットアップ** メニューで、<Backspace>を押して **初期化、リセット、接続、切断** 設定をクリアすると、設定が空白になります。
9. <Enter> を押して、それぞれの空白値を保存します。

10. 指定のフィールドをすべてクリアする場合は、<Enter > を押して **モデムダイヤルとパラメータのセットアップ** メニューを終了します。
11. **セットアップを config_name として保存** を選択して、<Enter> を押します。
12. **Minicom から終了** を選択して、<Enter> を押します。
13. コマンドシェルプロンプトで、`minicom <Minicom config ファイル名>` と入力します。
14. <Ctrl+a>、<x>、<Enter> を押して、Minicom を終了します。

Minicom ウィンドウがログイン画面を表示するか確認します。ログイン画面が表示されたら、正しく接続されています。これでログインの準備が完了し、CMC コマンド ライン インタフェースにアクセスできます。

必要な Minicom 設定

「表3-3」に従って Minicom を設定します。

表 3-3 Minicom 設定

設定の説明	必要な設定
Bps/Par/Bits	115200 8N1
ハードウェアフロー制御	○
ソフトウェアフロー制御	×
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の設定	**初期化、リセット、接続、切断** 設定をクリアして空白にします。

接続コマンドでサーバーまたは I/O モジュールに接続する

CMC は、サーバーのシリアル コンソールまたは I/O モジュールにリダイレクトする接続が確立できます。サーバーの場合は、シリアル コンソール リダイレクトはさまざまな方法で実行できます。

- CMC コマンドラインで connect または racadm connect コマンドを使う connect の詳細については、『Dell Chassis Management Controller 管理者リファレンスガイド Administrator Reference Guide』の **racadm connect** コマン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を使う
- iDRAC Serial Over LAN (SOL) 機能を使う

シリアル/Telnet/SSH コンソールでは、CMC は、connect コマンドをサポートして、サーバーまたは IOM モジュールとのシリアル接続を確立します。サーバーのシリアルコンソールには、オペレーティングシステムのシリアルコンソールの他にも、BIOS 起動およびセットアップ画面が含まれています。I/O モジュールの場合は、スイッチ シリアル コンソールが使えます。

△ **注意: CMC シリアルコンソールから実行した場合、connect -b オプションは CMC がリセットするまで接続したままになります。この接続は、セキュリティ上の潜在的なリスクとなりえます。**

メモ: connect コマンドは –b（バイナリ）オプションを提供します。–b オプションは未処理のバイナリデータを渡し、cfgSerialConsoleQuitKey は使用されません。また、CMC シリアルコンソールを使用してサーバーに接続すると、DTR 信号の変化（たとえば、デバッガに接続するためにシリアルケーブルが抜かれる）がログアウトを引き起こすことはありません。

メモ: IOM がコンソールリダイレクトをサポートしていない場合は、connect コマンドは空のコンソールを表示します。その場合、CMC コンソールに戻るには、エスケープシーケンスを入力してください。コンソールのデフォルトのエスケープシーケンスは <Ctrl>\ です。

管理下システムには最大 6 つの IOM があります。IOM に接続するには、次のように入力します。

```
connect switch-n
```

ここで n は IOM ラベルの a1、a2、b1、b2、c1 および c2 です。

IOM には A1、A2、B1、B2、C1、C2 のラベルが付いています。（シャーシにおける IOM の配置の図解については、「図10-1」を参照してください。）**connect** コマンドで IOM を参照する際は、「表

3-4 」で示されるように、IOM はスイッチにマッピングされています。

表 3-4 I/O モジュールからスイッチへのマッピング

I/O モジュールのラベル	スイッチ
A1	switch-a1
A2	switch-a2
B1	switch-b1
B2	switch-b2
C1	switch-c1
C2	switch-c2

メモ: 各シャーシで一度に 1 つの IOM 接続のみが可能です。

メモ: シリアル コンソールからパススルーに接続することはできません。

管理サーバーのシリアル コンソールに接続するには、connect server-n コマンドを使います。このとき、-n はサーバーのスロット番号を指定します。racadm connect server-n コマンドも使えます。-b オプションを指定したサーバー接続は、バイナリ通信が想定され、エスケープ文字が無効になります。iDRAC が使用不可の場合は、ホストへの経路がありません というエラーメッセージが表示されます。

connect server-n コマンドは、ユーザーによるサーバーのシリアル ポートのアクセスを有効にします。この接続が確立された後、ユーザーは、BIOS シリアル コンソールとオペレーティング システムのシリアル コンソールを含む CMC のシリアル ポート経由でサーバーのコンソールをリダイレクトできます。

メモ: BIOS 起動画面を表示するには、サーバーの BIOS セットアップで、シリアルリダイレクトを有効にしてください。また、端末エミュレータウィンドウは 80x25 に設定してください。そうしない場合、文字化けが画面に表示されます。

メモ: BIOS セットアップ画面ではすべてのキーが使えるわけではないため、ユーザーは CTRL+ALT+DEL や別のエスケープシーケンスを提供しなければなりません。最初のリダイレクト画面には、必要なエスケープ シーケンスが表示されます。

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

(「iKVM によるサーバーの管理」を参照)を使用して管理下サーバーに接続するか、iDRAC ウェブ GUI(**support.dell.com/manuals** にある『iDRAC ユーザーズガイド』を参照)から VKVM セッションを確立し、次の手順を実行する必要があります。

BIOS 内のシリアル通信はデフォルトでオフになっています。ホストテキストコンソールデータをシリアルオーバー LAN にリダイレクトするためには、COM1 を介したコンソールのリダイレクトを有効にする必要があります。BIOS 設定を変更するには:

1. 管理下サーバーを起動します。
2. POST 中に <F2> を押して BIOS セットアップユーティリティを起動します。
3. シリアル通信 にスクロールダウンして <Enter> を押します。ポップアップダイアログボックスのシリアル通信リストには、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

   方向キーを使用して、オプション間を移動します。
4. **COM1 経由のコンソールリダイレクトでオン** が有効になっていることを確認します。
5. **起動後のリダイレクト** を有効にします(デフォルトは **無効**)。このオプションは、その後の再起動での BIOS コンソールのリダイレクトを有効にします。
6. 変更を保存して終了します。
7. 管理下サーバーが再起動します。

シリアルコンソールリダイレクト用 Windows の設定

Microsoft®Windows Server® バージョンを実行しているサーバー(Windows Server 2003 以降)では設定は必要ありません。Windows は BIOS から情報を取得し、COM 1 を使用して Special Administration Console (SAC) コンソールを有効にします。

起動中に Linux をシリアルコンソールリダイレクト用に設定する

以下は、Linux GRand Unified Bootloader（GRUB）に固有の手順です。別のブートローダーを使用する場合も、同様の変更が必要です。

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、リダイレクトコンソールを表示するウィンドウまたはアプリケーションを 25 行 x 80 列に設定し、テキストが正しく表示されるようにしてください。この設定を行わないと、一部のテキスト画面が文字化けすることがあります。

/etc/grub.conf ファイルを次のように編集します。

1. ファイルの一般設定セクションを見つけ、次の 2 行を新たに追加します。

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

2. カーネル行に次の 2 つにオプションを追加します。

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

3. **/etc/grub.conf** に splashimage ディレクティブがある場合は、コメントアウトします。

次の例は、この手順で説明した変更を示しています。

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

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

title Red Hat Linux Advanced Server (2.4.9-e.3smp)
   root (hd0,0)
   kernel /boot/vmlinuz-2.4.9-e.3smp ro root= /dev/sda1 hda=ide-scsi console=ttyS0 console= ttyS1,57600
   initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3)
   root (hd0,00)
   kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s
   initrd /boot/initrd-2.4.9-e.3.im

#grub.conf （作成者： anaconda）
#
#このファイルに変更を加えた後 grub を再実行する
# 必要はありません。
# 通知：/boot パーティションがありません。これは
#すべてのカーネルと initrd パスが / に相対パスであることを意味します。例：
#root (hd0,0)
#kernel /boot/vmlinuz-version ro root= /dev/sdal
#initrd /boot/initrd-version.img
#
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz

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

title Red Hat Linux Advanced Server (2.4.9-e.3smp)
root (hd0,0)
kernel /boot/vmlinuz-2.4.9-e.3smp ro root= /dev/sda1 hda=ide-scsi console=ttyS0 console= ttyS1,57600
initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3)
root (hd0,00)
kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s
```

```
initrd /boot/initrd-2.4.9-e.3.im
```

/etc/grub.conf ファイルを編集するとき、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、テキストインタフェースを使用します。そうしないと、コンソールリダイレクトで GRUB 画面が表示されません。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
  ```

  これは、最初のオプションだけに `console=ttyS1,57600` を追加した例です。

起動後に Linux をサーバーシリアルコンソールリダイレクト用に設定する

/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` を設定する新しい行を追加します。

  ```
  co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
  ```

次の例は、新しい行が追加されたファイルを示しています。

```
#
# inittab  This file describes how the INIT process
#          should set up the system in a certain
#          run-level.
#
# Author:  Miquel van Smoorenburg
#          Modified for RHS Linux by Marc Ewing and
#          Donnie Barnes
#
# Default runlevel. The runlevels used by RHS are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you
#       do not have networking)
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:

# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit



l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6



# Things to run in every runlevel.
ud::once:/sbin/update

# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# When our UPS tells us power has failed, assume we have a few
# minutes of power left. Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have power installed and your
# UPS is connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
# If power was restored before the shutdown kicked in, cancel it.
```

```
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"



# Run gettys in standard runlevels
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
# xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon

#
#inittabこのファイルは、特定のランレベルで
#INIT プロセスがどのようにシステムをセットアップするか
#説明しています。
#
#作成者：Miquel van Smoorenburg
#RHS Linux 用に修正  修正者：Marc Ewing、
#Donnie Barnes
#
#デフォルトランレベル。RHS が使用するランレベル：
#0 - 停止 (initdefault はこの値に設定しないでください)
#1 - シングルユーザーモード
#2 - マルチユーザー、NFS なし（ネットワーク接続がない場合は
#3 と同様）
#3 - フルマルチユーザーモード
#4 - 未使用
#5 - X11
#6 - 再起動(initdefault はこの値に設定しないでください)
#
id:3:initdefault:

#システムの初期化。
si::sysinit:/etc/rc.d/rc.sysinit



l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6



#各ランレベルで実行するもの。
ud::once:/sbin/update

#Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

#UPS から停電が知らされたら、数分間分の
#電源が残っていることを仮定します。シャットダウンを 2 分間後にスケジュールします。
#電源が取り付けられており UPS が接続して
#正しく動作していることを前提とします。
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
#シャットダウンの前に電源が復元した場合は、割り込んでキャンセルします。
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"



#gettys を標準ランレベルで実行します。
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

#xdm をランレベル 5 で実行します。
#xdm i が別のサービスになりました。
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
```

目次ページに戻る

目次ページに戻る

用語集

Dell™ Chassis Management Controllerファームウェアバージョン 2.10 ユーザーガイド

Active Directory

Active Directory は、ユーザーデータ、セキュリティ、分散リソースのネットワーク管理を自動化する標準化された集中管理システムで、他のディレクトリとの相互運用を可能にします。Active Directory は、分散ネットワーク環境用に特別設計されています。

ARP

Address Resolution Protocol(アドレス解決プロトコル)の略語。ホストのインターネットアドレスからその Ethernet アドレスを見つける手法。

ASCII

American Standard Code for Information Interchange(情報交換用米国標準コード)の略語。文字、数字、その他の記号の表示と印刷に使用されるコード表現体系。

BIOS

Basic Input/Output System(基本出入力システム)の略語。周辺機器に最下位レベルのインタフェースを提供し、メモリへのオペレーティングシステムの読み込みなど、システム起動処理の最初のプロセスを制御するシステムソフトウェアの一部。

CA

認証局(CA)は、IT 業界で認知されたビジネス組織で、高水準で信頼できる審査、身元確認、その他の重要なセキュリティ要件を提供しています。CA には、Thawte や VeriSign などがあります。CA は CSR を受け取ると、CSR に含まれている情報を確認します。応募者が CA のセキュリティ標準を満たしていると、CA はネットワークおよびインターネットを介したトランザクションに対して、応募者を一意に識別する証明書を発行します。

CD

Compact disc(コンパクトディスク)の略語。

CLI

Command Line interface(コマンドラインインタフェース)の略語。

CMC

Dell Chassis Management Controller の略語。Dell PowerEdge™ システムにリモート管理機能と電源制御機能を提供します。

DHCP

Dynamic host configuration protocol(動的ホスト設定プロトコル)の略語。ネットワーク上のコンピュータに IP アドレスを動的に割り当てる手段。

DLL

Dynamic Link Library(ダイナミックリンクライブラリ)の略語。小さいプログラムから成るライブラリ。システムで実行している大きいプログラムが必要時に呼び出すことができます。これらの小さいプログラムは、大きいプログラムがプリンタやスキャナなど、個々のデバイスと通信できるようにします。

DNS

Domain name system(ドメインネームシステム)の略語。

FQDN

Fully qualified domain name(完全修飾ドメイン名)の略語。DNS ツリー階層内のモジュールの絶対的な位置を指定するドメイン名です。Microsoft® Active Directory® は 64 バイト以下の FQDN のみに対応しています。

FSMO

Flexible single master operation(フレキシブルシングルマスタオペレーション)の略語。拡張処理のアトミック性を保証する Microsoft Active Directory ドメインコントローラタスク。

GB1

シャーシ上のアップリンクポート。

GMT

Greenwich Mean Time(グリニッジ標準時)の略語。GMT は世界中のあらゆる場所に共通する標準時刻です。GMT はイギリスのロンドン郊外にあるグリニッジ天文台跡を通過する本初子午線(経度 0°)に基づく平均太陽時を反映しています。

GUI

Graphical User Interface(グラフィカルユーザーインタフェース)の略語。ウィンドウ、ダイアログボックス、ボタンなどの要素を使用するコンピュータ表示インタフェース。これに対し、コマンドプロンプトインタフェースでは、すべてのユーザー対話がテキストで表示され入力されます。

ICMP

Internet Control Message Protocol(インターネットコントロールメッセージプロトコル)の略語。オペレーティングシステムがエラーメッセージを送信する方法。

ID

Identifier(識別子)の略語。一般に、ユーザー識別子(ユーザー ID)やオブジェクト識別子(オブジェクト ID)を指すときに使用されます。

iDRAC

Dell Integrated Remote Access Controller の略語。Dell PowerEdge システムのリモート管理機能、クラッシュしたシステムのリカバリ機能、電源制御機能などを提供するシステム管理用ハードウェアとソフトウェアのソリューション。

iKVM

Avocent® Integrated KVM スイッチモジュール。シャーシへのホットプラグが可能なオプションのモジュールで、キーボード、マウス、ビデオからシャーシ内の 16 台のサーバーへのローカルアクセス、およびシャーシをアクティブな CMC に接続する Dell CMC コンソールの追加オプションを提供します。

IOMINF

I/O Module Infrastructure Device(I/O モジュール基盤装置)の略語。

IP

Internet Protocol(インターネットプロトコル)の略語。IP は TCP/IP のネットワーク層です。IP はパケットの経路選択、断片化、再構成などを行います。

IPMB

システム管理技術で使用される Intelligent Platform Management Bus の略語。

Kbps

Kilobits per second(1 秒当たりのキロビット)の略語。データ伝送速度を表す単位です。

LAN

Local Area Network（ローカルエリアネットワーク）の略語。

LDAP

Lightweight Directory Access Protocol（ライトウェイトディレクトリアクセスプロトコル）の略語。

LED

Light-Emitting Diode（発光ダイオード）の略語。

LOM

Local area network On Motherboard（マザーボード上のローカルエリアネットワーク）の略語。

MAC

Media Access Control（メディアアクセスコントロール）の略語。ネットワークノードとネットワーク物理レイヤ間のネットワークサブレイヤ。

MAC アドレス

Media Access Control アドレス。NIC の物理コンポーネントに組み込まれる固有アドレス。

Mbps

Megabits per second（1 秒当たりのメガビット数）略語。データ伝送速度を表す単位です。

MC

メザニンカード

Microsoft Active Directory

ユーザーデータ、セキュリティ、分散リソースのネットワーク管理を自動化し、他のディレクトリとの相互作用を可能にする一元管理型の標準化システム。Active Directory は、分散ネットワーク環境用に特別設計されています。

NIC

Network Interface Card（ネットワークインタフェースカード）の略語。ネットワークへの物理的な接続を提供するためにコンピュータに取り付けるアダプタ回路基板。

OID

Object Identifier（オブジェクト識別子）の略語。

OSCAR

On Screen Configuration and Reporting の略語。iKVM アクセス用のグラフィカルユーザーインタフェース。

PCI

Peripheral Component Interconnect（周辺機器相互接続）の略語。周辺機器をシステムに接続し、それらの周辺機器と通信するための標準インタフェースおよびバス技術。

POST

Power-On Self-Test（電源オンセルフテスト）の略語。コンピュータの電源を入れると、システムで自動的に実行される診断テストシーケンス。

RAC

リモートアクセスコントローラ

RAM

Random-Access Memory（ランダムアクセスメモリ）の略語。RAM はシステムに搭載される読み書き可能な汎用メモリ。

RAM ディスク

ハードディスクをエミュレートするメモリ常駐プログラム。

ROM

Read-Only Memory（読み取り専用メモリ）の略語。データを読み取れますが、書き込みはできません。

RPM

Red Hat Package Manager の略語。Red Hat Enterprise Linux オペレーティングシステムのパッケージ管理システム。RPM は、ソフトウェアパッケージのインストールを管理します。インストールプログラムに似ています。

SEL

システムイベントログまたはハードウェアログ

SMTP

Simple Mail Transfer Protocol（簡易メール転送プロトコル）の略語。システム間（通常はイーサネット経由）で電子メールを転送するのに使用します。

SNMP

Simple Network Management Protocol（シンプルネットワーク管理プロトコル）の略語。IP ネットワーク上のノードを管理する設計になっています。iDRAC は、SNMP によって管理されるデバイス（ノード）です。

SNMP トラップ

CMC で生成される通知（イベント）で、管理下システムの状況の変化や、ハードウェアの潜在的な問題に関する情報が含まれています。

SSH

Secure Shell（セキュアシェル）の略語。2 台のコンピュータ間でセキュアチャネルを介してデータをやり取りできるネットワークプロトコル。

SSL

Secure Sockets Layer（セキュアソケットレイヤ）の略語。ネットワークを介したデータ転送に安全な通信を提供するプロトコル。

STK

シャーシ上のスタックポート。

TCP / IP

Transmission Control Protocol/Internet Protocol の略語。ネットワーク層とトランスポート層のプロトコルを含む標準的な Ethernet プロトコル一式を意味します。

TFTP

Trivial File Transfer Protocol(簡易ファイル転送プロトコル)の略語。ディスクなしのデバイスやシステムに起動コードをダウンロードするために使用される簡易なファイル転送プロトコル。

UDP

User Datagram Protocol(ユーザーデータグラムプロトコル)の略語。

UPS

Uninterruptible Power Supply(無停電電源装置)の略語。

USB

Universal Serial Bus の略語。デバイスにインタフェースするためのシリアルバス規格。

UTC

Universal Coordinated Time(万国標準時)の略語。「GMT」を参照してください。

vKVM

仮想 KVM コンソール

VLAN

Virtual Local Area Network(仮想ローカルエリアネットワーク)の略語。

VNC

Virtual Network Computing(仮想ネットワークコンピューティング)の略語。

VT-100

Video Terminal(ビデオ端末)100 の略語。多くの共通端末エミュレーションプログラムによって使用されます。

WAN

Wide Area Network(広域通信網)の略語。

WWN

World Wide Name (ワールド ワイド ネーム) の略語。物理層のファイバー チャンネル ノードを示す固有の値。

ハードウェアログ

シャーシ上のハードウェアに関連するイベントのレコードで、CMC で生成されます。

バス

コンピュータ内の各種の機能単位を接続する伝導体のセット。バスは、伝送するデータの種類によって、データバス、アドレスバス、PCI バスなどと名付けられます。

ブレード

高密度ラック搭載向けに設計された1つの基板にすべての機能が集約されたサーバー。

拡張スキーマ

Active Directory と併用して CMC へのユーザーアクセスを決定するソリューション。Dell 定義のActive Directory オブジェクトを使用します。

標準スキーマ

Active Directory で使用されるソリューションで、CMC へのユーザーアクセスを決定します。Active Directory のグループオブジェクトのみを使用します。

管理ステーション

リモートから CMC にアクセスするシステム。

証明書署名要求 (CSR)

認証局にセキュアサーバー証明書を申請するデジタル要求。

遅延時間(OSCAR ユーザーインタフェース)

<画面の印刷> を押してから OSCAR メインダイアログボックスが表示されるまでの秒数。

非持続性ログ

CMC の再起動時にクリアされるログ。

目次ページに戻る

目次ページに戻る

Dell™ Chassis Management Controllerファームウェアバージョン 2.10 ユーザーガイド

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: 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。

_____

本書の内容は予告なく変更されることがあります。
© 2009 すべての著作権は Dell Inc. にあります。

Dell Inc. の書面による許可のない複製は、いかなる形態においても厳重に禁じられています。

本文書で使用される商標:Dell、DELL ロゴ、FlexAddress、OpenManage、PowerEdge、PowerConnect は、Dell Inc. の商標です。Microsoft、Active Directory、Internet Explorer、Windows、Windows NT、Windows Server、Windows Vista は、米国内および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、米国内および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、米国内およびその他の国における Novell Corporation の登録商標です。Intel は、Intel Corporation の登録商標です。UNIX は、米国内およびその他の国における The Open Group の登録商標です。Avocent は Avocent Corporation の商標であり、OSCAR は Avocent Corporation およびその関連会社の登録商標です。

Copyright 1998-2006 The OpenLDAP Foundation.All rights reserved.ソースおよびバイナリ形式での再配布は、変更の有無を問わず、OpenLDAP の公開ライセンスで承認されている範囲内でのみ許可されます。このライセンスのコピーは、配布パッケージ内の最上位レベルのディレクトリに入っている LICENSE ファイル、または **http://www.OpenLDAP.org/license.html**でご覧いただけます。OpenLDAP はOpenLDAP Foundation の登録商標です。個々のファイルや提供パッケージは、他社が著作権を所有している場合があり、その他の制約を受ける可能性があります。この製品はミシガン大学 LDAP v3.3 配布から派生しています。この製品には、公共ソースから派生した材料も含まれています。OpenLDAP に関する情報は **http://www.openldap.org/** から入手できます。Portions Copyright 1998-2004 Kurt D.Zeilenga.Portions Copyright 1998-2004 Net Boolean Incorporated.Portions Copyright 2001-2004 IBM Corporation.All rights reserved.ソースおよびバイナリ形式での再配布は、変更の有無を問わず、OpenLDAP の公開ライセンスで承認されている範囲内でのみ許可されます。Portions Copyright 1999-2003 Howard Y.H.Chu.Portions Copyright 1999-2003 Symas Corporation.Portions Copyright 1998-2003 Hallvard B.Furuseth.All rights reserved.ソースおよびバイナリ形式での再配布と使用は、変更の有無を問わず、この著作権表示を含めた形式でのみ許可されます。著作権所有者の名前を、書面による事前の許可なく、このソフトウェアの派生製品を推薦または宣伝する目的で使用することはできません。このソフトウェアは、明示または黙示の保証なしに「現状のまま」提供されます。Portions Copyright (c) 1992-1996 Regents of the University of Michigan.All rights reserved.ソースおよびバイナリ形式での再配布と使用は、この著作権表示を含め、米国アン・アーバーのミシガン大学への謝辞を記載した場合にのみ許可されます。この大学名を、書面による事前の許可なく、このソフトウェアの派生製品を推薦または宣伝する目的で使用することはできません。このソフトウェアは、明示または黙示の保証なしに「現状のまま」提供されます。

商標または製品の権利を主張する事業体を表すためにその他の商標および社名が使用されていることがあります。Dell Inc. はデル以外の商標や社名に対する所有権を一切否認します。

2009 年 8 月

目次ページに戻る

目次ページに戻る

FlexAddress の使用

Dell™ Chassis Management Controllerファームウェアバージョン 2.10 ユーザーガイド

FlexAddress 機能は、オプションのアップグレードです。この機能は、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）ネットワーク ID をシャーシで提供される WWN/MAC ID に置き換えることを可能にします。

各サーバーモジュールには、製造過程で一意の WWN および MAC ID が割り当てられます。FlexAddress 機能が登場する以前は、サーバーモジュールを取り替える際に WWN/MAC ID が変更してしまうため、新しいサーバーモジュールを認識するようにイーサネットネットワーク管理ツールや SAN リソースを再設定する必要がありました。

FlexAddress により、CMC は特定スロットに WWN/MAC ID を割り当て、工場出荷時設定の ID を無効にすることができます。サーバーモジュールを取り替えた場合でも、スロットベースの WWN/MAC ID は同じままとなります。この機能により、新しいサーバーモジュールに対応する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す。

また、工場設定の ID を無効にする処理は、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ます。サーバーモジュールに対して永久的な変更は行われません。サーバーモジュールを FlexAddress がサポートされていないシャーシに移動した場合は、工場設定の WWN/MAC ID が使用されます。

FlexAddress をインストールする前に、SD カードを USB メモリカードリーダーに挿入し、ファイル pwwn_mac.xml を表示することで、FlexAddress 機能カードに含まれている MAC アドレスの範囲を特定できます。SD カード上のこのクリアテキストの XML ファイルには、一意の MAC アドレス範囲で使用される 16 進数の開始 MAC アドレスとなる XML タグ（mac_start）が含まれます。mac_count タグは、SD カードによって割り当てられる MAC アドレスの総数です。割り当てられる MAC 範囲の合計は、次の式で求めることができます。

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

ここで、208 は mac_count を表し、次の式で求めることができます。
<mac_start> + <mac_count> - 1 = <mac_end>

例：(starting_mac)00188BFFDCFA + 0xCF =(ending_mac)00188BFFDDC9

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

FlexAddress の有効化

FlexAddress は SD カードに搭載されており、この機能を有効にするには、SD カードを CMC に挿入する必要があります。FlexAddress 機能を有効にするには、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 を有効にしない場合、これらのアップデートは不要です。下記の表で記載されるアップデートには、サーバーモジュール BIOS、I/O メザニン BIOS またはファームウェア、および CMC ファームウェアが含まれます。FlexAddress を有効にする前に、これらのアップデートを適用する必要があります。アップデートを適用しないと FlexAddress が正しく機能しない場合があります。

コンポーネント	最低必要なバージョン
Ethernet メザニン カード - Broadcom M5708t, 5709, 5710	ブートコードファームウェア 4.4.1 以降 iSCSI ブートファームウェア 2.7.11 以降 PXE ファームウェア 4.4.3 以降
FC メザニン カード - QLogic QME2472, FC8	BIOS 2.04 以降
FC メザニン カード - Emulex LPe1105-M4, FC8	BIOS 3.03a3 とファームウェア 2.72A2 以降
サーバーモジュール BIOS	(PowerEdge™ M600)BIOS 2.02 以降 (PowerEdge™ M605)BIOS 2.03 以降 PowerEdge M805

	PowerEdge M905 PowerEdge M610 PowerEdge M710
PowerEdgeM600/M605 LAN on motherboard (LOM)	ブートコードファームウェア 4.4.1 以降 iSCSI ブートファームウェア 2.7.11 以降
iDRAC	PowerEdge xx0x システムのバージョン 1.50 以降 PowerEdge xx1x システムのバージョン 2.10 以降
CMC	バージョン 1.11 以降

メモ: 2008年6月以降に発注したシステムには、正しいバージョンのファームウェアが装備されます。

FlexAddress 機能を正しく導入するには、BIOS とファームウェアを以下の順序でアップデートしてください。

1. メザニンカードのファームウェアと BIOS をすべてアップデートします。
2. サーバーモジュールの BIOS をアップデートします。
3. サーバーモジュールの iDRAC ファームウェアをアップデートします。
4. シャーシ内の CMC ファームウェアをすべてアップデートします。冗長 CMC がある場合は、必ず両方をアップデートしてください。
5. 冗長 CMC モジュールシステムではパッシブモジュールに、冗長なしのシステムでは CMC モジュール 1 つに SD カードを挿入します。

メモ: FlexAddress をサポートする CMC ファームウェア(バージョン 1.10 以降)がインストールされていないと、FlexAddress の機能は有効になりません。

SD カードのインストール手順については、『Chassis Management Controller (CMC) セキュアデジタル (SD) カード技術仕様』を参照してください。

メモ: FlexAddress 機能は SD カードに格納されています。システム機能障害の発生を防ぐため、SD カードに格納されているデータは暗号化されており、いかなる複製や変更も禁止されています。

メモ: SD カードはシャーシ 1 台につき 1 枚のみ使用できます。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。

SD 機能カードがインストールされていると、CMC の再起動時に FlexAddress 機能は自動的に有効になり、現在のシャーシにバインドされます。SD カードを冗長 CMC システムにインストールした場合は、冗長 CMC がアクティブになるまで FlexAddress 機能は有効になりません。冗長 CMC をアクティブにする方法については、『Chassis Management Controller (CMC) セキュアデジタル (SD) カード技術仕様』を参照してください。

CMC が再起動したら、「FlexAddress 有効化の検証」のセクションの手順に従い、アクティベーションプロセスを検証します。

FlexAddress 有効化の検証

FlexAddress の正しい有効化を確認するために、RACADM コマンドを使用して、SD 機能カードおよび FlexAddress 有効化を検証します。

SD 機能およびそれのステータスを検証するには、以下の RACADM コマンドを使用します。

```
racadm featurecard -s
```

下記の表では、コマンドによって返されるステータスメッセージが記載されています。

表 6-1 featurecard -s コマンドによって返されるステータスメッセージ

ステータスメッセージ	操作
機能カードが挿入されていません。	SD カードが正しく CMC に挿入されていることを確認してください。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 CMC であることを確認します。
挿入されている機能カードは有効で、次の FlexAddress 機能が含まれています。機能カードはこのシャーシにバインドされています。	処置の必要はありません。

挿入されている機能カードは有効で、次の FlexAddress 機能が含まれています。機能カードは他のシャーシにバインドされています。 svctag = ABC1234, SD card SN = 01122334455	SD カードを取り外し、現在のシャーシ用の SD カードを見つけて取り付けます。
挿入されている機能カードは有効で、次の FlexAddress 機能が含まれています。機能カードはシャーシにバインドされていません。	機能カードは、他のシャーシに移動したり、現在のシャーシで再び有効にしたりすることができます。現在のシャーシで再び有効にするには、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。

シャーシ上で有効なすべての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
```

このコマンドで、以下のステータスメッセージが返されます。

```
Feature = FlexAddress

Date Activated = 8 April 2008 - 10:39:40

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

シャーシ上に有効な機能が存在しない場合は、コマンドは次のメッセージを返します。

```
racadm feature -s

No features active on the chassis.
```

RACADM コマンドの詳細については、『Dell Chassis Management Controller 管理者リファレンスガイド』の feature および featurecard コマンドの項を参照してください。

FlexAddress の無効化

RACADM コマンドを使用して、SD カードをインストール前の状態に戻し、FlexAddress 機能を無効にすることができます。ウェブインタフェースでは、無効にする機能は提供されません。無効にすると、SD カードを元の状態に戻し、別のシャーシ上に装着し、有効にすることが可能になります。

メモ: SD カードは、物理的に CMC に取り付ける必要があり、無効化コマンドを実行する前に、シャーシの電源を切る必要があります。

カードが装着されていない状態、または異なるシャーシのカードを装着した状態で、無効化コマンドを実行した場合、機能は無効になりますが、カードに変更は加えられません。

FlexAddress の無効化

FlexAddress 機能を無効にし、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
```

コマンドを実行し、無効化に成功すると、以下のステータスメッセージが返されます。

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

コマンド実行前に、シャーシの電源を切らなかった場合、コマンドは失敗し、次のエラーメッセージが表示されます。

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

コマンドの詳細は、『Dell Chassis Management Controller 管理者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。

CLI を使用した FlexAddress の設定

メモ: シャーシ指定の MAC アドレスを iDRAC に出力するには、スロットとファブリックの両方を有効にする必要があります。

メモ: グラフィカルユーザーインタフェースを使用して FlexAddress ステータスを表示することもできます。詳細については、「FlexAddress」を参照してください。

コマンドラインインタフェースを使用して、ファブリックごとに FlexAddress を有効または無効にすることができます。また、スロットごとに、機能を有効/無効にすることも可能です。ファブリックごとに機能の有効化を行う場合は、有効にするスロットを選択できます。たとえば、ファブリック-A のみが有効な場合、有効になったスロットで FlexAddress はファブリック-A でのみ有効になります。その他のファブリックは、サーバー上で工場出荷時に割り当てられた WWN/MAC を使用します。この機能が動作するには、ファブリックを有効にし、サーバーの電源を切る必要があります。

FlexAddress が有効なスロットは、すべてのファブリックでも有効になります。たとえば、ファブリック-A および B を有効にし、ファブリック-A のスロット1で FlexAddress を有効にして、ファブリック-B のスロット1で無効にすることはできません。

ファイブリック上で有効または無効にするには、次の RACADM コマンドを使用します。

```
racadm setflexaddr [-f <ファブリック名> <状態>]
```

```
<ファブリック名> = A、B、C、or iDRAC
```

```
<状態> = 0 or 1
```

0 は無効、1 は有効を示します。

スロット上で有効または無効にするには、次の RACADM コマンドを使用します。

```
racadm setflexaddr [-i <スロット番号> <状態>]
```

```
<スロット番号> = 1 to 16
```

```
<状態> = 0 or 1
```

0 は無効、1 は有効を示します。

コマンドの詳細については、『Dell Chassis Management Controller 管理者リファレンスガイド』の setflexaddr コマンドの項を参照してください。

Linux 向け FlexAddress の追加設定

Linux ベースのオペレーティングシステム上で、サーバー指定の MAC ID からシャーシ指定の MAC ID に変更する場合は、追加の設定手順が必要となる場合があります。

- SUSE Linux Enterprise Server 9 および 10: ユーザーは、Linux システム上で YAST(Yet another Setup Tool)を実行し、ネットワークデバイスの設定を行い、ネットワークサービスを再起動する必要がある場合があります。
- Red Hat® Enterprise Linux® 4(RHEL) および RHEL 5: システム上の新しいまたは変更されたハードウェアを検知し、設定するユーティリティ(Kudzu)を実行します。Kudzu ではハードウェアの検出メニューが表示され、ハードウェアが削除されたり、新しいハードウェアが追加された場合に、MAC アドレスの変更を検出します。

CLI を使用した FlexAddress ステータスの表示

コマンドラインインタフェースを使用して、FlexAddress のステータス情報を表示することができます。シャーシ全体または特定のスロットのステータス情報の表示が可能です。表示される情報には、以下が含まれます。

- ファブリック構成
- FlexAddress 有効化/無効化
- スロット番号および名前
- シャーシ指定およびサーバー指定のアドレス
- 使用アドレス

シャーシ全体の FlexAddress ステータスを表示するには、次の RACADM コマンドを使用します。

```
racadm getflexaddr
```

特定のスロットの FlexAddrss ステータスを表示するには、次のコマンドを使用します。

```
racadm getflexaddr [-i <スロット番号>]
```

```
<スロット番号> = 1 to 16
```

FlexAddress 設定の詳細については、「CLI を使用した FlexAddress の設定」を参照してください。コマンドの詳細については、『Dell Chassis Management Controller 管理者リファレンスガイド』の getflexaddr コマンドの項を参照してください。

CLI を使用した FlexAddress の設定

FlexAddress を利用した Wake-On-LAN の使用

FlexAddress を初めて導入する場合、機能 を有効にするには、サーバーモジュールの電源を一度切ってから入れ直す手順が必要です。イーサネット デバイス上の FlexAddress は、サーバーモジュールの BIOS によってプログラムされます。サーバーモジュールの 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の電源がオンで動作可能である必要があります。電源オフして電源オンするサイクルが完了すると、Wake-On-LAN(WOL)機能にシャーシ指定 MAC ID が利用できるようになります。

FlexAddress のトラブルシューティング

本項には、FlexAddress のトラブルシューティング情報が含まれます。

1. 機能カードが取り外された場合、どうなりますか?

   何も起きません。機能カードを取り外したり、保管したり、そのままにすることができます。

2. あるシャーシで使用していた機能カードを取り外し、他のシャーシに取り付けた場合、どうなりますか？

ウェブインタフェースは、以下のエラーを表示します。

This feature card was activated with a different chassis. It must be removed before accessing the FlexAddress feature. (この機能カードは、異なるシャーシで有効になっています。 FlexAddress 機能にアクセスする前に、取り外す必要があります。)

Current Chassis Service Tag (現在のシャーシサービスタグ) = XXXXXXXX

Feature Card Chassis Service Tag (機能カードのシャーシサービスタグ) = YYYYYYYY

CMC ログに以下のエントリが追加されます。

cmc <date timestamp> : feature 'FlexAddress@XXXXXXX' not activated; chassis ID= 'YYYYYYY' (cmc <日付タイムスタンプ> : 'FlexAddress@XXXXXXX' の機能は有効ではありません; シャーシ ID='YYYYYYY')

3. 機能カードが取り外され、非 FlexAddress カードが取り付けられた場合は、どうなりますか？

カードへの変更または有効化は行われません。カードは CMC によって無視されます。この場合、$racadm featurecard -s のコマンドを実行すると、以下のメッセージが返されます。

No feature card inserted (機能カードが挿入されていません。)

ERROR: can't open file (エラー: ファイルを開くことができません。)

4. シャーシのサービスタグが再プログラムされた場合、そのシャーシに機能カードがバインドされていると、どうなりますか？

   - 元の機能カードが対象のシャーシまたは別のシャーシ上のアクティブな CMC にある場合は、ウェブインタフェースには次のエラーメッセージが表示されます。

     This feature card was activated with a different chassis. It must be removed before accessing the FlexAddress feature. (この機能カードは、異なるシャーシで有効になっています。FlexAddress 機能にアクセスする前に、取り外す必要があります。)

     Current Chassis Service Tag (現在のシャーシサービスタグ) = XXXXXXXX

     Feature Card Chassis Service Tag (機能カードのシャーシサービスタグ) = YYYYYYYY

     元の機能カードは対象のシャーシや他のシャーシで無効にできなくなります(ただし、デルサービスを使って元のシャーシサービスタグをシャーシに挿入してプログラムしなおし、元の機能カードを搭載した CMC が対象のシャーシで有効になる場合を除く)。

   - FlexAddress 機能は最初にバインドされたシャーシでは有効のままになります。対象のシャーシのバインド機能は新しいサービスタグを反映するように更新されます。

- 冗長 CMC システムに 2 つの機能カードがインストールされている場合は、どうなりますか？エラーは発生しますか？

アクティブ CMC に取り付けられた機能カードは有効になり、シャーシにインストールされます。2 つめのカードは CMC によって無視されます。

6. 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 モジュールに取り付ける前に、書き込み保護ラッチが「アンロック」の位置になっていることを確認してください。SD カードが書込み保護されていると、FlexAddress 機能をアクティブにできません。この場合、$racadm feature -s コマンドを実行すると、次のメッセージが返されます。

No features active on the chassis. ERROR: read only file system (シャーシ上に有効な機能はありません。エラー: 読み取り専用ファイルシステムです。)

7. アクティブな CMC モジュールに SD カードが存在しない場合は、どうなりますか？

$racadm featurecard -s コマンドを実行すると、次のメッセージが返されます。

```
No feature card inserted. (機能カードが挿入されていません。)
```

8. 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た場合、FlexAddress 機能はどうなりますか？

   FlexAddress 機能を使用する前に、サーバーモジュールの電源を切って、電源を入れ直す必要があります。サーバーの BIOS 更新が完了した後は、サーバーの電源を一度切断して、電源を入れ直さない限り、サーバーモジュールにシャーシ指定のアドレスが割り当てられません。

9. 単一の CMC を持つシャーシが、バージョン 1.10 以前のファームウェアにダウングレードされた場合、どうなりますか？

   - FlexAddress 機能と設定は、シャーシから削除されます。
   - このシャーシで機能を有効するのに使用した機能カードは変更されず、シャーシにバインドされたままになります。続いて、シャーシの CMC ファームウェアがバージョン 1.10 以降にアップグレードされると、FlexAddress 機能は元の機能カード（必要な場合）の再挿入、CMC のリセット（ファームウェアアップグレードの完了後に機能カードが挿入された場合）、および機能の再設定を行うことで再度有効になります。

10. 冗長 CMC を持つシャーシの CMC をバージョン 1.10 以前のファームウェアを持つ CMC と取り替える場合、現在の FlexAddress 機能と設定が削除されないようにするためには、次の手順に従う必要があります。

    a. アクティブな CMC ファームウェアのバージョンが常に 1.10 以降であるようにしてください。

    b. スタンバイ CMC を取り外し、新しい CMC を取り付けます。

    c. アクティブ CMC から、スタンバイ CMC のファームウェアをバージョン 1.10 以降にアップグレードします。

メモ: スタンバイ CMC ファームウェアを 1.10 以降にアップデートしなかった場合にフェイルオーバーが発生すると、FlexAddress 機能は設定されず、機能を再度有効にして設定しなおす必要があります。

11. FlexAddress で deactivation コマンドを実行したときに、SD カードがシャーシに挿入されていませんでした。SD カードを復旧するにはどのようにすればよいですか?

    FlexAddress が無効になっているときに SD カードが挿入されていなかった場合は、SD カードを使って別のシャーシに FlexAddress をインストールすることはできません。カードを使用できるように修復するには、カードをバインド先のシャーシ内の CMC に挿入しなおし、FlexAddress を再インストールしてから、FlexAddress を再度無効にします。

12. SD カードを正しくインストールし、すべてのファームウェア/ソフトウェアアップデートもインストールしています。FlexAddress は有効になっていますが、サーバー導入画面に何も表示されません。何が問題なのでしょうか ?

    これは、ブラウザのキャッシュの問題です。ブラウザを一度閉じてから、再度開いてください。

13. 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 機能は有効になったままで使用できます。すべてのファブリックとスロットがデフォルトで選択されます。

    メモ: シャーシの電源を落としてから、RACADM コマンド racresetcfg を発行することをお勧めします。

コマンドメッセージ

下の表に、RACADM コマンドおよび一般的な FlexAddress の状況における出力を示します。

表 6-2 FlexAddress コマンドおよび出力

状況 :	コマンド	出力
アクティブ CMC モジュールの SD カードが他のサービスタグにバインドされている。	$racadm featurecard -s	The feature card inserted is valid and contains the following feature(s) FlexAddress: The feature card is bound to another chassis, svctag = J310TF1 SD card SN =0188BFFE03A
アクティブ CMC モジュールの SD カードが同じサービスタグにバインドされている。		

	$racadm featurecard -s	The feature card inserted is valid and contains the following feature(s) FlexAddress: The feature card is bound to this chassis
アクティブ CMC モジュールの SD カードがどのサービスタグにもバインドされていない。	$racadm featurecard -s	The feature card inserted is valid and contains the following feature(s) FlexAddress: The feature card is not bound to any chassis
何らかの理由で FlexAddress 機能はシャーシ上で有効になっていない（SD カードが挿入されていない、破損した SD カード、機能が無効、SD カードが異なるシャーシにバインドされている）	$racadm setflexaddr [-f <ファブリック名> <スロット状態>] OR $racadm setflexaddr [-i <スロット#> <スロット状態 >]	ERROR: Flexaddress feature is not active on the chassis
ゲストユーザーがスロット/ファブリック上で FlexAddress の設定を試みる	$racadm setflexaddr [-f <ファブリック名> <スロット状態>] $racadm setflexaddr [-i <スロット#> <スロット状態 >]	ERROR: Insufficient user privileges to perform operation
シャーシの電源がオンの状態で FlexAddress 機能の無効化	$racadm feature -d -c flexaddress	ERROR: Unable to deactivate the feature because the chassis is powered ON
ゲストユーザーがシャーシ上の機能の無効化を試みる	$racadm feature -d -c flexaddress	ERROR: Insufficient user privileges to perform operation
サーバーモジュールの電源がオンの状態で、スロット/ファブリックの FlexAddress 設定を変更する	$racadm setflexaddr -i 1 1	ERROR: Unable to perform the set operation because it affects a powered ON server

---

FlexAddress DELL ソフトウェア製品ライセンス契約

本契約書は、ユーザーであるお客様と Dell Products, L.P または Dell Global B.V.との法的な契約となります。本契約は 、Dell 製品に同梱されているすべてのソフトウェア（以下、「本ソフトウェア」と総称します）に適用されます。お客様と本ソフトウェアの制作者または所有者との間で個別にライセンス契約は締結できません。本契約は本ソフトウェアまたはその他の知的財産の販売に関するものではありません。本ソフトウェアの財産所有権および知的所有権は本ソフトウェアの制作者または所有者に属します。本契約で明示的に付与されていない権利はすべて、本ソフトウェアの制作者または所有者が所有します。本ソフトウェアのパッケージを開梱または開封したり、本ソフトウェアをインストールまたはダウンロードしたり、本製品にあらかじめロードまたは組み込まれている本ソフトウェアを使用すると、本契約書の条項に同意したとみなされます。これらの条項に同意できない場合、直ちに本ソフトウェアのすべての製品（ディスク、印刷物、およびパッケージ）を返品し、あらかじめロードまたは組み込まれている本ソフトウェアはすべて削除してください。

本ソフトウェアの複製は、任意の時点において 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。本ソフトウェアの複数のライセンスを所有されている場合は、ライセンスを所有する限りいつでも、ライセンスの数だけ複製を使用できます。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がロードされている場合を「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、これら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されている場合は「使用」とみなしません。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ないようにしてください。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、ユーザー数と同数のライセンスを購入してから本ソフトウェアの使用を許可してください。お客様がデルの販売会社または関連会社である場合には、お客様は、デルまたはデルにより指名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の使用に関する監査を行う権利を付与し、監査にあたってはデルに協力することに同意し、かつ、本ソフトウェアの使用に関連するすべての記録をデルに提供することに同意します。監査は、お客様が本契約の条項を遵守しているかどうかに関する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、1 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、本ソフトウェア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、Dell 製品の販売または譲渡を目的に、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。お客様のコンピュータに付属のパッケージに、CD-ROM、3.5 インチディスクおよび 5.25 インチディスクが同梱されている場合は、お客様のコンピュータに適したディスクのみを使用してください。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、お客様に本ソフトウェアディスクが配送された日から 90 日間、通常の使用において材質または製作上の欠陥が生じないことを保証いたします。この保証はお客様に限定され、譲渡することはできません。すべての黙示的保証は、お客様が本ソフトウェアを入手した日から 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、この保証期間の制限は適用されない場合があります。Dell およびその供給業者の責任範囲およびお客様の救済措置は、次のいずれかに制限されます。(a)本ソフトウェアの購入代金を返却する。(b)お客様のコストとリスク負担で、本保証を満たさないディスクが返却承認番号付きで Dell に返却された場合、新しいディスクと交換する。いかなる事故、誤用、乱用、または Dell サポート以外のサービスや修正が原因でディスクの機能に不具合が生じた場合、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 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こと、エラーが無いことを保証するものではありません。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と、その使用および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 およびその関連供給会社は、商業性や特定目的への適合性に対する保証を含め、またそれらに限定せず、明示的であれ黙示的であれ、本ソフトウェアおよび同梱されるすべての印刷物に対する上記以外のいかなる保証をもいたしません。本限定保証は、お客様に特定の法的権利を与えるものです。国や地域によってはさらに他の権利が与えられる場合もあります。

本ソフトウェアの使用や使用できなかったことにより発生した利益の損失、営業の中断、データの消失、金銭的喪失などを含むあらゆる損害に対し、Dell またはその供給業者は、そのような損害の可能性を示唆していたとしても、一切の責任を負うものではありません。国や地域によっては、間接的または付随的な損害に対する責任の除外や制限が禁じられているため、一部のお客様にはこの制限は適用されません。

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用であることを期待して頒布されていますが、「現状のまま」提供されており、市場性および特定用途の適合性に関する暗黙的な保障に限らず、明示的または暗黙的にいかなる保証も行いません。いかなる原因によるものであれ、また、いかなる責任理論に基づくものであれ、契約、無過失責任、または不法行為のいずれによるにせよ(過失その他の場合を含む)、使用法の如何を問わず、本ソフトウェアの使用によって発生するいかなる直接的、間接的、偶発的、特別的、典型的、または派生的損害(代替品またはサービスの調達、使用機会、データ、もしくは利益の喪失、または営業の中断を含みますが、それらに限定されません)に対しても、デル、著作権保持者、または提供者は、かかる損害の可能性が示唆されていたとしても、いかなる場合も責任を負いません。

米国 政府機関の制限された権利

本ソフトウェアおよび本マニュアルは、48 C.F.R. 2.101 条で定義される「商品」で、48 C.F.R. 12.212 条の「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文書」で 構成されます。48 C.F.R. 12.212 条 および 48 C.F.R.227.7202-1 から 227.7202-4 条で定められているとおり、すべての米国政府機関エンド ユーザーは、本製品につき本契約に記載された権利のみに従ってソフトウェアおよび書類を取得します。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。

目次ページに戻る

目次ページに戻る

iKVM モジュールの使用

Dell™ Chassis Management Controllerファームウェアバージョン 2.10 ユーザーガイド

概要

Dell™ M1000e サーバーシャーシのローカルアクセス KVM モジュールは Avocent® Integrated KVM スイッチモジュール（iKVM）と呼ばれています。iKVM はキーボード、ビデオ、マウスなどのアナログスイッチで、シャーシに差し込みます。iKVM はシャーシにホットプラグできるオプションモジュールで、シャーシ内のサーバーとアクティブな CMC のコマンドラインにローカルのキーボード、マウス、ビデオでアクセスできるようになります。

iKVM ユーザーインタフェース

iKVM では、ホットキーでアクティブになる On Screen Configuration and Reporting（OSCAR®）グラフィカルユーザーインタフェースが使用されています。OSCAR では、アクセスするサーバーや Dell CMC コマンドラインをローカルのキーボード、ディスプレイ、マウスなどで選択できます。

シャーシ 1 つに 1 つの iKVM セッションのみが許可されています。

セキュリティ

OSCAR ユーザーインタフェースを使用すると、システムをスクリーンセーバーのパスワードで保護できます。ユーザーが定義した時間が経過すると、スクリーンセーバーモードになり、正しいパスワードを入力して OSCAR を再びアクティブにするまでアクセスが禁止されます。

スキャン

OSCAR ではサーバーのリストを選択できます。サーバーは OSCAR がスキャンモードの間に、選択した順序で表示されます。

サーバーの識別

CMC はシャーシ内のすべてのサーバーにスロット名を割り当てます。層接続から OSCAR インタフェースを使用してサーバーに名前を割り当てることもできますが、CMC が割り当てた名前が優先され、OSCAR を使用してサーバーに割り当てた新しい名前はすべて上書きされます。

CMC は固有の名前を割り当ててスロットを識別します。CMC ウェブインタフェースを使用してスロット名を変更する場合は、「スロット名の編集」を参照してください。RACADM を使用してスロット名を変更する場合は、『Dell Chassis Management Controller 管理者リファレンスガイド』の setslotname の項を参照してください。

ビデオ

iKVM ビデオ接続では、640 x 480（60Hz）から最大 1280 x 1024（60Hz）までのビデオ画面解像度がサポートされています。

プラグアンドプレイ

iKVM はデータ表示チャネル(DDC)プラグアンドプレイをサポートしています。DDC はビデオモニタの設定を自動化するもので、VESA DDC2B 規格に準拠しています。

FLASH アップグレード可能

CMC ウェブインタフェースまたは RACADM の **fwupdate** コマンドを使用して iKVM ファームウェアをアップデートできます。詳細については、「CMC からの iKVM の管理」を参照してください。

物理的な接続インタフェース

シャーシのフロントパネル、アナログコンソールインタフェース(ACI)、およびシャーシのリアパネルから、iKVM を介してサーバーまたは CMC CLI コンソールに接続できます。

メモ: シャーシの前面にあるコントロールパネルのポートは、オプションの iKVM 専用に設計されています。iKVM がない場合は、前面コントロールパネルのポートを使用できません。

iKVMの 接続手順

一度に 1 つの iKVM 接続のみが使用可能です。iKVM は各接続タイプに優先順位を割り当てるので、複数の接続がある場合は、1 つの接続だけが使用可能になり、その他は無効になります。

iKVM 接続の優先順位は以下のとおりです。

1. フロントパネル
2. ACI
3. リアパネル

たとえば、フロントパネルと ACI に iKVM 接続がある場合、フロントパネルの接続はアクティブなままで、ACI の接続が無効になります。ACI とリアパネルの接続がある場合は、ACI の接続が優先されます。

ACI 接続の層

iKVM では、ローカルでリモートコンソールスイッチポートを使用するか、Dell RCS® ソフトウェアからリモートコンソールを使用して、サーバーと iKVM の CMC コマンドラインコンソールとの層接続が可能です。iKVMは、以下の製品からの ACI 接続をサポートしています。

- 180AS、2160AS、2161DS-2*、2161DS-2、または 4161DS Dell Remote Console Switches™
- Avocent AutoView® スイッチシステム
- Avocent DSR® スイッチシステム
- Avocent AMX® スイッチシステム

* Dell CMC コンソール接続はサポートしていません。

メモ: iKVM は Dell 180ES と 2160ES への ACI 接続もサポートしていますが、階層化はシームレスではありません。この接続には USB から PS2 への SIP が必要です。

OSCAR の使用

この項では OSCAR インタフェースの概要を提供します。

ナビゲーションの基本

表9-1では、キーボードとマウスを使用して OSCAR インタフェースを移動する方法を説明します。

表 9-1 OSCAR キーボードとマウスの操作

キーまたはキーシーケンス	結果
• <Print Screen>-<Print Screen>	OSCAR の起動 の設定によって、これらのどのシーケンスを使用しても OSCAR を開くことができます。メイン ダイアログボックスの OSCAR の起動 セクションでチェックボックスをオンにして、OK をクリックすると、2 つ、3 つ、またはすべてのキーシーケンスを有効にできます。
• <Shift>-<Shift>	
• <Alt>-<Alt>	
• <Ctrl>-<Ctrl>	
<F1>	現在のダイアログボックスの ヘルプ 画面を開きます。
<Esc>	変更を保存せずに現在のダイアログボックスを閉じて、前のダイアログボックスに戻ります。 メイン ダイアログボックスでは、<Esc> で OSCAR インタフェースを終了して、選択したサーバーに戻ります。 メッセージボックスでは、ポップアップボックスを閉じて現在のダイアログボックスに戻ります。
<Alt>	下線付きの英字やその他の指定した文字と組み合わせて使用し、ダイアログボックスを開いたり、オプションを選択(チェックボックスをオンに)したり、処置を実行したりします。
<Alt>+<X>	現在のダイアログボックスを閉じて、前のダイアログボックスに戻ります。
<Alt>+<O>	OK ボタンを選択して、前のダイアログボックスに戻ります。
<Enter>	メイン ダイアログボックスでスイッチ操作を完了し、OSCAR を終了します。
シングルクリック、<Enter>	テキストボックスで、編集するテキストを選択し、左矢印キーと右矢印キーを有効にしてカーソルを移動します。<Enter> をもう一度押すと、編集モードが終了します。
<Print Screen>、<バックスペース>	他のキー入力がない場合は、前の選択項目に切り替えます。
<Print Screen>、<Alt>+<0>	ユーザーをサーバーから即座に切断します。サーバーが選択されません。ステータスフラグには「空き」と表示されます。(この処置はキーボードの =<0> にのみ適用され、キーパッドには適用されません。)
<Print Screen>、<Pause>	スクリーンセーバーモードを即座にオンにし、パスワード保護されている場合は、そのコンソールにアクセスできなくします。
上下の矢印キー	リストの行から行へとカーソルを移動します。
左右の矢印キー	テキストボックスの編集時に列内でカーソルを移動します。
<Home>/<End>	カーソルをリストの先頭(Home)または一番下(End)に移動します。
<Delete>	テキストボックスの文字を削除します。
数字キー	キーボードまたはキーパッドから入力します。
<Caps Lock>	無効になっています。大文字と小文字を切り替えるには、<Shift> キーを使用します。

OSCAR の設定

OSCAR の設定メニューからサーバーの設定に使用できる機能については、表9-2 で説明します。

表 9-2 OSCAR 設定メニューの機能

機能	目的
メニュー	サーバーのリスト表示をスロットの番号順と、名前のアルファベット順の間で切り替えます。
セキュリティ	• パスワードを設定してサーバーへのアクセスを制限します。 • スクリーンセーバーを有効にし、スクリーンセーバーが表示されるまでのアイドル時間を設定し、スクリーン保護モードを設定します。
フラグ	ステータスフラグの表示、タイミング、色、配置を変更します。

言語	OSCAR の全画面の言語を変更します。
ブロードキャスト	キーボードとマウスの操作で複数のサーバーを同時に制御するように設定します。
スキャン	最大 16 サーバーのカスタムスキャンパターンを設定します。

設定 ダイアログボックスにアクセスするには

1. <Print Screen> を押して OSCAR インタフェースを起動します。メイン ダイアログボックスが表示されます。
2. 設定 をクリックします。設定 ダイアログボックスが表示されます。

表示動作の変更

サーバーの表示順序を変更し、OSCAR の画面遅延時間を設定するには、メニュー ダイアログボックスを使用します。

メニュー ダイアログボックスにアクセスするには

1. <Print Screen> を押して OSCAR を起動します。メイン ダイアログボックスが表示されます。
2. 設定、メニュー の順にクリックします。メニュー ダイアログボックスが表示されます。

メイン ダイアログボックスでサーバーのデフォルトの表示順序を変更するには

1. サーバーを名前のアルファベット順に表示するには、名前 を選択します。

   または

   スロット を選択し、サーバーをスロット番号順に表示します。
2. OK をクリックします。

OSCAR をアクティブにするキーシーケンスを 1 つ以上割り当てるには

1. OSCAR の起動 メニューからキーシーケンスを選択します。
2. OK をクリックします。

OSCAR を起動するデフォルトのキーは <Print Screen> です。

OSCAR の画面遅延時間を設定するには

1. <Print Screen> を押してから OSCAR が表示されるまでの遅延を秒数（0 ～ 9）で入力します。<0> と入力すると、遅延なしで OSCAR が起動します。
2. OK をクリックします。

OSCAR を遅延表示する時間を設定すると、ソフトスイッチを完了できます。ソフトスイッチの実行方法については、「ソフトスイッチ」を参照してください。

ステータスフラグの制御

ステータスフラグはデスクトップに表示され、選択されているサーバーの名前、または選択されているスロットの状態を示します。フラグ ダイアログボックスを使用して、サーバーごとに表示するフラグを設定したり、フラグの色、透明性、表示時間、デスクトップ上の配置などを変更します。

表 9-3 OSCAR ステータスフラグ

フラグ	説明

	名前によるフラグの種類
	ユーザーがすべてのシステムから切断されたことを示すフラグ
	ブロードキャストモードが有効であることを示すフラグ

フラグ ダイアログボックスにアクセスするには

1. <Print Screen> を押します。メイン ダイアログボックスが表示されます。
2. 設定、フラグ の順にクリックします。フラグ ダイアログボックスが表示されます。

ステータスフラグの表示方法を指定するには

1. フラグを常に表示するには 表示 を選択し、切り替え後 5 秒間だけフラグを表示するには 表示と時間指定 を選択します。

   メモ: 時間指定 だけを選択すると、フラグは表示されません。

2. 表示色 セクションからフラグの色を選択します。オプションは黒、赤、青、紫です。
3. 表示モード で、無地のカラーフラグには不透明 を選択し、フラグからデスクトップが透けて見えるようにするには 透明 を選択します。
4. ステータスフラグをデスクトップに配置するには
   a. 位置の設定 をクリックします。フラグの位置設定 が表示されます。
   b. タイトルバーを左クリックし、デスクトップ上の任意の場所までドラッグします。
   c. フラグ ダイアログボックスに戻るには、右クリックします。

メモ: フラグの位置変更は、フラグ ダイアログボックスで OK をクリックするまでは保存されません。

5. OK をクリックして設定を保存します。

   変更を保存せずに終了するには、☒ をクリックします。

---

iKVM によるサーバーの管理

iKVM は最大 16 のサーバーをサポートするアナログスイッチマトリックスです。iKVM スイッチは OSCAR ユーザーインタフェースを使用してサーバーの選択と設定を行います。また、iKVM には CMC コマンドラインコンソールから CMC への接続を確立するためのシステム入力が含まれています。

周辺機器の互換性とサポート

iKVM は以下の周辺機器と互換性があります。

- QWERTY、QWERTZ、AZERTY、および日本語 109 配列の標準 PC USB キーボード。
- DDC をサポートしている VGA モニタ。
- 標準 USB ポインティングデバイス。
- iKVM のローカル USB ポートに接続している電源内蔵式 USB 1.1 ハブ。
- Dell M1000e シャーシのフロントパネルコンソールに接続している電動 USB 2.0 ハブ。

メモ: iKVM のローカル USB ポートではキーボートとマウスを複数使用できます。iKVM は入力信号を統合します。複数の USB キーボードまたはマウスから同時に入力信号があると、予測不能の結果が生じる可能性があります。

メモ: サポートされているキーボード、マウスおよび USB ハブのみ USB 接続できます。iKVM は、その他の USB 周辺機器から送信されるデータをサポートしていません。

サーバーの表示と選択

iKVM からサーバーを表示、設定、管理するには、OSCAR メイン ダイアログボックスを使用します。サーバーは名前またはスロットを基準に表示できます。スロット番号は、サーバーが使用するシャーシスロット番号です。スロット 列は、サーバーが取り付けられているスロット番号を示します。

メモ: Dell CMC コマンドラインはスロット 17 を占有しています。このスロットを選択すると、RACADM コマンドを実行し、サーバーのシリアル コンソールまたは I/O モジュールに接続する CMC コマンド ラインを表示します。

メモ: サーバー名とスロット番号は CMC によって割り当てられます。

メイン ダイアログボックスにアクセスするには、次の手順を実行します。

<Print Screen> を押して OSCAR インタフェースを起動します。メイン ダイアログボックスが表示されます。

または

パスワードが割り当てられている場合は、パスワード ダイアログボックスが表示されます。パスワードを入力して OK をクリックします。メイン ダイアログボックスが表示されます。

パスワード設定の詳細については、「コンソールのセキュリティの設定」を参照してください。

メモ: OSCAR の起動には 4 つのオプションがあります。メイン ダイアログボックスの OSCAR の起動 セクションでボックスを選択して、OK をクリックすると、1 つ、複数、またはすべてのキーシーケンスを有効にできます。

サーバーのステータス表示

シャーシのサーバーのステータスは、メイン ダイアログボックスの右側に表示されます。次の表で、ステータス記号について説明します。

表 9-4 OSCAR インタフェースのステータス記号

記号	説明
	(緑色のドット)サーバーはオンラインです。
	(赤色の X。)サーバーはオフラインまたはシャーシにありません。
	(黄色のドット)サーバーは利用できません。
	(緑色の A または B)サーバーは、英字:A=リアパネル、B=フロントパネルで示されるユーザーチャネルによってアクセスされています。

サーバーの選択

サーバーを選択するには、メイン ダイアログボックスを使用します。サーバーを選択すると、iKVM によってキーボードとマウスがそのサーバーの正しい設定に再構成されます。

- サーバーを選択するには

  サーバー名かスロット番号をダブルクリックします。

または

サーバーのリストがスロット順に表示されている場合は（スロット ボタンが押された状態）、スロット番号を入力して <Enter> を押します。

または

サーバーのリストが名前順に表示されている場合は（名前 ボタンが押された状態）、サーバー名の最初の文字をいくつか入力して固有として確立し、<Enter> を 2 回押します。

- 前のサーバーを選択するには

<Print Screen> を押してから <Backspace> を押します。このキーの組み合わせによって、前の接続と現在の接続が切り替わります。

- サーバーからユーザーを切断するには

<Print Screen> を押して OSCAR にアクセスしてから 切断 をクリックします。

または

<Print Screen> を押してから <Alt><0> を押します。この操作により、サーバーが選択されていない空きの状態になります。デスクトップのステータスフラグがアクティブな場合は、「空き」と表示されます。「ステータスフラグの制御を参照してください。

ソフトスイッチ

ソフトスイッチは、ホットキーシーケンスを使用したサーバー間の切り替えです。<Print Screen> を押して、サーバーの名前や数字を先頭から何文字か入力すると、ソフトスイッチでサーバーに切り替えることができます。前に遅延時間（<Print Screen> を押してから メイン ダイアログボックスが表示されるまでの秒数）を設定した場合は、その時間が経過する前にキーシーケンスを押すと、OSCAR インタフェースは表示されません。

OSCAR にソフトスイッチを設定するには

1. <Print Screen> を押して OSCAR インタフェースを起動します。メイン ダイアログボックスが表示されます。
2. 設定、メニュー の順にクリックします。メニュー ダイアログボックスが表示されます。
3. 表示 / 並べ替えキーの 名前 または スロット を選択します。
4. 画面遅延時間 フィールドに遅延時間を秒で入力します。
5. OK をクリックします。

サーバーにソフトスイッチするには

- サーバーを選択するには、<Print Screen> を押します。

手順 3 の選択に従ってサーバーのリストがスロット順に表示されている場合は（スロット ボタンが押された状態）、スロット番号を入力して <Enter> を押します。

または

手順 3 の選択に従ってサーバーのリストが名前順に表示されている場合は（名前 ボタンが押された状態）、サーバー名の最初の文字をいくつか入力して固有として確立し、<Enter> を 2 回押します。

- 前のサーバーに戻るには、<Print Screen> を押してから <Backspace> を押します。

ビデオ接続

iKVM はシャーシのフロントパネルとリアパネルにビデオ接続があります。フロントパネルの接続信号がリアパネルの接続信号より優先されます。モニタがフロントパネルに接続していると、ビデオ接続がリアパネルまで通らず、リアパネルの KVM 接続と ACI の接続が無効であるという OSCAR メッセージが表示されます。モニタが無効になると(フロントパネルから取り外すか CMC コマンドで無効にする)、リアパネルの KVM は無効のままですが、ACI の接続がアクティブになります。(接続の優先度の詳細については、「iKVMの 接続手順」を参照してください。)

フロントパネル接続を有効または無効にする手順の詳細については、「フロントパネルの有効または無効」を参照してください。

割り込み警告

通常、iKVM からサーバーコンソールに接続しているユーザーと、iDRAC GUI コンソールリダイレクト機能を使用して同じサーバーコンソールに接続している別のユーザーは、両者ともコンソールにアクセスして同時に入力できます。

この状況を防止するには、リモートユーザーが iDRAC GUI コンソールリダイレクトを開始する前に iDRAC ウェブインタフェースでローカルコンソールを無効にできます。ローカル iKVM ユーザーには、指定した時間中、接続の割り込みを知らせる OSCAR メッセージが表示されます。ローカルユーザーはサーバーへの iKVM 接続が終了する前に作業を完了する必要があります。

iKVM ユーザーが使用できる割り込み機能はありません。

メモ: リモートの iDRAC ユーザーが特定のサーバーのローカルビデオを無効にした場合は、そのサーバーのビデオ、キーボード、およびマウスが iKVM で使用できなくなります。OSCAR メニューでサーバーの状態が黄色のドットで表示され、ローカルでの使用がロックされているか使用不可であることを示します(「サーバーのステータス表示」を参照)。

コンソールのセキュリティの設定

OSCAR では iKVM コンソールのセキュリティ設定を指定できます。指定した遅延時間ほどコンソールが使用されなかった場合に作動するスクリーンセーバーモードを設定できます。作動すると、キーを押すかマウスを動かすまでコンソールはロックされたままになります。続行するには、スクリーンセーバーのパスワードを入力します。

セキュリティ ダイアログボックスを使用すると、パスワード保護を使用してコンソールをロックしたり、パスワードを設定または変更したり、スクリーンセーバーを有効にしたりできます。

メモ: iKVM のパスワードをなくしたり忘れたりした場合は、CMC ウェブインタフェースまたは RACADM を使用して iKVM 出荷時のデフォルトにリセットできます。「失くしたり忘れたりしたパスワードのクリア」を参照してください。

セキュリティダイアログボックスへのアクセス

1. <Print Screen> を押します。メイン ダイアログボックスが表示されます。
2. 設定、セキュリティ の順にクリックします。セキュリティ ダイアログボックスが表示されます。

パスワードの設定または変更

1. 新規 フィールドでシングルクリックして <Enter> を押すか、ダブルクリックします。
2. 新規 フィールドに新しいパスワードを入力し、<Enter> を押します。パスワードは大文字と小文字が区別され、5 ～ 12 文字必要です。少なくとも英字が 1 つと数字が 1 つ含まれていなければなりません。有効な文字は A ～ Z、a ～ z、0 ～ 9、スペースおよびハイフンです。
3. 再入力 フィールドにパスワードをもう一度入力して <Enter> を押します。
4. パスワードを変更するだけの場合は OK をクリックして、ダイアログボックスを閉じます。

コンソールのパスワード保護

1. 前の手順で説明した方法でパスワードを設定します。
2. スクリーンセーバーを有効にする チェックボックスをオンにします。
3. パスワード保護とスクリーンセーバーの起動を遅らせる アイドル時間(1 ～ 99)を分で入力します。
4. モード:モニタが ENERGY STAR® 準拠の場合は、Energy、それ以外の場合は スクリーン を選択します。

メモ: モードが Energy に設定されている場合は、アプライアンスがモニタをスリープモードにします。これは通常、モニタの電源がオフになり、緑色の電源 LED に代わって黄色が点灯することからわかります。モードが スクリーン に設定されている場合は、テスト中 OSCAR フラグが画面上のあちこちを移動します。テストが開始する前に、警告ポップアップボックスに次のメッセージが表示されます。"Energy モードにすると、ENERGY STAR 準拠でないモニタが損傷することがあります。ただし、開始直後にマウスまたはキーボード操作によってテストを中止できます。"

注意: Energy Star 準拠ではないモニタで Energy モードを使用すると、モニタが損傷する恐れがあります。

5. オプション:スクリーンセーバーテストをアクティブにするには、テスト をクリックします。スクリーンセーバーテスト ダイアログが表示されます。OK をクリックしてテストを開始します。

   テストに 10 秒かかります。完了すると、セキュリティ ダイアログボックスに戻ります。

ログイン

1. <Print Screen> を押して OSCAR を起動します。パスワード ダイアログボックスが表示されます。
2. パスワードを入力して OK をクリックします。メイン ダイアログボックスが表示されます。

自動ログアウトの設定

一定のアイドル時間が経過すると自動的にログアウトするように OSCAR を設定できます。

1. メイン ダイアログボックスで 設定、セキュリティ の順にクリックします。
2. アイドル時間 フィールドに、自動的に切断されるまで接続したままでいる時間を入力します。
3. OK をクリックします。

コンソールからのパスワード保護の削除

1. メイン ダイアログボックスから 設定、セキュリティ の順にクリックします。
2. セキュリティ ダイアログボックスで、新規 フィールドをシングルクリックして <Enter> を押すか、ダブルクリックします。
3. 新規 フィールドを空にして <Enter> を押します。
4. 再入力 フィールドをシングルクリックして <Enter> を押すか、ダブルクリックします。
5. 再入力 フィールドを空にして <Enter> を押します。
6. パスワードを除去するだけの場合は、OK をクリックします。

パスワード保護なしでスクリーンセーバーモードを有効にする方法

メモ: コンソールがパスワードで保護されている場合は、最初にパスワード保護を削除する必要があります。以下の手順を実行する前に、上記の手順を済ませください。

1. スクリーンセーバーを有効にする を選択します。
2. スクリーンセーバーの起動を遅らせる時間 (1 ～ 99)を分で入力します。
3. モニタが ENERGY STAR 準拠の場合は、Energy、それ以外の場合は スクリーン を選択します。

注意: Energy Star 準拠ではないモニタで Energy モードを使用すると、モニタが損傷する恐れがあります。

4. オプション:スクリーンセーバーテストをアクティブにするには、テスト をクリックします。スクリーンセーバーテスト ダイアログが表示されます。OK をクリックしてテストを開始します。

   テストに 10 秒かかります。完了すると、セキュリティ ダイアログボックスに戻ります。

   メモ: スクリーンセーバーモードを有効にすると、ユーザーがサーバーから切断され、サーバーは選択されません。ステータスフラグには「空き」と表示されます。

スクリーンセーターモードの終了

スクリーンセーバーモードを終了して メイン ダイアログボックスに戻るには、キーをどれか 1 つ押すか、マウスを動かします。

スクリーンセーバーをオフにするには

1. セキュリティ ダイアログボックスで、スクリーンセーバーを有効にする チェックボックスをオフにします。
2. OK をクリックします。

スクリーンセーバーを即座にオンにするには、<Print Screen> を押してから <Pause> を押します。

失くしたり忘れたりしたパスワードのクリア

iKVM のパスワードを失くしたり忘れたりした場合は、iKVM の出荷時のデフォルトのパスワードにリセットしてから変更できます。パスワードのリセットには CMC ウェブインタフェースか RACADM を使用します。

失くしたり忘れたりした iKVM パスワードを CMC ウェブインタフェースを使用してリセットするには

1. CMC ウェブインタフェースにログインします。
2. シャーシサブメニューから iKVM を選択します。
3. セットアップ タブをクリックします。iKVM 構成ページが表示されます。
4. デフォルト値の復元 をクリックします。

これで、OSCAR を使用してパスワードをデフォルトから変更できます。「パスワードの設定または変更を参照してください。

紛失したまたは忘れたパスワードを RACADM を使用してリセットするには、CMC に対応するシリアル/Telnet/SSH テキスト コンソールを開いて、ログイン後、以下を入力します。

```
racadm racresetcfg -m kvm
```

メモ: racresetcfg コマンドを使用すると、フロントパネル有効とDell CMC コンソール有効の設定がデフォルト値と異なる場合はリセットされます。

racresetcfg サブコマンドの詳細については、『Dell Chassis Management Controller 管理者リファレンス ガイド』の racresetcfg の項を参照してください。

言語の変更

OSCAR のテキストを対応言語のいずれかに変更するには、言語 ダイアログボックスを使用します。OSCAR のすべての画面が直ちに選択した言語に変わります。

OSCAR の言語を変更するには

1. <Print Screen> を押します。メイン ダイアログボックスが表示されます。
2. 設定、言語 の順にクリックします。言語 ダイアログボックスが表示されます。
3. 使用する言語のラジオボタンをクリックしてから OK をクリックします。

バージョン情報の表示

iKVM ファームウェアとハードウェアのバージョンを表示し、言語とキーボードの設定を確認するには、バージョン ダイアログボックスを使用します。

バージョン情報を表示するには

1. <Print Screen> を押します。メイン ダイアログボックスが表示されます。
2. コマンド、バージョンの表示 の順にクリックします。バージョン ダイアログボックスが表示されます。

バージョン ダイアログボックスの上半分にアプライアンスのサブシステムのバージョンが一覧になります。

3. ☒ をクリックするか、<Esc> を押して バージョン ダイアログボックスを閉じます。

システムのスキャン

スキャンモードでは、iKVM が自動的にスロットからスロットへ（サーバーからサーバーへ）とスキャンします。スキャンするサーバーと、各サーバーが表示される時間を秒で指定して、最大 16 のサーバーをスキャンできます。

スキャンリストにサーバーを追加するには

1. <Print Screen> を押します。メイン ダイアログボックスが表示されます。
2. 設定、スキャン の順にクリックします。スキャン ダイアログボックスが表示され、シャーシ内のすべてのサーバーが一覧になります。
3. スキャンするサーバーの横にあるチェックボックスをオンにします。

   または

   サーバー名かスロットをダブルクリックします。

   または

   <Alt > と、スキャンするサーバーの番号を押します。最大 16 のサーバーを選択できます。
4. 時間 フィールドに、スキャンがリストの次のサーバーに移動するまで iKVM が待つ時間（3 ～ 99）を秒で入力します。
5. 追加 / 削除 ボタンをクリックして OK をクリックします。

サーバーを スキャン リストから削除するには

1. スキャン ダイアログボックスで、削除するサーバーの横にあるチェックボックスをオンにします。

   または

   サーバー名かスロットをダブルクリックします。

   または

   クリア ボタンをクリックして、すべてのサーバーを スキャン リストから削除します。
2. 追加 / 削除 ボタンをクリックして OK をクリックします。

スキャンモードを開始するには

1. <Print Screen> を押します。メイン ダイアログボックスが表示されます。
2. コマンド をクリックします。コマンド ダイアログボックスが表示されます。
3. スキャン有効 チェックボックスをオンにします。
4. OK をクリックします。マウスとキーボードがリセットされたというメッセージが表示されます。
5. ☒ をクリックしてメッセージボックスを閉じます。

スキャンモードをキャンセルするには

1. OSCAR が開いており、メイン ダイアログボックスが表示されている場合は、リストからサーバーを選択します。

または

OSCAR が開いていない場合は、マウスを動かすか、キーボードでどれかキーを押します。現在選択されているサーバーでスキャンが停止します。

または

<Print Screen> を押します。メイン ダイアログボックスが表示されたら、リストからサーバーを選択します。

2. コマンド ボタンをクリックします。コマンド ダイアログボックスが表示されます。
3. スキャン有効 チェックボックスをオフにします。

サーバーへのブロードキャスト

システム内の複数のサーバーを同時に制御して、すべてのサーバーが同じ入力を受信するように設定できます。キー入力やマウスの動作を個別にブロードキャストすることもできます。

メモ: 最大 16 のサーバーに同時にブロードキャストできます。

サーバーにブロードキャストするには

1. <Print Screen> を押します。メイン ダイアログボックスが表示されます。
2. 設定、ブロードキャスト の順にクリックします。ブロードキャスト ダイアログボックスが表示されます。

メモ: キー入力のブロードキャスト:キー入力を使用する場合、キー入力が同じであると解釈されるためには、ブロードキャストを受信するすべてのサーバーでキーボードの状況が同じであることが必要です。つまり、<Caps Lock> と <Num Lock> のモードがすべてのキーボードで同じでなければなりません。iKVM は選択したサーバーにキー入力を同時に送信しますが、一部のサーバーの抑制によって伝送が遅延する場合があります。

メモ: マウス動作のブロードキャスト:マウスが正確に機能するには、すべてのサーバーのマウスドライバ、デスクトップ(同じアイコンの配置など)、ビデオ解像度が同じであることが必要です。また、マウスがすべての画面で同じ場所になければなりません。これらの条件を満たすのは難しいため、複数のサーバーにマウスの動作をブロードキャストすると、予測不能な結果が生じることがあります。

3. チェックボックスをオンにして、ブロードキャストコマンドを受信するサーバーのマウスやキーボードを有効にします。

または

上下の矢印を押して、目的のサーバーまでカーソルを移動します。キーボードのチェックボックスをオンにするには <Alt><K>、マウスのチェックボックスをオンにするには <Alt><M> を押します。他のサーバーにも同じ操作を繰り返します。

4. OK を押して設定を保存し、設定 ダイアログボックスに戻ります。☒ をクリック、または <Escape> を押して、メイン ダイアログボックスに戻ります。
5. コマンド をクリックします。コマンド ダイアログボックスが表示されます。
6. ブロードキャスト有効 チェックボックスをオンにしてブロードキャストをアクティブにします。ブロードキャスト警告 ダイアログボックスが表示されます。
7. OK をクリックしてブロードキャストを開始します。

キャンセルして コマンド ダイアログボックスに戻るには、☒ をクリック または <Esc> を押します。

8. ブロードキャストが有効になっている場合は、情報を入力し、ブロードキャストするマウスの動作を管理ステーションから実行します。リスト内のサーバーのみがアクセス可能です。

ブロードキャストをオフにするには

セキュリティ ダイアログボックスから、ブロードキャスト有効 チェックボックスをオフにします。

CMC からの iKVM の管理

フロントパネルの有効または無効

RACADM を使用してフロントパネルから iKVM へのアクセスを有効または無効にするには、CMC に対応するシリアル/Telnet/SSH テキストコンソールを開いて、ログイン後、以下を入力します。

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

<値> は 1(有効)または 0(無効)です。

config サブコマンドの詳細については、『Dell Chassis Management Controller 管理者リファレンスガイド』の config の項を参照してください。

ウェブインタフェースを使用してフロントパネルから iKVM へのアクセスを有効または無効にするには

1. CMC ウェブインタフェースにログインします。
2. システムツリーで iKVM を選択します。iKVM ステータスページが表示されます。
3. セットアップ タブをクリックします。iKVM 構成ページが表示されます。
4. 有効にするには、フロントパネル USB/ビデオ有効 チェックボックスをオンにします。

   無効にするには、フロントパネル USB/ビデオ有効 チェックボックスをオフにします。
5. 適用 をクリックして設定を保存します。

iKVM を介した Dell CMC コンソールの有効化

RACADM を使用して iKVM から Dell CMC コンソールへのアクセスを有効にするには、CMC に対応するシリアル/Telnet/SSH テキストコンソールを開いてログインした後、以下を入力します。

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

ウェブインタフェースを使用して Dell CMC コンソールを有効にするには

1. CMC ウェブインタフェースにログインします。
2. システムツリーで iKVM を選択します。iKVM ステータス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ます。iKVM 構成ページが表示されます。
4. iKVM から CMC CLI へのアクセスを許可する チェックボックスをオンにします。
5. 適用 をクリックして設定を保存します。

iKVM のステータスとプロパティの表示

Dell M1000e サーバーシャーシのローカルアクセス KVM モジュールは Avocent® Integrated KVM Switch Module または iKVM と呼ばれます。シャーシに関連付けられた iKVM の正常性の状態は、シャーシグラフィックス セクションの シャーシのプロパティ正常性 ページで閲覧することができます。

シャーシグラフィックス を使用して iKVM の正常性状態を表示するには

1. CMC ウェブインタフェースにログインします。
2. シャーシステータス ページが表示されます。シャーシグラフィックス の右側のセクションは、シャーシの背面図を表しており、iKVM の正常性状態が含まれます。iKVM の正常性状態は、iKVM サブグラフィックの色で示されます。
   - 緑色 - iKVM が存在し、電源がオンで CMC と通信中。悪条件の兆候なし。
   - 黄色 - iKVM が存在し、電源がオンまたはオフで、CMC と通信中または通信しておらず。悪条件が存在する可能性あり。
   - 灰色 - iKVM が存在し、電源がオフ。CMC と通信しておらず、悪条件の兆候なし。

3. 個別の iKVM サブグラフィックにマウスのカーソルを移動すると、該当するテキストヒントまたは画面ヒントが表示されます。テキストヒントは、対象の iKVM に関する追加情報を提供します。
4. iKVM サブグラフィックは、該当する CMC GUI ページにハイパーリンク付けされ、iKVM ステータスページに瞬時に移動することができます。

iKVM の詳細については、「iKVM モジュールの使用」を参照してください。

iKVM ステータスページを使って iKVM のステータスを表示するには

1. CMC ウェブインタフェースにログインします。
2. システムツリーで iKVM を選択します。iKVM ステータス ページが表示されます。

表9-5で、iKVM ステータス ページに表示される情報の説明を提供します。

項目	説明
存在	iKVM モジュールが 存在か 不在かを示します。
電源状態	iKVM の電源状態が オン か オフ か なし(不在)かを示します。
Name	iKVM ののの製品名を表示します。
メーカー	iKVM のメーカーを表示します。
パーツ番号	iKVM のパーツ番号を示します。パーツ番号は、ベンダーが提供する一意の識別子です。
ファームウェアバージョン	iKVM のファームウェアバージョンを示します。
ハードウェアバージョン	iKVM のハードウェアバージョンを示します。
フロントパネル接続済み	モニタがフロントパネルの VGA コネクタに 接続しているかどうかを示します(はいまたはいいえ)。この情報は、ローカルユーザーがシャーシのフロントパネルにアクセスできるかどうかを CMC が判別できるように提供されます。
リアパネル接続済み	モニタがリアパネルの VGA コネクタに接続している かどうかを示します(はいまたはいいえ)。この情報は、ローカルユーザーがシャーシのリアパネルにアクセスできるかどうかを CMC が判別できるように提供されます。
ポート層接続済み	iKVM は内蔵ハードウェアを使用して Dell と Avocent の外付け KVM アプライアンスにシームレスに層接続できるように設計されています。iKVM が層になっていると、その接続元の外付け KVM スイッチの画面ディスプレイからシャーシ内のサーバーにアクセスできます。
前面パネルの USB/ビデオを有効にする	フロントパネル VGA コネクタが有効かどうかを示します(はい または いいえ)。
iKVM から CMC へのアクセスを許可	iKVM からの CMC コマンドコンソールが有効かどうかを示します(はい または いいえ)。

iKVM ファームウェアのアップデート

CMC ウェブインタフェースまたは RACADM を使用して iKVM ファームウェアをアップデートできます。

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

1. CMC ウェブインタフェースにログインします。
2. システムツリーで シャーシ をクリックします。
3. アップデート タブをクリックします。アップデート可能なコンポーネント ページが表示されます。
4. iKVM 名をクリックします。ファームウェアのアップデート ページが表示されます。
5. 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。

メモ: iKVM ファームウェアイメージのデフォルト名は ikvm.bin です。この名前を変更することも可能です。

6. ファームウェアアップデートを開始する をクリックします。操作の確定を求めるダイアログボックスが表示されます。
7. はい をクリックして続行します。ファームウェアアップデートの進行状況 セクションでは、ファームウェアアップデートのステータス情報を提供します。イメージファイルがアップロードされる間、ページにステータスインジケータが表示されます。ファイルの転送時間は、接続速度によって大きく異なります。内部更新処理が始まると、ページは自動的に更新され、ファームウェア アップデートのタイマーが表示されます。その他の追記事項:
   - ファイル転送時に、更新 ボタンの利用、または他のページへ移動しないでください。
   - アップデートプロセスをキャンセルするには、ファイル転送およびアップデートのキャンセル をクリックします。このオプションは、ファイル転送時にのみ、利用可能です。
   - アップデート状態 フィールドにアップデートステータスが表示されます。このフィールドは、ファイル転送時に自動的に更新されます。一部の古いブラウザでは、この自動更新はサポートされていません。アップデート状態 フィールドを手動で更新するには、更新 をクリックします

メモ: iKVM のアップデートに最大 1 分程かかる場合があります。

アップデートが完了すると、iKVM がリセットし、新しいファームウェアにアップデートされ、アップデート可能なコンポーネント ページに表示されます。

RACADM を使用して iKVM ファームウェアをアップデートするには、CMC に対応するシリアル/Telnet/SSH テキスト コンソールを開いて、ログイン後、以下を入力します。

```
racadm fwupdate -g -u -a <TFTP サーバーの IP アドレス> - d <ファイルパス / ファイル名> -m kvm
```

例:

```
racadm fwupdate -gua 192.168.0.10 -d ikvm.bin -mkvm
```

fwupdate サブコマンドの詳細については、『Dell Chassis Management Controller 管理者リファレンスガイド』の fwupdate の項を参照してください。

トラブルシューティング

メモ: アクティブなコンソールリダイレクトセッションがあり、推奨解像度以下の画面で iKVM に接続している場合、ローカルコンソールでサーバーを選択すると、サーバーのコンソール解像度がリセットされることがあります。サーバーで Linux オペレーティングシステムを実行している場合は、ローカルモニターで X11 コンソールが表示されない可能性があります。iKVM で <Ctrl><Alt><F1> キーを押すと、Linux がテキストコンソールに切り替わります。

表 9-6 iKVM のトラブルシューティング

問題	考えられる原因と解決法
フロントパネルに接続しているモニタに「CMC コントロールによってユーザーが無効になりました」というメッセージが表示されます。	フロントパネルの接続が CMC によって無効になりました。 CMC ウェブインタフェースか RACADM を使用してフロントパネルを有効にできます。 ウェブインタフェースを使用してフロントパネルを有効にするには 1. CMC ウェブインタフェースにログインします。 2. システムツリーで iKVM を選択します。 3. セットアップ タブをクリックします。 4. フロントパネル USB/ビデオ有効 チェックボックスをオンにします。 5. 適用をクリックして設定を保存します。 RACADM を使用してフロントパネルを有効にするには、CMC に対応するシリアル/Telnet/SSH テキスト コンソールを開いて、ログイン後、以下を入力します。 `racadm config -g cfgKVMInfo - o cfgKVMAccesToCMCEnable 1`
リアパネルのアクセスが機能しません。	フロントパネルの設定が有効になり、現在フロントパネルにモニタが接続しています。 一度に 1 つの接続のみが許可されています。フロントパネルの接続は ACI とリアパネルの接続より優先されます。接続の優先度の詳細については、「iKVMの 接続手順」を参照してください。
リアパネルに接続しているモニタに、「現在別のアプライアンスが層にあるため、ユーザーが無効になりました」というメッセージが表示されます。	ネットワークケーブルが iKVM の ACI ポートコネクタとセカンダリ KVM アプライアンスに接続しています。 一度に 1 つの接続のみが許可されています。ACI 層接続はリアパネルのモニタ接続より優先されます。優先順位はフロントパネル、ACI、リアパネルの順になります。
iKVM のオレンジの LED が点滅しています。	3 つの原因が考えられます。 iKVM に問題があり、iKVM の再プログラミングが必要です。問題を解決するには、iKVM ファームウェアのアップデート手順に従ってください（「iKVM ファームウェアのアップデート」を参照）。 iKVM が CMC コンソールのインタフェースを再プログラミングしています。この場合は、CMC コンソールが一時的に使用不可になり、OSCAR インタフェースで黄色のドットで表されます。このプロセスに最大 15 分かかります。 iKVM ファームウェアがハードウェアのエラーを検出しました。詳細については、iKVM ステータスを参照してください。 ウェブインタフェースを使用して iKVM ステータスを表示するには

	1. CMC ウェブインタフェースにログインします。 2. システムツリーで iKVM を選択します。 RACADM を使用して iKVM ステータスを表示するには、CMC に対応するシリアル/Telnet/SSH テキスト コンソールを開いて、ログイン後、以下を入力します。 `racadm getkvminfo`
使用している iKVM は ACI ポートから外部 KVM スイッチまで層になっていますが、ACI 接続のすべてのエントリが使用不可です。 OSCAR インタフェースで状態のすべてに黄色のドットが表示されます。	フロントパネルの接続が有効になり、モニタが接続しています。フロントパネルはその他すべての iKVM 接続より優先されるため、ACI とリアパネルの接続は無効になります。 ACI ポートの接続を有効にするには、最初にフロントパネルのアクセスを無効にするか、フロントパネルに接続しているモニタを取り外します。外部 KVM スイッチ OSCAR のエントリがアクティブになりアクセス可能になります。 ウェブインタフェースを使用してフロントパネルを無効にするには 1. CMC ウェブインタフェースにログインします。 2. システムツリーで iKVM を選択します。 3. セットアップ タブをクリックします。 4. フロントパネル USB/ビデオ有効 チェックボックスをオフにします。 5. 適用をクリックして設定を保存します。 RACADM を使用してフロントパネルを無効にするには、CMC に対応するシリアル/Telnet/SSH テキスト コンソールを開いて、ログイン後、以下を入力します。 `racadm config -g cfgKVMInfo - o cfgKVMFrontPanelEnable 0`
OSCAR メニューで、Dell CMC 接続に赤い「X」が表示され、CMC に接続できません。	2 つの原因が考えられます。 Dell CMC コンソールが無効になっています。この場合は、CMC ウェブインタフェースか RACADM を使用してこれを有効にできます。 ウェブインタフェースを使用して Dell CMC コンソールを有効にするには 1. CMC ウェブインタフェースにログインします。 2. システムツリーで iKVM を選択します。 3. セットアップ タブをクリックします。 4. iKVM から CMC CLI へのアクセスを許可する チェックボックスをオンにします。 5. 適用 をクリックして設定を保存します。 RACADM を使用して Dell CMC 接続を有効にするには、CMC に対応するシリアル/Telnet/SSH テキスト コンソールを開いて、ログイン後、以下を入力します。 `racadm config -g cfgKVMInfo - o cfgKVMAccessToCMCEnable 1` CMC が初期化、スタンバイ CMC への切り替え、または再プログラミングを実行中のため、使用できません。この場合は、CMC が初期化が終了するまで待ってください。
OSCAR でサーバーのスロット名が「初期化中」と表示され、選択できません。	サーバーが初期化中か、そのサーバーの iDRAC が初期化に失敗しました。 まず 60 秒待ちます。サーバーがまだ初期化している場合は、初期化が完了するとスロット名が表示され、サーバーを選択できるようになります。 60 秒後、OSCAR にスロットが初期化中であると示された場合は、サーバーをシャーシから取り出して再び挿入します。この処置によって iDRAC が再初期化できます。

目次ページに戻る

目次ページに戻る

CMC のインストールと設定

Dell™ Chassis Management Controllerファームウェアバージョン 2.10 ユーザーガイド

この項では、CMC ハードウェアの取り付け方法、CMC へのアクセスを確立する方法、CMC を使うための管理環境を設定する方法、および CMC を設定するための手順について説明します。

- CMC への初期アクセスの設定
- ネットワーク経由による 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

更に、「冗長 CMC 環境について」では、CMC の冗長環境の導入と設定方法について記載しています。

作業を開始する前に

CMC 環境を設定する前に、デルサポートサイト **support.dell.com** から CMC ファームウェアの最新バージョンをダウンロードしてください。

また、システム付属の Dell システム管理ツールと説明書 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 はシャーシに組み込まれているので、取り付け作業は必要ありません。システムに取り付けられている CMC を使って開始するには、「管理ステーションへのリモートアクセスソフトウェアのインストール」を参照してください。

2 台目の CMC を取り付けて、プライマリ CMC のスタンバイとして使用できます。スタンバイ CMC 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。

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、Secure Shell (SSH)、またはオペレーティング システム内蔵のシリアル 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 を使用する場合は、『Dell Systems Management Tools and Documentation DVD』からインストールする必要があります。『Dell Systems Management Tools and Documentation DVD』は、システムに同梱されています。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 システム構築と更新ユーティリティが含まれます。
- SYSMGMT - Dell OpenManage Server Administrator など、システム管理ソフトウェアの製品が含まれます。
- Docs: 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 コントローラの説明書が含まれます。
- 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 support.dell.com から利用できる『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。

RACADM の Linux 管理ステーションへのインストール

1. root 権限でサポートされている Red Hat® Enterprise Linux® または SUSE® Linux Enterprise Server オペレーティング システムを実行しているシステムにログオンします。その後、管理されるシステム コンポーネントをインストールします。
2. DVD ドライブに『Dell Systems Management Tools and Documentation DVD』を挿入します。
3. 必要に応じて、mount コマンドまたは同様のコマンド を使用して DVD を希望する場所へマウントします。

メモ: Red Hat Enterprise Linux 5 オペレーティングシステムでは、DVD は - noexec mount オプションで自動マウントされています。このオプションでは、DVD から実行可能ファイルを実行することはできません。手動で DVD-ROM をマウントしてから実行ファイルを実行する必要があります。

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

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

5. RACADM コマンドのヘルプを表示するには、前のコマンドを入力した後「racadm help 」と入力してください。RACADM の詳細については、「RACADM コマンドラインインタフェースの使用」を参照してください。

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

```
racadm getconfig -f <ファイル名>
```

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、ルートでログインします。
2. 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判定します。rpm -qa | grep mgmtst- racadm コマンドを使用します。
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、rpm -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。デルサポートサイト **support.dell.com / manuals** にある『Dell システムソフトウェアサポートマトリックス』で「対応ブラウザ」の項を参照してください。

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

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

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

プロキシサーバー

プロキシサーバーを使っているときに管理ネットワークにアクセスできない場合、管理ネットワークのアドレスをブラウザの例外リストに追加してください。これにより、管理ネットワークにアクセスする際、ブラウザはプロキシサーバーを迂回することができます。

Internet Explorer

以下の手順に従って、Internet Explorer の例外リストを編集してください。

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、**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 **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 3.0 で例外リストを編集するには:

1. Firefox を起動します。
2. **ツール** → **オプション**(Windows 用)または**編集** → **プレファレンス** (Linux 用)をクリック**します**。
3. **詳細**、**ネットワーク** タブの順にクリックします。
4. **設定**をクリックします。
5. **手動でプロキシを設定する** を選択し、**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 ® フィッシング詐欺検出機能

管理システムの Internet Explorer 7 で Microsoft フィッシング詐欺検出機能 が有効になっており、かつCMC のインターネットアクセスがない場合、使用しているブラウザまたはリモート RACADM など他のインタフェースにかかわらず、CMC へのアクセスに数秒の遅延が伴うことがあります。以下の手順に従って、フィッシング詐欺検出機能を無効にしてください。

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

証明書失効リスト(CRL)のフェッチ

CMC がインターネットへのルートを持たない場合は、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。この機能は、CMC ウェブサーバーなどのサーバーが使用している証明書がインターネットから取得した失効した証明書の一覧にあるかテストするものです。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は数秒の遅延を引き起こす可能性があります。

以下の手順に従って、CRL のフェッチを無効にしてください。

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、**接続** 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** を選択解除します。
4. **OK** をクリックします。

Internet Explorer で CMC からファイルのダウンロード

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

以下の手順に従って、**暗号化されたページをディスクに保存しない** オプションを有効にしてください。

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、**接続** をクリックします。
3. セキュリティ セクションにスクロールして、**暗号化されたページをディスクに保存しない** を選択します。

Internet Explorer でアニメーションの再生

ウェブインタフェースとの間でファイルが送受信される際、ファイル転送アイコンが回転して転送が行われていることを示します。Internet Explorer では、このためにはブラウザがアニメーションを再生するように設定されていることが必要です（デフォルト設定）。

以下の手順に従って、アニメーションを再生するように Internet Explorer を設定してください。

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、**接続** をクリックします。
3. マルチメディア セクションにスクロールして、**Web ページのアニメーションを再生する** を選択します。

CMC への初期アクセスの設定

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。CMC ネットワークの設定方法については、「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。

CMC が管理ネットワークに接続されると、CMC と iDRAC への外部アクセスはすべて CMC 経由で行われます。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。

メモ: デルでは、iDRAC および CMC を使って実稼動ネットワークからシャーシ内の管理ネットワークを隔離 / 分離するというベストプラクティスをお勧めします。この管理ネットワーク上で管理および実稼動 / アプリケーショントラフィックが混在すると、輻輳 / 飽和状態が発生し、CMC および iDRAC の通信遅延が起こります。遅延が起こると、iDRAC が稼動中であっても CMC が iDRAC をオフライン状態と見なしたりするといった予期しないシャーシ動作が発生し、他の不要な動作が発生する原因になります。管理ネットワークを物理的に分離することができない場合は、CMC および iDRAC トラフィックをそれぞれ異なる VLAN に分離するというオプションもあります。CMC と個々の iDRAC ネットワークインタフェースは、`racadm setniccfg` コマンドを用いて VLAN を使用するように設定することもできます。詳細については、『Dell Chassis Management Controller 管理者リファレンスガイド』を参照してください。

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

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、各 CMC を管理ネットワークに接続してください。シャーシに CMC が 1 つしかない場合は、管理ネットワークへの接続数は 1 つです。シャーシのセカンダリ CMC スロットに冗長 CMC がある場合は、管理ネットワークの 接続数は 2 つです。

各 CMC には、GB1（アップリンクポート）および STK（スタックポート）の 2 つの RJ-45 Ethernet ポートがあります。基本的なケーブル接続では、GB1 ポートを管理ネットワークに接続し、STK ポートは使用しません。

注意: STK ポートを管理ネットワークに接続すると、予期しない結果が発生する可能性があります。

デイジーチェーン CMC ネットワーク接続

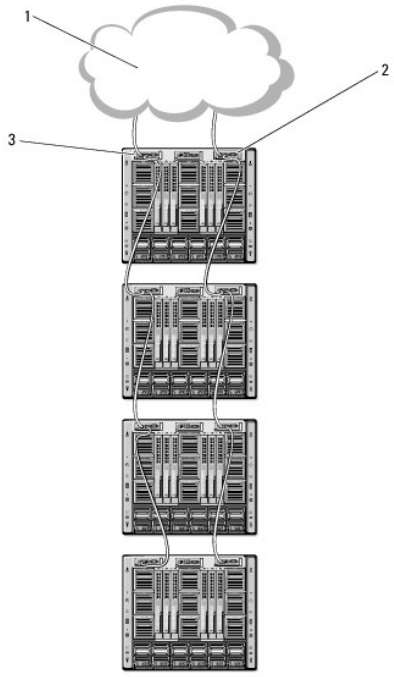
ラックに複数のシャーシがある場合は、4 つまでのシャーシをデイジーチェーン接続することで管理ネットワークへの接続数を削減できます。4 つのシャーシのそれぞれが 1 つずつ 冗長 CMC を持つ場合は、デイジーチェーン接続によって管理ネットワークへの接続数を 8 つから 2 つに減らすことができます。各シャーシが 1 つずつしか CMC を持たない場合には、接続数は 4 つから 1 つに減ります。

シャーシをデイジーチェーン接続する場合、GB1 が「アップリンク」ポート、STK が「スタック」ポートとなります。GB1 ポートは管理ネットワークに接続するか、ネットワークに近い方のシャーシにある CMC の STK ポートに接続します。STK ポートは、ネットワークから遠い方のシャーシにある CMC の GB1 ポートにのみ接続してください。

プライマリ CMC スロットにある CMC とセカンダリ CMC スロットにある CMC は別々にデイジーチェーン接続します。

図2-1 は、それぞれプライマリとセカンダリスロットに CMC を持つ 4 つのシャーシをデイジーチェーンした場合のケーブル接続を示します。

図 2-1 デイジーチェーン CMC ネットワーク接続



1	管理ネットワーク	2	セカンダリ CMC
3	プライマリ CMC		

以下の手順に従って、4 つのシャーシをデイジーチェーン接続します。

1. 最初のシャーシのプライマリ CMC の GB1 ポートを管理ネットワークに接続します。
2. 2 つ目のシャーシのプライマリ CMC の GB1 ポートを最初のシャーシのプライマリ CMC の STK ポートに接続します。
3. 3 つ目のシャーシがある場合は、そのシャーシのプライマリ CMC の GB1 ポートを 2 つ目のシャーシのプライマリ CMC の STK ポートに接続します。
4. 4 つ目のシャーシがある場合は、そのシャーシのプライマリ CMC の GB1 ポートを 3 つ目のシャーシの STK ポートに接続します。
5. シャーシ内に冗長 CMC がある場合は、上記と同じように、それぞれ相互に接続します。

注意: CMC 上の STK ポートは管理ネットワークに接続してはいけません。GB2 ポートは、別のシャーシ上の GB1 ポートにしか接続できません。STK ポートを管理ネットワークに接続すると、ネットワークに支障をきたし、データの損失を招く恐れがあります。

メモ: プライマリ CMC を決してセカンダリ CMC に接続しないでください。

メモ: STK ポートが別の CMC にチェーン接続されている CMC をリセットすると、チェーン後方の CMC のネットワークに支障を来たす可能性があります。チェーン後方の CMC は、ネットワーク接続が失われたことをログ記録し、冗長 CMC にフェールオーバーする場合があります。

CMC ネットワークの設定

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

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

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

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

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

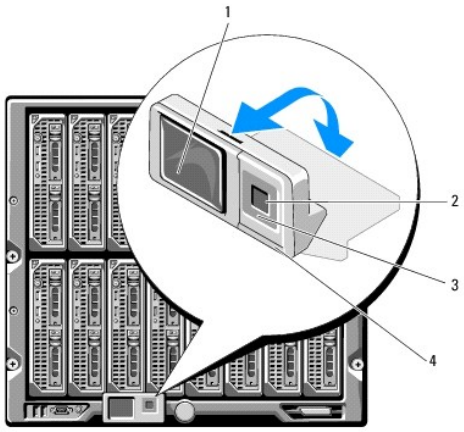
LCD 設定ウィザードを使用したネットワーク設定

メモ: LCD 設定ウィザードを使用してサーバーを設定するオプションは、CMC が導入されるか、またはデフォルトパスワードが変更されるまでに限って利用できます。パスワードが変更されない場合、LCD を引き続き利用して CMC を再設定できるため、セキュリティのリスクが発生します。

LCD はシャーシ前面の左下の角にあります。

図2-2 は、LCD パネルの図解です。

図 2-2 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)	4	状態インジケータ LED

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。

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正常性を示します。

- 青色の点灯は、正常であることを示します。
- 黄色の点滅は、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でシャーシを特定するための ID 信号です。

LCD 画面上での移動方法

LCD パネルの右側には 5 つのボタン、4 つの方向ボタン(上下左右)、中央のボタンがあります。

- 別の画面へ移動するには、右(次へ)と左(前の)方向ボタンを使用します。設定ウィザードの使用中はいつでも前の画面に戻ることができます。
- 画面上のオプション間を移動するには、上下の方向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、中央のボタンを使用します。

LCD パネルの使用の詳細については、『Dell Chassis Management Controller 管理者リファレンス ガイド』の「LCD パネル」の項を参照してください。

LCD 設定ウィザードの使用

1. シャーシの電源ボタンをオンにします。

   電源が投入される間、LCD 画面に一連の初期化画面が表示されます。使用準備が整ったら、言語の設定 画面が表示されます。

2. 方向ボタンを使って言語を選択し、中央のボタン押して **承認する / はい** を選択してから、中央のボタンを再度押します。
3. エンクロージャ 画面が開き、「エンクロージャを設定しますか?」という質問が表示されます。
   a. 中央のボタンを押して、CMC ネットワーク設定 画面に進みます。手順 4 を参照してください。
   b. **エンクロージャの設定** メニューを終了するには、いいえのアイコンを選択し、中央のボタンを押します。手順 9 を参照してください。
4. 中央のボタンを押して、CMC ネットワーク設定 画面に進みます。
5. 下向き方向ボタンを使って、ネットワーク速度(10Mbps、100Mbps、自動(1Gbps))を選択します。

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

   中央のボタンを押して、CMC ネットワーク設定 画面に進みます。

6. 使用しているネットワーク環境に適したデュプレックスモード(半二重または全二重)を選択します。

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

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

   中央のボタンを押して、CMC ネットワーク設定 画面に進みます。

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

   中央のボタンを押して、CMC ネットワーク設定 画面に進みます。

8. CMC の NIC IP アドレスを取得するモードを選択します。

動的ホスト構成プロトコル(DHCP)	CMC は IP 設定(IP アドレス、マスク、ゲートウェイ)をネットワーク上の DHCP サーバーから自動的に取得します。CMC には、ネットワーク上で割り当てられた一意の IP アドレスが割り当てられます。DHCP オプションを選択した場合は、中央のボタンを押します。iDRAC を設定しますか? の画面が表示されます。手順 10 に進みます。
静的	続く画面に、IP アドレス、ゲートウェイ、サブネットマスクを手動で入力します。 静的 オプションを選択した場合は、中央のボタンを押して次の CMC ネットワーク設定 画面へ進みます。 a. 左右方向キーを使って位置を移動し、上下方向キーを使って各位置の数値を選択することで、静的 IP アドレス を設定します。静的 IP アドレス の設定を終えたら、中央のボタンを押して先に進みます。 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。ネットワークの概要 画面が表示されます。 ネットワークの概要 画面には、入力した 静的 IP アドレス、サブネットマスク、ゲートウェイ の設定が表示されます。設定が正しいことを確認してください。設定を修正するには、左方向キーで移動し、中央のボタンを押して、対象の設定画面に戻ります。修正を終えたら、中央のボタンを押します。 d. 入力した設定が正しいことを確認してから、中央のボタンを押します。DNS を登録しますか?の画面が表示されます。

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

9. 前のステップで DHCP を選択した場合は、手順 10 に進みます。

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

   左右方向キーを使って位置を移動し、上下方向キーを使って各位置の数値を選択することで、静的 IP アドレス を設定します。静的 IP アドレス の設定を終えたら、中央のボタンを押して先に進

みます。

10. iDRAC を設定するかどうかを指定します。
    - いいえ: 手順 13 に進みます。
    - はい:中央のボタンを押して先に進みます。
11. ブレードに使用するインターネットプロトコル(IPv4、IPv6、または両方)を選択します。

動的ホスト構成プロトコル(DHCP)	iDRAC は IP 設定(IP アドレス、マスク、ゲートウェイ)をネットワーク上の DHCP サーバーから自動的に取得します。iDRAC には、ネットワークに割当てられた固有の IP アドレスが割当てられます。中央のボタンを押します。
静的	続く画面に、IP アドレス、ゲートウェイ、サブネットマスクを手動で入力します。 固定 オプションを選択した場合は、中央のボタンを押して次の iDRAC ネットワーク設定 画面へ進みます。 a. 左右方向キーを使って位置を移動し、上下方向キーを使って各位置の数値を選択することで、静的 IP アドレス を設定します。このアドレスは、最初のスロットに装着された iDRAC の静的 IP アドレスです。後続の iDRAC の固定 IP アドレスは、この IP アドレスを増分したスロット番号として算出されます。静的 IP アドレス の設定を終えたら、中央のボタンを押して先に進みます。 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。

a. IPMI LAN チャンネルの **有効** または **無効** を選択します。中央のボタンを押して処理を続けます。

b. iDRAC 構成画面で、インストールされているサーバーにすべての iDRAC ネットワーク設定を適用するには、承諾する / はい アイコンを反転表示して、中央のボタンを押します。インストールされているサーバーに iDRAC ネットワーク設定を適用しないようにするには、**いいえ** アイコンをハイライト表示させてから、中央のボタンを押して手順 c を続けます。

c. 次の iDRAC 構成画面で、新しくインストールされたサーバーにすべての iDRAC ネットワーク設定を適用するには、承認する / はい アイコンを反転表示してから、中央のボタンを押します。新しいサーバーがシャーシに挿入されると、LCD が以前に設定したネットワーク設定/ポリシーを使ってサーバーを自動展開するかどうかユーザーに尋ねます。新しくインストールされたサーバーに iDRAC ネットワーク設定を適用しない場合は、**いいえ** アイコンを反転表示してから中央のボタンを押します。新しいサーバーがシャーシに挿入されても、iDRAC ネットワーク設定は構成されません。

l. エンクロージャ画面で、すべてのエンクロージャ設定を適用するには、承諾する / はい アイコンを反転表示させてから中央のボタンを押します。エンクロージャの設定を適用するには、**いいえ** アイコンを反転表示させてから中央のボタンを押します。

m. IP の概要 画面では、設定した IP アドレスが正しいことを確認します。設定を修正するには、左方向キーで移動し、中央のボタンを押して、対象の設定画面に戻ります。修正を終えたら、中央のボタンを押します。必要に応じて、右方向キーで移動し、中央のボタンを押して、IP の概要 画面に戻ります。

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

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

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

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

ネットワーク経由による CMC へのアクセス

CMC ネットワーク設定を終えた後、次のいずれかのインタフェースを使って CMC にリモートアクセスできます。

- ウェブインタフェース
- Telnet コンソール
- SSH
- リモート RACADM

Telnet は、他のインタフェースを介して有効にすることができます。Telnet は、他のインタフェースと比較して、セキュリティ的に安全ではないため、デフォルトで無効になっています。

表2-1は、それぞれの CMC ネットワークインタフェースについて、説明します。

表 2-1 CMC インタフェース

インタフェース	説明

ウェブインタフェース	グラフィカルユーザーインタフェースを使って CMC へのリモートアクセスを提供します。ウェブインタフェースは CMC のファームウェアに組み込まれ、管理ステーションで対応ウェブブラウザから NIC インタフェースを介してアクセスします。 対応ウェブブラウザのリストは、デルサポートサイト **support.dell.com / manuals** にある『Dell システムソフトウェアサポートマトリックス』で「対応ブラウザ」の項を参照してください。
リモート RACADM コマンドラインインタフェース	管理ステーションからコマンドラインインタフェース (CLI) を使って CMC にリモートアクセスできます。リモート RACADM は、CMC の IP アドレスと共に **racadam -r** オプションを使用して、CMC 上でコマンドを実行します。
Telnet	ネットワーク経由でコマンドラインによる CMC へのアクセスを提供します。RACADM コマンド ライン インタフェースとサーバーまたは IO®モジュールのシリアルコンソールの接続に使われる **connect** コマンドは、CMC コマンド ラインから実行できます。 **メモ:** Telnet は、すべてのデータ(パスワードも含めて)をテキスト形式で送信するプロトコルです。機密情報を送信する場合は、SSH インタフェースを使用してください。
SSH	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。

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

CMC と iDRAC ウェブインタフェースは、対応ウェブブラウザを使って CMC NIC を介してアクセスでき、Dell Server Administrator または Dell OpenManage IT Assistant を使って起動できます。

対応ウェブブラウザのリストは、デルサポートサイト **support.dell.com / manuals** にある『Dell システムソフトウェアサポートマトリックス』で「対応ブラウザ」の項を参照してください。対応ウェブブラウザを使用して CMC にアクセスするには、「CMC ウェブインタフェースへのアクセス」を参照してください。Dell OpenManage IT Assistant については、「管理ステーションへのリモートアクセスソフトウェアのインストール」を参照してください。

Dell Server Administrator を使って CMC インタフェースにアクセスするには、管理ステーションで Server Administrator を起動します。Server Administrator ホームページの左ペインにあるシステムツリーで、**システム** → **メインシステムシャーシ** → **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 Server Administrator ユーザーズガイド』を参照してください。

Telnet または SSH を使って CMC コマンドラインにアクセスする方法については、「CMC にコマンドラインコンソールの使用を設定する方法」を参照してください。

RACADM の使い方の詳細については、「RACADM コマンドラインインタフェースの使用」を参照してください。

connect または racadm connect コマンドを使ってサーバーおよび IO モジュールに接続する詳細については、「接続コマンドでサーバーまたは I/O モジュールに接続する」を参照してください。

CMC ファームウェアのインストールまたはアップデート

CMC ファームウェアのダウンロード

ファームウェアのアップデートを開始する前に、デルサポートサイト **support.dell.com** から最新ファームウェアをダウンロードして、ファイルをローカルシステムに保存します。

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

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

メモ: CMC ファームウェアのアップデート中、シャーシ内の冷却ファンの一部または全部が全速回転します。これは正常な動作です。

メモ: ファームウェアアップデートは、デフォルトで現在の CMC 設定を保持します。アップデート処理中に、CMC 構成設定を工場出荷時のデフォルト設定にリセットするオプションがあります。

メモ: シャーシに冗長 CMC がある場合、両方とも同じファームウェアバージョンにアップデートすることが重要です。ファームウェアのバージョンが異なる場合、フェールオーバーが起きた際、予期せぬ結果になる恐れがあります。

RACADM **getsysinfo** コマンド(『Dell Chassis Management Controller 管理者リファレンス ガイド』の getsysinfo コマンドセクションを参照)または **シャーシ概要** ページ(「現在のファームウェアバージョンの表示」を参照)を使って、シャーシにインストールされている CMC の現在のファームウェア バージョンを表示します。

スタンバイ CMC がある場合は、1 つの操作で両方の CMC を同時にアップデートすることをお勧めします スタンバイ CMC をアップデートし終えたら、CMC の役割を交代させて新しくアップデートした CMC をプライマリにし、古いバージョンのファームウェアの CMC がスタンバイになるようにします（スワッピングルールについては、『Dell Chassis Management Controller ファームウェア管理者リファレンスガイド』の cmcchangeover コマンド セクションを参照）。これによって、次の CMC でファームウェアを更新する前に、更新完了とその新しいファームウェアが正しく機能しているかが確認できます。両方の CMC がアップデートされたら、**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。

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

ウェブインタフェースを使って CMC ファームウェアをアップデートする手順については、「CMC ファームウェアのアップデート」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 **fwupdate** サブコマンドを使用して CMC ファームウェアを更新する手順については、『Dell Chassis Management Controller 管理者リファレンスガイド』の fwupdate コマンドの項を参照してください。

CMC プロパティの設定

ウェブインタフェースまたは RACADM を使って、電力バジェット、ネットワーク設定、ユーザー、SNMP および電子メールによる警告などの CMC プロパティを設定できます。

ウェブインタフェースの使用方法の詳細については、「CMC ウェブインタフェースへのアクセス」を参照してください。RACADM の詳細については、「RACADM コマンドラインインタフェースの使用」を参照してください。

△ **注意: 複数の CMC 設定ツールを同時に使用すると、不測の結果が生じることがあります。**

電力バジェットの設定

CMC には、シャーシに電力バジェット、冗長、動的電源機能を提供する電力バジェットサービスがあります。

電源管理サービスは、電力消費量の最適化、および必要に応じて異なるモジュールに電力を再割り当てする機能を持ちます。

CMC 電力管理の詳細については、「Power Management」を参照してください。

ウェブインタフェースを使って電力バジェットおよびその他の電源設定を行う手順は、「電力バジェットの設定」 を参照してください。

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。

以下のいずれかのツールを使って、CMC ネットワーク設定行うことができます。

- RACADM — 「複数シャーシ内の複数 CMC の設定」を参照してください。

メモ: Linux 環境で CMC を展開する場合は、「RACADM の Linux 管理ステーションへのインストール」を参照してください。

- ウェブインタフェース — 「CMC ネットワークプロパティの設定」を参照してください。

ユーザーの追加と設定

RACADM または CMC ウェブインタフェースを使って CMC の追加、設定を行うことができます。また、Microsoft® Active Directory® を使ってユーザーの管理を行うこともできます。

RACADM を使って CMC のパブリックキーユーザーの追加、設定を行うには、「RACADM による SSH 経由の公開キー認証の設定」を参照してください。ウェブインタフェースを使ってユーザーの追加、設定を行うには、「CMC ユーザーの追加と設定」を参照してください。

CMC で Active Directory を使用する手順については、「CMC と Microsoft Active Directory との併用」を参照してください。

SNMP と電子メール警告の追加

特定のシャーシイベントが発生したときに、SNMP や電子メール警告を生成するように CMC を設定できます。詳細については、「SNMP アラートの設定」および「電子メール警告の設定」を参照してください。

リモート Syslog の設定

リモート syslog 機能は、CMC GUI または racadm コマンドを使用してアクティブ化 / 設定されます。設定オプションには、ログエントリを転送する場合に CMC が使用する syslog サーバー名(または IP アドレス)と UDP ポートが含まれています。設定では、最大 3 つの異なる syslog サーバー送信先を指定できます。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、新しい各ログエントリが CMC によって生成され、送信先に転送されます。

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

CMC サービスを設定するには:

1. CMC ウェブインタフェースにログインします。
2. **ネットワーク / セキュリティ** タブをクリックします。
3. サービス サブタブをクリックします。サービス ページが表示されます。

リモート syslog の詳細については、「表5-27」を参照してください。

冗長 CMC 環境について

プライマリ CMC が故障した場合にフェールオーバーするためのスタンバイ CMC を設置できます。

フェールオーバーは以下のような場合に行われます。

- RACADM **cmcchangeover** コマンドを実行した場合。(『Dell Chassis Management Controller 管理者リファレンスガイド』の cmcchangeover コマンドの項を参照してください。)
- アクティブ CMC で RACADM racreset コマンドを実行した場合。(『Dell Chassis Management Controller 管理者リファレンスガイド』の racreset コマンドの項を参照してください。)
- ウェブインタフェースでアクティブ CMC をリセットします。(「シャーシに対する電力制御操作の実行」に説明されている電力制御操作用の CMC のリセット 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 。
- プライマリ CMC が作動しなくなった場合。

メモ: CMC フェイルオーバーのイベントが起きると、iDRAC 接続とアクティブ CMC セッションはすべて失われます。セッションを失ったユーザーは、新しいプライマリ 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と、冗長性低下として報告されます。

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

メモ: スタンバイ CMC のインストールの詳細については、『ハードウェア取扱説明書』を参照してください。スタンバイ CMC に CMC ファームウェアをインストールする手順については、「CMC ファームウェアのインストールまたはアップデート」を参照してください。

プライマリ CMC の選択プロセス

2 つの CMC スロットには違いはありません。つまり、スロットによってアクティブかスタンバイかが決まるわけではありません。最初にインストールまたは起動した CMC がアクティブ CMC になります。CMC が 2 台設置されている場合に AC 電源を入れると、CMC シャーシスロット 1（左側）に取り付けられている CMC がアクティブ CMC になります。アクティブ CMC は青色 LED で示されます。

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

冗長 CMC の正常性状態の取得

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 CMC の正常性状態にアクセスする詳細については、「シャーシとコンポーネントの正常性状態の表示」を参照してください。

目次ページに戻る

目次ページに戻る

I/O ファブリック管理

Dell™ Chassis Management Controllerファームウェアバージョン 2.10 ユーザーガイド

シャーシは、最大 6 つのパススルーまたはスイッチ方式の I/O モジュール(IOMs)を収容できます。

これらの IOM は A、B、C という 3 つのグループに分類されます。各グループには、スロット 1 とスロット 2 があります。スロットには、シャーシの背面に左から右へ A1 | B1 | C1 | C2 | B2 | A2 と文字が割り当てられています。各サーバーは IOM に接続するためのメザニンカード(MC)用スロットを 2 つ持ちます。各 MC とそれに対応する IOM は同じファブリックでなければなりません。

シャーシは 3 つのファブリックまたはプロトコルタイプをサポートします。グループ内の IOM および MC は同一または互換性のあるファブリック タイプでなければなりません。

- **グループ A** IOMS は常にサーバーのオンボード Ethernet アダプタに接続されているので、グループ A のファブリックタイプは常に Ethernetです。
- グループ B については、IOM スロットは各サーバーモジュールの最初の MC(メザニンカード)スロットに永久的に接続されています。
- グループ C については、IOM スロットは各サーバーモジュールの 2 つめの MC(メザニンカード)に永久的に接続されています。

各 MC は 2 つの外部リンクをサポートしています。たとえば、最初の MC では、最初のリンクは永続的にグループ B のスロット 1 の IOM に接続し、2 番目のリンクは永続的にグループ B のスロット 2 の IOM に接続しています。

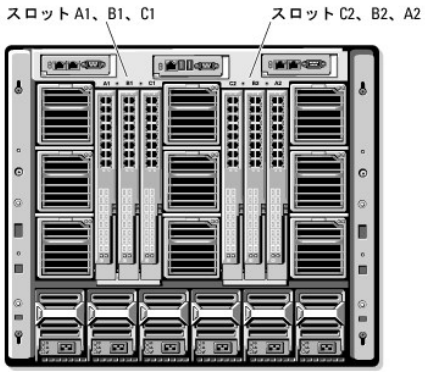
メモ: CMC CLI では、IOM は慣習的に switch-n と命名されます (A1=switch-1、A2=switch-2、B1=switch-3、B2=switch-4、C1=switch-5、C2=switch-6)。

ファブリック管理

ファブリック管理は、シャーシの確立されているファブリック タイプと互換性のないファブリックタイプを持つ IOM および MC のインストールにより起こる電気的、構成上、または接続性の問題を避ける役に立ちます。無効なハードウェア構成は、シャーシまたはそのコンポーネントに電気的または機能上の問題を引き起こす可能性があります。ファブリック管理は、電源投入による無効な構成を防止します。

図10-1 は、シャーシ内の IOM の位置を表示します。各 IOM の位置は、グループ番号(A、B、C)とスロット番号(1 または 2)で示されます。シャーシ上で、IOM スロット名は A1、A2、B1、B2、C1、C2 とマークされています。

図 10-1 IOM の位置を示すシャーシの背面図



CMC は無効なハードウェア構成に対してハードウェアログと CMC ログの両方にエントリを作成します。

例:

- ファイバチャネル IOM に接続された Ethernet MC は無効な構成です。ただし、同じ IOM グループに取り付けられた Ethernet スイッチおよび Ethernet パススルー IOM に接続された Ethernet MC は有効な構成です。
- スロット B1 と B2 にファイバチャネルパススルー IOM とファイバチャネルスイッチ IOM を実装した構成は、各サーバー上の最初の MC もファイバチャネルである場合は有効です。この場合、CMC は IOM とサーバーに電源を投入します。ただし、特定のファイバチャンネル冗長性ソフトウェアはこの構成に対応していないものもあり、すべての有効な構成が対応する構成であるとは限りません。

メモ: サーバー MC のファブリック検証は、シャーシの電源がオンのときにのみ実行されます。シャーシがスタンバイ電源で稼動している場合、サーバーモジュール上の iDRAC の電源は切れたままであるため、サーバーの MC ファブリックタイプを報告できません°MC ファブリックタイプは、サーバー上の iDRAC に電源が投入されるまでは、CMC に報告されません。

無効な構成

無効な構成には、3 つのタイプがあります。

- 無効な MC構成:新しく取り付けた MC ファブリック タイプが既存の IOM ファブリックと異なる場合
- 無効な IOM-MC 構成:新しく取り付けた IOM のファブリック タイプと冗長 MC のファブリック タイプが異なるかまたは互換性がない場合
- 無効な IOM-IOM 構成:新しく取り付けた IOM とグループ内の既存の IOM のファブリック タイプが異なるka互換性がない場合

無効なメザニンカード(MC)構成

1 台のサーバーの MC がそれに対応する IOM でサポートされていない場合に、MC 構成は無効になります。この場合、シャーシ内のすべての別のサーバーは稼働できますが、MC カードと一致しないサーバーは電源を入れることができません。

無効な IOM-メザニンカード(MC)構成

不一致の IOM は電源オフ状態のままとなります。CMC は 無効な構成および IOM 名を CMC とハードウェアログにエントリとして追加します。また、無効の原因となっている IOM のエラー LED を点滅させます。CMC が警告を送信する設定になっている場合は、このイベントに関する電子メールまたは SNMP 警告を送信します。

CMC およびハードウェアログの詳細については、「イベントログの表示」を参照してください。

無効な IOM-IOM 構成

CMC は、新しく取り付けた IOM を電源オフの状態にし、IOM のエラー LED を点滅させ、不一致に関するエントリを CMC およびハードウェア ログに作成します。

CMC およびハードウェアログの詳細については、「イベントログの表示」を参照してください。

初期電源投入シナリオ

シャーシをプラグインして電源を入れるとき、I/O モジュールがサーバーに優先されます。各グループの最初の IOM は他の IOM より先に電源投入できます。このとき、ファブリック タイプの検証は行われません。グループの最初のスロットに IOM がない場合は、そのグループの 2 番目のモジュールに電源が投入されます。両方のスロットに IOM がある場合は、2 番目のスロットにあるモジュールは最初のスロットにあるモジュールとファブリック タイプが比較されます。

IOM に電源が投入された後、サーバーが電源投入され、CMC はサーバーのファブリック タイプの一致を検証します。

ファブリックが同じである限り、パススルーとスイッチを同じグループに共存させることができます。スイッチとパススルー モジュールは、異なるベンダー製でも同じグループに入れることができます。

IOM 正常性の監視

IOM の正常性の状態は、2 つの方法で確認することができます。1 つは、シャーシステータス ページの シャーシグラフィックス セクション、もう 1 つは I/O モジュールステータス ページです。シャーシグラフィックス ページは、シャーシに取り付けられた IOM のグラフィック表示を提供します。

シャーシグラフィックスを使用して IOM の正常性の状態を閲覧するには

1. CMC ウェブインタフェースにログインします。
2. シャーシステータス ページが表示されます。シャーシグラフィックス の右側のセクションは、シャーシの背面図を表し、IOM の正常性の状態が含まれます。IOM の正常性の状態は、IOM のサブグラフィックの色で示されます。
   - 緑色 - IOM が存在し、電源がオンで CMC と通信中。悪条件の兆候はなし。
   - オレンジ色 - IOM が存在し、電源がオンまたはオフで、CMC と通信中または通信しておらず。悪条件が存在する可能性あり。
   - 灰色 - IOM が存在するが、電源がオフ。CMC と通信しておらず、悪条件の兆候なし。
3. 特定の IOM サブグラフィック上にカーソルを移動すると、該当するテキストヒントまたは画面ヒントが表示されます。テキストヒントは、IOM に関する追加情報を提供します。
4. IOM サブグラフィックは、該当する CMC GUI ページにハイパーリンク付けされ、対象の IOM と関連付けられた I/O モジュールステータス ページに瞬時に移動することができます。

I/O モジュールステータス ページを使用してすべての IOM の正常性の状態を閲覧するには

1. CMC ウェブインタフェースにログインします。
2. システムツリーのシャーシメニューで、I/O モジュールを選択します。
3. プロパティ タブをクリックします。
4. ステータス サブタブをクリックします。I/O モジュールステータス ページが表示されます。表10-1に、I/O モジュールステータス ページに表示される情報の説明を掲載します。.

表 10-1 I/O モジュールの情報

項目	説明		
スロット	シャーシ内の I/O モジュールの位置をグループ番号（A、B、C）とスロット番号（1 または 2）で示します。スロット名：A1、A2、B1、B2、C1、C2		
存在	IOM が存在するかどうかを示します（はい または いいえ）。		
正常性		OK	IOM が存在し、CMC と通信していることを示します。CMC とサーバー間で通信エラーが発生した場合は、CMC で IOM の正常性の状態を取得したり、表示することはできません。
		情報	正常性の状態（OK、警告、重大）に変化がない場合に IOM についての情報を表示します。
		警告	警告アラートが発行されたこと、および対応処置を取る必要があることを示します。システム管理者が対応処置を取らなかった場合は、IOM の保全性に影響するような重要または重大なエラーを引き起こす可能性があります。 警告が出される状態の例：IOM ファブリックとサーバーのメザニン カード ファブリックが不一致、無効な IOM 構成、新しく取り付けた IOM と同じグループの既存の IOM との不一致
		重大	少なくとも 1 つのエラー警告が発行されたことを示します。重大な状態は IOM のシステムエラーを示し、直ちに対応処置を取る必要があります。 重大な状態を引き起こす状態の例：IOM の故障が検出された場合、IOM が取り外された場合
	メモ: 正常性に変化があれば、ハードウェアと CMC ログの両方に記録されます。詳細については、「イベントログの表示」を参照してください。		
ファブリック	IOM のファブリックタイプを示します（ギガビットt Ethernet、10GE XAUI、10GE KR、10GE XAUI KR、FC 4 Gbps、FC 8 Gbps、SAS 3 Gbps、SAS 6 Gbps、Infiniband SDR、Infiniband DDR、Infiniband QDR、PCIe バイパス Generation 1、PCIe バイパス Generation 2）。 **メモ:** シャーシに搭載された IOM のファブリックタイプがわかっていると、同じグループ内で IOM の不一致が発生するのを防ぐのに効果的です。I/O ファブリックの詳細については、「I/O ファブリック管理」を参照してください。		
Name	IOM 製品名が表示されます。		
IOM 管理コンソールの起動		特定の IO モジュールを示すアイコンが存在する場合は、アイコンをクリックして新しいブラウザ ウィンドウまたはタブで IOM 管理コンソールを起動します。 **メモ:** このオプションは、管理されているスイッチ I/O モジュールに対してのみ利用可能です。パススルー I/O モジュールまたは管理されていない Infiniband スイッチには使えません。	

		メモ: I/O モジュールの電源がオフのためアクセスできない、その LAN インタフェースが無効である、またはモジュールが有効な IP アドレスに割当てられていない場合は、IOM GUI の起動オプションはその I/O モジュールに表示されません。 **メモ:** その場合は、I/O モジュールの管理インタフェースにログインするよう促されます。 **メモ:** 「個別 IOM のネットワーク設定」の説明に従って、CMC GUI で I/O モジュールの IP アドレスを設定することができます。
ロール		I/O モジュールにリンクすると、ロールに I/O モジュール スタック メンバーを表示します。メンバーとは、モジュールはスタック セットの一部です。マスターとは、モジュールはプライマリ アクセス ポイントです。
電源状態		IOM の電源状態:オン、オフ、なし(不在)を示します。
サービスタグ		IOM のサービスタグを表示します。サービス タグはサポートおよびメンテナンス用に Dell が提供する固有の識別子です。 正常性に変化があれば、ハードウェアと CMC ログの両方に記録されます。詳細については、「イベントログの表示」を参照してください。 **メモ:** パススルーにはサービス タグはありません。サービスタグがあるのは、スイッチだけです。

個別の IOM の正常性状態の表示

I/O モジュールステータス ページ(I/O モジュールステータス ページとは別)に、個別の IOM の概要が表示されます。

個別の IOM の正常性状態を表示するには:

1. CMC ウェブインタフェースにログインします。
2. システムツリーで I/O モジュール を展開します。すべての IOM (1 ～6) が展開されたI/O モジュール リストに表示されます。
3. システムツリーの I/O モジュール リストで表示したい IOM をクリックします。
4. ステータス サブタブをクリックします。I/O モジュールステータス ページが表示されます。

表10-2 では、I/O モジュールステータス ページに表示される情報について説明します。

表 10-2 I/O モジュール正常性状態の情報

項目	説明		
場所	シャーシ内の IOM の位置をグループ番号(A、B、C)とスロット番号(1 または 2)で示します。スロット名:A1、A2、B1、B2、C1、C2		
Name	IOM の名前が表示されます。		
存在	IOM が 存在 または 不在 かを示します。		
正常性		OK	IOM が存在し、CMC と通信していることを示します。CMC とサーバー間で通信エラーが発生した場合は、CMC で IOM の正常性の状態を取得したり、表示することはできません。
		情報	正常性の状態(OK、警告、重大)に変化がない場合に IOM についての情報を表示します。 情報ステータスを引き起こす状態の例:IOM の存在が検出された場合、ユーザーが IOM のパワーサイクルを要求した場合
		警告	警告アラートが発行されたこと、および対応処置を取る必要があることを示します。システム管理者が対応処置を取らなかった場合は、IOM の保全性に影響するような重要または重大なエラーを引き起こす可能性があります。 警告が出される状態の例:IOM ファブリックとサーバーのメザニンカードファブリックとの不一致、無効な IOM 構成、新しく取り付けた IOM と同じグループの既存の IOM との不一致
		重大	少なくとも 1 つのエラー警告が発行されたことを示します。重大な状態は IOM のシステムエラーを示し、直ちに対応処置を取る必要があります。 重大な状態を引き起こす状態の例:IOM の故障が検出された場合、IOM が取り外された場合
	メモ: 正常性に変化があれば、ハードウェアと CMC ログの両方に記録されます。ログの表示の詳細については、「ハードウェアログの表示」および「CMC ログの表示」を参照してください。		
電源状態	IOM の電源状態:オン、オフ、なし(不在)を示します。		
サービスタグ	IOM のサービスタグを表示します。サービス タグはサポートおよびメンテナンス用に Dell が提供する固有の識別子です。		
ファブリック	IOM のファブリックタイプを示します(ギガビットt Ethernet、10GE XAUI、10GE KR、10GE XAUI KR、FC 4 Gbps、FC 8 Gbps、SAS 3 Gbps、SAS 6 Gbps、Infiniband SDR、Infiniband DDR、Infiniband QDR、PCIe バイパス Generation 1、PCIe バイパス Generation 2)。 **メモ:** シャーシに搭載された IOM のファブリックタイプがわかっていると、同じグループ内で IOM の不一致が発生するのを防ぐのに効果的です。I/O ファブリックの詳細については、「I/O ファブリック管理」を参照してください。		
MAC アドレス	IOM のMAC アドレスを表示します。MAC アドレスは識別手段としてハードウェアベンダーによって割り当てられた固有のアドレスです。		

	メモ: パススルーには MAC アドレスはありません。MAC アドレスがあるのは、スイッチだけです。
ロール	モジュール同士がリンク付けされた場合の I/O モジュールのスタックメンバーシップを表示します。 • メンバー - モジュールはスタックセットの一部です。 • マスター - モジュールはプライマリアクセスポイントです。

個別 IOM のネットワーク設定

I/O モジュールセットアップ ページでは、IOM の管理に使うインタフェースのネットワーク設定を指定できます。Ethernet スイッチの場合、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(VLAN 1)の場合、このインタフェースを介して設定は行われません。

メモ: I/O モジュール構成 ページで設定を変更する際、IOM グループ A を設定するにはファブリック A 管理者権限が必要となり、IOM グループ B の場合はファブリック B 管理者権限、IOM グループ C の場合はファブリック C 管理者権限が必要となります。

メモ: Ethernet スイッチの場合、帯域内(VLAN1)および帯域外管理 IP アドレスが共に同じネットワーク上にあってはなりません。この場合、帯域外 IP アドレスは設定されないままとなります。デフォルトの帯域内管理 IP アドレスについては、IOM 文書を参照してください。

メモ: シャーシに存在する IOM のみ、表示されます。

メモ: Ethernet 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。

個別の IOM のネットワーク設定を行うには

1. CMC ウェブインタフェースにログインします。
2. システムツリーで I/O モジュール を展開します。セットアップ サブタブをクリックします。I/O モジュールネットワーク設定 ページが表示されます。
3. I/O モジュールのネットワーク設定を行うには、以下のプロパティ値を入力または選択して、適用 をクリックします。

メモ: 電源を投入できる IOM のみ、設定することが可能です。

メモ: CMC で IOM に設定した IP アドレスは、スイッチの永久的なスタートアップ設定に保存されません。IP アドレスの設定を永久的に保存するには、connect switch-n コマンドまたはracadm connect switch -nRACADM コマンドを入力するか、または IOM GUI への直接インタフェースを使用してこのアドレスをスタートアップ設定ファイルに保存する必要があります。

表 10-3 I/O モジュールのネットワーク設定

項目	説明
スロット	シャーシ内の IOM の位置をグループ番号(A、B、C)とスロット番号(1 または 2)で示します。スロット名:A1、A2、B1、B2、C1、C2 (スロット値を変更することはできません。)
Name	IOM 製品名が表示されます。(IOM 名を変更することはできません。)
電源状態	IOM の電源状況が表示されます。(このページから電源状況を変更することはできません。)
DHCP 有効	シャーシ上の IOM が動的ホスト構成プロトコル(DHCP)サーバーに自動的に IP アドレスを要求して取得できるようになります。 デフォルト:オン(有効) このオプションがオンの場合、IOM は IP 設定(IP アドレス、サブネットマスク、ゲートウェイ)をネットワーク上の DHCP サーバーから自動的に取得します。 **メモ:** この機能が有効な場合、IP アドレス、ゲートウェイおよびサブネットマスクのプロパティフィールド(このオプションのすぐ隣に位置する)は無効になり、過去に入力されたプロパティ値は無視されます。 このオプションがオフの場合、このオプションのすぐ隣の該当するテキストフィールドに、有効な 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する必要があります。
IP アドレス	IOM ネットワークインタフェースの IP アドレスを指定します。
サブネットマスク	IOM ネットワークインタフェースの サブネットマスクを指定します。
ゲートウェイ	IOM ネットワークインタフェースの ゲートウェイを指定します。

IOM ネットワーク設定のトラブルシューティング

以下のリストでは、IOM ネットワーク設定のトラブルシューティングを行う際の項目が含まれます。

- IP アドレスを設定して、適用 をクリックすると、CMC が値を早く読み込み過ぎて、0.0.0.0 と表示することもあります。スイッチに正しい IP アドレスが設定されているか確認するには、更新ボタンをクリックします。
- IP/マスク/ゲートウェイに正しい値を設定しなかった場合、スイッチはこれら値を適用せず、すべてのフィールドに 0.0.0.0 が表示されます。一般的なエラーには、以下が含まれます。
  - 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の入力。
  - スイッチに直接接続しているネットワーク以外のアドレスにデフォルトゲートウェイを設定。

IOM ネットワーク設定の詳細に関しては、「Dell™ PowerConnect™ M6220 Switch Important Information 文書」および「Dell™ PowerConnect™ 6220 Series Port Aggregator ホワイトペーパー」を参照してください。

目次ページに戻る

目次ページに戻る

概要

Dell™ Chassis Management Controllerファームウェアバージョン 2.10 ユーザーガイド

Dell™ Chassis Management Controller (CMC) はホット プラグ可能なシステム管理ハードウェアおよびソフトウェアのソリューションで、Dell PowerEdge™ M1000e シャーシ システムのリモート管理と電源制御の機能を提供するように設計されています。

CMC は、温度、ハードウェアの誤った構成、電源障害、ファン速度に関する警告やエラーの電子メール警告や SNMP トラップ警告を送信するように設定できます。

CMC は自身のマイクロプロセッサとメモリを持っており、差し込んだモジュラシャーシから電源が供給されます。

CMC を使い始める際は、「CMC のインストールと設定」を参照してください。

このリリースの新機能

このリリースの CMC では、次の機能がサポートされています。

- IPv6 — CMC では IPv6 プロトコルがサポートされるようになりました。

  IPv6 Ready Logo Committee の目的は、IPv6 仕様適合性試験と相互接続性試験の定義、セルフテストツールへのアクセス提供、および IPv6 Ready Logo の取得にあります。CMC および iDRAC は Phase-2 IPv6 Ready Logo の認証を受けており、ロゴ ID は 02-C-000378(Dell PowerEdge M1000e)です。IPv6 Ready Logo プログラムについては、**www.ipv6ready.org** を参照してください。

- VLAN タギング — CMC および iDRACs では、ネットワークトラフィックを仮想 LAN(VLAN)に割り当てることができるようになりました。
- Active Directory アカウントのシングルサインオン — シングルサインオンによって、ローカルシステム上の Microsoft® Active Directory® を使用して認証されたユーザーは、これらの資格情報を CMC ウェブユーザーインタフェースに自動的に適用できます。
- Smart Card を用いた二要素認証 — ユーザーの認証にパスワードだけでなく スマートカードと PIN を加えることでセキュリティを強化しました。
- SSH 経由の公開キー認証 — ユーザー ID / パスワードの組み込みや入力を行う必要をなくしたことで、SSH スクリプトの自動化を促進します。
- 電力管理強化 — 柔軟な電力装置冗長性モード(1+1、2+1、3+1)を用意しました。フォールトトレラントな AC 冗長性モード(1+1、2+2、3+3)も追加しました。
- 追加エラーレポートオプション — iDRAC システムイベントログが **ブレードステータス** ページに表示されるため、iDRAC にログインして表示する必要がなくなりました。また、CMC イベントはリモート syslog サーバーにも送信されるようになりました。
- リモート仮想メディアファイルの共有オプション — ネットワーク上の共有ドライブのファイルを CMC 経由で 1 つまたは複数のブレードにマッピングしたり、オペレーティングシステムを導入および更新に使用できます。
- CMC からサーバーの SEL 項目を読み取ったり、クリアしたりできます。

CMC 管理機能

CMC は次の管理機能を提供します。

- CMC 冗長環境
- IPv4 および IPv6 のダイナミック DNS(DDNS)の登録
- SNMP、ウェブインタフェース、iKVM、または Telnet/SSH 接続を利用したリモートシステム管理と監視

- Microsoft® Active Directory® 認証のサポート — 標準スキーマまたは拡張スキーマを使ってユーザー ID とパスワードを Active Directory で一元管理
- 監視 — システム情報やコンポーネントのステータスにアクセス可能
- システムイベントログへのアクセス — ハードウェアログと CMC ログへのアクセスを提供
- さまざまなコンポーネントのファームウェアアップデート - CMC、サーバー、iKVM および I/O モジュールのインフラストラクチャデバイス
- Dell OpenManage™ ソフトウェア統合 — Dell OpenManage Server Administrator または IT Assistant から CMC ウェブベースインタフェースを起動
- CMC 警告 — 電子メールメッセージまたは SNMP トラップを使って管理対象ノードに関する潜在的な問題を警告
- リモート電源管理 — シャーシコンポーネントのシャットダウンやリセットといったリモート電源管理機能を管理コンソールから提供
- 電源使用率のレポート
- Secure Sockets Layer(SSL)暗号化 — ウェブインタフェースからセキュアなリモートシステム管理を提供
- 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
- 役割(ロール)ベースの権限 — さまざまなシステム管理タスクに応じて割り当て可能な権限
- 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、工場出荷時割り当ての World Wide Name/Media Access Control(WWN/MAC) ID をシャーシ割り当ての WWN/MAC ID への置き換え(詳細は「FlexAddress の使用」を参照)
- シャーシのコンポーネントステータスおよび正常性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
- 一度に複数の iDRAC 管理コンソール ファームウェアを更新
- LCD iDRAC 設定ウィザードによる iDRAC ネットワーク構成のサポート
- 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 フェイルオーバー、サーバーの仮想「再接続」

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。

- Active Directory(オプション)またはハードウェアに保存されているユーザー ID とパスワードによるユーザー認証
- システム管理者が各ユーザーに特定の権限を設定できる役割(ロール)ベースの許可
- ウェブインタフェースを介してのをユーザー ID とパスワードの設定
- 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

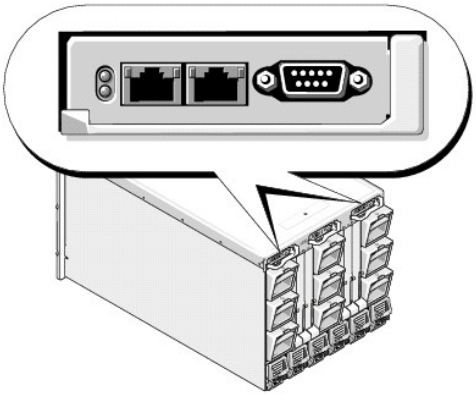
  メモ: Telnet は SSL 暗号化をサポートしていません。

- 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回数の制限によって制限を越えた IP アドレスからのログインを阻止
- 設定可能なセッション自動タイムアウトおよび同時セッション数
- 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

図1-1 は、CMC(差し込み)の前面図とシャーシ内の CMC スロット位置を表示しています。

図 1-1 Dell M1000e シャーシと CMC



ハードウェア仕様

TCP / IP ポート

CMC のリモートアクセス用にファイアウォールを開くときにポート情報を提供する必要があります。

表1-1 に、CMC がサーバー接続を監視するポートを示します。表1-2 に、CMC がクライアントに使用するポートを示します。

表 1-1 CMC サーバーリスニングポート

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

表 1-2 CMC クライアントポート

ポート番号	機能
25	SMTP
53	DNS
68	DHCP で割り当てた IP アドレス
69	TFTP
162	SNMP トラップ
514*	リモート syslog
636	LDAPS
3269	グローバルカタログ(GC)用 LDAPS
*設定可能なポート	

対応リモートアクセス接続

表1-3 は接続機能のリストです。

表 1-3 対応リモートアクセス接続

接続	機能
CMC NIC	• CMC GbE ポート経由での 10Mbps/100Mbps/1Gbps Ethernet 接続 • DHCP のサポート • SNMP トラップと電子メールによるイベント通知 • CMC ウェブインタフェース専用ネットワークインタフェース • iDRAC と I/O モジュール (IOM) 用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などの Telnet/SSH コマンドコンソールおよび RACADM CLI コマンドに対応
シリアルポート	• システムブート、リセット、電源投入、およびシャットダウンコマンドなどのシリアルコンソールおよび racadm CLI コマンドに対応 • 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をサポート • 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 モジュールに接続できます。
その他の接続	• Avocent® Integrated KVM Switch Module (iKVM) 経由での Dell CMC コンソールへのアクセス

対応プラットフォーム

CMC は、M1000e プラットフォーム用に設計されたモジュラシステムをサポートします。CMC との互換性の詳細については、デバイスのマニュアルを参照してください。

サポートされるプラットフォームの最新情報に関しては、デルサポートサイト **support.dell.com** にある『Dell PowerEdge 互換性ガイド』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、**デルサポートサイト support.dell.com** にある『Dell システム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。

CMC ウェブインタフェースのローカライズバージョンを表示するには:

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

対応管理コンソールアプリケーション

CMC は、Dell OpenManage IT Assistant と統合できます。詳しくは、デルサポートサイト support.dell.com から入手可能な IT Assistant の説明書を参照してください。

WS-Management のサポート

Web Services for Management (WS-MAN) は、システム管理に使用する SOAP (Simple Object Access Protocol) ベースのプロトコルです。WS-MAN は、ネットワーク上でデータを共

有および管理するための相互運用可能なプロトコルです。CMC は、WS-MAN を使用して、Distributed Management Task Force(DMTF)の Common Information Model(CIM)ベースの管理情報を提供します。CIM 情報では、管理下システムで利用可能なセマンティクスと情報タイプを定義します。Dell 組み込み型のサーバープラットフォーム管理インタフェースはプロファイルごとに整理されています。各プロファイルは個々の管理ドメインおよび機能エリアのインタフェースを定義します。さらに、追加機能用のインタフェースを提供する多数のモデルやプロファイル拡張機能も定義されています。

WS-Management にアクセスするには、ポート 443 から Secured Socket Layer(SSL)プロトコル経由で基本認証を使用して、ローカルユーザー権限でログインする必要があります。ユーザーアカウント設定の詳細については、『Dell Chassis Management Controller ファームウェア管理者リファレンス ガイド』の cfgSessionManagement データベースのプロパティの項を参照してください。

WS-Management で使用できるデータは、次の DMTF プロファイルバージョン 1.0.0 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るデータのサブセットです。

- 割り当て機能プロファイル
- ベースメトリックプロファイル
- ベースサーバープロファイル
- コンピュータシステムプロファイル
- モジュラシステムプロファイル
- 物理アセットプロファイル
- Dell 電源割り当てプロファイル
- Dell 電源プロファイル
- Dell 電源トポロジプロファイル
- 電源状況管理プロファイル
- プロファイル登録プロファイル
- レコードログプロファイル
- リソース割り当てプロファイル
- ロールベース認証プロファイル
- センサープロファイル
- サービスプロセッサプロファイル
- 簡易 ID 管理プロファイル
- Dell Active Directory クライアントプロファイル
- 起動制御プロファイル
- Dell 簡易 NIC プロファイル

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。ユーザーアカウント設定の詳細については、『Dell Chassis Management Controller ファームウェア管理者リファレンス ガイド』の cfgSessionManagement データベースのプロパティの項を参照してください。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。

このほか、デルテクニカルセンター **www.delltechcenter.com** には、実装ガイド、ホワイトペーパー、プロファイル、コードサンプルに関する資料が揃っています。詳細については、以下を参照してください。

- DTMF ウェブサイト: www.dmtf.org/standards/profiles/
- WS-MAN リリースノートまたは Read Me ファイル。
- **www.wbemsolutions.com / ws_management.html**
- DMTF WS-Management 仕様: **www.dmtf.org / standards / wbem / wsman**

その他のマニュアル

このユーザーズガイド以外にも、次の文書にも CMC のセットアップと操作に関する追加情報が記載されています。これらすべての文書は、support.dell.com でアクセスできます。

- CMC オンラインヘルプでは、ウェブインタフェースの使用方法について説明しています。
- 『Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification』は、BIOS およびファームウェアの最小バージョン、インストール方法および使用方法についての情報を提供します。
- 『Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers ユーザーガイド』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™ IT Assistant ユーザーズガイド』には、IT Assistant に関する情報が記載されています。
- サードパーティ製管理コンソールアプリケーションのマニュアル
- 『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』では、システムアップデート対策の一環としての DellUpdate Packages の入手と使用法について説明しています。

また、以下のシステムマニュアルには、CMC のインストール先のシステムに関する詳細が含まれています。

- システムに付属のマニュアルの「安全にお使いいただくために」には、安全および認可機関に関する重要な情報が記載されています。規制の詳細については、www.dell.com/regulatory_compliance にある Regulatory Compliance(法規制の遵守)ホームページを参照してください。保証情報は、このマニュアルに含まれている場合と、別の文書として付属する場合があります。
- 『ラック取り付けガイド』および『ラック取り付け手順』では、システムをラックに取り付ける方法を説明しています。
- 『ハードウェアオーナーズマニュアル』では、システムの機能、トラブルシューティングの方法、およびコンポーネントの取り付け方や交換方法について説明しています。
- システム管理ソフトウェアのマニュアルでは、ソフトウェアの機能、動作条件、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、ソフトウェア、またはマニュアルの変更について記載されたアップデート情報がシステムに付属していることがあります。

  メモ: このアップデート情報には、他の文書の内容を差し替える情報が含まれていることがあるので、必ず最初にお読みください。

- リリースノートまたは readme ファイルには、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や、上級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。
- IOM ネットワーク設定の詳細については、『Dell PowerConnect® M6220 Switch Important Information 文書』および『Dell PowerConnect 6220 Series Port Aggregator ホワイトペーパー』を参照してください。

目次ページに戻る

目次ページに戻る

Power Management

Dell™ Chassis Management Controllerファームウェア
バージョン 2.10 ユーザーガイド

概要

Dell™ PowerEdge™ M1000e サーバーエンクロージャは、市場で最も電力効率が高いモジュラーサーバです。これは、高効率の電源装置とファンを装備するように設計され、システム内の通気を最適化するレイアウトがとられています。また、エンクロージャ内全体を通して電力を最適化するコンポーネントが使用されています。最適化されたハードウェア設計、およびシャーシ管理コントローラ (CMC)、電源装置、iDRAC に内蔵されている高性能の電源管理機能によって、ユーザーは電力効率を向上させ、その電源環境を完全管理することを可能にします。

Dell PowerEdge M1000e モジュラーエンクロージャは AC 電力を収容し、すべてのアクティブな内部電源装置ユニット(PSU)に電力を配分します。このシステムは、最大 7928 ワット の AC 電力をサーバーモジュールとそれに接続されるエンクロージャのインフラストラクチャに割り当てます。

メモ: 実際の電源供給は、設定と負荷に基づいています。

M1000e の電力管理機能は、管理者が電力消費量を削減できるようにエンクロージャを設定し、独自の要件や環境に対応できるように電源管理をカスタマイズする作業をお手伝いします。

PowerEdge M1000e エンクロージャは、PSU の動作に影響を与え、管理者にシャーシの冗長性状態を報告する方法を決める 3 つの冗長性ポリシーのいずれかに設定可能です。

AC 冗長性モード

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が AC 電源障害に耐えるモードで操作できるようにすることです。電源障害の原因としては、AC 電力グリッド、ケーブル配線、または PSU 自体の障害が考えられます。

システムの AC 冗長性を設定する場合、PSU は一致するセット (グリッド) に分けられます。PSU スロット 1、2、3 は最初のグリッド (グリッド A)、PSU スロット 4、5、6 は 2 番目のグリッド (グリッド B) にそれぞれ分けられます。一致するセット内の各 PSU は異なる AC 電力グリッドに属しており、適切な AC 冗長性モードで操作できるようにケーブル配線する必要があります。負荷はすべてのアクティブな PSU 間に分散されます。1 つの PSU 上の負荷は全容量の 50% を超えてはいけません。個々の PSU で障害が発生した場合は、AC 冗長性によって一方の AC 電力グリッド全体または全容量の最大 50% までの喪失を許容できます。モジュラーエンクロージャシステムには十分な電源が供給し続けられます。

AC 冗長性モードは 6 台の PSU 構成の工場出荷時の設定モードであり、シャーシの AC 冗長性が設定されていることを示します。

メモ: システムは、必要な条件が満たされた場合にのみ AC 冗長性モードで作動します。つまり、各 AC 電力グリッドには一致する PSU を指定する必要があり、全体の負荷は 1 つのグリッドの容量を超えてはなりません。

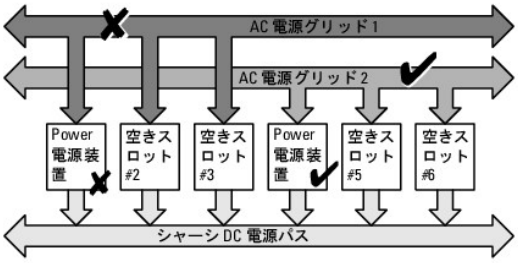
AC 冗長性レベル

CMC は 1+1、2+2、3+3 という 3 つのレベルの N+N AC 冗長性をサポートしています。

AC 冗長性では、CMC はすべてのアクティブな電源装置をオンラインとしてレポートします。これは、一方のグリッドで電源障害が発生した場合に、ダウンタイムが生じないようにするために行われます。一方のグリッド内の N 台の PSU のどれかで障害が発生すると、エンクロージャ冗長性ステータスは 冗長性なし として報告されます。冗長性の喪失 イベントを警告するように設定している場合は、電子メールおよび SNMP 警告が管理者宛てに送信されます。

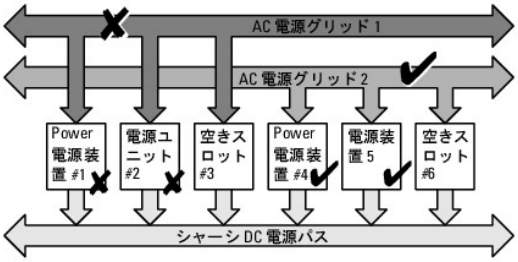
- 1+1 AC 冗長性レベル — 1 台以上の PSU が各 AC グリッドに接続されています。

図 8-1 1+1 冗長性レベル



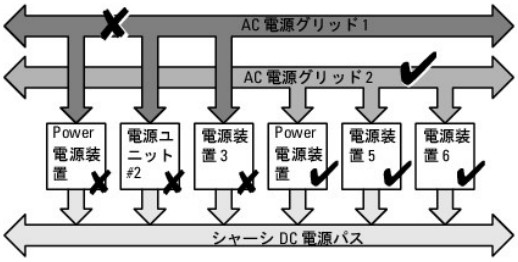
- 2+2 AC 冗長性レベル — 2 台以上の PSU が各 AC グリッドに接続されています。

図 8-2 2+2 冗長性レベル



- 3+3 AC 冗長性レベル — 3 台の PSU が各電力グリッドに接続されています。3 台の PSU でエンクロージャ全体に電源を供給できるため、この構造は AC グリッドにエラーが発生してもエンクロージャへの電力を失うことなく影響も受けません。

図 8-3 3+3 冗長性レベル



メモ: この構成で 1 台の PSU に障害が発生すると、障害側の残りの 2 台の PSU に **オンライン** のマークが付きます。この状態で、残りの PSU のいずれかに障害が発生しても、システムの動作が中断されることはありません。PSU に障害が発生すると、シャーシの正常性に非重要のマークが付きます。小さいグリッドでシャーシ電源をすべて割り当てることができない場合は、AC 冗長性は **冗長性なし** と報告され、シャーシの正常性は **重要** と表示されます。

メモ: すべてのブレードを操作するのにシャーシで必要な PSU は 3 台だけです。ただし、AC 冗長性をサポートするには、バランスのとれた PSU セットが必要です。つまり、半分は電源の供給能力を計算する場合に使用し、残りの半分は AC 冗長性を確保するのに使用します。インストールした PSU の台数がサーバーを操作するのに必要な数よりも少ない場合、冗長性は **冗長性なし** と報告されるか、サーバーで電源を入れることができない可能性があります。

電源装置冗長モード

電源装置冗長モードは冗長電源グリッドがない場合に便利ですが、ユーザーは 1 台の PSU の障害でモジュラーエンクロージャのサーバーが停止しないようにする対策が必要です。この目的で、1 台の PSU の容量がオンライン予約されています。これによって、電源装置の冗長性プールが作成されます。

このプール外で取り付けられた PSU は使用されません。プール内のいずれかの PSU で障害が発生した場合に、これらの PSU が冗長性プールに取り込まれます。

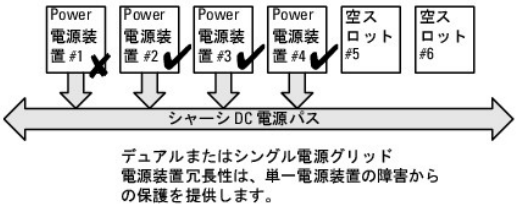
電源装置の冗長性レベル

CMC は 1+1、2+1、3+1 という 3 つのレベルの電源装置の冗長性をサポートします。このオプションを使うと、1 台の PSU に障害が発生しても耐えられるように、追加の PSU が常に接続された状態になります。図8-4 には、最初の 4 つの PSU スロットに 4 台の PSU がある構成が示されていますが、CMC では指定された PSU スロット位置に 4 台の PSU が存在する必要はありません。

DPSE (動的電源供給) を使用すると、PSU をスタンバイ状態にできます。

スタンバイ状態は物理的な状態 (OFF) を表します。DPSE を有効にすると、余剰 PSU はスタンバイモードになり、効率アップと節電につながります。

図 8-4 電源装置の冗長性: 3+1 の PSU 冗長性



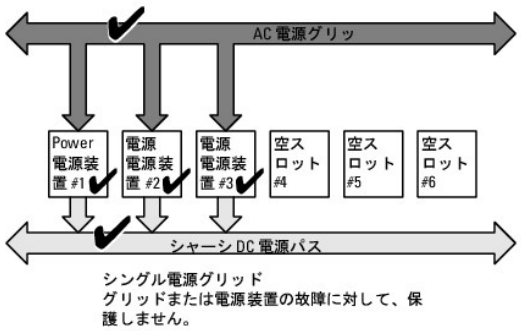
冗長性なしモード

冗長性なしモードは、3 台の PSU 構成の工場出荷時のデフォルトであり、シャーシに電源の冗長性が設定されていないことを示します。この構成のとき、シャーシの全体的な冗長性が常に冗長性なしであることを示します。

図8-5 には、最初の 3 つの PSU スロットに 3 台の PSU の設定が含まれていますが、CMC では指定の PSU スロットの位置に 3 台の PSU ユニットが存在する必要はありません。

メモ: シャーシ内のすべてのアクティブな PSU は **オンライン** としてリストされており、電源効率を高めるために余剰 PSU はオフになっています。また、DPSE が有効な場合は、**スタンバイ** のマークが付いています。DPSE が **冗長性なし** モードで無効になっている場合、シャーシ内のすべての PSU は **オンライン** としてリストされています。

図 8-5 冗長性なし



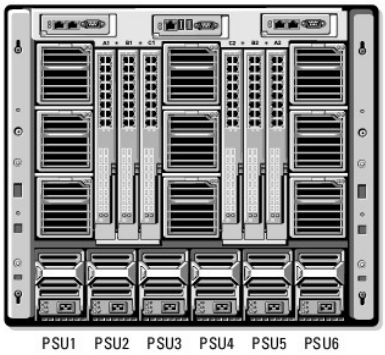
1 台の PSU で障害が発生すると、シャーシの電源割り当てをサポートするために、必要に応じて他の PSU がスタンバイモードが解除されます。4台の PSU がありそのうち 1 台で障害が発生すると、4 台目の PSU がオンラインになります。シャーシには最大 6 台の PSU をオンラインにできます。

DPSE を有効にすると、余剰 PSU がスタンバイモードにされ、効率アップと節電につながります。

ハードウェアモジュールの電力バジェット

図8-6 には、6 台の PSU 構成のシャーシが示されています。PSU は、エンクロージャの左端から 1 ～ 6 の番号が付けられています。

図 8-6 PSU 6 台構成のシャーシ



CMC は、インストールさ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の電力バジェットを維持します。

CMC は、電源をシャーシ内の CMC インフラストラクチャとブレードサーバーに割り当てます。CMC インフラストラクチャはファン、I/O モジュール、iKVM (存在する場合) などのシャーシ内のコンポーネントから構成されています。シャーシには、iDRAC 経由でシャーシと通信する最大 16 台のブレードサーバーを搭載できます。詳細については、『iDRAC ユーザーズガイド』(**support.dell.com / manuals**) を参照してください。

iDRAC は、ブレードサーバーの電源を投入する前に、CMC に電力エンベロープ要件を渡します。電力エンベロープは、サーバーを作動し続けることができる最大/最小電力要件から構成されています。iDRAC の初期想定は、ブレードサーバー内のすべてのコンポーネントが最大電力量を消費し、実際のブレード条件よりも電力量が高い場合が多い、という最悪のケースに基づいています。

サーバーがエンクロージャで電源投入されると、iDRAC ソフトウェアは電源要件を推定し直して、電力エンベロープの変更を要求します(通常は削減)。

CMC は要求された電力をブレードサーバーに供給し、割り当てられたワット量が使用可能なバジェットから減算されます。サーバーに電力要求量が与えられると、サーバーの iDRAC ソフトウェアは実際の電力消費量を継続的に監視します。実際の電力要件に応じて、iDRAC 電力エンベロープは時間の経過に伴い変更される場合があります。iDRAC は、サーバーが割り当てられた電力を完全に消費している場合にのみ、電力アップを要求します。

ただし、負荷が大きい場合は、電力消費量をユーザーの設定した**システム入力電力の上限**より低い状態に保つため、サーバーのパフォーマンスを低下させる場合があります。

PowerEdge M1000e エンクロージャは、ほとんどのサーバー設定で最高の性能を発揮するために十分な電力を供給できますが、利用可能なサーバー構成の多くでは、エンクロージャが供給可能な最大電力を消費することはありません。データセンター施設でエンクロージャの電力プロビジョニングを設定するとき、M1000e を使うと、ユーザーはシステム入力電力上限を指定して、全体的なシャーシの AC 電力が与えられたしきい値を超えないようにできます。CMC は最初に、ファン、IO モジュール、iKVM(装着されている場合)、および CMC の実行に十分な電力を確保します。この電力の割当ては、シャーシ インフラに割当てた入力電力と呼びます。エンクロージャ内のサーバーに電源を投入した後は、サーバーの電源を切ることを必要とするような **システム入力電力上限** を下げる試みは失敗します。

総電力バジェットをシステム入力電力上限の値より低くする必要がある場合は、CMC がサーバーの値を要求された最大電力より低い値に割り当てます。サーバーには個々の**サーバー**の優先度設定に基づいて電力が割り当てられます。たとえば、優先度 1 のサーバーは最大電力を取得し、優先度 2 のサーバーは優先度 1 のサーバーの後に電力を取得する、というようになります。**システム入力の最大電力容量** とユーザーが設定した **システム入力電力上限** によっては、優先度が低いサーバーが取得する電力量は、優先度 1 のサーバーよりも少ない場合があります。

シャーシにサーバーを追加するなどの構成上の変更を行う場合は、システム入力電力上限 を上げる必要があることがあります。モジュラーエンクロージャに必要な電力は、温度条件が変わり、ファンを高速で運転する必要がある場合、つまり電力消費量を増やす必要が発生した場合にも増加します。また、I/O モジュールや iKVM を追加する場合にも、モジュラーエンクロージャの必要電力が増加します。サーバーの電源が入っていない場合でも、管理コンソールへの電源供給を維持するため、サーバーはり極めて少ない量の電力を消費します。供給電力が十分ある場合のみ、追加サーバーへの電源投入をモジュラーエンクロージャ内で行うことができます。システム入力電力上限をいつでも最大 7928 ワットまで増量して、追加サーバーに電力を供給することができます。

電力割り当てを削減するモジュラーエンクロージャ内の変更には、サーバーの電源オフ、サーバー、I/O モジュール、または iKVM の取り外し、シャーシの電源オフ状態への移行などがあります。シャーシがオンの場合にもオフの場合にも、**システム入力電力上限** を再設定できます。

サーバー スロットの電力プロパティの設定

CMC では、エンクロージャの 16 個のサーバー スロットのそれぞれの電力プロパティをユーザーが設定できます。プロパティ設定は 1 (優先度高) ～ 9 (優先度低)です。この設定は、シャーシのスロットに割り当てられ、スロットの優先度は、そのスロットに装着されるサーバーに継承されます。CMC はスロットの優先度を使ってエンクロージャの優先度の高いサーバーに電力バジェットを割り当てます。

デフォルトのサーバースロット優先度設定に従って、電力はすべてのスロットに均等に割り当てられます。スロットの優先度を変更することで、管理者がどのサーバーに電力供給が必要か優先順位を付けることができます。より重要なサーバー モジュールの優先度をデフォルトの 1 にしたまま、それほど重要でないサーバー モジュールの優先度を 2 以上に設定すると、優先度が 1 のサーバー モジュールに先に電力が供給されます。優先度の高いサーバーには最大電力が割り当てられますが、優先度の低いサーバーには、最大の性能を発揮するために必要な電力が共有されない、または全く電力が供給されない場合があります。これは、設定された優先度の度合いとサーバーが必要とする電力量に依存します。

システム管理者が、手動で優先度の高いサーバーより先に優先度の低いサーバーモジュールの電源を入れると、優先度の低いサーバーモジュールがその電源割り当てを最小まで下げられる最初のモジュールになります。使用可能な電力割り当てを使い果たすと、CMC は優先度の低いまたは同じサーバーの電力を最小電力レベルまで下げることで利用可能になった電力量を再利用します。

メモ: I/O モジュール、ファン、および iKVM (存在する場合) に最も高い優先度が指定されます。CMC が電力を再利用するのは、優先度の高いモジュールまたはサーバーの電力ニーズを満たすためのみです。

電源装置の動的制御

DPSE(動的電源供給)モードは、デフォルトで無効に設定されています。DPSE は、シャーシの電源を入れるために必要最小限の PSU のみを使用することで節電する結果、オンライン PSU の効率的な利用が実現されます。こうすることで、PSU の寿命が長くなり、発熱を減らし、より効率の良い電力レベルで運転電力を供給することで節電します。

CMC は、エンクロージャ全体の電力割り当てを監視し、不要な PSU をスタンバイ状態にすることで、シャーシの総合電力割り当てを少数の PSU でまかないます。オンライン PSU の利用率が高いほどより効率的であるため、効率の向上につながると同時に、スタンバイ PSU の寿命も延長できます。

アクティブな PSU の台数が少ないほどシステムの運用効率が上がるので、以下が可能になります。

- DPSE の 冗長性なし モードでは、最小台数の PSU のみがオンラインであるため、高い電力効率が得られます。不要な PSU はスタンバイモードになります。
- DPSE の PSU 冗長性 モードでも、電力効率を得ることができます。構成への電力供給用に 1 台と PSU の故障に備えて冗長性を提供するために 1 台の、最低 2 台の PSU をアクティブにします。PSU 冗長性 モードでは 1 台の PSU の故障に対して保護を提供しますが、AC グリッドを喪失した場合は保護されません。
- DPSE の AC 冗長性 モードは、6 台のうち最低 2 台をアクティブ(各電力グリッドに 1 台ずつ)にして、部分的に負荷のかかるモジュラーエンクロージャ構成の効率と最大電力供給のバランスを保ちます。
- DPSE を無効にすると、6 台すべてを稼働して付加を分散させるため効率性が下がるため、各電源装置の利用率も低下します。

DPSE は、ここで説明された 3 つのすべての電源装置冗長性構成(冗長性なし、電源装置冗長性、AC の冗長性)を有効にできます。

- DPSE の 冗長性なし 構成では、M1000e は スタンバイ 状態で最大 5 台の電源ユニットを保持できます。PSU 6 台の構成では、一部の PSU ユニットを使用しないでスタンバイ状態にしておくことで、電力効率を向上させます。この構成でオンライン PSU を取り外したり、故障が発生したりすると、スタンドバイ 状態の PSU を オンライン に切り替えます。ただし、スタンドバイ PSU をアクティブにするために最大 2 秒間かかるため、サーバーモジュールが 冗長性なし 構成に移行する間、電力が供給されない場合があります。

メモ: このの PSU 3 台の構成では、サーバー負荷によって PSU が スタンドバイ に移行できないことがあります。

- 電源装置冗長性 構成では、エンクロージャは電源投入に必要な PSU 以外に、追加 PSU の電源を常にオンに保ち、オンライン のマークを付けます。電源使用量を監視し、システム全体の負荷に応じて、最大 4 台の PSU を スタンバイ 状態に移行できます。PSU 6 台の構成では、最低 2 台の電源ユニットが常にオンに保たれます。

  電源装置冗長性 構成のエンクロージャでは、常に 1 台の余剰 PSU がオンになっているため、オンライン PSU が 1 台故障しても、インストールされているサーバーモジュールに十分に電源を供給することができます。オンライン PSU に故障が発生すると、スタンドバイ PSU がオンラインになります。複数の PSU が同時に故障すると、スタンドバイ PSU を立ち上げている間、いくつかのサーバー モジュールに電源が供給されない場合があります。

- AC 冗長性 構成では、シャーシの電源投入時にすべての電源装置がオンになります。電力使用量が監視され、システム構成と電力使用量に余裕がある場合は、各 AC グリッドから 1 台ずつ、2 台 1 組の PSU が スタンバイ 状態に移行されます(1+1 冗長性レベルを除く)。グリッドにある PSU の オンライン 状態はミラーしているため、エンクロージャは、グリッドへの電力を喪失してもエンクロージャへの電力に支障なく電力を維持することができます。

  AC 冗長性 構成で電力要求が高まると、PSU をペア(各 AC グリッドから 1 台ずつ)で スタンドバイ 状態から起動します。こうして、デュアルグリッド冗長性に必要なミラー構成を維持します。

メモ: DPSE を有効にすると、電力要求が 3 つのすべての電源冗長性ポリシーモードで高まると、スタンバイ PSU が **オンライン** になり電力を再利用します。

冗長性ポリシー

冗長性ポリシーは、CMC がシャーシへの電力供給をどのように管理するか決定付ける一連の設定可能なプロパティです。以下の冗長性ポリシーは、PSU の動的制御の有無にかかわらず設定可能で

す。

- AC 冗長性
- 電源装置冗長性
- 冗長性なし

シャーシのでデフォルト冗長性構成は、表8-1 に示す通り、構成する PSU の数に依存します。

表 8-1 デフォルトの冗長構成

PSU 構成	デフォルトの冗長性ポリシー	デフォルトの PSU 動的制御設定
PSU 6 台	AC 冗長性	無効
PSU 3 台	冗長性なし	無効

AC 冗長性

PSU 6 台の AC 冗長性モードでは、6 台の PSU はすべてアクティブです。左側の PSU 3 台を 1 つの AC 電源グリッドに、そして右側の 3 台を別の電源グリッドに接続する必要があります。

△ **注意: システムエラーを回避し、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 セットを別々の 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、まだ機能している AC グリッドに接続されている 3 台の PSU でサーバーやインフラストラクチャに支障なく引き続き電力を供給します。

△ **注意: 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)。この条件が満たされていない場合は、冗長性が喪失する可能性があります。**

電源装置冗長性

電源装置冗長性を有効にすると、シャーシの PSU を 1 台予備として保持して、どの 1 台の PSU が故障してもサーバーやシャーシへの電力が低下しないようにしています。電源装置冗長性モードでは、最大 4 台の PSU が必要です。追加の PSU が存在する場合、DPSE が有効な場合にはそれらを使って電力効率を上げます。冗長性を喪失した後にエラーが発生すると、シャーシ内のサーバーの電源が低下する可能性があります。

冗長性なし

3 台までの PSU の電源を使用して、シャーシ全体に電力を供給します。したがって、6 台の PSU シャーシでは、どの 3 台の PSU が故障した場合でも、シャーシは引き続きフル稼働します。

△ **注意: 冗長性なしのモードでは、3 台の PSU のみを使用し、予備の PSU はありません。使用されている 3 台の PSU のうち 1 台が故障すると、サーバーの電源とデータが失われる可能性があります。**

節電と電力バジェットの変更

ユーザー設定の電力上限値に達したときに、CMC は節電を実行することができます。電力要求がユーザー設定の **システム入力電力上限** を超えると、CMC は優先度の低い順にサーバーへの電力供給を低減することで、シャーシ内の優先度の高い方のサーバー用に電力が解放されることになり、

シャーシ内のすべてまたは複数のスロットが同じ優先順位を持つ設定になっている場合、CMC はサーバーのスロット番号の小さい順にサーバーへの電力を低減させます。たとえば、スロット 1 と 2 にあるサーバーが同じ優先順位を持つ場合、スロット 1 のサーバーの電力の方がスロット 2のサーバーの電力より先に低減されます。

メモ: シャーシ内のサーバーにそれぞれ 1 ～ 9 の番号を与えることで優先順位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順位は 1 です。低い番号の方が優先順位が高くなります。

サーバーの優先順位を割り当てる手順は、「RACADM の使用」を参照してください。

GUI を使用してサーバーの優先順位を割り当てることができます。

1. システムツリーで **サーバー** をクリックします。
2. **電源管理** タブ→ **優先順位** サブタブを選択します。

冗長性ポリシーが低下またはない状態の PSU 障害

節電モードでは、PSU 障害などの電力不足イベントが発生した場合に、CMC はサーバーへの電力を低減します。サーバーへの電力を低減した後、CMC はシャーシの電力必要量を再算出します。電源条件が満たされていない場合、CMC は低優先順位ブレードサーバーの電源もオフにする場合があります。

電力必要量が電力バジェット内の間、高優先順位サーバーへの電力供給が増分的に復元されます。

メモ: 冗長ポリシーを設定する場合は、「電力バジェットと冗長性の設定」を参照してください。

新規サーバーの制御ポリシー

新しいサーバーに電源が投入され、新しいサーバーの追加によってシャーシの電力必要量が使用可能な電力を超える場合、CMC は新しいサーバーに十分な電力を供給するために、優先順位が低いサーバーへの電力を低減させる必要があるかもしれません。これは、システム管理者がサーバーをフルパワーで稼動させるのに必要な電力量より低い電力上限値をシャーシに設定した場合、またはシャーシ内のすべてのサーバーに必要なワーストケース電力に満たない電力しか利用できない場合に発生する可能性があります。優先度の低いサーバーへの電力を低減させることで十分な電力が解放されない場合は、新しいサーバーを起動できないことがあります。

シャーシと新しいサーバーを含むすべてのサーバーをフルパワーで稼動させるのに必要な最大持続電力がワーストケース電力必要量です。この電力量が利用可能な場合、ワーストケース電力必要量より低い電力がサーバーに割り当てられることはなく、新しいサーバーを起動することが可能です。

ワーストケース電力必要量を満たすことができない場合、新しいサーバーを起動するために必要な電力が解放されるまで、優先度の低いサーバーへの電力は低減されます。

表8-2 は、上記シナリオにて、新しいサーバーに電源投入されたときに行われた操作を説明しています。

表 8-2 サーバーの電源投入が試行されたときの CMC の対応

ワーストケース電力が使用可能	CMC の対応	サーバー電源オン
○	節電は不要	許可
×	節電を実施 • 新しいサーバーに必要な電力が使用可能 • 新しいサーバーに必要な電力が使用不可	許可 不許可

PSU が失敗すると、非重要な正常性状態になり、PSU 障害イベントが生成されます。PSU を取り外すと、PSU の取り外しイベントが発生します。

いずれかのイベントが発生した結果、冗長性が喪失した場合は、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。

後続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は、サーバーのパフォーマンスが低下するか、ひどい場合には、サーバーの電源が切断される恐れがあります。これらの電源切断は優先順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切断されます。

表8-3では、さまざまな PSU 冗長構成における PSU の電源切断または PSU の取り外しに対するファームウェアの対応を示します。

表 8-3 PSU の障害または取り外しによるシャーシへの影響

PSU 構成	PSU 動的制御	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。
冗長性なし	無効	必要に応じて、優先度の低いサーバーへの電力を低減します。
AC 冗長性	有効	CMC はユーザーに AC 冗長性の喪失を警告します。PSU の故障または取り外しにより失われた電力バジェットを補うために、スタンバイの 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 の故障または取り外しにより失われた電力バジェットを補うために、スタンバイの PSU(存在する場合)の電源がオンになります。
冗長性なし	有効	必要に応じて、優先度の低いサーバーへの電力を低減します。

冗長性ポリシーが低下またはない状態の PSU 障害

ユーザーが PSU または PSU の AC コードを取り外すと、CMC は電力の節約を開始します。CMC は、電力消費量がシャーシ内の残りの PSU でまかなうことができるようになるまで優先順位の低いサーバーへの電力を低減させます。複数台の PSU を取り外した場合、CMC は 2 台目の PSU が取り外されたときに電力必要量を再計算して、ファームウェアの対応を決定します。電源条件が満たされていない場合、CMC は低優先順位ブレードサーバーの電源を切断する場合があります。

制限値

- CMC は、優先順位の高いサーバーに電源投入するために優先順位の低いサーバーの電源を自動的に切ることはありませんが、ユーザーが電源を切ることはできます。
- PSU 冗長性ポリシーの変更は、シャーシ内の PSU の台数によって制限されます。M1000e シャーシは、PSU 3 台または 6 台の構成で出荷されます。冗長性ポリシー に記載されている 3 つの PSU 冗長構成のうちのいずれを選択することもできます。

システム イベント ログの電源供給および冗長性ポリシーの変更

電源供給状態および電力冗長性ポリシーの変化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)に記録される電源供給関連のイベントは、電力供給の追加と削除、電力供給入力の追加と削除、電源供給出力の追加と削除、およびアサート停止です。表8-4 下の一覧は、電源供給の変化に関連する SEL 項目です。

表 8-4 電源供給の変化に対する SEL イベント

電源供給イベント	システム イベント ログ (SEL) の項目
差し込み	電源供給の存在がアサートされた
取り外し	電源供給の存在のアサートが停止された
AC 入力受信	電源供給入力喪失のアサートが停止された
AC 入力喪失	電源供給入力喪失がアサートされた
DC 出力生成	電源供給不良のアサートが停止された
DC 出力喪失	電源供給不良がアサートされた

SEL で項目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 電力ポリシー、または 電源装置冗長 電力ポリシーのいずれかに設定されているモジュラーエンクロージャに対する冗長性の喪失および冗長性の回復です。冗長なし 電力ポリシーに設定されているモジュラーエンクロージャは、不十分なリソースに対する SEL 項目を記録し、冗長なし 電力ポリシーは、機能している電力供給台数がエンクロージャ電源供給装置の最小台数 3 台より低くなると記録されます。同様に、機能的な電力供給数を回復すると、SEL 項目が十分なリソースとなり、冗長なし 電力ポリシーが記録されます。表8-5 下の一覧は、電源冗長ポリシーの変化に関連する SEL 項目です。

表 8-5 電源冗長性状態変化の SEL イベント

電力ポリシーイベント	システムイベントログ (SEL) の項目
冗長性喪失	冗長性喪失がアサートされた
冗長性上昇	冗長性上昇がアサートされた

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、冗長性がある状態でシステムが稼動している場合は、全体的な電源正常性は通常、**OK** になります。しかし、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、AC 冗長性から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、すぐに冗長性が喪失したり、冗長性が回復する可能性があります。

電源の設定と管理

ウェブベースまたは RACADM インタフェースを使って CMC 上の電源制御の管理と設定を行うことができます。具体的には、以下のことが可能です。

- シャーシ、サーバーおよび PSU への電力割り当て、消費量およびステータスの表示
- シャーシのシステム入力電力上限と冗長性ポリシーの設定
- 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

PSU の正常性状態の表示

電源装置ステータス ページには、シャーシに関連付けられている PSU の状態が表示されます。

ウェブインタフェースの使用

PSU の正常性状態は、2 つの方法で表示させることができます。1 つは シャーシステータス ページの シャーシグラフィックス セクション、もう 1 つは 電源装置ステータス ページです。シャーシグラフィックス ページは、シャーシに取り付けられたすべての PSU のグラフィック表示を提供します。

シャーシグラフィックス を使用してすべての PSU の正常性状態を表示するには

1. CMC ウェブインタフェースにログインします。
2. シャーシステータス ページが表示されます。シャーシグラフィックス の右側のセクションは、シャーシの背面図を表し、すべての PSU の正常性状態が含まれます。PSU の正常性状態は、PSU サブグラフィックの色で示されます。
   - 緑色 — PSU が存在し、電源がオンで CMC と通信中。悪条件の兆候なし。
   - 黄色 — PSU 障害を示します。エラー状態の詳細については、CMC ログを参照してください。
   - 灰色 — PSU の初期化中（通常はシャーシの電源投入または PSU の挿入時）に表示されます。PSU が存在し、電源がオフ。CMC と通信しておらず、悪条件の兆候なし。
3. 個別の PSU サブグラフィック上にマウスのカーソルを移動すると、該当するテキストヒントまたは画面ヒントが表示されます。テキストヒントは、対象 PSU に関する追加情報を提供します。
4. PSU サブグラフィックは、該当する CMC GUI ページにハイパーリンクされ、すべての PSU の 電源装置ステータス ページに即座に移動することができます。

電源装置ステータス を使用して PSU の正常性状態を表示するには

1. CMC ウェブインタフェースにログインします。
2. システムツリーで 電源装置 を選択します。電源装置ステータス ページが表示されます。

表8-6 および 表8-7 に、電源装置ステータス ページに表示される情報の説明を掲載します。

表 8-6 電源装置の正常性状態の情報

項目	説明
名前	電源装置ユニットの名前 PS-[n] を表示します。[n] は電源装置番号です。

存在	PSU が 存在 または 不在 かを示します。		
正常性		OK	PSU が存在し、CMC を通信を行っていることを示します。CMC と電源装置間で通信エラーが発生した場合は、CMC で PSU の正常性の状態を取得または表示できません。
		警告	警告のみが発行されたこと、および対応処置を取る必要があることを示します。システム管理者が設定した時間内に対応処置を取らなかった場合は、シャーシの保全性に影響するような重要または重大なエラーを引き起こす可能性があります。
		重大	少なくとも 1 件の不良警告が電源供給に対して発行されたことを示します。重大度状態は、シャーシの電源エラーを示し、直ちに対応処置を取る必要があります。
電源状態	電源装置の電源状態を示します(次のいずれか 1 つ):初期化中、オンライン、スタンバイ、診断中、故障、冗長化、**オフライン**または不在。		
容量	電源容量がワットで表示されます。		

表 8-7 システム電源の正常性状態の情報

項目	説明
全体的な電源正常性	シャーシ全体の電源管理の正常性状態(**OK、非重要、重要、回復不可、その他、不明**)を示します。
システム電源の状態	シャーシの電源状態(**オン**、オフ、電源オン、電源オフ)を示します。
冗長性	電源装置冗長性の状態を示します。有効値は次のとおりです。 **いいえ**: 電源装置は非冗長です。 **はい** — 完全冗長化されています。

RACADM の使用

CMC に対応するシリアル/Telnet/SSH テキスト コンソールを開いて、ログイン後、以下を入力します。

```
racadm getpminfo
```

出力詳細を含む getpminfo の詳細については、デルサポートサイト **support.dell.com** の『Chassis Management Controller 管理者リファレンスガイド』を参照してください。

消費電力ステータスの表示

CMC は、システム全体で実際に消費している入力電力を **消費電力ステータス** ページに表示します。

ウェブインタフェースの使用

メモ: 電力の管理を行うには、**シャーシ制御システム管理者**の権限が必要です。

1. CMC ウェブインタフェースにログインします。
2. システムツリーで シャーシ を選択します。
3. 電力管理タブの消費電力サブタブをクリックします。消費電力 ページが表示されます。

表8-8から表8-11では、**消費電力** ページに表示される情報について説明します。

メモ: **システム** ツリー→ **ステータス** タブにある **電源装置** から電力冗長性ステータスを表示することもできます。

RACADM の使用

CMC に対応するシリアル/Telnet/SSH テキスト コンソールを開いて、ログイン後、以下を入力します。

```
racadm getpminfo
```

表 8-8 リアルタイム電力統計

項目	説明
システム入力電力	PSU の AC 入力側から測定したシャーシ内のすべてのモジュールの現在の累積電力消費量を示します。 システム入力電力の値は、ワットおよび BTU/時単位で示されます。
ピークシステム電力	値が最後にクリアされてから消費された最大システムレベル入力電力を表示します。このプロパティによって、経時的に記録されているシステムごと(シャーシとモジュール)の最大電力消費量を追跡できます。この値をクリアにするには、バジェットステータス ページの 設定サブタブをクリックします。ピークシステム電力の値は、ワットおよび BTU/時単位で示されます。
ピークシステム電力の開始時間	ピークシステム電力消費量の値が最後にクリアにされた日時を表示します。タイムスタンプは、hh:mm:ss MM/DD/YYYY の形式で表示されます。hh は時間(0～24)、mm は分(00～60)、ss は秒(00～60)、MM は月(1～12)、DD は日(1～31)、そして YYYY は年を表します。ピーク/最小電力統計のリセット ボタンのクリック時、CMC のリセット時、またはフェールオーバー時にこの値はリセットされます。
ピークシステム電力のタイムスタンプ	記録期間中に記録されたピークシステム電力消費の発生日時を示します。タイムスタンプは **hh:mm:ss MM/DD/YYYY** 形式で表示されます。ここで、**hh** は時間(0～24)、**mm** は分(00～60)、**ss** は秒(00～60)、**MM** は月(1～12)、**DD** は日(1～31)、**YYYY** は年を表します。
最小システム電力	ユーザーが前回この値をクリアした後の最小システムレベルの AC 電力消費量をワットで表示します。このプロパティによって、経時的に記録されているシステムごと(シャーシとモジュール)の最小電力消費量を追跡できます。この値をクリアにするには、**バジェットステータス** ページの **設定**サブタブをクリックします。最小システム電力の値は、ワットおよび BTU/時単位で示されます。ピーク/最小電力統計のリセット ボタンのクリック時、CMC のリセット時、またはフェールオーバー時にこの値はリセットされます。
最小システム電力の開始時間	最小システム電力消費量の値が最後にクリアにされた日時を表示します。タイムスタンプは、hh:mm:ss MM/DD/YYYY の形式で表示されます。hh は時間(0～24)、mm は分(00～60)、ss は秒(00～60)、MM は月(1～12)、DD は日(1～31)、そして YYYY は年を表します。ピーク/最小電力統計のリセット ボタンのクリック時、CMC のリセット時、またはフェールオーバー時にこの値はリセットされます。
最小システム電力のタイムスタンプ	記録機間中に記録された最小システム電力消費の発生日時を示します。タイムスタンプの形式は、**ピークシステム電力のタイムスタンプ** で説明したとおりです。
システムアイドル電力	シャーシのアイドル状態の推定電力消費量が表示されます。アイドル状態とは、シャーシの電源がオンで、すべてのモジュールが電力を消費しているシャーシの状態のことを指します。これは、推定値であり、測定値ではありません。 この推定値は、シャーシ基盤コンポーネント(I/O モジュール、ファン、iKVM、iDRAC コントローラおよび前面パネル LCD)に割り当てられた電力、および電源がオンの状態にあるすべてのサーバーに割り当てられた最小電力要件の累積値として算出されます。システムアイドル電力の値は、ワットおよび BTU/時単位で示されます。
システム潜在電力	シャーシが最大出力で動作している場合の推定電力消費量を表示します。最大電力消費量は、シャーシの電源がオンで、すべてのモジュールが最大出力で電力を消費しているシャーシの状態を示します。この値は、システム構成の履歴データ(総電力消費量)の推定値であり、測定値ではありません。この推定値は、シャーシ基盤コンポーネント(I/O モジュール、ファン、iKVM、iDRAC コントローラおよびフロントパネル LCD)に割り当てられた電力、そして電源がオンの状態になっているすべてのサーバーに割り当てられた最小電力要件の累積値として算出されます。システム潜在電力の値は、ワットおよび BTU/時単位で示されます。
システム入力電流測定値	シャーシ内の各 PSU モジュールの入力電流消費量の合計値に基づいて、シャーシの総入力電流消費量を表示します。システム入力電流測定値は、アンプ(Amp)単位で表示されます。

表 8-9 リアルタイムエネルギー統計ステータス

項目	説明
システムエネルギー消費量	PSU の AC 入力側から測定したシャーシ内のすべてのモジュールの現在の累積エネルギー消費量を示します。 この値は、累積値で KWh 単位で表示されます。
システム エネルギー消費開始時間	システムエネルギー消費量の値が最後にクリアされ、新しい測定サイクルが開始された日時を表示します。タイムスタンプは、hh:mm:ss MM/DD/YYYY の形式で表示されます。hh は時間(0～24)、mm は分(00～60)、ss は秒(00～60)、MM は月(1～12)、DD は日(1～31)、そして YYYY は年を表します。この値は、エネルギー統計のリセット ボタンでリセットされますが、CMC リセット時またはフェールオーバー時にはリセットされません。
システムエネルギー消費量タイムスタンプ	システムエネルギー消費量が表示するために算出された日時を表示します。タイムスタンプは、hh:mm:ss MM/DD/YYYY の形式で表示されます。hh は時間(0～24)、mm は分(00～60)、ss は秒(00～60)、MM は月(1～12)、DD は日(1～31)、そして YYYY は年を表します。

表 8-10 システム電源の状態

項目	説明
全体的な電源正常性	シャーシの電源サブシステムの正常性状態(**OK**、**非重大**、**重大**、**回復不可**、**その他**、**不明**)を示します。
システム電源の状態	シャーシの電源状態(**オン**、**オフ**、**電源オン**、**電源オフ**)を示します。
冗長性	冗長ステータスを示します。有効値は次のとおりです。

	いいえ — PSU は非冗長です。 **はい** — 完全冗長化されています。

表 8-11 サーバーモジュール

項目	説明
スロット	サーバーモジュールの場所を表示します。**スロット** は、サーバー モジュールをシャーシ内の場所で識別する連番(1 ～ 16)です。
Name	サーバー名を表示します。サーバー名はユーザーによって再定義できます。
存在	サーバーがスロットにあるかどうかを示します(ある または ない)。フィールドに拡張#(# は 1-8)が表示される場合、それに続く番号がマルチスロットサーバーのメインスロットとなります。
実測値 (AC)	サーバーが実際に消費する電力をリアルタイムで計測した値です。測定値は、ワット数で表示されます。
電流累積開始時間	開始時間フィールドに指定された時刻移行にサーバーが実際に消費した電力をリアルタイムで測定した値です。測定値は、キロワット時(kWh)で表示されます。
ピーク消費時間スタンプ	サーバーが一度に消費するピーク電力を表示します。ピーク消費電力の発生時間は、タイムスタンプ フィールドに記録されます。測定値は、ワット数で表示されます。

電力バジェット状態の表示

CMC は **電力バジェットステータス** ページに電源サブシステムの電源状態の概要を表示します。

ウェブインタフェースの使用

メモ: 電力の管理を行うには、**シャーシ制御システム管理者**の権限が必要です。

1. CMC ウェブインタフェースに**ログイン**します。
2. システムツリーで シャーシ を選択します。
3. 電力の管理 タブをクリックします。電力バジェットステータス ページが表示されます。

表8-12 から 表8-15 では、**電力バジェットステータス** ページに表示される情報について説明します。

この情報の設定を行うには、「電力バジェットと冗長性の設定」を参照してください。

RACADM の使用

CMC に対応するシリアル/Telnet/SSH テキスト コンソールを開いて、ログイン後、以下を入力します。

```
racadm getpbinfo
```

出力詳細を含む、getpbinfo の詳細については、『Chassis Management Controller 管理者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。

表 8-12 システム電源のポリシー設定

項目	説明
システム入力電力の上限値	システム全体(シャーシ、CMC、サーバー、I/O モジュール、電源装置、iKVM、ファン)のユーザー定義による電力消費上限値を示します。CMC は、サーバーへの電力割り当てを低減することで、または優先度の低いサーバーモジュールの電源を落とすことで、この上限値を守ります。システム入力電力の上限値は、ワット、BTU/時およびパーセント単位で表示されます。

	シャーシの電力消費量が システム入力電力上限値 を超える場合、総電力消費量が上限値を下回るまで、優先度の低いサーバーのパフォーマンスが低減されます。 サーバーが同じ優先度に設定されている場合は、サーバーのスロット番号の順序に基づいて、電力低減または電源オフされるサーバーが選択されます。たとえば、スロット 1 のサーバーは最初に選択され、スロット 16 のサーバーは最後に選択されます。
冗長性ポリシー	現在の冗長性の設定:AC 冗長性、電源装置冗長性、冗長性なし を示します。 **AC 冗長性** — 入力電力はすべての PSU 間で負荷分散されます。このうち半分は 1 つの AC グリッドに配線され、残り半分は別のグリッドに配線されます。システムが AC 冗長性 モードで最適運用されているとき、電源はアクティブな電源装置すべての間で負荷分散されています。AC グリッドに障害が発生した場合は、機能している AC グリッドに接続されている PSU が 100% の容量で引き継ぎます。 **電源装置冗長性** — どの PSU が故障してもサーバーモジュールやシャーシの電源障害が引き起こされないように、シャーシ内で最大定格の PSU 容量がスペアとして保たれます。 **電源装置冗長性**は 6 台すべての PSU を使用せず、最大 4 台の PSU を使用します。その他の PSU は、DPSE が有効な場合は、スタンバイモードになります。 **冗長性なし:** 1 つの AC 回路(グリッド)上にある全部で 3 台の PSU からの電力が、シャーシ、サーバー、I/O モジュール、iKVM、CMC を含むシャーシ全体の電源投入に使用されます。 △ **注意: 冗長性なし モードは一度に 3 台だけ PSU を使用し、バックアップはありません。使用している 3 台のうち 1 台に障害が発生すると、サーバーモジュールの電源とデータが消失する可能性があります。**
電源装置の動的制御	**電源装置の動的制御** が有効か無効かを示します。この機能を有効にすると、冗長性ポリシーとシステムの電源要件に基づいて、CMC はあまり使用されていない CMC をスタンバイモードにします。使用量の少ない PSU をスタンバイモードにすることで、オンライン PSU の使用率と効率を上げることができ、節電につながります。

表 8-13 電力バジェット

項目	説明
システム入力最大電力容量	利用可能な電源装置がシステムに供給できる最大入力電力(ワット)。
予備の入力冗長電力	AC グリッドや PSU が故障した場合に利用できる予備の冗長電力量(ワット)を示します。 シャーシが AC 冗長性 モードで作動するように設定されている場合、予備の 入力冗長電力 は AC グリッドが故障した場合に利用できる予備の電力量となります。 シャーシが 電源装置冗長性 モードで作動するように設定されている場合、予備の入力冗長電力 は特定の PSU が故障した場合に利用できる予備の電力量となります。
サーバーに割り当てられた入力電力	設定に基づいて CMC がサーバーに割り当てる累積入力電力(ワット)を表示します。
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	CMC がシャーシインフラストラクチャ(ファン、IO モジュール、iKVM、CMC、スタンバイ CMC およびサーバー上の iDRAC)に割り当てる累積入力電力(ワット)を表示します。
割り当て可能な総入力電力	シャーシの動作に使用できる総電力バジェット(ワット)を示します。
スタンバイ入力電力容量	電源装置が故障、またはシステムから電源装置が取り外された場合に、利用できるスタンバイ入力電力(ワット)を表示します。システムに 4 台以上の電源装置が搭載され、PSU 動的制御が有効になっている場合に、このフィールドに測定値が表示されます。 **メモ:** スタンバイ入力電力容量の値に寄与しないスタンバイモードの PSU もあります。この場合、この PSU は、割り当て可能な総入力電力 の値に寄与しています。

表 8-14 サーバーモジュール

項目	説明
スロット	サーバーモジュールの場所を表示します。**スロット** は、サーバー モジュールをシャーシ内の場所で識別する連番(1 ～ 16)です。
Name	サーバー名を表示します。サーバー名はユーザーによって再定義できます。
タイプ	サーバーのタイプが表示されます。
優先度	シャーシの電力バジェットの目的で、サーバースロットに割り当てられた優先順位を示します。CMC は、電力制限値に基づいて電力を低減させたり再割り当てする必要がある場合や電源装置や電源グリッドが故障した場合の再計算にこの値を使用します。 **優先順位:** 1(最高)から 9(最低) デフォルト:**1** **メモ:** サーバースロットの優先順位は、スロットに差し込まれたサーバーではなくサーバースロットに関連付けられています。サーバーをシャーシ内の別のスロット、または別のシャーシに移動すると、そのサーバーの優先順位はそれが新しく差し込まれたスロットに割り当てられている優先順位になります。
電源状態	サーバーの電源状態を表示します。 - 該当なし: CMC はサーバーの電源状態を特定できていません。 - オフ: サーバーまたはシャーシの電源がオフです。 - オン: シャーシおよびサーバーともに電源がオンです。 - 電源投入中: 電源オフおよび電源オンの間の一時的な状態です。電源サイクルが完了すると、電源状態は オン になります。 - 電源切断中: 電源オンおよび電源オフの間の一時的な状態です。電源サイクルが完了すると、電源状態は オフ になります。

バジェット割り当て - 実測値	サーバーモジュールへの電力バジェットの割り当てを示します。 • 実測値:各サーバーに割り当てられている電力バジェット

表 8-15 システム電源装置

項目	説明
Name	PSU の名前が PS-n の形式で表示されます。ここで、n は電源装置番号です。
電源状態	PSU の 電源状態:**初期化中、オンライン、スタンバイ、診断中、故障、不明、または**不在(欠如)**を示します**。
入力電圧	電源装置の現在の入力電圧(ボルト)を表示します。
入力電流	電源装置の現在の入力電流を表示します。
定格出力	電源装置の最大定格出力を表示します。

電力バジェットと冗長性の設定

CMC の電力管理サービスはシャーシ全体(シャーシ、サーバー、IOM、iKVM、CMC、PSU)の電力消費量を最適化し、電力需要に基づいて別のモジュールに電力を再割り当てします。

ウェブインタフェースの使用

メモ: 電力の管理を行うには、**シャーシ制御システム管理者** の権限が必要です。

1. **CMC ウェブインタフェースにログインします。**
2. システムツリーで シャーシ を選択します。
3. 電力管理 タブ→ 設定 サブタブをクリックします。バジェット / 冗長性の設定ページ が表示示されます。
4. 必要に応じて、「表8-16」に記載されるプロパティの一部またはすべてを設定します。
5. 適用 をクリックして変更を保存します。

バジェット / 冗長性の設定 ページの内容を更新するには、更新 をクリックします。内容を印刷するには、印刷 をクリックします。

表 8-16 設定可能な電力バジェット / 冗長性のプロパティ

項目	説明
システム入力電力の上限値	システム入力電力の上限値は、システムがサーバーおよびシャーシインフラストラクチャに割り当てることができる最大 AC 電力です。ユーザーは、電源がオンになったサーバーおよびシャーシインフラストラクチャの最小必要電力を超える値に設定することができます。この値より低い上限値に設定することはできません。 サーバーおよびシャーシインフラストラクチャに割り当てた電力は、シャーシ -> 電力管理 -> 電力バジェット ステータスページ配下の 電力バジェット セクションにあるユーザーインタフェース、または CLI RACADM ユーティリティコマンド (`racadm getpbinfo`) を介して確認することができます。 現在の電源割り当てを低減するために 1 台以上のサーバーの電源をオフにし、システム入力電力容量 を低い値に再設定する、またはサーバーに電源を投入する前に容量限界を設定することができます。 この設定を変更する際は、どの単位の値も入力することができます。インタフェースは、最後に設定した単位フィールドの値が利用されます。 **メモ:** 容量計画については、www.dell.com/calc の Datacenter Capacity Planner(DCCP)ツールを参照してください。 **メモ:** 値の変更がワット単位で指定された場合は、実際に適用される値と同じになります。しかし、BTU/時 またはパーセント単位で指定した変更は、実際に適用される値と異なる場合があります。これは、これらの値をワット数に変換してたから適用し、丸め誤差が発生するためです。
冗長性ポリシー	以下のオプションから選択できます。 • 冗長性なし:1 つの AC 回路(グリッド)上にある全部で 3 台の PSU からの電力が、シャーシ、サーバー、I/O モジュール、iKVM、CMC を含むシャーシ全体の電源投入に使用されます。 **メモ:** 冗長性なし モードでは一度に 3 台までの PSU しか使用されません。PSU が 3 台しか取り付けられていない場合は、バックアップは使用できません。3 台のうち 1 台の電源

	装置が故障すると、サーバーの電源が落ち、データを損失する恐れがあります。3 台を超える数の PSU がある場合は、追加の PSU をスタンバイモードで配置すると、DPSE が有効な場合に電力効率を上げることができます。 • 電源装置冗長性: どの電源装置 が故障してもサーバーモジュールやシャーシの電源が切れないように、シャーシ内で最大定格の電源装置がスペアとして保持されます(ホットスペア)。 電源装置冗長性 モードは、6 台すべての電源装置を利用せず、最大 4 台、最小 2 台の電源装置を利用します。追加の電源装置が存在する場合は、スタンバイモードにすると、DPSE が有効な場合に電力効率を上げることができます。電源装置冗長性 モードは、シャーシの電力消費量が定格電力を超える場合、サーバーモジュールに電源投入されないようにします。このモードで 2 台の電源装置が故障すると、シャーシ内の一部またはすべてのサーバーモジュールの電源が切れてしまう可能性があります。サーバーモジュールの性能はこのモードでは低下しません。 • AC 冗長性: このモードでは、6 台の PSU が 2 つの電力グリッドに分けられます(PSU 1-3 を電力グリッド 1 に、PSU 4-6 を電力グリッド 2 に接続)。この設定では、6 台すべての PSU がオンラインになります。PSU が故障したり、AC 電力を失ったりした場合は、冗長性ステータスは喪失状態になります。
電源装置の動的制御の有効化	電力の動的管理が有効になります。動的制御 モードでは、消費電力に基づいて電源装置の電源をオン(オンライン)またはオフ(スタンバイ)にし、シャーシ全体の電力消費量を最適化します。 たとえば、電力バジェットが 5000 ワットで、冗長ポリシーが AC 冗長性モードに設定され、6 台の電源装置があると仮定します。CMC は、4 台の電源装置が AC 冗長性を保ち、残りの 2 台をスタンバイモードにすることを判断します。新しくインストールしたサーバーにさらに 2000W の電力が必要な場合や、既存のシステム設定の電力効率を向上させる必要がある場合は、2 台のスタンバイ状態の電源装置が追加されます。
シャーシ電源ボタンを無効にする	(選択した場合、)シャーシ電源ボタンを無効にします。チェックボックスがオンになっているときに、シャーシの電源ボタンを押してシャーシの電源状態を変更しようとすると、このアクションは無視されます。

RACADM の使用

冗長性を有効にして冗長性ポリシーを設定するには:

メモ: 電力の管理を行うには、**シャーシ制御システム管理者**の権限が必要です。

1. CMC に対応するシリアル/Telnet/SSH テキスト コンソールを開いて、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、次のように入力します。

     ```
     racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy <値>
     ```

     ここで、<値> は 0(冗長性なし)、1(AC 冗長性)、2(電源装置冗長性)です。デフォルトは 0 です。

     例えば、次のコマンドでは

     ```
     racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy 1
     ```

     は、冗長性ポリシーを 1 に設定します。
   - PSU の動的制御を有効または無効にするには、次のように入力します。

     ```
     racadm config -g cfgChassisPower -o cfgChassisDynamicPSUEngagementEnable <値>
     ```

     ここで、<値> には 0(無効)または 1(有効)を指定できます。デフォルトは 1 です。

     例えば、次のコマンドでは

     ```
     racadm config -g cfgChassisPower -o cfgChassisDynamicPSUEngagementEnable 0
     ```

     は、PSU の動的制御を無効にします。

シャーシ電源の RACADM コマンドの詳細については、『CMC 管理者リファレンス ガイド』config、getconfig、getpbinfo、cfgChassisPower の項を参してください。

サーバーに優先度を割り当てる方法

サーバーの優先度により、必要とされる電力が増えたときに CMC がどのサーバーから電力を受けるかが決まります。

メモ: サーバーに割り当てる優先度は、サーバー自体ではなく、そ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した場合、新しいスロットの場所の優先度を再設定する必要があります。

メモ: 電力の管理を行うには、**シャーシ設定システム管理者**の権限が必要です。

ウェブインタフェースの使用

1. CMC ウェブインタフェースにログインします。
2. サーバー を選択します。サーバーステータス ページが表示されます。
3. 電源管理タブをクリックします。サーバーの優先度 ページが表示され、シャーシ内のすべてのサーバーが一覧表示されます。
4. 1 台、複数台、またはすべてのサーバーに対する優先度(1 ～ 9、1 が最高の優先度)を選択します。デフォルト値は 1 です。複数のサーバーに同一の優先度を割り当てることも可能です。
5. 適用 をクリックして変更を保存します。

RACADM の使用

CMC に対応するシリアル/Telnet/SSH テキスト コンソールを開いて、ログイン後、以下を入力します。

```
racadm config -g cfgServerInfo -o cfgServerPriority - i <スロット番号> <優先順位>
```

ここで、<スロット番号>(1～16)はサーバーの位置を表し、<優先順位> は 1～9 の数値です。

例えば、次のコマンドでは

```
racadm config -g cfgServerInfo -o cfgServer Priority - i 5 1
```

スロット 5 に装着されたサーバーに 1 の優先順位を設定します。

電力バジェットの設定

メモ: 電力の管理を行うには、**シャーシ制御システム管理者**の権限が必要です。

ウェブインタフェースの使用

1. CMC ウェブインタフェースにログインします。
2. システムツリーで シャーシ をクリックします。コンポーネントの正常性 ページが表示されます。
3. 電源管理 タブをクリックします。電力バジェットステータス ページが表示されます。
4. 設定 サブタブをクリックします。バジェット / 冗長性の設定 ページが表示されます。
5. 7928 ワットまでのバジェット値を システム入力電力の上限値 テキストフィールドに入力します。

メモ: 電力バジェットは、全部で 6 台の PSU のうち、最大 3 台までに制限されています。お使いのシャーシの電力限界を超える AC 電力バジェット値を設定しようとすると、エラーメッセージが表示されます。

メモ: 値の変更がワット単位で指定された場合は、実際に適用される値と同じになります。しかし、BTU/時 またはパーセント単位で指定した変更は、実際に適用される値と異なる場合があります。これは、これらの値をワット数に変換してたから適用し、丸め誤差が発生するためです。

6. 適用 をクリックして変更を保存します。

RACADM の使用

CMC に対応するシリアル/Telnet/SSH テキスト コンソールを開いて、ログイン後、以下を入力します。

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

ここで、<値> は 2715～7928 の範囲の数値で、電源の上限値をワット数で表します。デフォルトは 7928 です。

例えば、次のコマンド

```
racadm config -g cfgChassisPower -o cfgChassisPowerCap 5400
```

は、最大電力バジェットを 5400 ワットに設定します。

メモ: 電力バジェットは、全部で 6 台の PSU のうち、最大 3 台までに制限されています。お使いのシャーシの電力容量を超える AC 電力バジェット値を設定しようとすると、エラーメッセージが表示されます。

電源バジェットを維持するためのサーバー電力の低減

システムの消費電力量をユーザー設定の**システムの入力電力の上限値**の範囲内に保つために、さらに電力が必要な場合は、優先順位の低いサーバーへの電力割り当てが低減されます。たとえば、新しいサーバーが追加された場合§CMC は優先順位が低いサーバーへの電力を低減し、新しいサーバーに供給する電力を増やすことができます。優先順位の低いサーバーへの電力割り当てを低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が実行できるだけの十分な電力が確保されるまで、サーバーの性能を低減します。

CMC は次の 2 つの場合にサーバーの電力割り当てを低減します。

- 合計消費電力量が設定可能な**システムの入力電力の上限値**を超える場合（「電力バジェットの設定」を参照）
- 非冗長構成で電力故障が発生した場合

サーバーへの優先レベルの割り当ての詳細については、「シャーシに対する電力制御操作の実行」を参照してください。

シャーシに対する電力制御操作の実行

メモ: 電力の管理を行うには、**シャーシ制御システム管理者**の権限が必要です。

メモ: 電源制御操作はシャーシ全体に影響します。IOM 上での電力制御操作については、「IOM 上で電源制御操作の実行」を参照してください。サーバー上での電力制御操作については、「サーバーに対する電力制御操作の実行」を参照してください。

CMC は、ユーザーが順を追ったシャットダウンなどシャーシ全体（シャーシ、サーバー、IOM、iKVM、PSU）におけるいくつかの電源管理操作をリモート実行できるようにします。

ウェブインタフェースの使用

1. CMC ウェブインタフェースにログインします。
2. システムツリーで シャーシ を選択します。
3. 電源管理 タブをクリックします。電力バジェットステータス ページが表示されます。
4. 制御 サブタブをクリックします。電力管理 ページが表示されます。
5. 以下の **電源制御操作** のいずれかのラジオボタンをクリックして選択します。
   - **システムの電源を入れる** — シャーシの電源を入れます（シャーシの電源がオフのときに電源ボタンを押す操作と同じ）。シャーシの電源がすでにオンの場合は、このオプションが無

効になっています。

メモ: この操作は、シャーシおよびその他のサブシステム（サーバー上の iDRAC、IOM および iKVM）の電源をオンにします。サーバーの電源はオンになりません。

- **システムの電源を切る** — シャーシの電源を切ります。シャーシの電源がすでにオフの場合は、このオプションが無効になっています。

メモ: この操作は、シャーシ（シャーシ、サーバー、IOM、iKVM および電源装置）の電源をオフにします。CMC は電源オンのままですが、仮想スタンバイ状態になります。電源装置およびファンがこの状態にある CMC を冷却します。また、電源装置は、低速で動作するファンに対しても電力を供給します。

- システムの電源を入れなおす（コールドブート）— サーバーの電源を切ってから再起動します。シャーシの電源がすでにオフの場合は、このオプションが無効になっています。

メモ: この操作は、シャーシ全体（シャーシ、常に電源オンに設定されているサーバー、IOM、iKVM および電源装置）の電源をオフにし、再起動します。

- **CMC のリセット**— 電源を切ることなく CMC をリセットします（ウォームリブート）（CMC の電源がすでに オフ の場合は、このオプションは無効になっています）。

メモ: この操作では CMC のみがリセットされます。その他のコンポーネントは影響されません。

- **強制シャットダウン** — この操作は、シャーシ全体（シャーシ、サーバー、IOM、iKVM および電源装置）を強制的に電源オフにします。この場合、電源をオフにする前に、サーバーのオペレーティングシステムを正常に終了させることはしません。

- **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。
- OK をクリックして、電力管理の操作（システムのリセットなど）を行います。

RACADM の使用

CMC に対応するシリアル/Telnet/SSH テキスト コンソールを開いて、ログイン後、以下を入力します。

```
racadm chassisaction -m chassis <操作>
```

ここで、<操作> は、powerup（電源投入）、 powerdown（電源切断）、powercycle（パワーサイクル）、nongraceshutdown（強制シャットダウン）またはreset（リセット）を指します。

IOM 上で電源制御操作の実行

各 IOM でリセットやパワーサイクルをリモート実行できます。

メモ: 電力の管理を行うには、**シャーシ制御システム管理者**の権限が必要です。

ウェブインタフェースの使用

1. **CMC ウェブインタフェースにログインします。**
2. I/O モジュール を選択します。I/O モジュールのステータス ページが表示されます。
3. 電源管理 タブをクリックします。電力制御 ページが表示されます。
4. リストで IOM の隣にあるドロップダウンメニュから実行する操作（リセット または パワーサイクル）を選択します。
5. **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。
6. 電力の管理操作を実行するには、OK をクリックします（たとえば、 IOM をパワーサイクルする場合）。

RACADM の使用

CMC に対応するシリアル/Telnet/SSH テキスト コンソールを開いて、ログイン後、以下を入力します。

```
racadm chassisaction -m switch-<n> <操作>
```

ここで <n> は、1 ～ 6 の数値で IOM(A1, A2, B1, B2, C1, C2)を指定し、<操作>は、powercycle(パワーサイクル)または reset(リセット)のどちらかの実行したい操作を示します。

サーバーに対する電力制御操作の実行

メモ: 電力の管理を行うには、**シャーシ制御システム管理者**の権限が必要です。

CMC は、ユーザーがシャーシ上の個別のサーバー上で順を追ったシャットダウンなどの電源管理操作をリモート実行できるようにします。

ウェブインタフェースの使用

1. **CMC ウェブインタフェースにログインします。**
2. システムツリー内の サーバー を展開し、電力制御操作の対象とするサーバーを選択します。サーバーステータス ページが表示されます。
3. 電源管理 タブをクリックします。サーバーの電力管理 ページが表示されます。
4. 電源ステータス は、以下で示すサーバーの電源ステータスを表示します。
   - N/A: CMC はサーバーの電源状態を特定できていません。
   - オフ - サーバーまたはシャーシのどちらかの電源がオフです。
   - オン - シャーシおよびサーバーともに電源がオンです。
   - 電源投入中 - 電源オフおよび電源オンの間の一時的な状態です。操作が完了すると、電源状態 は オン になります。
   - 電源切断中 - 電源オンおよび電源オフの間の一時的な状態です。操作が完了すると、電源状態 は オフ になります。
5. 以下の **電源制御操作** のいずれかのラジオボタンをクリックして選択します。
   - **サーバーの電源を入れる** — サーバーの電源を入れます(サーバーの電源がオフのときに電源ボタンを押す操作と同じ)。サーバーの電源がすでにオンの場合は、このオプションが無効になっています。
   - **サーバーの電源を切る** — サーバーの電源を切ります(サーバーの電源がオンのときに電源ボタンを押す操作と同じ)。
   - 正常なシャットダウン — サーバーの電源を切ってから再起動します。
   - **サーバーをリセットする(ウォームブート)** — サーバーの電源を切らないで再起動します。サーバーの電源が オフ の場合は、このオプションは無効になっています。
   - **サーバーの電源を入れなおす(コールドブート)** — サーバーの電源を切ってから再起動します。サーバーの電源が オフ の場合は、このオプションは無効になっています。
6. **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。
7. OK をクリックして、電源管理の操作(サーバーのリセットなど)を行います。

メモ: すべての電源管理の操作は、サーバー → 電源管理 → 管理 ページで複数のサーバーに対して行えます。

RACADM の使用

CMC に対応するシリアル/Telnet/SSH テキスト コンソールを開いて、ログイン後、以下を入力します。

```
racadm serveraction -m <モジュール> <アクション>
```

ここで、<モジュール> はシャーシ内のスロット番号 1～16 でサーバーを指定し、<操作> は実行する操作(電源投入、電源切断、パワーサイクル、 正常シャットダウン、ハードリセット を指定します。

トラブルシューティング

電源供給および電力に関連する問題のトラブルシューティングは、「トラブルシューティングとリカバリ」を参照してください。

目次ページに戻る

目次ページに戻る

RACADM コマンドラインインタフェースの使用

Dell™ Chassis Management Controllerファームウェアバージョン 2.10 ユーザーガイド

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

RACADM インタフェースは、使用する **racadm** 実行プログラムの保存場所によって「ローカル」と「リモート」に分類されます。

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。

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

リモート RACADM コマンドをスクリプトで使用して、複数 CMC を設定することができます。CMC はスクリプトに対応していないため、スクリプトを直接 CMC で実行することはできません。複数の CMC を設定する方法については、「複数シャーシ内の複数 CMC の設定」を参照してください。

シリアル、Telnet、SSH コンソールの使用

シリアルまたは Telnet/SSH 接続、あるいは iKVM 上の Dell CMC コンソールを使って CMC にログインできます。CMC をシリアルまたはリモートアクセス用に設定する場合は、「CMC にコマンドラインコンソールの使用を設定する方法」を参照してください。一般的に使用されるサブコマンドオプションは、表4-2 に一覧表示されています。全 RACADM サブコマンドの一覧表は、『Dell Chassis Management Controller 管理者リファレンス ガイド』の RACADM サブコマンドの章を参照してください。

CMC へのログイン

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

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

これで、CMC にログインできます。

テキストコンソールの起動

ネットワーク、シリアルポート、または iKVM を通して Dell CMC コンソールから Telnet または SSH を使用して CMC にログインできます。Telnet または SSH セッションを開いて、CMC に接続し、ログインします。

iKVM を介した CMC への接続方法については、「iKVM モジュールの使用」を参照してください。

RACADM の使用

RACADM サブコマンドは、シリアル、Telnet、SSH コンソールのコマンド プロンプト、または通常のコマンドプロンプトから、リモート実行できます。

RACADM サブコマンドを使って、CMC プロパティを設定し、リモート管理タスクを実行します。RACADM サブコマンドのリストを表示するには、次のように入力します。

```
racadm help
```

オプションやサブコマンドなしで実行する場合、RACADM は構文情報、およびサブコマンドとヘルプへのアクセス方法を表示します。個々のサブコマンドの構文とコマンドラインオプションを表示するには、次のように入力します。

```
racadm help <サブコマンド>
```

RACADM サブコマンド

表4-1 に、RACADM の一般的なサブコマンドを簡単に示します。シンタックスまたは有効な入力値などを含む RACADM サブコマンドの一覧表は、『Dell Chassis Management Controller 管理者リファレンス ガイド』の RACADM サブコマンドの章を参照してください。

メモ: connect コマンドは RACADM コマンドとビルトイン CMC コマンドの両方で使用できます。connect、exit、quit、および logout コマンドは CMC のビルトインコマンドで、RACADM コマンドではありません。これらのコマンドはリモート RACADM で使用することはできません。これらコマンドの使用に関する詳細は、「接続コマンドでサーバーまたは I/O モジュールに接続する」を参照してください。

RACADM サブコマンドを入力するときは、コマンドに racadm を前付けしてください。例:

```
racadm help
```

表 4-1 RACADM サブコマンド

コマンド	説明
help	CMC サブコマンドの説明を一覧表示します。
help <サブコマンド>	指定したサブコマンドの使用方法の概要を一覧表示します。
?	CMC サブコマンドの説明を一覧表示します。
?<サブコマンド>	指定したサブコマンドの使用方法の概要を一覧表示します。
arp	ARP テーブルの内容を表示します。ARP エントリの追加や削除はできません。
chassisaction	シャーシ、スイッチ、KVM の電源投入、電源切断、リセット、パワーサイクルを実行します。
clrraclog	CMC ログをクリアして、ログをクリアしたユーザーと時刻を示すエントリを 1 つ作成します。
clrsel	システムイベントログのエントリをクリアします。
cmcchangeover	冗長 CMC 環境で CMC のステータスをアクティブとスタンバイの間で切り替えます。
config	CMC の設定を行います。
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。connect サブコマンドの使用に関するヘルプは、「接続コマンドでサーバーまたは I/O モジュールに接続する」を参照してください。
deploy	必要なプロパティを指定することでサーバーを導入します。
feature	アクティブな機能および無効になっている機能を表示します。
機能カード	機能カードのステータス情報を表示します。
fwupdate	システムコンポーネントのファームウェアアップデートを実施し、ファームウェアのアップデートステータスを表示します。
getassettag	シャーシの管理タグを表示します。
getchassisname	シャーシの名前を表示します。
getconfig	現在の CMC 設定のプロパティを表示します。
getdcinfo	一般的な I/O モジュールとドーターカードの誤設定情報を表示します。.
getflexaddr	スロット/ファブリックごとに、FlexAddress の有効/無効化ステータスを表示します。-i オプションと共に使用した場合、このコマンドは特定スロットの WWN および

	MAC アドレスを表示します。
getioinfo	一般 I/O モジュール情報を表示します。.
getkvminfo	iKVM についての情報を表示します。
getled	モジュールの LED 設定を表示します。
getmacaddress	サーバーの MAC アドレスを表示します。
getmodinfo	モジュールの構成とステータス情報を表示します。.
getniccfg	コントローラの現在の IP 設定を表示します。
getpbinfo	電力バジェット状態の情報を表示します。
getpminfo	電力バジェット状態の情報を表示します。
getraclog	CMC ログを表示します。
getractime	CMC 時間を表示します。
getredundancymode	CMC の冗長性モードを表示します。
getsel	システムイベントログ(ハードウェアログ)を表示します。
getsensorinfo	システムセンサーについての情報を表示します。
getslotname	シャーシ内のスロットの名前を表示します。
getssninfo	アクティブセッションに関する情報を表示します。
getsvctag	サービスタグを表示します。
getsysinfo	CMC とシステムの一般情報を表示します。
gettracelog	CMCtrace ログを表示します。-i と共に使用すると、CMC トレースログ内のエントリ数を表示します。
getversion	現在使用するソフトウェアのバージョン、型式情報、更新可能なデバイスかどうかなどの情報を表示します。
ifconfig	現在の CMCの IP 設定を表示します。
netstat	ルーティングテーブルと現在の接続を表示します。
ping	送信先の IPv4 アドレスが現在のルーティングテーブルの内容で CMC から到達可能かどうかを確認します。
ping6	送信先の IPv6 アドレスが現在のルーティングテーブルの内容で CMC から到達可能かどうかを確認します。
racdump	包括的なシャーシステータスおよび構成状況の情報と共に、イベントログの履歴を表示します。導入後の構成検証およびデバッグ時に使用します。
racreset	CMC をリセットします。
racresetcfg	CMC をデフォルト設定にリセットします。
remoteimage	リモートサーバー上のメディアファイルを接続、切断、または導入します。
serveraction	管理下システムの電源管理を行います。
setassettag	シャーシの管理タグを設定します。
setchassisname	シャーシの名前を設定します。
setflexaddr	シャーシ上で FlexAddress が有効になった際に、特定のスロット/ファブリック上で FlexAddress を有効/無効にします。
setled	モジュールの LED 設定を設定します。
setniccfg	コントローラの IP 設定を指定します。
setractime	CMC 時間を設定します。
setslotname	シャーシ内のスロットの名前を設定します。
setsysinfo	シャーシの名前と場所を設定します。
sshpkauth	最大 6 つの異なる SSH 公開キーのアップロード、既存のキーの削除、CMC 内に既に存在するキーの表示が可能です。
sslcertdownload	認証局が署名した証明書をダウンロードします。
sslcertupload	認証局が署名した証明書またはサーバー証明書を CMC にアップロードします。
sslcertview	認証局が署名した証明書またはサーバー証明書を CMC で表示します。
sslcsrgen	SSL CSR を生成してダウンロードします。
sslresetcfg	CMC ウェブ GUI で使用される自己署名の証明書を再生成します。
testemail	CMC NIC で CMC に電子メールを送信させます。
testfeature	指定の機能の設定パラメータを確認できます。たとえば、簡易認証(ユーザー名とパスワード)または認証(シングルサインオンまたは Smart Card ログイン)によって Active Directory の設定をテストすることができます。
testtrap	CMC に CMC NIC 経由でSNMPを送信させます。
traceroute	IPv4 パケットがコマンドネットワークノードに到達するまでの経路を印刷します。
traceroute6	IPv6 パケットがコマンドネットワークノードに到達するまでの経路を印刷します。

RACADM へのリモートアクセス

表4-2に、リモート RACADM サブコマンドのオプションを掲載しています。

表 4-2 リモート RACADM サブコマンドオプション

オプション	説明
-r <racIpAddr> -r <racIpAddr>:<ポート>	コントローラのリモート IP アドレスを指定します。 CMC のポート番号がデフォルトのポート(443)と異なる場合は、<ポート番号> を使用します。
-i	インタラクティブにユーザーのユーザー名とパスワードを問い合わせるように RACADM に指示します。
-u <ユーザー名>	コマンドのトランザクションの認証に使用するユーザー名を指定します。-u オプションを使用すると、-p オプションも必要になり、-i オプション(インタラクティブ)は使用できなくなります。
-p <パスワード>	コマンドのトランザクションを認証するパスワードを指定します。-p オプションを使用すると、-i オプションは使用できなくなります。

RACADM にリモートアクセスするには、以下のコマンドを入力します。

```
racadm -r <CMC IP アドレス> -u <ユーザー名> -p <パスワード> <サブコマンド> <サブコマンドオプション>
```

```
racadm -i -r <CMC IP アドレス> <サブコマンド> <サブコマンドオプション>
```

メモ: -i オプションは、RACADM にユーザー名とパスワードの入力をインタラクティブにプロンプトするよう指示します。**-i** オプションを指定しない場合は、-u と -p オプションを使ってコマンド内でユーザー名とパスワードを指定する必要があります。

例:

```
racadm -r 192.168.0.120 -u root -p calvin getsysinfo
```

```
racadm -i -r 192.168.0.120 getsysinfo
```

CMC の HTTPS ポート番号をデフォルトポート(443)からカスタムポートに変更した場合は、次の構文を使用する必要があります。

```
racadm -r <CMC IP アドレス>:<ポート> -u <ユーザー名> -p <パスワード> <サブコマンド> <サブコマンドオプション>
```

```
racadm -i -r <CMC IP アドレス>:<ポート> <サブコマンド> <サブコマンドオプション>
```

racadm リモート機能の有効 / 無効化

メモ: デルでは、これらのコマンドをシャーシで実行することを推奨しています。

CMC 上での RACADM リモート機能はデフォルトで有効になっています。以下のコマンドでは、-g はオブジェクトが属する設定グループを指定し、-o は設定する設定オブジェクトを指定します。

RACADM リモート機能を無効にするには、次を入力します。

```
racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 0
```

RACADM リモート機能を再び有効にするには、次を入力します。

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

RACADM のリモート使用

メモ: RACADM のリモート機能を使用する前に、CMC の IP アドレスを設定してください。CMC の設定の詳細については、「CMC のインストールと設定」を参照してください。

RACADM コンソールのリモートオプション (-r) を使うと、管理下システムに接続してリモートコンソールまたは管理ステーションから RACADM サブコマンドを実行できます。リモート機能を使用するには、有効なユーザー名 (-u オプション)、パスワード (-p オプション)、および CMC IP アドレスが必要です。

RACADM へのリモートアクセスを試みる前に、それにアクセスする権限があることを確認してください。ユーザー権限を表示するには、次を入力します。

```
racadm getconfig -g cfguseradmin -i n
```

ここで、n はユーザー ID (1〜16) です。

ユーザー ID がわからない場合は、異なる n 値を試してください。

メモ: RACADM リモート機能は、対応ブラウザを通して管理ステーション上でのみ使用できます。詳細については、デルサポートサイト **support.dell.com / manuals** の『Dell システムソフトウェアサポートマトリックス』の対応ブラウザの項を参照してください。

メモ: RACADM リモート機能を使用する場合には、次に示すようなファイル操作で RACADM サブコマンドを使っているフォルダへの書き込み権限が必要になります。例:

```
racadm getconfig -f <ファイル名> -r <IP アドレス>
```

または

```
racadm sslcertupload -t 1 -f c:\cert\cert.txt
```

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は、設定グループは設定ファイルの一環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対して適用されます。

以下は、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

RACADM エラーメッセージ

RACADM CLI エラーメッセージの詳細については、「トラブルシューティング」を参照してください。

RACADM を使用した CMC の設定

メモ: 初めて CMC を設定する場合、リモートシステムで RACADM コマンドを実行するには、**root** ユーザーとしてログインします。別のユーザーを作成して、CMC の設定許可を与えることもできます。

CMC を最も迅速に設定する方法は、CMC ウェブインタフェースを利用することです(「CMC ウェブインタフェースの使用」を参照)。ただし、CLI またはスクリプト設定を使用したり、複数の CMC の設定をする場合は、管理下システムに CMC と一緒にインストールされる RACADM を使用してください。

CMC IPv4 ネットワークプロパティの設定

CMC への初期アクセスの設定

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。

ここでは、RACADM コマンドを使って CMC ネットワークの初期設定を行う手順を説明します。ここで説明するすべての設定は、フロントパネル LCD を使って行うことができます。「LCD 設定ウィザードを使用したネットワーク設定を参照してください。

注意: CMC ネットワーク設定画面の設定を変更すると、現行のネットワーク接続が遮断されることがあります。

ネットワークのサブコマンドの詳細については、『Dell Chassis Management Controller 管理者リファレンス ガイド』の RACADM サブコマンドおよびプロパティデータベースグループとオブジェクト定義の章を参照してください。

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 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、互いから独立しています。

現在の IPv4 ネットワーク設定の表示

NIC、DHCP、ネットワーク速度、デュプレックス設定の概要を表示するには、次を入力します。

```
racadm getniccfg
```

または

```
racadm getconfig -g cfgCurrentLanNetworking
```

現在の IPv6 ネットワーク設定の表示

ネットワーク設定の概要を表示するには、次を入力します。

```
racadm getconfig -g cfgIpv6LanNetworking
```

シャーシタイプの IPv4 と IPv6 アドレス指定情報を表示するには、次を入力します。

```
racadm getsysinfo
```

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することもできます。

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>
```

現在のネットワーク設定の表示

NIC、DHCP、ネットワーク速度、デュプレックス設定の概要を表示するには、次を入力します。

```
racadm getniccfg
```

または

```
racadm getconfig -g cfgCurrentLanNetworking
```

シャーシの IP アドレスとDHCP、MAC アドレス、DNS 情報を表示するには、次を入力します。

```
racadm getsysinfo
```

ネットワーク LAN の設定

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

メモ: 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。

メモ: シャーシに 2 つの CMC(プライマリとスタンバイ)があり、両方ともネットワークに接続していると、プライマリ CMC が故障した場合にスタンバイ CMCが自動的にそのネットワーク設定を継承します。

CMC NIC の有効化

CMC IPv4 NIC を有効 / 無効にするには、次を入力します。

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

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

メモ: CMC IPv4 NIC はデフォルトで有効になっています。

CMC IPv6 アドレス指定を有効 / 無効にするには、次を入力します。

```
racadm config -g cfgIpv6LanNetworking -o cfgNicEnable 1
```

```
racadm config -g cfgIpv6LanNetworking -o cfgNicEnable 0
```

メモ: CMC IPv6 アドレス指定はデフォルトで無効になっています。

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

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

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

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

```
racadm config -g cfgLanNetworking -o cfgNicGateway <静的ゲートウェイ>
```

```
racadm config -g cfgLanNetworking -o cfgNicNetmask <静的サブネットマスク >
```

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

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

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6AutoConfig 0
```

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6Address <IPv6 アドレス>
```

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6PrefixLength 64
```

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

NIC アドレスの DCHP の有効 / 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。詳細については、「CMC への初期アクセスの設定」を参照してください。

DHCP を使用した DNS IP アドレスの取得機能の有効 / 無効化

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

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

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

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

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

DNS の静的 IP アドレスの設定

メモ: これらの設定は、DHCP を使用した DNS アドレスの取得機能が無効になっていない場合は、無効になります。

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（IPv4 専用）

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

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

  メモ: DNS サーバーによっては、31 文字以内の名前しか登録できません。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: 以下の設定は、cfgDNSRegisterRac を 1 に設定することで DNS サーバー上に CMC を登録した場合にのみ有効です。

- CMC 名 デフォルトでは、DNS サーバー上の CMC 名は cmc-<サービスタグ> です。DNS サーバー上の CMC の名前を変更するには、次を入力します。

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

ここで、<名前> は 63 文字以内の英数字とハイフンを使って指定します。例:cmc-1、d-345

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

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

ここで、<名前> は 254 文字以内の英数字とハイフンを使って指定します。例:p45、a-tz-1、r-id-001

オートネゴシエーション、デュプレックスモード、ネットワーク速度の設定

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

オートネゴシエーションを無効にして、デュプレックス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 <デュプレックス モード>
```

このコマンドで、

<デュプレックスモード> は 0(半二重)または 1(全二重 、デフォルト)です。

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

このコマンドで、

<速度> は 10 または 100(デフォルト)です。

最大転送単位(MTU)の設定

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(デフォルトは 1500)。

メモ: IPv6 では最低 1280 の MTU が必要です。IPv6 が有効であり、**cfgNetTuningMtu** が低い値に設定されている場合は、1280 の MTU を使用します。

SMTP サーバー IP アドレスの設定

CMC を有効にして、Simple Mail Transfer Protocol(SMTP)を使って指定した IP アドレスに電子メール警告を送信できます。この機能を有効にするには、次を入力します。

```
racadm config -g cfgRemoteHosts -o cfgRhostsFwUpdateIpAddr <SMTP IP アドレス>
```

ここで、<SMTP IP アドレス> はネットワーク上の SMTP サーバーの IP アドレスです。

メモ: ネットワークに、IP アドレスのリースを定期的に発行したり更新したりする SMTP サーバーがあり、アドレスが異なる場合は、指定した SMTP サーバー IP アドレスの変更によって、このプロパティ設定が機能しない期間があります。そのような場合は、DNS 名を使用してください。

ネットワークセキュリティの設定

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

IP 範囲チェックの有効化

IP フィルタは着信ログインの 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。

- cfgRacTuneIpRangeAddr
- cfgRacTuneIpRangeMask

着信 IP アドレスを使ってログインできるのは、以下の両方のアドレスが同一である場合に限られます。

a. **cfgRacTuneIpRangeMask**(ビットワイズ)および着信 IP アドレス

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

RACADM を使用したユーザーの設定

作業を開始する前に

CMC のプロパティデータベースには 16 のユーザーを設定できます。CMC ユーザーを手動で有効にする前に、現在のユーザーが存在するか確認します。新しい CMC を設定している場合や、RACADM の `racresetcfg` コマンドを実行した場合、現在のユーザーは、パスワードが `calvin` の `root` のみが存在します。`racresetcfg` サブコマンドは、CMC を元のデフォルトにリセットします。

注意: racresetcfg コマンドをすべての設定パラメータとして使用すると、元のデフォルトにリセットされるので注意してください。それまでに行った変更がすべて失われます。

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

ユーザーの存在を確認するには、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 -u <ユーザー名>
```

または

1 ～ 16 までの各索引に、次のコマンドを 1 回ずつ入力することもできます。

```
racadm getconfig -g cfgUserAdmin -i <索引>
```

複数のパラメータとオブジェクト ID が現在値と一緒に表示されます。対象オブジェクトは次の 2 つです。

```
# cfgUserAdminIndex=XX
```

```
cfgUserAdminUserName=
```

cfgUserAdminUserName オブジェクトに値がない場合は、cfgUserAdminIndex オブジェクトで示されるその索引番号は使用可能です。「=」(等号)の後に名前が表示される場合は、インデックスがそのユーザーによって使用されています。

メモ: RACADM config サブコマンドを使ってユーザーを手動で追加または削除する場合は、-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。前の例に表示された cfgUserAdminIndex オブジェクトに「#」文字があることに注意してください。また、グループ / オブジェクトを書き込むことを指定するために **racadm** config -f racadm.cfg コマンドを使用する場合は、インデックスは指定できません。最初に使用可能な索引に新しいユーザーが追加されます。この動作によって、プライマリ CMC と同じ設定を持つセカンダリ CMC を設定するときの柔軟性が得られます。

CMC ユーザーの追加

新しいユーザーを CMC 設定に追加する場合は、基本的なコマンドをいくつか使用できます。以下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、『Dell Chassis Management Controller 管理者リファレンス ガイド』のデータベースプロパティの章の表5-18、表5-19、および表 3-1 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 へのログイン権限を持つ「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一覧については、『Dell Chassis Management Controller ファームウェア管理者リファレンス ガイド』のデータベース プロパティの章の表 3-1 を参照してください。デフォルトの権限値は 0 で、これはユーザーの権限が有効になっていないことを示します。

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 john
```

```
racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456
```

```
racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminPrivilege 0x00000001
```

```
racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminEnable 1
```

正しい権限を持つユーザーが追加されたことを確認するには、次のいずれかのコマンドを使用します。

```
racadm getconfig -u john
```

または

```
racadm getconfig –g cfgUserAdmin –i 2
```

RACADM による SSH 経由の公開キー認証の設定

作業を開始する前に

SSH インタフェース経由のサービスユーザー名には、最大 6 つの公開キーを設定できます。公開キーを追加または削除する前に、表示コマンドを使って設定済みのキーを確認してください。これは、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です サービスユーザー名は、SSH 経由で CMC にアクセスする場合に使用できる特殊なユーザーアカウントです。SSH 経由の PKA を正しく設定して使用すれば、CMC へのログイン時にユーザ名またはパスワードを入力する必要がありません。これは、自動化されたスクリプトを設定してさまざまな機能を実行する場合に便利です。

この機能の設定準備をする際は、以下の点に気をつけてください。

- この機能を管理するための GUI サポートは用意されていません。使用できるのは RACADM のみです。
- 新しい公開キーを追加する場合は、追加時に既存のキーがインデックスにないことを確認します。CMC では、新しいキーを追加する前に、前のキーが削除されているかどうかの確認作業は行われません。新しいキーを追加すると、SSH インタフェースが有効な間、自動的に有効になります。
- 公開キーの公開キーコメントセクションを使用する場合は、最初の 16 文字のみが CMC によって使用されることに注意してください。すべての PKA ユーザーはサービスユーザー名を使用してログインします。そのため、RACADM `getssninfo` コマンドを使用する場合は、SSH ユーザーを識別できるように公開キーコメントが使用されます。

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

  ```
  racadm getssninfo

  種類 ユーザー IP アドレス ログイン日時

  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、『Dell Chassis Management Controller 管理者リファレンスガイド』を参照してください。

Windows 用の公開キーの生成

公開キーは、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で必要になります。公開 / 秘密キーペアを生成する方法は 2 通りあります。1 つは、Windows を実行しているクライアントの PuTTY キー生成アプリケーションを使用する方法で、もう 1 つは、Linux を実行しているクライアントの `ssh-keygen` を使用する方法です。

この項では、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。

Windows クライアント用の PuTTY キー生成を使用して基本キーを作成するには

1. アプリケーションを起動し、生成するキータイプとして 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 より小または 4096 より大のキーを追加すると CMC ではメッセージが表示されない場合がありますが、ログインしようとするとこれらのキーは失敗します。

3. **生成** をクリックし、指示に従ってマウスをウィンドウ内に移動します。

   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。プライベートキーを必ず保存します。

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および貼り付けます。

Windows 用の公開キーの生成

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

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

メモ: オプションは大文字と小文字を区別します。

ここで、

-t オプションでは dsa または rsa を指定できます。

–b オプションは 768～4096 のビット暗号化サイズを指定します。

–C オプションを使用すると、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。

パスフレーズはオプションです。

手順に従ってください。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。

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、すべてのキーを 1～6 の数字で置き換えます。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を使用して公開キーを CMC に追加するには、次を入力します。

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

メモ: リモート RACADM ではファイルのアップロードオプションのみを使用できます。

公開キーの権限については、『Dell Chassis Management Controller 管理者リファレンスガイド』のデータベースプロパティの章にある表 3-1 を参照してください。

テキストのアップロードオプションを使用して公開キーを追加するには、次を入力します。

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

公開キーの削除

公開キータイプを削除するには、次を入力します。

```
racadm sshpkauth –I svcacct –k 1 –d
```

公開キータイプをすべて削除するには、次を入力します。

```
racadm sshpkauth –I svcacct –k all –d
```

公開キー認証を使用したログイン

公開キーをアップロードすると、パスワードを入力せずに、SSH 経由で CMC にログインできるようになります。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することも可能です。コマンドラインオプションは、セッションがコマンドの完了時に終了するという点で、リモート RACADM と同じように動作します。例:

ログイン

```
ssh service@<ドメイン>
```

または

```
ssh service@<IP アドレス>
```

ここで、IP アドレスには CMC の IP アドレスを指定します。

racadm コマンドの送信

```
ssh service@<ドメイン> racadm getversion
```

```
ssh service@<ドメイン> racadm getsel
```

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

CMC ユーザーの権限を有効にする方法

ユーザーに特定の管理権限(ロールベースの権限)を与えるには、まず「作業を開始する前に」で説明する手順に従って、使用可能なユーザー索引を探します。その後、新しいユーザー名とパスワードを使用して次のコマンドラインを入力します。

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一覧については、『Dell Chassis Management Controller 管理者リファレンス ガイド』のデータベースプロパティの章の表 3-1 を参照してください。デフォルトの権限値は 0 で、これはユーザーの権限が有効になっていないことを示します。

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

CMC ユーザーの無効化

RACADM を使って、CMC ユーザーだけを個別に手動で無効にすることができます。設定ファイルを使ってユーザーを無効にすることはできません。

次の例は、CMC ユーザーを削除するときに使用できるコマンド構文です。

```
racadm config -g cfgUserAdmin -i 2 cfgUserAdminPrivilege 0x0
```

SNMP と電子メール警告の設定

シャーシ上で特定のイベントが発生した際に、SNMP イベント トラップ や電子メール警告を送信するように CMC を設定できます。詳細および手順については、「SNMP アラートの設定」および「電子メール警告の設定」を参照してください。

トラップ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）、または完全修飾されたドメイン名（FQDN）で指定できます。お使いのネットワーキング技術 / 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。

メモ: **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切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）。

複数シャーシ内の複数 CMC の設定

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

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

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

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

   メモ: 生成される設定ファイルは myfile.cfg です。このファイル名は変更できます。

   メモ: .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 ファイルをに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。

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

   ```
   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。

2. 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。
3. 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
   ```

4. 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(ステップ 1)はプライマリ CMC の設定を要求し、**myfile.cfg** ファイルを生成します。必要に応じて、ファイル名を変更したり、別の場所に保存することができます。

getconfig コマンドを使用して、次の操作を実行できます。

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

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

CMC 設定ファイルの作成

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

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

メモ: **getconfig** サブコマンドの詳細については、『Dell Chassis Management Controller 管理者リファレンス ガイド』を参照してください。

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

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

.cfg ファイルを作成するときは、次のガイドラインに従ってください。

- パーサーが索引付けされたグループを見つけた場合、これはさまざまな索引との差を表すアンカー付きオブジェクトの値です。

  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すべて CMC が設定されたときに修正されたものです。修正されたオブジェクトが新しいインデックスを表す場合、設定中 CMC にそのインデックスが作成されます。

- ユーザーは **.cfg** ファイルの必要なインデックスを指定できません。

  インデックスを作成したり、削除することができます。時間と共に、使用済みおよび未使用のインデックスでグループがフラグメント化される可能性があります。索引が存在する場合は、変更されます。索引が存在しない場合は、最初に使用できる索引が使用されます。この方法では、管理しているすべての CMC 間でインデックスの一致をとる必要がないので、インデックス エントリを柔軟に追加できます。新しいユーザーは、最初に使用可能な索引に追加されます。1 つの CMC で正しくパースおよび実行される **.cfg** ファイルは、すべてのインデックスが一杯で新しいユーザーを追加しなければならない場合に、別の CMC では正しく実行されない場合があります。

- 同等のプロパティを持つ CMC を両方共に設定するには、`racresetcfg` サブコマンドを使用します。

  `racresetcfg` サブコマンドを使って CMC をデフォルトにリセットして、`racadm config -f <ファイル名>.cfg` コマンドを実行します。**.cfg** ファイルに、必要なオブジェクト、ユーザー、インデックス、およびその他のパラメータがすべて含まれていることを確認します。全オブジェクトとグループの一覧表は、『Dell Chassis Management Controller 管理者リファレンス ガイド』のデータベース プロパティの章を参照してください。

注意: racresetcfg サブコマンドを使用すると、データベースと CMC NIC は元のデフォルトの設定にリセットされ、ユーザーとユーザー設定はすべて削除されます。root (ルート)ユーザーは使用可能ですが、その他のユーザーの設定もデフォルトにリセットされます。

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 <ファイル名>.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 <ファイル名>.cfg コマンドを異なる CMC 上で実行します。

  例:

  ```
  #
  # これはコメントです。
  [cfgUserAdmin]
  cfgUserAdminPageModemInitString=<Modem init # not a comment>
  ```

- グループエントリはすべて大カッコ([と])で囲む必要があります。

  グループ名を示す右カッコ(])は一列目になければなりません。このグループ名は、そのグループ内の他のオブジェクトよりも前に指定する必要があります。関連するグループ名が含まれていないオブジェクトは、エラーを生成します。構成データは、『Dell Chassis Management Controller 管理者リファレンス ガイド』のデータベースプロパティの章の定義に従って、グループにまとめられます。

  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] -{グループ名}
  ```

  ```
  cfgNicIpAddress=143.154.133.121 {オブジェクト名} { オブジェクト値}
  ```

- すべてのパラメータは、「object(オブジェクト)」、「=」、または「value(値)」の間に空白を入れずに「object=value」のペアとして指定されます。

  値の後にあるスペースは無視されます。値の文字列内にあるスペースは変更されません。'=' の右側の文字はそのまま使用されます(例: 2 つ目の 「=」、「#」、「[」、「]」、など)。これらの文字は、有効なモデムチャットスクリプト文字です。

  ```
  [cfgLanNetworking] -{グループ名}
  cfgNicIpAddress=143.154.133.121 {オブジェクト値}
  ```

- **.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、使用する索引を指定できません。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 <ファイル名>.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 <グループ名> -o <アンカーオブジェクト> -i <インデックス 1-16> <一意のアンカー名>
  ```

- インデックスグループの行は、**.cfg** ファイルからは削除できません。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、エラーを警告します。

  次のコマンドを使用して、手動で索引オブジェクトを削除する必要があります。

  ```
  racadm config -g <グループ名> -o <オブジェクト名> -i <インデックス 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。

  索引付きグループの内容を表示するには、次のコマンドを使用します。

```
racadm getconfig -g <グループ名> -i <インデックス 1 ～16>
```

- インデックス付きグループの場合、オブジェクトアンカーは [ ] の組の後にくる最初のオブジェクトでなければなりません。次は、現在の索引付きグループの例です。

```
[cfgUserAdmin]

cfgUserAdminUserName=<ユーザー名>
```

`racadm getconfig -f <myexample>.cfg` と入力すると、現在の CMC 設定用の .**cfg** ファイルが構築されます。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。

CMC IP アドレスの変更

設定ファイルの CMC IP アドレスを変更するには、不要な <変数>=<値> のエントリをすべて削除します。IP アドレス変更に関連する 2 つの <変数>=<値> エントリを含め、"[" と "]" が付いた実際の変数グループのラベルのみが残ります。

例:

```
#

# オブジェクトグループ"cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1
```

このファイルは次のようにアップデートされます。

```
#

# オブジェクトグループ"cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.9.143

# コメント、以下の行は無視されます
```

```
cfgNicGateway=10.35.9.1
```

racadm config -f <myfile>.cfg コマンドは、このファイルをパースし、行番号ごとにエラーを探します。ファイルが正しければ、該当するエントリがその内容で更新されます。さらに、前の例の getconfig コマンドを使用して、更新を確認できます。

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

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

RACADM を使用して iDRAC でプロパティを設定する方法

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

cfgLanNetworking

cfgIPv6LanNetworking

cfgRacTuning

cfgRemoteHosts

cfgSerial

cfgSessionManagement

プロパティのデフォルト値と範囲の詳細については、『Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise for Blade Servers ユーザーガイド』を参照してください。

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

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

例:

```
$ racadm getconfig -g cfgSessionManagement -m server-1

# cfgSsnMgtWebServerMaxSessions=N/A

# cfgSsnMgtWebServerActiveSessions=N/A

# cfgSsnMgtWebServerTimeout=N/A
```

```
# cfgSsnMgtSSHMaxSessions=N/A

# cfgSsnMgtSSHActiveSessions=N/A

# cfgSsnMgtSSHTimeout=N/A

# cfgSsnMgtTelnetMaxSessions=N/A

# cfgSsnMgtTelnetActiveSessions=N/A

# cfgSsnMgtTelnetTimeout=N/A
```

トラブルシューティング

表4-3 は、リモート RACADM に関する一般的な問題を掲載しています。

表 4-3 シリアルおよび RACADM コマンドの使用:よくあるお問い合わせ(FAQ) よくあるお問い合わせ(FAQ)

質問	回答
CMC リセットを実行した後 (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?	CMC のリセットが完了するまで待ってから、別のコマンドを発行してください。
RACADM サブコマンドを使用する場合に、不明なエラーが表示されます。	RACADM を使用するとき、次のようなエラーが 1 つまたは複数発生することがあります。 • ローカルエラーメッセージ — 構文、入力ミス、誤った名前などの問題。 例: ERROR: <メッセージ> RACADM **help** サブコマンドを使って、正しい構文と使用方法を表示します。 • CMC 関連のエラーメッセージ — CMC が対処できないエラー。「racadm コマンドエラー」と表示されることもあります。 デバッグ情報を取得するには、**racadm gettracelog** と入力します。
リモート RACADM を使用しているとき、プロンプトが「>」に変わって「$」に戻せません。	コマンド内で二重引用符 (") を入力すると、CLI が「>」に変わって、すべてのコマンドがキューされます。 「$」のプロンプトに戻すには、<Ctrl>-d と入力します。

以下のコマンドの利用を試みましたが、「見つかりません」のエラーが返されました。
 	
`$ logout`
 	
`$ quit`
	logout および quit コマンドは、CMC CLI インタフェースでサポートされていません。

目次ページに戻る

目次ページに戻る

トラブルシューティングとリカバリ

Dell™ Chassis Management Controllerファームウェアバージョン 2.10 ユーザーガイド

概要

本項では、リモートシステムで問題が発生した場合に CMC ウェブインタフェースを使って行うリカバリと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。

- リモートシステムの電源管理
- シャーシ情報の表示
- イベントログの表示
- 診断コンソールの使用
- 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) 問題のトラブルシューティング
- ネットワーク問題のトラブルシューティング
- 警告の不具合のトラブルシューティング
- 忘れしまったパスワードの無効化
- エラーコードおよびログ

シャーシ監視ツール

シャーシ上のコンポーネントを識別するための LED の設定

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

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

ウェブインタフェースの使用

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:

1. CMC ウェブインタフェースにログインします。
2. システムツリーで シャーシ をクリックします。
3. トラブルシューティング タブをクリックします。
4. 識別 サブタブをクリックします。識別 ページが開いて、シャーシ上のすべてのコンポーネントの一覧が表示されます。
5. 特定のコンポーネント LED の点滅を有効にするには、そのデバイス名の横のボックスを選択し、点滅 をクリックします。
6. 特定のコンポーネント LED の点滅を無効にするには、そのデバイス名の横のボックスを選択し、非点滅 をクリックします。

RACADM の使用

CMC に対応するシリアル/Telnet/SSH テキスト コンソールを開いて、ログイン後、以下を入力します。

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

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

- server-n(n=1〜16)
- switch-n(n=1〜6)
- cmc-active

および <ledState> は LED を点滅させるかどうかを指定します。設定オプション:

- 0 — 点滅なし(デフォルト)
- 1 — 点滅

SNMP アラートの設定

シンプル ネットワーク 管理プロトコル(SNMP)トラップまたは イベント トラップ は、電子メール イベント警告と似ています。CMC から一方的に送信されるデータを管理ステーションが受信するために使用します。

CMC でイベントトラップを生成するように設定できます。表11-1は、SNMP および電子メール警告をトリガーするイベントの概要を提供します。電子メール警告の詳細については、「電子メール警告の設定」を参照してください。

メモ: CMC バージョン 2.10 以降、SNMP では IPv6 を使用できるようになりました。イベント警告の宛先として IPv6 アドレスまたは完全修飾されたドメイン名(FQDN)を入力できます。

イベント	説明
ファンプローブエラー	ファンの稼動速度が遅すぎるか、稼動していません。
バッテリプローブ警告	バッテリが機能停止しました。
温度プローブ警告	温度が高温、低温の限界に近づいています。
温度プローブエラー	温度が高すぎるか低すぎて適切な操作が行えません。
冗長性低下	ファンおよび / または電源装置の冗長性が少なくなりました。
冗長性喪失	ファンまたは電源装置に冗長性がありません。
電源装置警告	電源装置がエラー状態に近づいています。
電源装置エラー	電源装置が故障しました。
電源装置がありません	あるはずの電源装置がありません。
ハードウェアログエラー	ハードウェアのログが機能していません。
ハードウェアログ警告	ハードウェアログがほとんどいっぱいです。
サーバーの不在	存在するはずのサーバーがありません。
サーバーエラー	サーバーが機能していません。
KVM の不在	存在するはずの KVM がありません。
KVM エラー	KVM が機能していません。
IOM の不在	存在するはずの IOM がありません。
IOM エラー	IOM が機能していません。
ファームウェア バージョンの不一致	シャーシまたはサーバーのファームウェアが一致していません。
シャーシ電力しきい値エラー	シャーシ内の電力消費量がシステム入力電力上限を超えました。

ウェブインタフェースまたは RACADM を使って SNMP 警告を追加、設定できます。

ウェブインタフェースの使用

メモ: SNMP 警告を追加または設定するには、シャーシ設定システム管理者 の権限が必要となります。

メモ: セキュリティを強化するために、root(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。root アカウントは、CMC に付属のデフォルト管理者アカウントです。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、ユーザー ID 1 をクリックして ユーザー設定 ページを開きます。そのページのヘルプには、ページの右上にある ヘルプ リンクからアクセスできます。

1. CMC ウェブインタフェースにログインします。
2. システムツリーで シャーシ を選択します。
3. 警告管理 タブをクリックします。シャーシイベント ページが表示されます。
4. 警告の有効化:
   a. 警告を有効にするイベントのチェックボックスを選択します。すべてのイベントの警告を有効にするには、すべて選択 チェックボックスを選択します。
   b. 適用 をクリックして設定を保存します。
5. トラップ設定 サブタブをクリックします。シャーシイベント警告送信先 ページが表示されます。
6. 空の 送信先 フィールドに有効なアドレスを入力します。

   メモ: 有効なアドレスとは、トラップ警告を受信するアドレスを指します。「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

7. 送信先管理ステーションが属する SNMP コミュニティ文字列 を入力します。

   メモ: **シャーシイベント警告送信先** ページのコミュニティ文字列は、**シャーシ→ ネットワーク / セキュリティ→ サービス** ページのコミュニティ文字列とは異なります。SNMP トラップのコミュニティ文字列は、CMC が管理ステーション宛の送信トラップに使用します。**シャーシ→ ネットワーク / セキュリティ→ サービス** ページのコミュニティ文字列は、管理ステーションが CMC の SNMP デーモンにクエリする際に使用されます。

8. 適用 をクリックして変更を保存します。

警告送信先へのイベントトラップをテストするには:

1. CMC ウェブインタフェースにログインします。
2. システムツリーで シャーシ を選択します。
3. 警告管理 タブをクリックします。シャーシイベント ページが表示されます。
4. トラップ設定 タブをクリックします。シャーシイベント警告送信先 ページが表示されます。
5. 送信先の隣にある テストトラップ 行の 送信 をクリックします。

メモ: トラップ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)、または完全修飾されたドメイン名(FQDN)で指定できます。お使いのネットワーキング技術 / 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切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)。

RACADM の使用

1. CMC に対応するシリアル/Telnet/SSH テキスト コンソールを開いて、ログインします。

   メモ: SNMP と電子メール警告の両方に設定できるフィルタマスクは 1 つだけです。既にフィルタマスクを選択している場合は、手順 2 をスキップできます。

2. 警告を有効にするには、次を入力します。

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

3. CMC に生成させたいイベントを指定するには、次を入力します。

   ```
   racadm config -g cfgAlerting -o cfgAlertingFilterMask <マスク値>
   ```

   ここで、<マスク値> は 0x0 ～ 0x017fffdf の 16 進値です。

マスク値を得るには、科学計算用電卓を 16 進モードで使い、<OR> キーで各マスクの第 2 値(1、2、4、...)を追加します。

たとえば、バッテリプローブ警告 (0x2)、電源装置エラー (0x1000)、KVM エラー (0x80000) 用トラップ警告を有効にするには、2 <OR> 1000 <OR> 200000 を入力して <=> キーを押します。

結果の 16 進値は 208002 で、RACADM コマンドのマスク値は 0x208002 です。

表 11-2 イベントトラップのフィルタマスク

イベント	フィルタマスク値
ファンプローブエラー	0x1
バッテリプローブ警告	0x2
温度プローブ警告	0x8
温度プローブエラー	0x10
冗長性低下	0x40
冗長性喪失	0x80
電源装置警告	0x800
電源装置エラー	0x1000
電源装置がありません	0x2000
ハードウェアログエラー	0x4000
ハードウェアログ警告	0x8000
サーバーの不在	0x10000
サーバーエラー	0x20000
KVM の不在	0x40000
KVM エラー	0x80000
IOM の不在	0x100000
IOM エラー	0x200000
ファームウェア バージョンの不一致	0x00400000
シャーシ電力しきい値エラー	0x01000000

4. トラップ警告を有効にするには、次を入力します。

```
racadm config -g cfgTraps -o cfgTrapsEnable 1 -i < インデックス>
```

ここで、<インデックス> は 1～4 の値です。インデックス番号は、CMC によりトラップ警告の送信先として設定可能な 4 つまでの送信先 IP の識別に使用されます。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)、または完全修飾されたドメイン名(FQDN)で指定できます。

5. トラップ警告の送信先 IP アドレスを指定するには、次を入力します。

```
racadm config -g cfgTraps -o cfgTrapsAlertDestIPAddr <IP アドレス> -i <インデックス>
```

ここで、<IP アドレス> は有効な IP アドレスで、<インデックス> 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するには、次を入力します。

```
racadm config -g cfgTraps -o cfgTrapsCommunityName <コミュニティ名> -i <インデックス>
```

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

トラップ警告の送信先 IP アドレスを 4 つまで設定できます。送信先をさらに追加するには、手順 2 ～6 を繰り返します。

メモ: 手順 2～6 のコマンドは、指定するインデックス (1～4) の既存の設定をすべて上書きします。インデックスに既に値が設定されているかを調べるには、racadm get config -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、その値が cfgTrapsAlertDestIPAddr と cfgTrapsCommunityName オブジェクトに表示されます。

警告送信先へのイベントトラップをテストするには:

```
racadm testtrap -i <インデックス>
```

ここで、<インデックス> は 1～4 の値で、テストする警告送信先を表します。インデックス番号がわからない場合は、次を入力します。

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

電子メール警告の設定

CMC が環境についての警告やコンポーネント エラーなどのシャー シイベントを検出した場合、電子メール警告を 1 つまたは複数の電子メールアドレスに送信するように設定できます。

表11-1 は、SNMP および電子メール警告をトリガーするイベントの概要を提供します。電子メール警告の詳細については、「SNMP アラートの設定」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 SNMP 警告を追加および設定できます。

ウェブインタフェースの使用

メモ: 電子メール警告を追加または設定するには、シャーシ設定管理者 の権限が必要です。

1. CMC ウェブインタフェースにログインします。
2. システムツリーで シャーシ を選択します。
3. 警告管理 タブをクリックします。シャーシイベント ページが表示されます。
4. 警告の有効化:
   a. 警告を有効にするイベントのチェックボックスを選択します。すべてのイベントの警告を有効にするには、すべて選択 チェックボックスを選択します。
   b. 適用 をクリックして設定を保存します。
5. 電子メール警告設定 サブタブをクリックします。電子メール警告の送信先 ページが表示されます。
6. SMTP サーバー IP アドレスを指定します。
   a. SMTP(電子メール)サーバー フィールドを見つけて、SMTP ホスト名または IP アドレスを入力します。

   メモ: CMC の IP アドレスから送信された電子メールを受け入れるように SMTP 電子メールサーバーを設定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。この設定をセキュアに行う手順は、SMTP サーバーのマニュアルを参照してください。

   b. 警告を発信する送信元電子メールアドレスを入力します。デフォルトの送信元電子メールアドレスを使用する場合は、空白のままにします。デフォルトの送信元アドレスは、cmc@[IP アドレス] です。ここで、[IP_address] は、CMC の IP アドレスを指します。値を入力する場合は、電子メール アドレスの構文は、「電子メール名[@ドメイン] 」です。電子メール ドメインは、オプションで指定することができます。「@ドメイン」 を指定しない場合にアクティブな CMC ネットワークドメインが存在すると、差出人電子メール アドレスとして「電子メール名@cmc. ドメイン」 が使用されます。「@ドメイン」 を指定しない場合にアクティブな CMC ネットワークドメインが存在しないと、CMC の IP アドレスが使用されます(例: 電子メール名@[IP アドレス])。
   c. 適用 をクリックして変更を保存します。
7. 警告を受け取る電子メール アドレスを指定します。
   a. 空白の 送信先電子メールアドレス フィールドに有効な電子メールアドレスを入力します。
   b. オプションで 名前 も入力できます。この名前は、電子メールを受信するエンティティとなります。無効な電子メール アドレスに入力された名前は、無視されます。
   c. 適用 をクリックして設定を保存します。

テストメールを警告送信先電子メール アドレスに送信するには、以下を行います。

1. CMC ウェブインタフェースにログインします。
2. システムツリーで シャーシ を選択します。
3. 警告管理 タブをクリックします。シャーシイベント ページが表示されます。
4. 電子メール警告設定 サブタブをクリックします。電子メール警告の送信先 ページが表示されます。
5. 送信先の隣にある 送信先電子メールアドレス 行の 送信 をクリックします。

RACADM の使用

1. CMC に対応するシリアル/Telnet/SSH テキスト コンソールを開いて、ログインします。
2. 警告を有効にするには、次を入力します。

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

メモ: SNMP と電子メール警告の両方に設定できるフィルタマスクは 1 つだけです。既にフィルタマスクを選択している場合は、手順 3 をスキップできます。

3. CMC に生成させたいイベントを指定するには、次を入力します。

```
racadm config -g cfgAlerting -o cfgAlertingFilterMask <マスク値>
```

ここで、<マスク値> は 0x0～ 0x017fffdf の 16 進数値で、0x で始まる形式でなければなりません。表11-2は、各イベントタイプのフィルタマスクを提供します。有効にするフィルターマスクの 16 進値の計算方法は、「RACADM の使用」の手順 3 を参照してください。

4. 電子メール警報を有効にするには、以下を入力します。

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable 1 -i <インデックス>
```

ここで、<インデックス> は 1～4 の値です。インデックス番号は、CMC により 4 つまでの設定可能な電子メール送信先の識別に使用されます。

5. 電子メール警報を受け取る受信先電子メール アドレスを指定するには、以下を入力します。

```
racadm config -g cfgEmailAlert -o cfgEmailAlertAddress <電子メールアドレス> -i <インデックス>
```

ここで、<電子メールアドレス> は有効な電子メール アドレスで、<インデックス> は手順 4 で指定したインデックス値です。

6. 電子メール警告の受信者の名前を指定するには、以下を入力します。

```
racadm config -g cfgEmailAlert -o cfgEmailAlertAddress <電子メール名> -i <インデックス>
```

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

7. cfgRhostsSmtpServerIpAddr データベース プロパティを設定してSMTP ホストを設定するには、以下を入力します。

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

ここで、host.domain は、正式なドメイン名です。

電子メール警報を受け取る受信先電子メールアドレスは最大4件設定できます。それ以上の電子メールアドレスを追加するには、手順 2～6 を繰り返します。

メモ: 手順 2～6 のコマンドは、指定するインデックス (1～4) の既存の設定をすべて上書きします。インデックスに既に値が設定されているかを調べるには、racadm get config -g cfgEmailAlert -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、その値が cfgEmailAlertAddress と cfgEmailAlertEmailName オブジェクトに表示されます。

リモートシステムのトラブルシューティングの最初のステップ

以下は、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際に確認すべき事項です。

1. 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?
2. 電源がオンの場合は、オペレーティングシステムが正しく機能していますか、それともクラッシュまたはフリーズしていますか?
3. 電源がオフの場合は、突然オフになりましたか?

シャーシ上の電源監視と電源制御コマンドの実行

ウェブインタフェースまたは RACADM を使用して、以下を行うことができます。

- システムの現在の電源状態の表示。
- 再起動するとき、オペレーティングシステムから正常なシャットダウンを実行して、システムをオンまたはオフにします。

CMC 上での電源管理、および電力バジェット、冗長性、電源制御の設定の詳細は、「Power Management」を参照してください。

電力バジェット状態の表示

ウェブインタフェースまたは RACADM を使ってシャーシ、サーバー、PSU の電力バジェット状態を表示する方法は、「消費電力ステータスの表示」を参照してください。

電源制御操作の実行

CMC ウェブインタフェースまたは RACADM を使ってシステムの電源オン、電源オフ、リセットまたは電源サイクルを行う手順は、「シャーシに対する電力制御操作の実行」、「IOM 上で電源制御操作の実行」および「サーバーに対する電力制御操作の実行」を参照してください。

電源ユニットのトラブルシューティング

電源ユニットおよび電源関係の問題のトラブルシューティングには下の項目をお使いください。

- 不具合: 電源冗長性ポリシーを AC 冗長性に設定する試みに失敗しました。
  - 対策 A: この操作には、入力電源を受け取っている 2、4、または 6 台の電源装置(各グリッドに 1、2、または 3 台ずつ)がモジュラーエンクロージャ内に存在し、機能している必要があります。AC 電源の完全な冗長性 運用を実現するには、冗長性ポリシーを AC 冗長性に変更する前に、電源装置 6 台による完全 PSU 構成が利用可能であることを確認してください。
  - 対策 B: すべての電源装置が 2 台の AC グリッドに適切に接続されているか確認します。左側の電源装置 3 台は AC グリッドに接続し、右側の電源装置は別の 3 台の AC グリッドに接続し、すべての AC グリッドが正しく機能しているか確認します。電源冗長性は、いずれかの AC グリッドが正しく機能していない場合には AC 冗長性に設定できません。
- 不具合: AC コードが接続されており、電力配分装置も AC に電力を送っているのにも関わらず、PSU にエラー(AC なし)が表示されます。
  - 対策: AC コードを確認して交換してください。電力配分装置が供給する電力が十分であるかを点検および確認してください。それでも不具合が解消されない場合は、デルのカスタマサービスに電源装置装置の交換を依頼してください。
- 不具合: Dynamic Power Supply Engagement を有効にしても、どの電源装置画面もスタンドバイにならない。
  - 対策: この現象は、AC 冗長性の電源装置構成が 6 台で、エンクロージャ操作に電源装置が 3 台以上必要な場合に発生します。エンクロージャの余剰電力が 1台分の電源装置を超える場合にのみ、それぞれがオンラインで冗長関係にある組み合わせの電源装置セットがスタンドバイに変わります。
- 不具合: 新しいサーバーを電源装置が 6 台構成のエンクロージャに挿入しましたが、電源がオンになりません。
  - 対策 A: システムの電源入力設定を確認します。追加サーバーに電源を供給するには低すぎる電源構成になっているかもしれません。
  - 対策 B: 新しく追加したサーバーを装備するスロットの電源設定を確認し、他のサーバーのスロットと比べて引く設定されていないかを確認してください。
- 不具合: モジュラーの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ります。
  - 対策: CMC 1.2 以上のバージョンには、エンクロージャがユーザーが設定した電力容量のピークに近づくとサーバーへの配分を減少させるダイナミックファン電源管理機能が装備されています。これは、サーバーの性能を下げることで電力入力がシステム入力電力上限を超えないようにしているため、ファンへの電力が分配される原因になっています。これは、正常な

状態です。

- 不具合: ピーク時の余剰電力に 2000 W と表示されます。
  - 対策: 現行の構成ではエンクロージャに 2000 W の余剰電力があり、システム入力電力上限はサーバーの性能に影響を与えることなくこの報告された量まで安全に下げることができます。
- 不具合: シャーシが 6 台の電源装置による AC 冗長性構成で運用されていたにも関わらず、AC グリッドにエラーが発生した後、サーバーのサブセットに電力が供給されなくなりました。
  - 対策: この現象は、AC グリッドのエラーが発生したときに電源装置が適切に AC グリッドに接続されていない場合に発生します。AC 冗長性ポリシーでは、左側の 3 台の電源装置を1つの AC グリッドに接続し、右側の 3 台の電源装置を別の AC グリッドに接続することが必要です。PSU3 と PSU4 が間違った AC グリッドに接続されている場合など、2 台の PSU が適切に接続されていないと、AC グリッドのエラーにより、優先順位が最も低いサーバーへの電源装置を失う原因になります。
- 不具合: PSU にエラーが発生した後、優先順位の低いサーバーに電力が供給されなくなった。
  - 対策: これは、エンクロージャの電力ポリシーが 冗長性なし に設定されている場合には正常な動作です。今後サーバーの電源がオフになる電源装置エラーを回避するには、シャーシを 4 台以上の電源装置構成にし、電源装置冗長性ポリシーを PSU 障害がサーバーの運用に影響しない設定にしてください。
- 不具合: データ センターの周囲温度が上がるとサーバー全体の性能が低下します。
  - 対策: これは、システム入力電力上限がサーバーへの割り当て電力を減らすことでファンに電力を供給しなければならない電源構成に設定されている場合に発生する可能性があります。システム入力電力上限を、サーバーの性能に影響を与えずにファンに十分な電力を供給できる値に増やしてください。

シャーシサマリの表示

CMC は、シャーシ、プライマリとセカンダリ CMC、iKVM、ファン、温度センサー、I/O モジュール (IOM) のロールアップ概要を表示します。

ウェブインタフェースの使用

シャーシ、CMC、iKVM、IOM のサマリを表示するには:

1. CMC ウェブインタフェースにログインします。
2. システムツリーで シャーシ を選択します。
3. サマリ タブをクリックします。シャーシサマリ ページが表示されます。

表11-3、表11-4、表11-5 および 表11-6 に、提供される情報を説明しています。

項目	説明
Name	シャーシの名前を表示します。この名前は、ネットワーク上のシャーシを識別します。シャーシの名前の設定に関する詳細は、「スロット名の編集」を参照してください。
Model	シャーシのモデルまたはメーカーを表示します。例:PowerEdge 2900
サービスタグ	シャーシのサービスタグを表示します。サービスタグはサポートとメンテナンスのためにメーカーが提供する一意の識別子です。
Asset Tag	シャーシの管理タグを表示します。
場所	シャーシの場所を表示します。
CMC フェールオーバー準備完了	スタンバイ CMC (存在する場合)が(はい または いいえ)で、フェールオーバー能力があるかを示します。
システム電源の状態	システムの電源状態を表示します。

項目	説明
プライマリ CMC 情報	
Name	CMC の名前を表示します。例:Primary CMC、Standby CMC
説明	CMC の目的を簡単に説明します。
日時	アクティブまたはプライマリ CMC で設定されている日付と時刻を示します。
アクティブ CMC ロケーション	アクティブ CMC またはプライマリ CMC のスロットの位置を示します。

冗長性モード	スタントバイ CMC がシャーシに存在するかどうかを表示します。
プライマリファームウェアバージョン	アクティブ または プライマリ CMC のファームウェアバージョンを示します。
ファームウェア最終更新日	ファームウェアが最後に更新された日付を示します。アップデートが行われていない場合は、このプロパティには なし と表示されます。
ハードウェアバージョン	アクティブ CMC またはプライマリ CMC のハードウェアバージョンを示します。
MAC アドレス	CMC NIC の MAC アドレスを示します。MAC アドレスはネットワーク上の CMC の一意の識別子です。
IP アドレス	CMC NIC の IP アドレスを示します。
ゲートウェイ	CMC NIC のゲートウェイを示します。
サブネットマスク	CMC NIC のサブネットマスクを示します。
DHCP を使用(NIC IP アドレス用)	CMC が動的ホスト構成プロトコル(DHCP)サーバーに IP アドレスを要求して取得できるかどうかを示します(はい または いいえ)。このプロパティのデフォルト設定は いいえ です。
プライマリ DNS サーバー	プライマリ DNS サーバーの名前を示します。
代替 DNS サーバー	代替 DNS サーバーの名前を示します。
DNS ドメイン名に DHCP を使用	DNS ドメイン名を取得するために DHCP を使用するかどうかを示します(はい、いいえ)。
DNS ドメイン名	DNS ドメイン名を示します。
スタンバイ CMC 情報	
存在	セカンダリ(スタンバイ) CMC が設置されているかを示します(はい または いいえ)。
スタンバイファームウェアバージョン	スタンバイ CMC に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します。

項目	説明
存在	iKVM モジュールが存在するかどうかを示します(はい または いいえ)。
Name	iKVM の名前を表示します。名前はネットワーク上の iKVM を識別します。
メーカー	iKVM のモデルまたはメーカーを表示します。
パーツ番号	iKVM のパーツ番号を示します。パーツ番号は、ベンダーが提供する一意の識別子です。パーツ番号の命名規則はベンダーによって異なります。
ファームウェアバージョン	iKVM のファームウェアバージョンを示します。
ハードウェアバージョン	iKVM のハードウェアバージョンを示します。
電源状態	iKVM の電源状態:オン、オフ、なし(不在)。
前面パネルの USB/ビデオを有効にする	前面パネルの VGA または USB コネクタが有効になっているかどうかを示します(はい または いいえ)。
CMC CLI への iKVM からのアクセスを許可する	iKVM 上で CLI アクセスが有効になっているどうかを示します(はい または いいえ)。

項目	説明
場所	IOM が装着されているスロットを示します。6 つのスロットがグループ名(A、B、C)とスロット番号(1 または 2)によって識別されます。スロット名:A-1、A-2、B-1、B-2、C-1、C-2。
存在	IOM が存在するかどうかを示します(はい または いいえ)。
Name	IOM 名を表示します。
ファブリック	ファブリックの種類を表示します。
電源状態	IOM の電源状態:オン、オフ、なし(不在)を示します。
サービスタグ	IOM のサービスタグを表示します。サービスタグはサポートとメンテナンス用にデルが提供する一意の識別子です。

RACADM の使用

1. CMC に対応するシリアル/Telnet/SSH テキスト コンソールを開いて、ログインします。
2. シャーシと CMC のサマリを表示するには、次を入力します。

```
racadm getsysinfo
```

iKVM サマリを表示するには、次を入力します。

```
racadm getkvminfo
```

IOM サマリを表示するには、次を入力します。

```
racadm getioinfo
```

シャーシとコンポーネントの正常性状態の表示

ウェブインタフェースの使用

シャーシとシャーシコンポーネントの正常性を表示するには、次を入力します。

1. CMC ウェブインタフェースにログインします。
2. システムツリーで シャーシ を選択します。シャーシサマリ ページが表示されます。

シャーシグラフィックス セクションは、シャーシの前面および背面図をグラフィック表示します。グラフィック表示により、シャーシに内蔵されたコンポーネントおよびステータスの概要を視覚的に把握することができます。

各グラフィックは、取り付けられたコンポーネントをリアルタイムに表します。コンポーネントの状態は、コンポーネントのサブグラフィックの色で示されます。

- 緑色 - コンポーネントが存在し、電源がオンで CMC と通信中。悪条件の兆候なし。
- オレンジ色 - コンポーネントが存在し、電源がオンまたはオフで CMC と通信中または通信しておらず。悪条件が存在する可能性があり。
- 灰色 - コンポーネントが存在するが、電源がオフ。CMC と通信しておらず、悪条件の兆候なし。

コンポーネントのサブグラフィックにマウスのカーソルを移動すると、該当するテキストヒントまたは画面ヒントが表示されます。コンポーネントステータスは動的に更新され、現在の状態を反映するように、コンポーネントのサブグラフィックの色およびテキストヒントも自動的に変更します。

コンポーネントのサブグラフィックは、該当する CMC GUI ページにハイパーリンクされ、対象のコンポーネントのステータスページに即座に移動することができます。

コンポーネントの正常性 セクションは、アイコンと共に各コンポーネントのステータスを表示します。表11-7 は、各アイコンを説明します。

項目	説明	
	OK	コンポーネントが存在し、CMC と通信していることを示します。
	情報	正常性の状態に変化がない場合は、コンポーネントに関する情報が表示されます。
	警告	警告アラートが発行されたこと、および対応処置を取る必要があることを示します。管理者が指定した時間内に修正処置を取らなかった場合は、コンポーネントエラーや、コンポーネントと CMC 間の通信エラー、シャーシの整合性に影響する重要または重大なエラーを引き起こす可能性があります。
	重大	少なくとも 1 つのエラー警告が発行されたことを示します。つまり、CMC はまだコンポーネントと通信できますが、正常性に関する深刻な状態が報告されています。速やかな対応処置が必要です。修正しなかった場合は、コンポーネントに障害が発生し、CMC との通信が停止します。

	不明	シャーシに初めて電源が投入されたときに表示されます。すべてのシャーシコンポーネントは最初、完全に電源が投入されるまで「不明」と表示されます。
	値なし	コンポーネントがスロットにないか、CMC がコンポーネントと通信できないことを示します。 **メモ:** シャーシが不在になることはあり得ません。

RACADM の使用

CMC に対応するシリアル/Telnet/SSH テキスト コンソールを開いて、ログイン後、以下を入力します。

```
racadm getmodinfo
```

イベントログの表示

ハードウェアログと CMC ログ ページに、管理下システムで発生した重大なシステムイベントが表示されます。

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とリモート 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の権限が必要です。

メモ: 特定のイベントが発生したときに電子メールまたは 電子メール SNMP トラップを送信するように CMC を設定できます。警告を送信するように CMC を設定する方法については、「SNMP アラートの設定」および「電子メール警告の設定」を参照してください。

ハードウェアログのエントリ例

```
重要システムソフトウェアイベント：冗長性喪失

Wed May 09 15:26:28 2007 標準システムソフトウェアイベント：ログのクリアがアサートされました。

Wed May 09 16:06:00 2007 警告システムソフトウェアイベント：予測エラーがアサートされました。

Wed May 09 15:26:31 2007 重要システムソフトウェアイベント：ログ満杯がアサートされました。

Wed May 09 15:47:23 2007 不明システムソフトウェアイベント：不明なイベント
```

ウェブインタフェースの使用

CMC ウェブインタフェースではハードウェアログの表示や削除、テキストファイルバージョンの保存が可能です。

表11-8 に、CMC ウェブインタフェースのハードウェアログ ページに表示される情報とその説明を示します。

ハードウェアログを表示するには：

1. CMC ウェブインタフェースにログインします。
2. システムツリーで シャーシ をクリックします。
3. ログ タブをクリックします。
4. ハードウェアログ サブタブをクリックします。ハードウェアログ ページが表示されます。

ハードウェアログのコピーを管理ステーションまたはネットワークに保存するには:

ログの保存 をクリックします。ダイアログボックスが開いたら、ログのテキストファイルの保存場所を選択します。

メモ: ログはテキストファイルとして保存されるため、ユーザーインタフェースで重大度を示すのに使用されるグラフィックイメージは表示されません。重大度は、テキストファイルで OK、情報、不明、警告、重大と示されます。
日付 / 時刻のエントリは昇順で表示されます。<システム起動> が 日付 / 時刻列に表示される場合は、日時を記録できないモジュールのシャットダウンまたはスタートアップ中にイベントが発生したという意味です。

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。

項目	説明		
重大度		OK	修正処置を必要としない 正常なイベントを示します。
		情報	重大度 の状態が変化していないイベントに関する情報のエントリを示します。
		不明	システムエラーを防ぐために 早めに修正処置を講じる必要のある 非重要イベントを示します。
		警告	システムエラーを防ぐために 直ちに修正処置を講じる必要のある 重要イベントを示します。
		重大	システムエラーを防ぐために、直ちに対応処置を講じる必要のある重要イベントを示します。
日時	イベントが発生した正確な日時を示します(例:2007 年5 月 2 日 16 時 26 分 55 秒)。日付 / 時刻が空白の場合は、システム起動時にイベントが発生しました。		
説明	CMC が生成したイベントについて短い説明を提供します(例:冗長性喪失、サーバー挿入など)。		

RACADM の使用

1. CMC に対応するシリアル/Telnet/SSH テキスト コンソールを開いて、ログインします。
2. ハードウェアログタイプを表示するには、次を入力します。

```
racadm getsel
```

ハードウェアログをクリアするには、次を入力します°

```
racadm clrsel
```

CMC ログの表示

CMC は、シャーシ関連のイベントのログを生成します。

メモ: 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の権限が必要です。

ウェブインタフェースの使用

CMC ウェブインタフェースでは、ハードウェアログの表示や削除、テキストファイルバージョンの保存が可能です。

ログは、行見出しをクリックすることにより、ソース、日付 / 時刻、または 説明 を基準に並べ替えできます。再度、行見出しをクリックすると、並ぶ順序が逆になります。

表11-9 に、CMC ウェブインタフェースのCMC ログ ページに表示される情報とその説明を示します。

CMC ログを表示するには:

1. CMC ウェブインタフェースにログインします。
2. システムツリーで シャーシ をクリックします。
3. ログ タブをクリックします。
4. CMC ログ サブタブをクリックします。CMC ログ ページが表示されます。

CMC ログのコピーを管理下ステーションまたはネットワークに保存するには、ログを保存 をクリックします。ダイアログボックスが開いたら、ログのテキストファイルの保存場所を選択します。

表 11-9 CMC ログ情報

コマンド	結果
ソース	イベントを引き起こしたインタフェースを示します(例:CMC)。
日時	イベントが発生した正確な日時を示します(例:2007 年5 月 2 日 16 時 26 分 55 秒)。
説明	処置について短い説明を表示します(例:ログアウト、ログインエラー、ログクリア)。説明は CMC によって生成されます。

RACADM の使用

1. CMC に対応するシリアル/Telnet/SSH テキスト コンソールを開いて、ログインします。
2. ハードウェアログタイプを表示するには、次を入力します。

```
racadm getraclog
```

ハードウェアログをクリアするには、次を入力します°

```
racadm clrraclog
```

ファームウェアアップデートのエラーコード

CMC ログは、ログ情報の一部としてエラーコードも表示できます。以下の表では、ファームウェアアップデートの CMC ログのエラーコードを記載しています。

表 11-10 ファームウェアアップデートのエラーコード

エラークラス	エラー値（16進数）	エラー値（10進数）
ERR_NO_PRIVILEGE	0x1400	5120
ERR_LOC_CMC_STATE	0x1401	5121
ERR_INV_TARG_LINK	0x1402	5122
ERR_ILLEGAL_CMC_STATE	0x1403	5123
ERR_MX_NULL_PARAM	0x1404	5124
ERR_CLASS_UNSUPPORTED	0x1405	5125
ERR_INAPPROPRIATE_REQUEST	0x1406	5126
ERR_MX_BAD_PARAM	0x1407	5127
ERR_INVALID_TARGET	0x1408	5128
ERR_URL_NOT_FOUND	0x1409	5129
ERR_CANCEL_PID_KILL	0x140A	5130
ERR_REROUTE_PEER	0x140B	5131
ERR_BAD_URL	0x140C	5132
ERR_PAYLOAD_TOO_BIG	0x140D	5133
ERR_BAD_IP_CONV	0X140E	5134
ERR_BAD_HDR_PARAM	0x140F	5135
ERR_BAD_FILENAME	0x1410	5136
ERR_TARGET_NOT_READY	0x1411	5137
ERR_TFTP_GET_FAIL	0x1412	5138
ERR_WAITPID_FAIL	0x1413	5139
ERR_REBOOT_FAIL	0x1414	5140
ERR_UNSUPPORTED_PROTOCOL	0x1415	5141
BAD_FTP_PASSWORD	0x1416	5142
ERR_FORK_FAILED	0x1417	5143
ERR_MALLOC_ERROR	0x1418	5144
ERR_PEER_ABSENT	0x1419	5145
ERR_UPDATE_FAIL	0x141A	5146
ERR_OPEN_FILE_FAIL	0x141B	5147
ERR_IMAGE_FILE_NOT_ACCESSIBLE	0x141C	5148
ERR_FCNTL_GET_FAIL	0x141D	5149
ERR_FCNTL_SET_FAIL	0x141E	5150
ERR_POLL_FAIL	0x141F	5151
ERR_SEND_FAIL	0x1420	5152
ERR_CONNECT_FAIL	0x1421	5153
ERR_SOCKET_FAIL	0x1422	5154
ERR_RESOLVE_REMOTE_IP_ADDR_FAIL	0x1423	5155
ERR_TIMEOUT	0x1424	5156
ERR_RECV_FAIL	0x1425	5157
ERR_INVENTORY_COUNT	0x1426	5158
ERR_FWUPD_INIT_CALL	0x1427	5159
ERR_FWUPD_START_UPDATE_CALL	0x1428	5160
ERR_OP_NOT_CANCELABLE	0x1429	5161
BAD_FTP_USERNAME	0x142A	5162
DEVICE_NOT_AVAILABLE	0x142B	5163

診断コンソールの使用

診断コンソール ページは、上級ユーザーやをテクニカルサポートを受けているユーザーが CLI コマンドを使って CMC ハードウェアに関連した問題を診断するために使用します。

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の権限が必要です。

診断コンソール ページにアクセスするには、次の手順を行います。

1. CMC ウェブインタフェースにログインします。
2. システムツリーで シャーシ をクリックします。
3. トラブルシューティング タブをクリックします。
4. 診断 サブタブをクリックします。診断コンソール ページが表示されます。

診断 CLI コマンドを実行するには、RACADM コマンドの入力 フィールドにコマンドを入力して 送信 をクリックします。診断結果ページが表示されます。

診断コンソール ページに戻るには、診断コンソール ページに戻る または 更新 をクリックします。

診断こーソールは、RACADM コマンドと共に、「表11-11」に記載されるコマンドをサポートしています。

表 11-11 対応診断コマンド

コマンド	結果
arp	アドレス解決プロトコル（ARP）テーブルの内容を表示します。ARP エントリの追加や削除はできません。
ifconfig	ネットワークインタフェーステーブルの内容を表示します。
netstat	ルーティングテーブルの内容を表示します。
ping <IP アドレス>	送信先の <IP アドレス> が現在のルーティングテーブルの内容で CMC から到達可能かどうかを確認します。このオプションの右側のフィールドに送信先の IP アドレスの入力が必要です。ICMP（インターネットコントロールメッセージプロトコル）エコーパケットが現在のルーティングテーブルの内容に基づいて宛先 IP アドレスに送信されます。
gettracelog	トレースログを表示します（ログが表示されるまでに数秒かかることがあります）。gettracelog -i コマンドはトレースログ内のコード数を返します。 **メモ:** gettracelog コマンドの詳細については、『Dell Chassis Management Controller 管理者リファレンスガイド』の gettracelog コマンドの項を参照してください。

コンポーネントのリセット

コンポーネントのリセットページで、ユーザーは、アクティブ CMC をリセットしたり、仮想のサーバーを取り付けてサーバーの抜き差し動作を発生させたりすることができます。シャーシにスタンドバイ CMC がある場合にアクティブ CMC をリセットすると、フェイルオーバーが発生し、スタンドバイ 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 コマンド管理者の権限が必要です。

診断コンソール ページにアクセスするには、次の手順を行います。

1. CMC ウェブインタフェースにログインします。
2. システムツリーで シャーシ をクリックします。
3. トラブルシューティング タブをクリックします。
4. コンポーネントのリセット サブタブをクリックします。更新可能なコンポーネント ページが表示されます。コンポーネントのリセット ページの CMC サマリの部分には以下の情報が表示されます。

属性	説明		
正常性		OK	CMC が存在し、コンポーネントで通信が行われています。
		情報	正常性の状態（OK、警告、重大）に変化がない場合にサーバーについての情報を表示します。
		警告	警告アラートが発行されたこと、および対応処置を取る必要があることを示します。管理者が指定した時間内に対応処置を取らなかった場合は、CMC の保全性に影響するような重要または重大なエラーを引き起こす可能性があります。
		重大	少なくとも 1 つのエラー警告が発行されたことを示します。重大な状態は CMC のシステム エラーを示し、直ちに対応処置を取る必要があります。

日時	CMC の日付と時刻を MM/DD/YYYY の形式で表示します。このとき、MM は月、DD は日、YYYY は年を示します。
アクティブ CMC ロケーション	プライマリ CMC の場所を表示します。
冗長性モード	シャーシにスタンドバイ CMC がある場合は冗長を表示し、シャーシにスタンドバイ CMC がない場合は冗長なしが表示されます。

5. コンポーネントのリセットページの 仮想サーバーの装着の部分には以下の情報が表示されます。

属性	説明		
スロット	シャーシでサーバーが装着されているスロットを示します。スロット名は、1 ～16 の連番 ID で、シャーシでサーバーが装着されている場所を示します。		
Name	各スロットのサーバー名を表示します。		
存在	サーバーがスロットにあるかどうかを示します(ある または ない)。		
正常性		OK	サーバーが存在し CMC と通信していることを示します。CMC とサーバー間で通信エラーが発生した場合は、CMC でサーバーの正常性の状態を取得または表示できません。
		情報	正常性の状態(OK、警告、重大)に変化がない場合にサーバーについての情報を表示します。
		警告	警告アラートが発行されたこと、および対応処置を取る必要があることを示します。管理者が指定した時間内に対応処置を取らなかった場合は、サーバーの保全性に影響するような重要または重大なエラーを引き起こす可能性があります。
		重大	少なくとも 1 つのエラー警告が発行されたことを示します。重大な状態は CMC のシステム エラーを示し、直ちに対応処置を取る必要があります。
iDRAC ステータス	iDRAC に管理コントローラを内蔵するサーバーの状態を表示します。 l 該当なし - サーバーがない、またはシャーシの電源が入っていません l レディ - iDRAC が利用可能状態であり、正常に動作しています l 障害あり - iDRAC ファームウェアが破損しています。iDRAC ファームウェア更新ユーティリティを使ってファームウェアを修復します。 l エラー - iDRAC と通信できません。仮想装着チェックボックスを使ってエラーを消去します。これがうまくできない場合は、手動でサーバーを削除および交換してエラーを消去してください。 l FW 更新 - iDRAC ファームウェアを更新しています。更新が完了するまで別の操作をしないでください。 l 初期化 - iDRAC をリセットしています。コントローラの電源サイクルが完了するまで別の操作をしないでください。		
電源状態	サーバーの電源状態を表示します。 l 該当なし: CMC はサーバーの電源状態を特定できていません。 l オフ: サーバーまたはシャーシに電源がオフです。 l オン: シャーシおよびサーバーともに電源がオンです。 l 電源投入中 - 電源オフおよび電源オンの間の一時的な状態です。電源サイクルが完了すると、電源状態は オン になります。 l 電源切断中 - 電源オンおよび電源オフの間の一時的な状態です。電源サイクルが完了すると、電源状態は オフ になります。		
仮想装着	チェックボックスを選択して仮想にサーバーの抜き差しを行います。		

6. サーバーを仮想で抜き差しするには、サーバーの抜き差しチェックボックスを選択して 選択の適用 を選択します。この操作を行うと、サーバーの抜き差し動作が可能になります。
7. CMC のリセット / フェイルオーバーを選択すると、アクティブ CMC をリセットします。スタンバイ CMC が存在し、シャーシが完全冗長化されている場合は、フェイルオーバーが発生し、スタンバイ CMC がアクティブになります。

ネットワークタイムプロトコル (NTP) 問題のトラブルシューティング

CMC をネットワーク経由でリモートタイムサーバーの時間と同期するよう設定した後は、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。その後も変更されない場合は、トラブルシューティングを行ってください。CMC が時計と同期しない理由には以下が考えられます。

- NTP Server 1、NTP Server 2、NTP Server 3 の設定に問題がある
- 間違ったホスト名または IP アドレスが入力された
- ネットワークに CMC と設定された NTP サーバーとの通信を妨げる接続性の問題がある
- NTP サーバーホストの解決を妨げる DNS の問題がある

CMC は、このような問題を解決するためのツール、およびトラブルシューティングの貴重な情報源となる CMC トレース ログを提供しています。このログには、NTP に関連するエラーに関するエラー メッセージが含まれます。CMC が設定されているリモート NTP サーバーのいずれかと同期できない場合は、ローカル システム クロックからそのタイミングを取得します。

CMC がリモートタイムサーバーではなくてローカルシステムクロックと同期する場合は、トレースログに以下のような情報が記録されます。

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

次の racadm コマンドを入力することで、ntpd ステータスを確認することもできます。

```
racadm getractime –n
```

設定されているいずれかのサーバーに対して '*' が表示されていない場合は、設定が正しくない可能性があります。上記コマンドの出力には、サーバーが同期しない原因をデバッグする場合に役立つ詳細な NTP 統計も含まれています。Windows ベースの NTP サーバーを設定しようとする場合は、ntpd の MaxDist パラメータを増やすと問題が解決される場合があります。このパラメータを変更する場合は、事前に変更に伴う影響について読んで理解しておいてください。特に、デフォルト設定は、ほとんどの NTP サーバーを動作するのに十分な大きさを持っています。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
```

変更後は、NTP を無効にして ntpd を再起動し、5～10 秒後に NTP を再度有効にします。

メモ: NTP を再同期するにはさらに 3 分かかることがあります。

NTP を無効にするには、次を入力します。

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpEnable 0
```

NTP を有効にするには、次を入力します。

```
racadm config –g cfgRemoteHosts –o cfgRhostsNtpEnable 1
```

NTP サーバーの構成が正しいはずなのに、この情報がトレース ログに記録されている場合は、CMC が設定されているどの NTP サーバーとも同期できないということになります。

他の NTP 関連のトレースログがあれば、問題解決に役立ちます。NTP サーバーの IP アドレス設定ミスの場合は、以下のような記録が残されます。

```
Jan 8 19:59:24 cmc ntpd[1423]: Cannot find existing interface for address 1.2.3.4 Jan 8 19:59:24 cmc ntpd[1423]: configuration of 1.2.3.4
failed
```

NTP サーバーの設定に間違ったホスト名があると、以下のようなトレース ログが記録されます。

```
Aug 21 14:34:27 cmc ntpd_initres[1298]: host name not found: blabla Aug 21 14:34:27 cmc ntpd_initres[1298]: couldn't resolve `blabla', giving
up on it
```

CMC GUI から gettracelog コマンドを入力して トレースログを表示する方法については、「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、色および点滅 / 点滅なしで情報を提供します。

- 緑色の LED の点灯は、コンポーネントの電源がオンであることを示します。緑色の LED の点滅は、ファームウェアアップデートなど、重要ではあるが日常的なイベントを示します。この間、装

置は作動していません。これはエラーではありません。

- モジュール上のオレンジの LED の点滅は、モジュールのエラーを示します。
- 青色の LED の点滅は、ユーザーが設定可能で、識別に利用できます（「シャーシ上のコンポーネントを識別するための LED の設定」を参照）。

表11-14 は、シャーシ上の一般的な LED パターンを記載しています。

表 11-14 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	意味
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、無灯	電源オフ
	青色、点灯	マスター / プライマリ
	青色、点滅	ユーザー設定のモジュールの識別
	オレンジ色、点灯	不使用
	黄色の点滅	エラー
	青色、無灯	スレーブ / スタンバイ
iKVM	緑色、点灯	電源オン
	緑色、点滅	ファームウェアのアップロード中
	緑色、無灯	電源オフ
	オレンジ色、点灯	不使用
	黄色の点滅	エラー
	オレンジ色、無灯	エラーなし
サーバー	緑色、点灯	電源オン
	緑色、点滅	ファームウェアのアップロード中
	緑色、無灯	電源オフ
	青色、点灯	標準
	青色、点滅	ユーザー設定のモジュールの識別
	オレンジ色、点灯	不使用
	黄色の点滅	エラー
	青色、無灯	エラーなし
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、無灯	電源オフ
	青色、点灯	正常 / スタックマスター
	青色、点滅	ユーザー設定のモジュールの識別
	オレンジ色、点灯	不使用
	黄色の点滅	エラー
	青色、無灯	エラーなし / スタックスレーブ
IOM（パススルー）	緑色、点灯	電源オン
	緑色、点滅	不使用
	緑色、無灯	電源オフ
	青色、点灯	標準
	青色、点滅	ユーザー設定のモジュールの識別
	オレンジ色、点灯	不使用
	黄色の点滅	エラー
	青色、無灯	エラーなし
ファン	緑色、点灯	ファン作動中
	緑色、点滅	不使用
	緑色、無灯	電源オフ
	オレンジ色、点灯	ファンタイプを認識できません、CMC ファームウェアをアップデートしてください。
	黄色の点滅	ファンエラー。タコメーターの範囲外です。
	オレンジ色、無灯	不使用

PSU	(楕円)緑色、点灯	AC OK
	(楕円)緑色、点滅	不使用
	(楕円)緑色、無灯	AC エラー
	オレンジ色、点灯	不使用
	黄色の点滅	エラー
	オレンジ色、無灯	エラーなし
	(円)緑色、点灯	DC OK
	(円)緑色、無灯	DC エラー

無応答 CMC のトラブルシューティング

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。

どのインタフェース(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 を観察し、DB-9 シリアルポートを使ってリカバリ情報を取得するか、CMC ファームウェアイメージを回復することで、CMC の機能性を確認できます。

LED を観察して問題を特定する

シャーシに取り付けられている CMC の前面に向かって、カードの左側に LED が 2 つあります。

上部の LED — 上部の緑の LED は電源の状態を示します。オンでない場合:

1. AC 電源があり、少なくとも 1 台の電源装置があることを確認してください。
2. CMC カードが正しく取り付けられていることを確認してください。取り出しハンドルを引き、CMC を取り外してから挿入し直し、ボードがしっかり挿入されて、ラッチが正しく閉まっていることを確認します。

下部の LED — 下部の LED はマルチカラーです。CMC がアクティブで作動しており、問題がないときは青色です。問題が検出されると、オレンジ色になります。これらの問題は、次の 3 つのいずれかのイベントによって引き起こされたものです。

- コアエラー この場合、CMC ボードを取り替える必要があります。
- セルフテストエラー この場合、CMC ボードを取り替える必要があります。
- イメージの破損 このエラーは、CMC ファームウェアイメージをアップロードすることで回復できます。

メモ: 標準の CMC 起動およびリセットには、CMC が OS に完全に読み込まれ、ログインできるまでに 1 分以上かかります。アクティブ CMC では青色 LED が点灯しています。冗長 2 台の CMC 構成の場合は、スタンバイ CMC では上部の緑色の LED だけが点灯しています。

リカバリ情報は DB-9 シリアルポートから入手します。

下部の LED がオレンジ色の場合、リカバリ情報が CMC の前面にある DB-9 シリアル ポートから利用できます。

リカバリ情報を得るには:

1. CMC とクライアントコンピュータの間に NULL モデムケーブルを取り付けます。
2. 任意のターミナルエミュレータ(ハイパーターミナル や Minicom など)を開けます。8 ビット、パリティなし、フロー制御なし、ボーレート 115200 に設定します。

   5 秒おきにコアメモリエラーのエラーメッセージが表示されます。
3. <Enter> を押します。リカバリ プロンプトが表示されたら、追加情報が利用できます。プロンプトはCMC スロット番号とエラータイプを示します。

   問題の原因といくつかのコマンドの構文を表示するには、次を入力します。

```
recover
```

その後 <Enter> を押します。プロンプト例:

```
recover1[セルフテスト] CMC 1 セルフテストエラー

recover2[ファームウェアイメージ不良] CMC2 のイメージが破損しています。
```

- プロンプトがセルフテストエラーを示している場合、CMC 上には修理可能なコンポーネントはありません。この CMC は故障しているため、デルに返品する必要があります。
- プロンプトが FW イメージ不良 を示している場合は、「ファームウェアイメージのリカバリ」の手順に従って問題を解決してください。

ファームウェアイメージのリカバリ

CMC は、正常な CMC OS 起動が可能でない場合、リカバリモードになります。リカバリモードでは、少数のコマンドのサブセットを使用してファームウェアアップデートファイルの **firmimg.cmc** をアップロードすることでフラッシュデバイスを再プログラムできます。これは、正常のファームウェアアップデートで使用されるのと同じファームウェアイメージファイルです。リカバリプロセスでは、現在の進行状況を示し、回復が完了後、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:

```
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 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、CMC を ping することはできません。recover ping <TFTP サーバー IP アドレス> 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 後にrecover reset コマンドを使う必要があるかもしれません。

ネットワーク問題のトラブルシューティング

内部 CMC トレースログを使うと、CMC の警告とネットワークのデバッグを行うことができます。CMC ウェブインタフェース(「診断コンソールの使用」を参照)または RACADM (「RACADM コマンドラインインタフェースの使用」および「Dell Chassis Management Controller 管理者リファレンスガイド」の gettracelog コマンドを参照)を使ってトレースログにアクセスできます。

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したパケットを追跡します。
- DDNS — DNS の動的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。

パスワードを忘れたとき

注意: 修理作業の多くは、認定されたサービス技術者のみが行うことができます。お客様は、製品マニュアルで許可されている範囲に限り、またはオンラインサービスもしくはテレホンサービスとサポートチームの指示によってのみ、トラブルシューティングと簡単な修理を行うことができます。デルで認められていない修理(内部作業)による損傷は、保証の対象となりません。製品に付属のマニュアルに書かれている、安全にお使いいただくための注意をお読みになり、指示に従ってください。

管理操作を行うには、システム管理者 の権限が必要となります。CMC ソフトウェアには、ユーザーアカウントをパスワード保護するセキュリティ機能が搭載されていますが、システム管理者アカウントのパスワードをお忘れになった場合、この機能を無効にすることができます。システム管理者アカウントのパスワードを忘れた場合、CMC ボードの PASSWORD_RSET ジャンパを利用して回復することができます。

CMC ボードには、「図11-1」で示すように、2 ピンのパスワードリセットコネクタが搭載されています。リセットコネクタにジャンパが取り付けられている場合、デフォルトのシステム管理者アカウントおよびパスワードが有効になり、ユーザー名: root および パスワード: calvin に設定されます。システム管理者アカウントは、アカウントが削除された場合やパスワードが変更された場合でも、リセットされます。

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

1. ハンドルに付いている CMC リリースラッチを押し、ハンドルを回してモジュールの前面パネルから離します。CMC モジュールをエンクロージャから引き出します。

メモ: 静電気放出(ESD)によって装置内部の電子部品が損傷する恐れがあります。その状況によっては、ESD は人体や物体に蓄積され、CMC などの別の物体に放出されることがあります。ESD による損傷を防ぐには、装置内部の電子部品に触れる前に、静電気を身体から逃がしてください。

2. パスワードリセットコネクタからジャンパプラグを取り外し、2 ピンのジャンパを取り付けて、デフォルトのシステム管理者アカウントを有効にします。CMC ボード上のパスワードジャンパの位置については、「図11-1」を参照してください。

図 11-1 パスワードリセットジャンパの位置

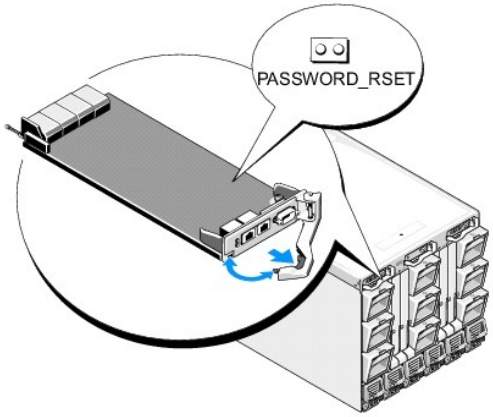


表 11-15 CMC パスワードジャンパの設定

PASSWORD_RSET	(デフォルト)	パスワードリセット機能は無効です。
		パスワードリセット機能は有効です。

3. CMC モジュールをエンクロージャの中に入れます。切断したケーブルをすべて再接続します。
4. GUI インターフェースを利用して次の手順に従い、モジュールをアクティブにします。
   a. シャーシ ページに移動し、電源管理 タブの 制御 サブタブをクリックします。
   b. CMC のリセット(ウォームブート) ボタンを選択します。
   c. 適用 をクリックします。
5. CMC が自動的に冗長モジュールにフェールオーバーし、そのモジュールがアクティブになります。デフォルトのシステム管理者ユーザー名(root)およびパスワード(calvin)を使用してアクティブな CMC にログインします。必要に応じて、ユーザーアカウントの設定を復元します。既存のアカウントおよびパスワードは無効にならず、アクティブなままとなります。

アカウントの更新を完了したら、2 ピンジャンパを取り外し、ジャンパプラグを元に戻します。

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

1. ハンドルに付いている CMC リリースラッチを押し、ハンドルを回してモジュールの前面パネルから離します。CMC モジュールをエンクロージャから引き出します。
2. 2 ピンジャンパを取り外し、ジャンパプラグを元に戻します。

3. CMC モジュールをエンクロージャの中に入れます。切断したケーブルをすべて再接続します。

トラブルシューティング警告

CMC 警告のトラブルシューティングを行う際は、CMC ログおよびトレースログを使用します。電子メールまたは SNMP トラップの配信のすべての試み（成功または失敗）は、CMC ログに記録されます。特定のエラーに関する追加情報は、トレースログに記録されます。ただし、SNMP ではトラップの配信を確認できないため、ネットワークアナライザや Microsoft の **snmputil** などのツールを使って、管理下システム上のパケットをトレースすることをお勧めします。

ウェブインタフェースを使って SNMP 警告の設定を行うことができます。詳細については、「SNMP アラートの設定」を参照してください。

目次ページに戻る

目次ページに戻る

CMC ウェブインタフェースの使用

Dell™ Chassis Management Controllerファームウェアバージョン 2.10 ユーザーガイド

CMC は、CMC プロパティとユーザーの設定、リモート管理タスクの実行、障害に対してリモート（管理下）システムのトラブルシューティングが可能なウェブ インタフェースを提供します。日常のシャーシ管理には CMC ウェブインタフェースをご使用ください。本章では、CMC ウェブインタフェースを使って一般的なシャーシ管理タスクを行う方法について説明します。

すべての設定タスクはローカル RACADM コマンドまたはコマンド ライン コンソール（シリアル コンソール、Telnet、または SSH）を使って実行することもできます。ローカル RACADM の使用方法については、「RACADM コマンドラインインタフェースの使用」を参照してください。コマンドラインコンソールの使用方法については、「CMC にコマンドラインコンソールの使用を設定する方法」を参照してください。

メモ: Microsoft® Internet Explorer® でプロキシを通して接続する際、エラーメッセージ「XML ページを表示できません」が表示される場合、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へのアクセス

IPv4 経由で CMC ウェブインタフェースにアクセスするには

1. サポートされているウェブブラウザのウィンドウを開きます。

   対応ウェブブラウザの最新情報については、**デルサポートサイト** support.dell.com にある『Dell システム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。

   `https://<CMC の IP アドレス>`

   デフォルトの HTTPS ポート番号（ポート 443）が変更されている場合は、次のように入力します。

   `https://<CMC の IPアドレス>:<ポート番号>`

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

   CMC のログイン ページが表示されます。

IPv6 経由で CMC ウェブインタフェースにアクセスするには

1. サポートされているウェブブラウザのウィンドウを開きます。

対応ウェブブラウザの最新情報については、**デルサポートサイト** support.dell.com にある『Dell システム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。

   `https://[<CMC の IPアドレス>]`

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

   デフォルト値（443）をまだ使用している場合は、URL で HTTPS ポート番号を指定しなくてもかまいません。そうでない場合は、ポート番号を指定してください。ポート番号が指定された IPv6 CMC URL の構文は以下のとおりです。

   `https://[<CMC の IP アドレス>]:<ポート番号>`

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

   CMC の **ログイン ページ**が表示されます。

ログイン

メモ: 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。

メモ: デフォルトの CMC ユーザー名は **root**、パスワードは **calvin** です。 root アカウントは、CMC に付属のデフォルト管理者アカウントです。セキュリティを強化するために、初期セットアップ中に 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。

メモ: CMC では、, , , などの拡張 ASCII 文字、および英語以外の言語で主に使用されるその他の文字がサポートされていません。

メモ: 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。

CMC ユーザーまたは Microsoft® Active Directory® ユーザーとしてログインしてください。

ログインするには:

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

   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. Password（パスワード）フィールドに CMC ユーザーパスワードまたは Active Directory ユーザーパスワードを入力します。

   メモ: このフィールドでは大文字と小文字が区別されます。

3. OK をクリックするか、Enter キーを押します。

ログアウト

ウェブインタフェースにログインした後、各ページの右上の角にある ログアウト をクリックすることでいつでもログアウトできます。

メモ: ページ上で入力した設定や情報は忘れず適用（保存）してください。変更を適用せずにログアウトしたりそのページから移動すると、変更内容は失われます。

CMC の基本設定

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使用する名前を設定できます。（デフォルト名は「Dell Rack System」です。）たとえば、シャーシ名の SNMP クエリでが、ここで設定した名前が返されます。

シャーシ名を設定するには：

1. CMC ウェブインタフェースにログインします。コンポーネントの正常性 ページが表示されます。
2. セットアップ タブをクリックします。シャーシ一般設定 ページが表示されます。
3. シャーシ名 フィールドに新しい名前を入力して、適用 をクリックします。

CMC の日時の設定

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

1. CMC ウェブインタフェースにログインします。コンポーネントの正常性 ページが表示されます。
2. セットアップタブをクリックします。シャーシ一般設定 ページが表示されます。
3. 日付 / 時刻 サブタブをクリックします。日付 / 時刻 ページが表示されます。
4. 日付および時刻をネットワーク時間プロトコル (NTP) サーバーと同期させるには、NTP を有効にするをチェックして、最大3台まで NTPサーバーを指定します。
5. 日付や時刻を手動で設定するには、, NTP を有効にするのチェックを外して、日付と時刻フィールドを編集し、ドロップダウンメニューからタイムゾーンを選択して適用をクリックします。

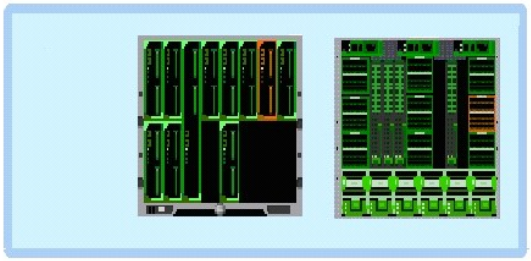
コマンドラインインタフェースを使って日付と時刻を設定するには、『Dell Chassis Management Controller 管理者リファレンスガイド』の `config` コマンドと `cfgRemoteHosts` データベースプロパティグループの項を参照してください。

システム正常性状態の監視

シャーシとコンポーネント概要の表示

CMC はシャーシのグラフィック表示を シャーシグラフィックス ページに表示し、取り付けられたコンポーネントのステータスの概要を視覚的に提供します。シャーシグラフィックス ページは動的に更新され、現在の状態を反映するようにコンポーネントサブグラフィックの色およびテキストヒントも自動的に変更されます。

図 5-1 ウェブインタフェースにおけるシャーシグラフィックスの例



コンポーネンの正常性ページは、シャーシ、プライマリおよびスタンドバイ CMC、サーバーモジュール、IO モジュール (IMO)、ファン、iKVM、電源 (PUS)、および温度センサの全体的な健康状態を表示します。シャーシサマリ ページは、シャーシ、プライマリおよびスタンバイ CMC、iKVM および IOM のテキストベースの概要を提供します。シャーシおよびコンポーネントの概要を表示する手順については、「シャーシサマリの表示」を参照してください。

シャーシとコンポーネントの正常性状態の表示

シャーシグラフィックス ページは、シャーシの正面および背面図を表示します。この表示により、シャーシに内蔵されたコンポーネントおよびステータスの概要を視覚的に把握することができます。

コンポーネントの正常性 ページでは、すべてのシャーシコンポーネントの全般的な正常性状態が表示されます。シャーシグラフィックスおよびコンポーネントの正常性状態を表示する手順については、「シャーシとコンポーネントの正常性状態の表示」を参照してください。

電力バジェット状態の表示

電力バジェット状態 ページには、シャーシ、サーバー、およびシャーシ電源装置の電力バジェット状態が表示されます。

電力バジェット状態を表示する手順については、「消費電力ステータスの表示」を参照してください。CMC 電源管理の詳細については、「Power Management」を参照してください。

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、次の手順で簡単に入手することができます。

- システム ツリーで サーバー を展開します。展開されたサーバーリストにすべてのサーバー（0 ～16）が表示されます。サーバーなしのスロットは名前が灰色で表示されます。
- カーソルをサーバーのスロット名またはスロット番号の上に重ねると、ツールヒントとしてサーバーのモデル名とサービス タグ番号が表示されます（あれば）。

すべてのサーバーの正常性状態の表示

すべてのサーバーの正常性状態は、2 つの方法で表示することができます。1 つはシャーシステータス ページの シャーシグラフィックス セクション、もう 1 つは サーバーステータス ページ。シャーシグラフィックス には、シャーシに取り付けられたすべてのサーバーの概略図が表示されます。。

シャーシグラフィックスを使用してすべてのサーバーの正常性状態を表示するには

1. CMC ウェブインタフェースにログインします。
2. シャーシステータス ページが表示されます。シャーシグラフィックスの中央のセクションには、シャーシの正面図とすべてのサーバーの正常性状態が表示されます。サーバーの正常性は、サーバーサブグラフィックの色で示されます。
   - 緑色 - サーバーが存在し、電源がオンで CMC と通信中。悪条件の兆候なし。
   - 黄色 - サーバーが存在し、電源がオンまたはオフで、CMC と通信中または通信しておらず。悪条件が存在する可能性あり。
   - 灰色 - サーバーが存在し、電源がオフ。CMC と通信しておらず、悪条件の兆候なし。

サーバーステータス ページには、シャーシ内のサーバーの概要が表示されます。

すべてのサーバーの正常性状態を表示するには：

1. CMC ウェブインタフェースにログインします。
2. システムツリーで サーバー を選択します。サーバーステータス ページが表示されます。

表5-1 では、サーバーステータス ページに表示される情報の説明を提供しています。

項目	説明
スロット	サーバーの場所を表示します。スロット番号はシャーシ内の場所に基づいてサーバーを識別するシリアル番号です。
Name	サーバー名を示します。サーバー名はデフォルトで スロット名（SLOT-01 ～ SLOT-16）によって識別されます。

	メモ: サーバー名はデフォルトから変更できます。手順については、「"スロット名の編集"」を参照してください。		
Model	サーバーのモデル名を表示します。このフィールドが空白の場合は、サーバーは存在しません。このフィールドに # の拡張子（ここで、# の値は 1～8）が表示された場合は、その番号 # がマルチスロットサーバーの主なスロットになります。		
正常性		OK	サーバーが存在し CMC と通信していることを示します。
		情報	正常性の状態に変化がない場合は、サーバーに関する情報が表示されます。
		警告	警告アラートが発行されたこと、および対応処置を取る必要があることを示します。 システム管理者が指定した時間内に対応処置を取らなかった場合は、デバイスの保全性に影響するような重要または重大なエラーを引き起こす可能性があります。
		重大	少なくとも 1 つのエラー警告が発行されたことを示します。重大な状態はサーバーのシステムエラーを示し、直ちに対応処置を取る必要があります。
		値なし	サーバーがスロットにない場合は、正常性情報は表示されません。
iDRAC GUI の起動		アイコンを左クリックして、新しいブラウザウィンドウまたはタブでサーバー用の iDRAC 管理コンソールを起動します。このアイコンは、サーバーに対して次のすべての条件を満たした場合に限り表示されます。 1. サーバーが存在する 2. シャーシの電源が入っている 3. サーバーの LAN インターフェースが有効である **メモ:** サーバーがシャーシから取り外された、iDRAC の IP アドレスが変更された、または iDRAC のネットワーク接続に問題が発生した場合は、Launch iDRAC GUI アイコンをクリックすると、iDRAC LAN インターフェースのエラーページが表示される場合があります。	
電源状態	シャーシの電源状態を示します。 - 該当なし: CMC はサーバーの電源状態を特定していません。 - オフ - サーバーまたはシャーシのどちらかの電源がオフです。 - オン - シャーシおよびサーバーともに電源がオンです。 - 電源投入中 - 電源オフおよび電源オンの間の一時的な状態です。操作が完了すると、電源状態は オン になります。 - 電源切断中 - 電源オンおよび電源オフの間の一時的な状態です。操作が完了すると、電源状態は オフ になります。		
サービスタグ	サーバーのサービスタグを表示します。サービスタグはサポートとメンテナンスのためにメーカーが提供する一意の識別子です。サーバーが不在の場合、このフィールドは空になります。		

iDRAC 管理コンソールを起動する方法とシングルサインオンポリシーの詳細については、「シングルサインオンを使って iDRAC を起動する」を参照してください。

スロット名の編集

スロット名 ページでは、シャーシのスロット名を更新できます。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、二重引用符（"、ASCII 34）を除く印刷可能な最大 15 文字の ASCII 文字（ASCII コード 32～126）のみ使用できます。RACADM コマンドで特殊文字（~!@#$%^&*）を使用してスロット名を変更する場合は、CMC に正常に引き渡すためには、名前文字列を二重引用符で囲む必要があります。
- スロット名はシャーシ内で一意でなければなりません。複数のスロットに同じ名前を割り当てることはできません。
- スロット名では大文字と小文字は区別されません。Server-1、server-1、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-
  - KVMKVM
  - DRAC-
  - MC-
  - Chassis
  - Housing-Left
  - Housing-Right
  - Housing-Center

- Server-1 から Server-16 までの文字列を使用することはできますが、対応するスロットに割り当てる必要があります。たとえば、Server-3 はスロット 3 では有効ですが、スロット 4 では無効です。ただし、Server-03 は、どのスロットに対しても有効な名前です。

メモ: スロット名の変更には シャーシ設定管理者 の権限が必要です。

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

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

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

スロット名を編集するには:

1. CMC ウェブインタフェースにログインします。
2. システムツリーの シャーシ メニューで サーバー を選択します。
3. 設定タブからスロット名のタブをクリックします。スロット名 ページが表示されます。
4. スロット名 フィールドにスロットの新しい名前を入力します。名前を変更するスロットすべてに対してこの操作を繰り返します。
5. 適用 をクリックします。
6. サーバーに対してデフォルトのスロット名 (サーバーのスロット位置に応じて SLOT-01 ～ SLOT-16) に戻すには、デフォルト値に戻すを押します。

サーバーの First Boot Device（最初の起動デバイス）の設定

最初の起動デバイス ページでは、各サーバーの CMC の最初の起動デバイスを指定できます。これは対象のサーバーの実際の最初の起動デバイスではない場合があり、またそのサーバー上に存在するデバイスではない場合もあります。これは、そのサーバーに関して、CMC がサーバーへ送信するデバイスで、最初の起動デバイスとして利用するデバイスを表しています。

デフォルト起動デバイスを設定できるほか、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特別なイメージから起動できるように、1 回限りの起動デバイスを設定することも可能です。

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。 表5-2 に、指定できる起動デバイスをリストします。

表 5-2 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	サーバーのハードドライブから起動します。
ローカル CD/DVD	サーバー上の CD/DVD ドライブから起動します。
仮想フロッピー	仮想フロッピードライブから起動します。フロッピードライブ（またはフロッピーディスクイメージ）は管理ネットワーク上の別のコンピュータ上にあり、iDRAC GUI コンソールビューアで接続されます。
仮想 CD/DVD	仮想 CD/DVD ドライブまたは CD/DVD ISO イメージから起動します。この光学式ドライブまたは ISO イメージファイルは管理ネットワーク上の別のコンピュータまたはディスク上にあり、iDRAC GUI コンソールビューアで接続されます。
iSCSI	インターネット SCSI（小型コンピュータシステムインタフェース）から起動します。
ローカル SD カード	ローカル SD （セキュア デジタル）カードから起動します。M610/M710/M805/M905 システムにのみ対応しています。
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。

メモ: サーバー用の最初の起動デバイスを設定するには、**サーバー管理者**の権限またはシャーシ設定システム管理者の権限が必要で、 iDRAC にログインする必要があります。

シャーシ内の一部またはすべてのサーバーの第 1 起動デバイスを設定するには、以下の手順を実行します。

1. CMC ウェブインタフェースにログインします。
2. システムツリーの **サーバー** をクリックし、次に **セットアップ→ 最初の 起動デバイスの導入** の順にクリックします。サーバーのリストが 1 行に 1 台ずつ表示されます。

3. リストボックスから、各サーバーで使用する起動デバイス を選択します。
4. サーバーを起動するたびに選択したデバイスから起動するには、そのサーバーの **ブートワンス**チェックボックスのチェックを外します。

   次回のみ選択したデバイスから起動するには、そのサーバーの **ブートワンス**チェックボックスを選択します。
5. **適用** をクリックします。

個別のサーバーの正常性状態の表示

個々のサーバーの正常性状態は、2 つの方法で表示することができます。1 つはシャーシステータス ページの シャーシグラフィックス セクション、もう 1 つは サーバーステータス ページです。

シャーシグラフィックス ページは、シャーシに取り付けられた個別サーバーのグラフィック表示を提供します。

シャーシグラフィックスを使用して個別サーバーの正常性状態を表示するには

1. CMC ウェブインタフェースにログインします。
2. シャーシステータス ページが表示されます。シャーシグラフィックスの中央のセクションは、シャーシの前面図を表しており、個別サーバーの正常性状態が含まれます。サーバーの正常性は、サーバーサブグラフィックの色で示されます。
   - 緑色 - サーバーが存在し、電源がオンで CMC と通信中。悪条件の兆候なし。
   - 黄色 - サーバーが存在し、電源がオンまたはオフで、CMC と通信中または通信しておらず。悪条件が存在する可能性あり。
   - 灰色 - サーバーが存在し、電源がオフ。CMC と通信しておらず、悪条件の兆候なし。
3. 個別のサーバーサブグラフィックにマウスのカーソルを移動すると、該当するテキストヒントまたは画面ヒントが表示されます。テキストヒントは、対象サーバーに関する追加情報を提供します。
4. サーバーサブグラフィックは、該当する CMC GUI ページにハイパーリンク付けされ、対象のサーバーのサーバーステータスページに瞬時に移動することができます。

サーバーステータス ページ（サーバー ステータス ページとは別）には、サーバーの概要、およびサーバーの管理に使用されるファームウェアである Integrated Dell Remote Access Controller (iDRAC) 用のウェブインタフェースの起動ポイントが表示されます。

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

個別のサーバーの正常性状態を表示するには:

1. CMC ウェブインタフェースにログインします。
2. システムツリーで拡張 サーバー を選択します。すべてのサーバー (1 ～16) が展開されたサーバーリストに表示されます。
3. 表示するサーバー（スロット）をクリックします。サーバーステータス ページが表示されます。

表5-3 から 表5-8 では、サーバーステータス ページに表示される情報を説明しています。

項目	説明		
スロット	シャーシでサーバーが装着されているスロットを示します。スロット番号は 1～16（シャーシには使用できるスロットが 16 個あります）の連番 ID で、シャーシのサーバーの場所を識別します。		
スロット名	サーバーがあるスロットの名前を示します。		
存在	サーバーがスロットにあるかどうかを示します（はい または いいえ）。サーバーが不在の場合、サーバーの正常性、電源状態、サービスタグ情報 は不明です（表示されません）。		
正常性		OK	サーバーが存在し CMC と通信していることを示します。CMC とサーバー間で通信エラーが発生した場合は、CMC でサーバーの正常性の状態を取得または表示できません。
		情報	正常性の状態（OK、警告、重大）に変化がない場合にサーバーについての情報を表示します。

		警告	警告アラートが発行されたこと、および対応処置を取る必要があることを示します。 システム管理者が指定した時間内に対応処置を取らなかった場合は、サーバーの保全性に影響するような重要または重大なエラーを引き起こす可能性があります。
		重大	少なくとも 1 つのエラー警告が発行されたことを示します。重大な状態はサーバーのシステムエラーを示し、直ちに対応処置を取る必要があります。
		値なし	サーバーがスロットにない場合は、正常性情報は表示されません。
サーバーモデル	シャーシ内のサーバーのモデルを示します。例：PowerEdge M600 および PowerEdge M605		
サービスタグ	サーバーのサービスタグを表示します。サービスタグはサポートとメンテナンス用にデルが提供する一意の識別子です。サーバーが不在の場合、このフィールドは空になります。		
iDRAC ファームウェア	現在サーバーに設置されている iDRAC のバージョン。		
CPLD バージョン	サーバーの Complex Programmable Logic Device（CPLD）のバージョン番号を表示します。		
BIOS バージョン	サーバーの BIOS バージョン を示します。		
OS	サーバーのオペレーティングシステムを示します。		

表 5-4 個別サーバーステータス - iDRAC システムイベントログ

項目	説明		
重大度		OK	修正処置を必要としない正常なイベントを示します。
		情報	重大度 の状態が変化していないイベントに関する情報のエントリを示します。
		不明	不明 / 未分類のイベントを示します。
		警告	システムエラーを防ぐために 早めに修正処置を講じる必要のある非重要イベントを示します。
		重大	システムエラーを防ぐために直ちに修正処置を講じる必要のある 重要イベントを示します。
日時	イベントが発生した正確な日時を示します（例：2007 年5 月 2 日 16 時 26 分 55 秒）。		
説明	イベントの簡単な説明を示します。		

項目	説明
LAN 有効	LAN チャンネルが有効 (オン) と無効 (オフ) のどちらであるかを示します。

項目	説明
有効	IPv4 プロトコルが LAN 上で使用されている（オン）かどうかを示します。サーバーで IPv6 がサポートされていない場合、IPv4 プロトコルは常に有効になり、この設定は表示されません。
DHCP 有効	DHCP (動的ホスト設定プロトコル) が有効 (Yes) または無効 (No) のどちらであるか示します。 このオプションが有効 (Yes)の場合、サーバーは IP 設定（IP アドレス、サブネットマスク、ゲートウェイ）をネットワーク上の DHCP サーバーから自動的に取得します。サーバーには常に、ネットワーク上で割り当てられた固有の IP アドレスがあります。

IPMI over LAN を有効になっています	IPMI LAN チャンネルが有効（オン）または無効（オフ）のいずれかを示します。
IP アドレス	iDRAC ネットワーク インタフェースの IP アドレスを指定します。
サブネットマスク	iDRAC ネットワーク インタフェースのサブネットマスクを指定します。
ゲートウェイ	iDRAC ネットワーク インタフェースの ゲートウェイを指定します。

項目	説明
有効	IPv6 プロトコルが LAN 上で使用されている（オン）かどうかを示します。
自動設定の有効化	IPv6 の自動設定機能が有効（オン）であるかどうかを示します。 自動設定が有効である場合は、サーバーはネットワーク上の IPv6 ルータから IPv6 設定（**IPv6 アドレス、プレフィックス長、IPv6 ゲートウェイ**）を自動的に取得します。サーバーには常に、ネットワーク上で割り当てられた一意の IPv6 アドレスがあり、最大 16 の IPv6 アドレスを持つことができます。
リンクのローカルアドレス	CMC の MAC アドレスに基づいて CMC に割り当てられた IPv6 アドレス。
ゲートウェイ	iDRAC ネットワークインタフェースの IPv6 ゲートウェイを表示します。
IPv6 アドレス	iDRAC ネットワークインタフェースの IPv6 アドレスを表示します。最大 16 のアドレスを表示できます。プレフィックス長はゼロ以外の場合は、前方スラッシュ（"/"）の後に指定されます。

項目	説明
スロット	シャーシでサーバーが装着されているスロットを表示します。
場所	入出力モジュールが装着されている場所を表示します。グループ名（A、B、または C）およびスロット番号（1 または 2）の組み合わせで 6 箇所が識別されます。ロケーション名：A1、A2、B1、B2、C1、または C2
ファブリック	入出力ファブリックの種類を表示します。
サーバー指定	コントローラのハードウェアに埋め込まれたサーバー指定の WWN/MAC アドレスを表示します。「該当なし」を表示する WWN/MAC アドレスは、指定されたファブリック用のインタフェースがインストールされていないことを示します。
シャーシ指定	特定のスロットで使用されるシャーシ指定の WWN/MAC アドレスを表示します。「該当なし」を表示する WWN/MAC アドレスは、FlexAddress 機能がインストールされていないことを示します。 **メモ：** サーバー指定 または シャーシ指定 のカラムの緑色のチェックマークは、アクティブなアドレスの種類を示します。 **メモ：** FlexAddress を有効にすると、サーバーがインストールされていないスロットに、内蔵型 Ethernet コントローラー (ファブリック A) に対するシャーシ指定 MAC/WWN 割り当てを表示します。スロットに装着されたサーバーでファブリックを使用しない限り、ファブリック B および C 用のシャーシ指定アドレスに「該当なし」を表示します。これは、未使用のスロットに同じタイプのファブリックを使用することを仮定しています。

iDRAC 管理コンソールを起動する方法とシングルサインオンポリシーの詳細については、「シングルサインオンを使って iDRAC を起動する」を参照してください。

IOM の正常性状態の表示

IOM の正常性の状態は、2 つの方法で確認することができます。1 つは シャーシステータス ページの シャーシグラフィックス セクション、もう 1 つは I/O モジュールステータス ページです。シャーシグラフィックス ページには、シャーシに取り付けられた IOM の図が表示されます。

シャーシグラフィックスを使用して IOM の正常性の状態を閲覧するには

1. CMC ウェブインタフェースにログインします。
2. シャーシステータス ページが表示されます。シャーシグラフィックス の右側のセクションには、シャーシの背面図と IOM の正常性の状態が表示されます。IOM の正常性の状態は、IOM のサブグラフィックの色で示されます。
   - 緑色 - IOM が存在し、電源がオンで CMC と通信中。悪条件の兆候はなし。
   - 黄色 - IOM が存在し、電源がオンまたはオフで、CMC と通信中または通信しておらず。悪条件が存在する可能性あり。
   - 灰色 - IOM が存在するが、電源がオフ。CMC と通信しておらず、悪条件の兆候なし。
3. 特定の IOM サブグラフィック上にカーソルを移動すると、該当するテキストヒントまたは画面ヒントが表示されます。テキストヒントは、IOM に関する追加情報を提供します。
4. IOM サブグラフィックは、該当する CMC GUI ページにハイパーリンクされ、対象の IOM と関連付けられた I/O モジュールステータス ページに即座に移動することができます。

I/O モジュールステータス ページには、シャーシに関連付けられているすべての IOM の概要が表示されます。ウェブインタフェースまたは RACADM を使って IOM の正常性を表示する手順は、「IOM 正常性の監視」 を参照してください。

ファンの正常性状態の表示

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

すべてのサーバーの正常性状態は、2 つの方法で表示することができます。1 つは シャーシステータス ページの シャーシグラフィックス セクション、もう 1 つは ファンステータス ページ。シャーシグラフィックス ページには、シャーシに取り付けられたファンの図が表示されます。シャーシグラフィックスを使用してすべてのファンの正常性状態を表示するには

1. CMC ウェブインタフェースにログインします。
2. シャーシステータス ページが表示されます。シャーシグラフィックスの中央のセクションには、シャーシの背面図とファンの正常性状態が表示されます。ファンの正常性状態は、ファンサブグラフィックの色で示されます。
   - 緑色 - ファンが存在し、電源がオンで CMC と通信中。悪条件の兆候なし。
   - 黄色 - ファンが存在し、電源がオンまたはオフで、CMC と通信中または通信しておらず。悪条件が存在する可能性あり。
   - 灰色 - ファンが存在し、電源がオフ。CMC と通信しておらず、悪条件の兆候なし。
3. 個別のファンサブグラフィックにマウスのカーソルを移動すると、該当するテキストヒントまたは画面ヒントが表示されます。テキストヒントは、対象ファンに関する追加情報を提供します。
4. ファンサブグラフィックは、該当する CMC GUI ページにハイパーリンク付けされ、ファンステータス ページに瞬時に移動することができます。

ファンス テータス ページには、シャーシ内のファンの状態と速度の測定値 (RPM) が表示されます。ファンは 1 台または複数台です。

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

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

ファン装置の正常性状態を表示するには

1. CMC ウェブインタフェースにログインします。
2. システムツリーで ファン を選択します。ファンステータス ページが表示されます。

表5-9 では、サーバーステータス ページに表示される情報の説明を提供しています。

項目	説明		
Name	ファンの名前を FAN-n 形式で表示します（n はファンの番号）。		
存在	ファン装置 が存在するかどうかを示します（**はい** または **いいえ**）。		
正常性		OK	ファン装置が存在し CMC と通信していることを示します。CMC とファン装置間で通信エラーが発生した場合は、CMC でファン装置の正常性状態を取得または表示できません。
		重大	少なくとも 1 つのエラー警告が発行されたことを示します。重大状態とは、ファン装置上のシステムの障害を示し、過熱やシステムのシャットダウンを避けるために 直ちに対応処置を取る必要があります。
		不明	シャーシが最初に電源が入ったときに表示されます。CMC とファン装置間で通信エラーが発生した場合は、CMC でファン装置の正常性状態を取得または表示できません。
速度	ファン内の速度を RPM で表示します。		

iKVM ステータスの表示

Dell M1000e サーバーシャーシのローカルアクセス KVM モジュールは Avocent® Integrated KVM Switch Module または iKVM と呼ばれます。シャーシに関連付けられた iKVM の正常性状態は、シャーシグラフィックス ページで閲覧できます。

シャーシグラフィックス を使用して iKVM の正常性状態を表示するには

1. CMC ウェブインタフェースにログインします。
2. シャーシステータス ページが表示されます。シャーシグラフィックスの中央のセクションには、シャーシの背面図と iKVM の正常性状態が表示されます。iKVM の正常性状態は、iKVM サブグラフィックの色で示されます。
   - 緑色 - iKVM が存在し、電源がオンで CMC と通信中。悪条件の兆候なし。
   - 黄色 - iKVM が存在し、電源がオンまたはオフで、CMC と通信中または通信しておらず。悪条件が存在する可能性あり。
   - 灰色 - iKVM が存在し、電源がオフ。CMC と通信しておらず、悪条件の兆候なし。
3. 個々の iKVM サブグラフィックにマウスのカーソルを重ねると、該当するテキストヒントまたは画面ヒントが表示されます。テキストヒントは、対象の iKVM に関する追加情報を提供します。
4. iKVM サブグラフィックは、該当する CMC GUI ページにハイパーリンクされており、iKVM ステータスページに即座に移動することができます。

iKVM ステータスの表示と iKVM のプロパティの設定手順については、以下を参照してください。

- 「iKVM のステータスとプロパティの表示」
- 「フロントパネルの有効または無効」
- 「iKVM を介した Dell CMC コンソールの有効化」
- 「iKVM ファームウェアのアップデート」

iKVM の詳細については、「iKVM モジュールの使用」を参照してください。

PSU の正常性状態の表示

シャーシに関連付けられた PSU の正常性状態は、シャーシステータス ページの シャーシグラフィックス セクションと 電源装置ステータス ページに表示できます。シャーシグラフィックス ページには、シャーシに取り付けられたすべての PSU の概略図が表示されます。

シャーシグラフィックス を使用してすべての PSU の正常性状態を表示するには

1. CMC ウェブインタフェースにログインします。
2. シャーシステータス ページが表示されます。シャーシグラフィックス の右側のセクションには、シャーシの背面図とすべての PSU の正常性状態が表示されます。PSU の正常性状態は、PSU サブグラフィックの色で示されます。
   - 緑色 - PSU が存在し、電源がオンで CMC と通信中。悪条件の兆候なし。
   - 黄色 - PSU が存在し、電源がオンまたはオフで、CMC と通信中または通信しておらず。悪条件が存在する可能性あり。
   - 灰色 - PSU が存在し、電源がオフ。CMC と通信しておらず、悪条件の兆候なし。
3. 個別の PSU サブグラフィック上にマウスのカーソルを移動すると、該当するテキストヒントまたは画面ヒントが表示されます。テキストヒントは、対象 PSU に関する追加情報を提供します。
4. PSU サブグラフィックは、該当する CMC GUI ページにハイパーリンクされており、すべての PSU の 電源装置ステータス ページに即座に移動できます。

電源装置ステータス ページには、シャーシに関連付けられている PSU の状態が表示されます。CMC 電力管理の詳細については、「Power Management」を参照してください。

PSU の正常性状態を表示するには

1. CMC ウェブインタフェースにログインします。
2. システムツリーで 電源装置 を選択します。電源装置ステータス ページが表示されます。

表5-10 および 表5-11 で、電源装置ステータス ページに表示される情報について説明します。

項目	説明		
名前	PSU の名前 PS-n が表示されます。ここで n は電源装置番号です。		
存在	電源装置 が存在するかどうかを示します（はい または **いいえ**）。		
正常性		OK	PSU が存在し、CMC を通信を行っていることを示します。PSU の正常性が OK であることを示します。CMC とファン装置間で通信エラーが発生した場合は、CMC で PSUの正常性の状態を取得または表示できません。
		重大	PSU が故障しており、正常性がクリティカルな状態にあることを示します。**速やかな対応処置が必要です。** 早急に対応処置を行わないと、電源喪失によりコンポーネントはシャットダウンしてしまう可能性があります。
		不明	シャーシが最初に電源が入ったときに表示されます。CMC と PSU 間で通信エラーが発生した場合には、CMC は PSU の正常性状態を取得または表示できません。
電源状態	PSU の電源状態（オンライン、オフ、または スロットが空）が表示されます。		
容量	電源容量がワットで表示されます。		

表 5-11 システム電源の状態

項目	説明
全体的な電源正常性	シャーシ全体の電源管理の正常性状態（**OK、非重大、重大、回復不可、その他、不明**）を示します。
システム電源の状態	シャーシの電源状態（オン、オフ、電源オン、電源オフ）を示します。
冗長性	電源装置冗長性の状態を示します。有効値は次のとおりです。 **いいえ**: 電源装置は非冗長です。 **はい** — 完全冗長化されています。

温度センサ状態の表示

温度センサ情報 ページには、シャーシ全体の（シャーシ、サーバー、IOM、iKVM）の温度プローブの状態と読み取り値が表示されます。

メモ: 温度プローブ値は編集できません。しきい値を超えると警告が生成され、ファン速度が変化します。たとえば、CMC 周囲温度プローブがしきい値を超えると、シャーシ内のファンの速度が上昇します。

温度プローブ の正常性状態を表示するには

1. CMC ウェブインタフェースにログインします。
2. システムツリーで 温度センサー を選択します。 温度センサー情報 ページが表示されます。

表5-12 で、温度センサー情報 ページに表示される情報について説明します。

項目	説明		
ID	温度プローブの数値の ID を表示します。		
名前	シャーシ、サーバー、IOM、iKVM の各温度プローブの名前を表示します。例：Ambient Temp、Server 1 Temp、I/O Module 1、iKVM Temp		
存在	サーバーがシャーシ内に存在する（はい）か、存在しない（いいえ）かを示します。		
正常性		OK	温度プローブが存在し CMC と通信していることを示します。温度プローブが正常に動作していることを示します。

		重大	温度プローブが故障しており、危険な状態にあることを示します。**速やかな対応処置が必要です。**
		不明	シャーシが最初に電源が入ったときに表示されます。CMC と温度プローブ間で通信エラーが発生すると、CMC で温度プローブの状態を取得または表示できません。
読み取り値	現在の温度を摂氏（°C）および華氏（°F）で示します。		
最大しきい値	エラー警告が発行される最高温度を（°C）および華氏（°F）で示します。		
最小しきい値	エラー警告が発行される最低温度を（°C）および華氏（°F）で示します。		

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 の表示

WWN/MAC サマリ ページは、シャーシ内のスロットの WWN 設定および MAC アドレスを表示します。

ファブリック構成

ファブリック構成 セクションでは、ファブリック A、ファブリック B およびファブリック C に取り付けられた入力/出力ファイブリックの種類が表示されます。緑色のチェックマークは、ファブリックが FlexAddress が有効になっていることを示します。FlexAddress 機能は、シャーシ指定およびスロット固定の WWN/MAC アドレスをシャーシ内のさまざまなファイブリックおよびスロットに展開するために使用します。この機能は、ファブリックおよびスロットごとに有効にすることができます。

メモ: FlexAddress 機能の詳細については、「FlexAddress の使用」を参照してください。

WWN / MAC アドレス

WWN/MAC アドレス の部分は、サーバースロットが現在空の状態の場合でも、全サーバーに割当てられた WWN/MAC の情報を表示します。 位置は、I/O モジュールが取り付けられたスロットの位置を表示します。6 つのスロットがグループ名（A、B または C）およびスロット番号（1 または 2）の組み合わせで識別され、A1、A2、B1、B2、C1 または C2 のスロット名で示されます。iDRAC はサーバーの統合管理コントローラです。ファブリック は、I/O ファブリックの種類を表示します。サーバー指定 は、コントローラのハードウェアに埋め込まれたサーバー指定の WWN/MAC アドレスを表示します。シャーシ指定 は、特定のスロットで使用されるシャーシ指定の WWN/MAC アドレスを表示します。サーバー指定 または シャーシ指定 のカラムの緑色のチェックマークは、アクティブなアドレスの種類を示します。シャーシ指定アドレスは、シャーシの FlexAddress が有効でスロット持続アドレスを示す場合に割当てられます。シャーシ指定アドレスが選択されている場合は、サーバーが別のサーバーと交換された場合でもそのアドレスを使用します。

CMC ネットワークプロパティの設定

メモ: ネットワーク設定を変更すると、現在のネットワークにログインするときに接続が失われる場合があります。

CMC への初期アクセスの設定

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。

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。

1. ウェブインタフェースにログインします。
2. システムツリーで **シャーシ** を選択します。
3. ネットワーク / セキュリティ 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。
4. DHCP を使用（CMC NIC IP アドレス用）チェックボックスをオンまたはオフにすることで、CMC の DHCP を有効または無効にします。
5. DHCP を無効にした場合は、IP アドレス、ゲートウェイ、サブネットマスクを入力します。
6. ページの下部の **変更の適用** をクリックします。

ネットワーク LAN の設定

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

メモ: コミュニティ文字列や SMTP サーバー IP アドレスなどネットワーク設定 ページ上の設定は、CMC とシャーシの外部設定の両方に影響します。

メモ: シャーシに 2 つの CMC（プライマリとスタンバイ）があり、両方ともネットワークに接続していると、プライマリ CMC が故障した場合にスタンバイ CMCが自動的にそのネットワーク設定を継承します。

1. ウェブインタフェースにログインします。
2. **ネットワーク / セキュリティ** タブをクリックします。
3. 表5-13～表5-15で説明されている CMC ネットワーク設定を指定します。
4. **変更の適用** をクリックします。

IP 範囲および IP ブロック設定を設定するには、詳細設定 ボタンをクリックします（ 「CMC ネットワークセキュリティの設定」を参照）。

ネットワーク設定 ページの内容を更新するには、更新をクリックします。

ネットワーク設定 ページの内容を印刷するには、印刷をクリックします。

表 5-13 ネットワークの設定

設定	説明
CMC MAC アドレス	シャーシの MAC アドレスを表示します。これはネットワーク上でこのシャーシを識別する一意の ID です。
CMC NIC を有効にする	CMC の NIC を有効にします。 デフォルト：有効 このオプションがオンの場合 • CMC はコンピュータネットワークと通信するので、ネットワーク経由でアクセスできます。 • ウェブ インタフェース、CLI（リモート RACADM）、WSMAN、Telnet、CMC に関連付けられた SSH が使用可能です。 このオプションがオフの場合 • CMC NIC はネットワーク通信できません。 • CMC からシャーシへの通信はできません。 • ウェブ インタフェース、CLI（リモート RACADM）、WSMAN、Telnet、および CMC に関連付けられた SSH は使用できません。 • サーバー iDRAC ウェブインタフェース、ローカル CLI、I/O モジュール、iKVM は通常どおり使用可能です。 • iDRAC と CMC のネットワークアドレスを取得できます。この場合は、シャーシの LCD から取得します。 **メモ:** シャーシ内の他のネットワークアクセス可能なコンポーネントへのアクセスは、シャーシ上のネットワークが無効になった（または失われた）場合でも影響はありません。
DNS への CMC の登録	このプロパティは DNS サーバーに CMC 名を登録します。 デフォルト:デフォルトでオフ（無効） **メモ:** 一部の DNSサーバーでは、31 文字以内の名前しか登録できません。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。
DNS の CMC 名	DNS への CMC の登録 を選択している場合にのみ CMC 名が表示されます。デフォルトの CMC 名は CMC_service_tag で、service tag はシャーシのサービスタグ番号です。例： CMC-00002 最大文字数は 63 文字です。最初の文字は英字（a-z、A-Z）で、英数字（a-z、A-Z、0-9）またはハイフン（-）が続く必要があります。
DNS ドメイン名に DHCP を使用	デフォルトの DNS ドメイン名を使用します。このチェックボックスは、**DHCP を使用（NIC IPアドレス用）** が選択されている場合にのみ使用できます。 デフォルト：有効
DNS ドメイン名	デフォルトの DNS ドメイン名は空白になっています。このフィールドは、DNS ドメイン名の DHCP を使用 のチェックボックスが選択されている場合にのみ編集可能です。
オートネゴシエーション（1 Gb)	CMC が一番近くのルーターまたはスイッチと通信して、デュプレックスモードとネットワーク速度を自動設定するか（オン）、デュプレックスモードとネットワーク速度をユーザーが手動で設定可能にするかを決定します（オフ）。 デフォルト：オン オートネゴシエーションがオンの場合は、CMC が自動的に最も近いルーターと通信するか、または 1 Gb の速度に切り替わり実行されます。

	オートネゴシエーションがオフの場合は、デュプレックスモードとネットワーク速度を手動で設定する必要があります。
ネットワーク速度	使用しているネットワーク環境に応じて、ネットワーク速度を 100 Mbps、または 10 Mbps に設定します。 **メモ:** ネットワークのスループットを効果的にするには、ネットワーク速度 の設定をネットワーク設定に合わせる必要があります。ネットワーク速度 をネットワーク設定の速度より下げると、帯域幅の消費が増えてネットワーク通信が遅くなります。使用しているネットワークがネットワーク速度を超える速度をサポートしているかどうかを判断し、それに従って設定してください。ネットワーク設定がこれらの値のどれにも一致しない場合は、オートネゴシエーション を使用するか、ネットワーク装置のメーカーに問い合わせてください。 **メモ:** 1000 Mb または 1 Gb の速度にするには、オートネゴシエーションを選択します。
デュプレックスモード	ネットワーク環境に応じて、デュプレックスモードを全二重または半二重に設定します。 意味: オートネゴシエーション が 1 つのデバイスに対してオンになっているが、他のデバイスではオフであるような場合、オートネゴシエーションを使用しているデバイスは他のデバイスのネットワーク速度を判定できますが、デュプレックスモードは判定できません この場合、オートネゴシエーション時に、デュプレックスモードはデフォルトで半二重になります。このような二重モードの不一致によって、ネットワーク接続が低速になります。 **メモ:** ネットワーク速度とデュプレックスモードの設定は、オートネゴシエーション が オン に設定されている場合は使用できません。
MTU	最大伝送単位（MTU）のサイズまたはインタフェースを通して渡すことのできる最大のパケットサイズを設定します。 設定範囲：576～1500 デフォルト：1500 **メモ:** IPv6 では最低 1280 の MTU が必要です。IPv6 が有効であり、**cfgNetTuningMtu** が低い値に設定されている場合は、1280 の MTU を使用します。

表 5-14 IPv4 設定

設定	説明
IPv4 の有効化	CMC が IPv4 プロトコルを使ってネットワーク上で通信できるようにします。このボックスをクリアしても、IPv6 ネットワークの導入が阻止されることはありません。デフォルト：チェック済み（有効）
DHCP 有効	CMC が IPv4 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できるようになります。デフォルト：オン（有効） このオプションがオンの場合、CMC は IPv4 設定（IP アドレス、サブネットマスク、ゲートウェイ）をネットワーク上の DHCP サーバーから自動的に取得します。CMC には常に、ネットワーク上で割り当てられた一意の IP アドレスがあります。 **メモ:** この機能を有効にすると、**静的 IP アドレス**、 **静的サブネットマスク**、**静的ゲートウェイ** の各プロパティフィールド（**ネットワーク設定** ページ上のこのオプションに隣接）は無効になり、これらのプロパティに前回入力した値は無視されます。 このオプションがオンでない場合は、**ネットワーク設定** ページ上の このオプションのすぐとなりにあるテキストフィールドに **静的 IP アドレス**、**静的サブネットマスク**、**静的ゲートウェイ** を手動で入力する必要があります。
静的 IP アドレス	CMC NIC の IPv4 アドレスを指定します。
静的サブネットマスク	CMC NIC の静的 IPv4 サブネットマスクを指定します。
静的ゲートウェイ	CMC NIC の IPv4 ゲートウェイを指定します。 **メモ:** **静的 IP アドレス**、**静的サブネットマスク**、 **静的ゲートウェイ**の各フィールドは、**DHCP 有効**（これらのフィールドの前にあるプロパティフィールド）が無効（オフ）である場合にのみアクティブです。この場合、ネットワーク上で使用するには CMC の**静的 IP アドレス**、**静的サブネットマスク**、**静的ゲートウェイ**を手動で入力する必要があります。 **メモ:** **静的 IP アドレス**、**静的サブネットマスク**、 **静的ゲートウェイ**の各フィールドは、シャーシデバイスのみに適用されます。これらのフィールドは、サーバーネットワーク、ローカルアクセス、I/O モジュール、iKVM など、シャーシソリューション内の他のネットワークアクセス可能なコンポーネントには影響しません。
DHCP を使用して DNS サーバーアドレスを取得する	静的設定ではなく、DHCP サーバーから一次と二次の INS サーバーアドレスを取得します。 デフォルト: デフォルトでオン (有効) **メモ:** DHCP を使用（NIC IP アドレス用） が有効になっている場合は、DHCP を使用して DNS サーバーアドレスを取得する プロパティを有効にします。 このオプションがオンの場合、CMC はネットワーク上の DHCP サーバーから自動的にその DNS IP アドレスを取得します。 **メモ:** このプロパティを有効にすると、静的優先 DNS サーバーと 静的代替 DNS サーバーのプロパティフィールド（ネットワーク設定 ページ上のこのオプションの直後にある）は非アクティブになり、これらのプロパティに対してそれまでに入力された値はすべて無視されます。 このオプションが選択されていない場合、CMC は静的優先 DNS サーバーと静的代替 DNS サーバーから DNS IP アドレスを取得します。これらのサーバーのアドレスは、ネットワーク設定 ページ上のこのオプションの直後にあるテキストフィールドで指定します。
静的優先 DNS サーバー	優先 DNS サーバーの静的 IP アドレスを指定します。静的優先 DNS サーバーは、DHCP を使用して DNS サーバーアドレスを取得する が無効になっているときにのみ組み込まれます。.
静的代替 DNS サーバー	代替 DNS サーバーの静的 IP アドレスを指定します。静的代替 DNS サーバーは、DHCP を使用して DNS サーバーアドレスを取得する が無効になっているときにのみ組み込まれます。.代替 DNSサーバーがない場合は、0.0.0.0 の IP アドレスを入力してください。

表 5-15 IPv6 の設定

設定	説明
IPv6 の有効化	CMC が IPv6 プロトコルを使ってネットワーク上で通信できるようにします。このボックスをクリアしても、IPv4 ネットワークの導入が阻止されることはありません。デフォルト：チェック済み（有効）
自動設定の有効化	CMC が IPv6 プロトコルを使って、この情報を提供するために設定された IPv6 ルータから、IPv6 関連のアドレスとゲートウェイ設定を取得できるようにします。CMC では、ネットワーク上で一意の IPv6 アドレスが生成されます。 デフォルト：オン（有効） **メモ：** この機能を有効にすると、**静的 IPv6 アドレス**、**静的プレフィックス長**、**静的ゲートウェイ** の各プロパティフィールド（ネットワーク設定ページ上の このオプションに隣接）は無効になり、これらのプロパティに前回入力した値は無視されます。 このオプションがオンでない場合は、ネットワーク設定ページ上の このオプションに隣接するテキストフィールドに**静的 IPv6 アドレス**、静的プレフィックス長、静的ゲートウェイを手動で入力する必要があります。
静的 IPv6 アドレス	自動設定が有効でない場合に、CMC NIC の IPv6 アドレスを指定します。
静的プレフィックス長	自動設定が有効でない場合に、CMC NIC の IPv6 プレフィックス長を指定します。
静的ゲートウェイ	自動設定が有効でない場合に、CMC NIC の静的 IPv6 ゲートウェイを指定します。 **メモ：** **静的 IPv6 アドレス**、**静的プレフィックス長**、**静的ゲートウェイ**の各フィールドは、**自動設定の有効化** （これらのフィールドの前にあるプロパティフィールド）が無効（オフ）である場合にのみアクティブです。この場合、IPv6 で使用するには CMC の**静的 IPv6 アドレス**、 **静的プレフィックス長**、**静的ゲートウェイ**を手動で入力する必要があります。 **メモ：** **静的 IPv6 アドレス**、**静的プレフィックス長**、**静的ゲートウェイ**の各フィールドは、シャーシデバイスのみに適用されます。これらのフィールドは、サーバーネットワーク、ローカルアクセス、I/O モジュール、 iKVM など、シャーシソリューション内の他のネットワークアクセス可能なコンポーネントには影響しません。
静的優先 DNS サーバー	優先 DNS サーバーの静的 IPv6 アドレスを指定します。静的優先 DNS サーバーの項目を使用するのは、**DHCP を使用して DNS サーバーアドレスを取得する** が無効またはオフになっている場合のみです。IPv4 および IPv6 設定エリアには、このサーバーの項目があります。
静的代替 DNS サーバー	代替 DNS サーバーの静的 IPv6 アドレスを指定します。代替 DNS サーバーがない場合は、"::" の IPv6 アドレスを入力します。静的代替 DNS サーバーの項目を使用するのは、**DHCP を使用して DNS サーバーアドレスを取得する** が無効またはオフになっている場合のみです。IPv4 および IPv6 設定エリアには、このサーバーの項目があります。

CMC ネットワークセキュリティの設定

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

1. ウェブインタフェースにログインします。
2. **ネットワーク / セキュリティ** 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。
3. 詳細設定 ボタンをクリックします。ネットワークセキュリティ ページが表示されます。
4. CMC ネットワークセキュリティの設定

表5-16 に、**ネットワークセキュリティ** ページの**設定**について説明します。

メモ： IP 範囲と IP ブロック設定は、IPv4 のみに適用可能です。

表 5-16 ネットワークセキュリティページの設定

設定	説明
IP 範囲を有効にする	IP 範囲のチェック機能を有効にします。この設定により、CMC にアクセスできる IP アドレスの範囲を定義できます。
IP 範囲のアドレス	範囲チェック用のベース IP アドレスを指定します。
IP 範囲のマスク	CMC にアクセスできる IP アドレス範囲を定義します。このプロセスは IP 範囲チェックと呼ばれます。 IP 範囲チェックを使うと、IP アドレスがユーザー定義の範囲にあるクライアントまたは管理ステーションからのみ CMC にアクセスできるようになります。その他のログインはすべて拒否されます。 例： IP 範囲マスク：255.255.255.0 (11111111.11111111.11111111.00000000) IP 範囲のアドレス：192.168.0.255 (11000000.10101000.00000000.11111111) 上記により、IP アドレス範囲は、192.168.0 を含む任意のアドレス、つまり 192.168.0.0～192.168.0.255 の任意のアドレスになります。

IP ブロックを有効にする	IP アドレスのブロック機能を有効にします。これにより、あらかじめ選択された時間帯に特定の IP アドレスからのログイン失敗回数を制限します。
• **IP ブロックエラーカウント**	IP アドレスからのログイン失敗回数を設定して、それを超えた場合にそのアドレスからのログインを拒否します。
• **IP ブロックエラー時間枠**	IP ブロックのペナルティ時間をトリガするために、IP ブロックのログイン失敗回数を数える時間枠を秒で指定します。
• **IP ブロックペナルティ時間**	失敗回数が制限値を超えた IP アドレスからのセッションをすべて拒否する時間を秒で指定します。 **メモ:** IP ブロックのエラーカウント、IP ブロックのエラーウィンドウ、IP ブロックの ペナルティ時間 フィールドは、IP ブロック有効 チェックボックス（これらのフィールドの前にある プロパティ フィールド）がオン（有効）の場合にのみアクティブです。この場合、IP ブロックのエラーカウント、IP ブロックのエラー ウィンドウ、IP ブロックのペナルティ時間 プロパティを手動で入力する必要があります。

5. 適用 をクリックして設定を保存します。

ネットワークセキュリティ ページの内容を更新するには、更新をクリックします。

ネットワークセキュリティ ページの内容を印刷するには、印刷をクリックします。

VLAN 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。

1. ウェブインタフェースにログインします。
2. **ネットワーク / セキュリティ** タブ → **VLAN** サブタブをクリックします。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。

3. CMC/iDRAC VLAN 設定を行います。

   表5-17 に、**ネットワークセキュリティ** ページの**設定**について説明します。

表 5-17 VLAN タグ設定

設定	説明
スロット	シャーシでサーバーが装着されているスロットを示します。スロット番号は 1～16（シャーシには使用できるスロットが 16 個あります）の連番 ID で、シャーシのサーバーの場所を識別します。
名前	各スロットのサーバー名を表示します。
有効	チェックボックスが選択されている場合は、VLAN を有効にします。VLAN はデフォルトで無効になっています。
優先度	フレームの優先順位レベルを示します。このレベルは、異なるタイプのトラフィック（音声、ビデオ、データ）の優先順位を決定するのに使用できます。有効な優先順位は 0～7 です。0（デフォルト）は最も低い優先順位を示し、7 は最も高い優先順位です。
ID	VLAN ID を表示します。有効な VLAN ID は 1～4000 および 4021～4094 です。デフォルトの VLAN ID は 1 です。

4. **適用** をクリックして設定を保存します。

シャーシ→ **サーバー**? **設定** タブ→ **VLAN** サブタブから、このページにアクセスすることもできます。

CMC ユーザーの追加と設定

CMC を使用してシステムを管理し、システムのセキュリティを確保するには、適切な管理者権限（ロールベースの権限）を持つ一意のユーザーを作成してください。セキュリティを強化するために、特定のシステムイベントが発生したときに特定のユーザーに電子メールで警告を送るように設定することもできます。

ユーザータイプ

CMC ユーザーと iDRAC ユーザーの 2 つのユーザータイプがあります。CMC ユーザーは「シャーシユーザー」とも呼ばれます。また、iDRAC がサーバー上に介在するため、iDRAC ユーザーは「サーバーユーザー」とも呼ばれます。

CMC ユーザーは、ローカルユーザーまたは Active Directory ユーザーにすることができます。また、iDRAC ユーザーも、ローカルユーザーまたは Active Directory 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を作成することはできず、またサーバーから CMC ユーザーを作成することもできません。このルールにより、サーバーのセキュリティと整合性は保護されます。

表5-18、表5-19 および 表5-20 は、CMC ユーザーの権限（ローカルまたは Active Directory）を説明し、付与された権限に基づいて、サーバーおよびシャーシ上で CMC ユーザーが行うことができる操作を説明します。ここでは、「ユーザー」とは CMC ユーザーを意味します。サーバーユーザーを指す場合は「サーバーユーザー」と明記します。

表 5-18 ユーザータイプ

権限	説明
CMC ログインユーザー	**CMC ログインユーザー**の権限を持つユーザーは CMC にログインできます。ログイン権限のみを持つユーザーはすべての CMC データを表示できますが、データの追加や変更、コマンドの実行はできません。 ユーザーはログイン権限なしで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。そのユーザーのログイン権限が復元した場合にも、その前に与えられていたその他のすべての権限を保持できます。
シャーシ設定システム管理者	シャーシ設定システム管理者の権限を持つユーザーは、以下のデータを追加または変更できます。 • シャーシを識別する（シャーシ名やシャーシの位置など） • シャーシに特別に割り当てられている（静的または DHCP IP モード、静的 IP アドレス、静的ゲートウェイ、静的サブネットマスクなど） • シャーシにサービスを提供する（日時、ファームウェアアップデート、CMC リセットなど） • シャーシに関連している（スロット名やスロットの優先順位など） これらのプロパティはサーバーに適用されますが、正確にはサーバーそのものでなくスロットに関連付けられるシャーシプロパティです。このため、スロット名とスロットの優先順位は、サーバーがスロットにあるなしに関係なく、追加または変更することができます。 サーバーが別のシャーシに移動されると、サーバーは新しいシャーシのそのスロットに割り当てられているスロット名と優先順位を継承します。前のスロット名と優先順位はそのまま前のシャーシに残ります。
ユーザー設定システム管理者	ユーザー設定システム管理者の権限を持つユーザーは、以下を行うことができます。 • 新規ユーザーの追加 • 既存のユーザーの削除 • ユーザーのパスワードの変更 • ユーザー権限の変更 • ユーザーのログイン権限を有効または無効にしますが、ユーザーの名前やデータベース内のその他の権限は保持されます。
ログのクリアシステム管理者	クリアシステム管理者の権限を持つ CMC ユーザーは、ハードウェアログと CMC ログをクリアできます。
シャーシ制御システム管理者（電源コマンド）	シャーシ電源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を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の制御
サーバー管理者	サーバーシステム管理者権限は、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。 CMC サーバーシステム管理者の権限を持つユーザーがサーバー上で実行するアクションを発行すると、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、CMC サーバーシステム管理者はサーバーにシステム管理者権限がない場合でも、それを無視してコマンドを送信できます。 サーバーシステム管理者権限がない場合、シャーシで作成されたユーザーは以下のすべての条件が満たされた場合にのみ、サーバー上でコマンドを実行することができます。 • 同じユーザー名がサーバー上に存在する • サーバー上の同じユーザー名に全く同じパスワードが指定されている • ユーザーはコマンドを実行する権限を持っている サーバーシステム管理者権限のない CMC ユーザーがサーバー上で実行するアクションを発行すると、CMC はユーザーのユーザー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、ユーザーは操作を実行することができません。
	ユーザーが対象のサーバーに存在し、パスワードが一致する場合は、サーバーはサーバー上でユーザーに与えられた権限で応答します。CMC ファームウェアはサーバーから返された権限に基づいてユーザーが操作を実行する権利があるかどうかを判断します。

	以下のリストに、サーバー管理者が持つサーバー上の権限と実行できる操作を示します。これらの権限は、シャーシユーザーがシャーシ上でのサーバーシステム管理者権限を持っていない場合にのみ適用されます。
サーバー管理者（続き）	サーバー設定システム管理者: • IP アドレスの設定 • ゲートウェイの設定 • サブネットマスクの設定 • 最初の起動デバイスの設定 ユーザー設定システム管理者: • iDRAC ルートパスワードの設定 • iDRAC のリセット サーバー制御システム管理者: • 電源オン • 電源オフ • パワーサイクル • 正常なシャットダウン • サーバーの再起動
テスト警告ユーザー	テスト警告ユーザーの権限を持つ CMC ユーザーは、テスト警告メッセージを送信できます。
コマンドのデバッグシステム管理者	デバッグ管理者権限を持つ CMC 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	ファブリック A 管理者の権限を持つ CMC ユーザーは、I/O スロットのスロット A1 またはスロット A2 にある ファブリック A IOM の設定を行うことができます。
ファブリック B システム管理者	ファブリック B 管理者の権限を持つ CMC ユーザーは、I/O スロットのスロット B1 またはスロット B2 にある ファブリック B IOM の設定を行うことができます。
ファブリック C システム管理者	ファブリック C 管理者の権限を持つ CMC ユーザーは、I/O スロットのスロット C1 またはスロット C2 にある ファブリック C IOM の設定を行うことができます。

CMC ユーザーグループは、あらかじめ割り当てられたユーザー権限を持つ一連のユーザーグループを提供します。 表5-18に、権限がリストされています。下の表に、ユーザーグループとそれらに事前定義されているユーザー権限を示します。

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てから、事前定義されている権限に新しい権限を追加したりいずれかの権限を削除したりすると、CMC グループは自動的に カスタム に変更されます。

表 5-19 CMC グループ権限

ユーザーグループ	与えられる権限
管理者	• CMC ログインユーザー • シャーシ設定システム管理者 • ユーザー設定システム管理者 • ログのクリアシステム管理者 • サーバー管理者 • テスト警告ユーザー • コマンドのデバッグシステム管理者 • ファブリック A システム管理者 • ファブリック B システム管理者 • ファブリック C システム管理者
パワーユーザー	• 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） • サーバー管理者 • テスト警告ユーザー • ファブリック A システム管理者 • ファブリック B システム管理者 • ファブリック C システム管理者
ゲストユーザー	CMC ログインユーザー
カスタム	以下の権限を任意の組み合わせで選択します。 • CMC ログインユーザー • シャーシ設定システム管理者 • ユーザー設定システム管理者 • ログのクリアシステム管理者 • シャーシ制御システム管理者（電源コマンド） • スーパーユーザー • サーバー管理者 • テスト警告ユーザー

	• コマンドのデバッグシステム管理者 • ファブリック A システム管理者 • ファブリック B システム管理者 • ファブリック C システム管理者
なし	割り当てられたアクセス権はありません。

表 5-20 CMC システム管理者、パワーユーザー、ゲストユーザー間の権限の比較

権限セット	システム管理者のアクセス権	パワーユーザーアクセス権	ゲストユーザーアクセス権
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）	✔	✔	✖
スーパーユーザー	✔	✖	✖
サーバー管理者	✔	✔	✖
テスト警告ユーザー	✔	✔	✖
コマンドのデバッグシステム管理者	✔	✖	✖
ファブリック A システム管理者	✔	✔	✖
ファブリック B システム管理者	✔	✔	✖
ファブリック C システム管理者	✔	✔	✖

ユーザーの追加と管理

ウェブインタフェースの ユーザー と ユーザー設定 ページで、CMC ユーザーについての情報の表示、新しいユーザーの追加、既存のユーザーの設定の変更を行うことができます。

16 人までのローカルユーザーを設定できます。追加のユーザーが必要な場合、会社が Microsoft® Active Directory® サーバーソフトウェアを使用していれば、CMC へのアクセスを提供するように Active Directory を設定できます。このように Active Directory を設定することによって、16 人のローカルユーザーに加えて、Active Directory ソフトウェアの既存のユーザーに CMC ユーザー権限を追加して制御できます。詳細については、「CMC と Microsoft Active Directory との併用」を参照してください。

ユーザーは、ウェブインタフェース、Telnet シリアル、SSH、iKVM セッションからログインできます。最大 22 のアクティブセッション（ウェブインタフェース、Telnet シリアル、SSH、iKVM などの任意の組み合わせ）をユーザー間で分割できます。

メモ: セキュリティを強化するために、root（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。root アカウントは、CMC に付属のデフォルト管理者アカウントです。root アカウントのデフォルトパスワードを変更するには、User ID 1（ユーザー ID 1）をクリックして ユーザー設定 ページを開きます。そのページのヘルプには、ページの右上にある ヘルプ リンクからアクセスできます。

CMC ユーザーの追加と設定

メモ: 以下の手順を実行するには、ユーザー設定システム管理者）権限が必要です。

1. ウェブインタフェースにログインします。
2. **ネットワーク / セキュリティ** タブをクリックし、**ユーザー** サブタブをクリックします。ユーザー ページが開いて、ルートユーザーを含む**各ユーザーのユーザー ID、**ユーザー名、CMC 権限、**ログイン状況が**表示されます。設定に使用できるユーザー ID には、ユーザー情報が一切表示されません。
3. 使用可能なユーザー 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。

   ユーザー ページの内容を更新するには、更新 をクリックします。ユーザー ページの内容を印刷するには、印刷 をクリックします。
4. そのユーザーの一般設定を選択します。

   表5-21 では、新規または既存の CMC ユーザー名とパスワードを設定するための **一般** 設定について説明します。

表 5-21 一般ユーザー設定

プロパティ	説明
ユーザー ID	（読み取り専用）CLI のスクリプトに使用される 16 のプリセットの連番でユーザーを識別します。ユーザー ID は、CLI ツール (RACADM) を使用してユーザーを設定する際、特定のユーザーを識別するために使用します。ユーザー ID は編集できません。 ユーザールートの情報を編集する場合、このフィールドは静的です。ルートのユーザー名は編集できません。
ユーザーを有効にする	ユーザーの CMC へのアクセスを有効または無効にします。
ユーザー名	ユーザーに関連付けられている一意の CMC ユーザー名の設定または表示を行います。ユーザー名には 16 文字まで使用できます。CMC ユーザー名には、前方スラッシュ（/）やピリオド（.）を含むことはできません。 **メモ:** ユーザー名を変更した場合、新しい名前は次回のログインまでユーザーインタフェースに表示されません。新しいユーザー名を適用した直後、変更をチェックできるように、すべてのユーザーログインが許可されます。
パスワードの変更	既存のユーザーパスワードを変更できるようにします。新しいパスワード フィールドで新しいパスワードを設定します。 新しいユーザーを設定している場合は、パスワードの変更 チェックボックスは選択できません。既存のユーザーの設定を変更する場合にのみ選択できます。
パスワード	既存のユーザーの新しいパスワードを設定します。パスワードを変更する場合は、パスワードの変更 チェックボックスも選択する必要があります。パスワードは 20 文字まで指定でき、入力する際は各文字がドットで表示されます。
パスワードの確認	新しいパスワード フィールドに入力したパスワードを確認します。 **メモ:** 新しいパスワード と 新しいパスワードの確認 フィールドは、（1）新しいユーザーを設定するとき、または（2）既存のユーザーの設定の編集を行うために パスワードの変更 チェックボックスを選択したときにのみ編集可能です。

5. ユーザーを CMC ユーザーグループに割り当てます。 表5-18は、 CMC ユーザー権限について説明します。 表5-19 では、**CMC ユーザー権限** 設定用の **ユーザーグループのアクセス権** について説明します。 表5-20では、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を行います。

   CMC Group（CMC グループ）ドロップダウンメニューからユーザー特権の設定を選択すると、そのグループについてあらかじめ定義された設定に従って、有効に設定された特権（リスト内のチェックボックスにチェックが入った状態）が表示されます。

   各ユーザーの特権の設定は、チェックボックスのチェックを入れたり解除したりしてカスタマイズします。CMC グループを選択したり、またはカスタムユーザー特権の選択を行った後で、設定を保存するには 変更の適用 をクリックします。
6. **変更の適用** をクリックします。

ユーザー設定 ページの内容を更新するには、更新をクリックします。.

ユーザー設定 ページの内容を印刷するには、印刷をクリックします。.

Microsoft Active Directory 証明書の設定と管理

メモ: CMC に Active Directory を設定するには、シャーシ設定システム管理者の権限が必要です。

メモ: Active Directory 設定および、Active Directory を標準スキーマまたは拡張スキーマで設定する方法の詳細に関しては、「CMC と Microsoft Active Directory との併用」を参照してください。

MicrosoftActive Directory サービスを使用して、CMC にアクセスできるようにソフトウェアを設定できます。Active Directory サービスを使用すると、既存ユーザーの CMC ユーザー権限を追加したり管理することができます。

Active Directory メインメニュー ページにアクセスするには:

1. ウェブインタフェースにログインします。
2. **ネットワーク / セキュリティ** タブをクリックして、**Active Directory** サブタブをクリックします。Active Directory メインメニュー ページが表示されます。

表5-22に、Active Directory メインメニュー ページのオプションを示します。

表 5-22 Active Directory メインメニューページのオプション

フィールド	説明
設定	CMC の以下の ActiveDirectory 設定を設定して管理します。CMC 名、ルートドメイン名、CMC ドメイン名、ActiveDirectory 認証タイムアウト、ActiveDirectory スキーマの選択（拡張または標準）、役割グループの設定。
AD 証明書のアップロード	認証局の署名入り Active Directory の証明書を CMC にアップロードします。Active Directory から取得するこの証明書によって CMC へのアクセスが許可されます。
証明書のダウンロード	Windows ダウンロードマネージャを使用して、CMC サーバー証明書を管理ステーションまたは共有ネットワークにダウンロードします。このオプションを選択して 次へ をクリックすると、ファイルのダウンロード ダイアログボックスが表示されます。このダイアログボックスで、管理ステーションまたは共有ネットワークにサーバー証明書を保存する場所を指定します。
証明書の表示	CMC にアップロードされた認証局の署名入り Active Directory のサーバー証明書が表示されます。 **メモ:** デフォルトでは、認証局が発行した Active Directory 用のサーバー証明書は CMC にありません。認証局が署名した最新のサーバー証明書をアップロードする必要があります。
Kerberos Keytab のアップロード	Active Directory の Kerberos Keytab を CMC にアップロードします。**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。 **メモ:** CMC には、Active Directory 用の Kerberos Keytab はありません。現在生成された Kerberos Keytab をアップロードする必要があります。詳細については、「シングルサインオンの設定」を参照してください。

Active Directory の設定（標準スキーマと拡張スキーマ）

メモ: CMC に Active Directory を設定するには、シャーシ設定システム管理者の権限が必要です。

メモ: Active Directory の機能を設定または使用する前に、Active Directory サーバーと CMC との通信が設定されていることを確認してください。

1. Active Directory サーバー用のすべての Secure Socket Layer (SSL) 証明書が同じ認証局の署名を持ち、CMC にアップロードされていることを確認します。
2. ウェブインタフェースにログインして、Active Directory メインメニュー に移動します。
3. **設定** を選択して、**次へ** をクリックします。**Active Directory の設定と管理** ページが表示されます。
4. 共通設定 見出しの下の Active Directory を有効にする チェックボックスを選択します。
5. 残りの フィールドに必要な情報を入力します。表5-23を参照してください 。

表 5-23 Active Directory 共通設定プロパティ

設定	説明

ルードメイン名	Active Directory が使用するドメイン名を指定します。ルートドメイン名はフォレストの完全修飾ルートドメイン名です。 **メモ：** ルードメイン名は x.y という命名規則に従った有効なドメイン名でなければなりません。この x は文字間に空白文字が入っていない 1～256 文字 ASCII 文字列、 y は com、edu、gov、int、mil、net、org などの有効なドメインタイプで指定します。 デフォルト： null（空白）
AD タイムアウト	Active Directory クエリが完了するまでの時間（秒）。最小値は 15 秒以上です。 デフォルト：120 秒
検索する AD サーバーの指定（オプション）	（選択した場合、）ドメインコントローラとグローバルカタログ上の指示呼び出しを有効にします。このオプションを有効にする場合は、次の設定でドメインコントローラとグローバルカタログの場所も指定する必要があります。 **メモ：** Active Directory の CA 証明書に記載の名前は指定のActive Directory サーバーまたはグローバルカタログサーバーとは一致しません。
ドメインコントローラ	Active Directory サービスのインストール先のサーバーを指定します。 このオプションは、**検索する AD サーバーの指定（オプション）** が有効である場合にのみ使用できます。
グローバルカタログ	Active Directory ドメインコントローラにおけるグローバルカタログの場所を指定します。グローバルカタログは Active Directory フォレストを検索するためのリソースを提供します。 このオプションは、**検索する AD サーバーの指定（オプション）** が有効である場合にのみ使用できます。

6. Active Directory スキーマの選択 の見出しの下にある Active Directory スキーマを選択します。表5-24を参照してください 。
7. 拡張スキーマを選択した場合は、拡張スキーマの設定 セクションに必要な情報を入力してから、 手順 9 に進みます。標準スキーマ を選択した場合は、手順 8 に進みます。
   - CMC デバイス名 – Active Directory の CMC カードを一意に識別する名前です。CMC 名はドメインコントローラで作成した新しい CMC のコモンネーム（CN）と同じでなければなりません。名前は 1 ～ 256 文字の ASCII 文字列で指定します。空白文字は使用できません。デフォルト： null（空白）
   - CMC ドメイン名 – Active Directory CMC オブジェクトがあるドメインの DNS 名（文字列）です（例：cmc.com）。名前は x.y から成る有効なドメイン名にします。x は文字間に空白文字のない 1～256 の ASCII 文字列で、y は com、edu、gov、int、mil、net、org などの有効なドメインタイプです。デフォルト： ヌル（空白）

   メモ： NetBIOS 名を使用しないでください。CMC ドメイン名 は CMC デバイスオブジェクトがあるサブドメインの完全修飾ドメイン名です。

表 5-24 Active Directory スキーマオプション

設定	説明
標準スキーマを使用	Active Directory で標準スキーマを使用します。このスキーマでは、ActiveDirectory グループオブジェクトしか使用しません。 標準スキーマオプションを使用するように CMC を設定する前に、まず Active Directory ソフトウェアを設定する必要があります。: 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. グループを作成するか、既存のグループを選択します。グループの名前とこのドメインの名前はウェブインタフェースまたは RACADM を使って CMC 上で設定する必要があります。
拡張スキーマを使用	Active Directory で拡張スキーマを使用します。このスキーマでは、Dell 定義の Active Directory オブジェクトを使用します。 Active Directory の拡張スキーマオプションを使用するように CMC を設定する前に、まず Active Directory ソフトウェアを設定する必要があります。 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 を使って CMC Active Directoryのプロパティを設定します。

8. 標準スキーマを選択した場合は、標準スキーマの設定 セクションに次の情報を入力します。拡張スキーマ を選択した場合は、手順 9 に進みます。
   - ロールグループ – CMC に関連付けられているロールグループ。ロールグループの設定を変更するには、ロールグループリストのロールグループ番号をクリックします。**ロールグループの設定** ページが表示されます。

   メモ： 指定した新しい設定を適用する前にロールグループリンクをクリックすると、設定の内容が失われます。新しい設定を失うことのないように、ロールグループリンクをクリックする前に 適用 をクリックしてください。

   - グループ名 –CMC カードに関連付けられている Active Directory のロールグループを識別する名前。
   - グループのドメイン – グループが置かれているドメイン。
   - グループ権限 – グループの権限レベル。

- **適用** をクリックして設定を保存します。

Active Directory の設定と管理 ページの内容を更新するには、更新 をクリックします。

Active Directory の設定と管理 ページの内容を印刷するには、印刷 をクリックします。

Active Directory のロールグループを設定するには、個々のロールグループ（1 ～ 5）をクリックします。表5-19および 表5-18を参照してください。

メモ: Active Directory の設定と管理 ページの設定を保存するには、カスタムロールグループ ページに進む前に適用 をクリックします。

認証局署名付き Active Directory 証明書のアップロード

Active Directory メインメニュー ページから

1. **AD 証明書のアップロード**を選択して、**次へ** をクリックします。**証明書のアップロード** ページが表示されます。
2. テキストフィールドにファイルのパスを入力するか、参照 をクリックしてファイルを選択します。

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。

3. **適用** をクリックします。証明書が無効の場合は、エラーメッセージが表示されます。

Active Directory CA 証明書をアップロードする ページの内容を更新するには、更新 をクリックします。

Active Directory CA 証明書をアップロードする ページの内容を印刷するには、印刷 をクリックします。

認証局署名付き Active Directory 証明書の表示

メモ: Active Directory サーバー証明書を CMC にアップロードした場合は、証明書がまだ有効であり、期限が切れていないことを確認してください。

Active Directory メインメニュー ページから

1. **証明書の表示** を選択して、**次へ** をクリックします。
2. **Active Directory の CA 証明書** ページの適切なボタンをクリックして続行します。

表 5-25. Active Directory CA 証明書の情報

フィールド	説明
シリアル番号	証明書のシリアル番号
タイトル情報	タイトルによって入力された証明書の属性
発行者情報	発行者によって返された証明書の属性
有効期間の開始	証明書の発行日。
有効期間の終了	証明書の有効期限日。

3. **Active Directory の CA 証明書を表示する** ページの内容を更新するには、更新 をクリックします。

Active Directory の CA 証明書を表示する ページの内容を印刷するには、**印刷** をクリックします。

SSL とデジタル証明書を使用した CMC 通信のセキュリティ確保

ここでは、CMC に組み込まれているデータセキュリティの機能について説明します。

- SSL (Secure Sockets Layer)
- 証明書署名要求 (CSR)
- SSL メインメニューへのアクセス
- 新しい CSR の生成
- サーバー証明書のアップロード
- サーバー証明書の表示

SSL (Secure Sockets Layer)

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

SSL は、SSL を有効にしたシステムで次のタスクを実行します。

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

この暗号処理は高度なデータ保護を提供します。CMC では、北米のインターネットブラウザで一般的に使用されている最も安全な暗号化方式である 128 ビットの SSL 暗号化標準を採用しています。

CMC Web サーバーには、デルが署名をした SSL デジタル証明書（サーバー ID）が含まれています。インターネットで高度なセキュリティを確保するには、新しい証明書署名要求（CSR）を生成する要求を CMC に送信して、ウェブサーバー SSL 証明書を置き換えてください。

証明書署名要求 (CSR)

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

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

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

SSL メインメニューへのアクセス

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

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

1. ウェブインタフェースにログインします。
2. **ネットワーク / セキュリティ** タブをクリックして、**SSL サブタブ**をクリックします。SSL メインメニュー ページが表示されます。

SSL メインメニュー ページオプションを使って、認証局に送信する CSR を生成します。CSR 情報は CMC ファームウェアに保存されています。

新しい証明書署名要求の生成

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

表 5-26 SSL メインメニューオプション

フィールド	説明
新規証明書署名要求（CSR）の生成	このオプションを選択し、**次へ** をクリックして証明書署名要求（CSR）の生成 ページを表示されます。そこで安全なウェブ証明書を要求する CSR 要求を生成して認証局に送信できます。 **メモ:** 新しい CSR は、ファームウェアにある古い CSR を上書きします。認証局が CSR を受け入れるには、 CMC の CSR が、認証局から返される証明書と一致する必要があります。
生成された CSR に基づいたサーバー証明書のアップロード	このオプションを選択し、**次へ** をクリックして **証明書のアップロード** ページを表示します。そこで会社が所有している既存の証明書をアップロードし、CMC へのアクセス制御に使用できます。 **メモ:** CMC で受け入れられるのは、X509、Base 64 エンコードの証明書のみです。DER でエンコードされた証明書は受け入れられません。新しい証明書をアップロードすると、CMC で受け取ったデフォルトの証明書が置き換えられます。
ウェブサーバーキーと証明書のアップロード	このオプションを選択し、**次へ** をクリックして **ウェブサーバーキーと証明書のアップロード** ページを表示します。そこで会社が所有している既存のウェブサーバーキーとサーバー証明書をアップロードし、CMC へのアクセス制御に使用できます。 **メモ:** CMC は、X.509、Base64 エンコードされた証明書のみ受け入れます。バイナリの DER でエンコードされた証明書は受け入れられません。新しい証明書をアップロードすると、CMC で受け取ったデフォルトの証明書が置き換えられます。
サーバー証明書の表示	このオプションを選択し、**次へ** ボタンをクリックして サーバー証明書の表示 ページを表示されます。そこで現在のサーバー証明書を表示できます。

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

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

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

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

CSR を生成するには：

1. **SSL メインメニュー** ページで、**新しい証明書署名要求（CSR）の生成** を選択して、**次へ** をクリックします。**証明書署名要求（CSR）の生成** ページが表示されます。
2. 各 CSR 属性値の値を入力します。

   表5-27 に、**証明書署名要求（CSR）の生成** ページのオプションを示します。
3. 生成 をクリックします。ファイルのダウンロード ダイアログボックスが表示されます。
4. csr.txt ファイルを管理ステーションまたは共有ネットワークに保存します。（このままファイルを開いて、後で保存することも可能です。）このファイルを後で CA に提出することになります。

表 5-27 証明書署名要求（CSR）の生成 ページのオプション

フィールド	説明
共通名	認証する名前（通常は www.xyzcompany.com/ のような ウェブサーバーのドメイン名）。

	有効： 英数字（A ～ Z、a ～ z、0 ～ 9）、ハイフン、下線、ピリオド。 無効：上記の英数字以外の文字（@ # $ % & * など）、主に英語以外の言語で使用される文字（、、、 など）。
組織名	自分の組織に関連付けられた名前（例：XYZ Corporation）。 有効：英数字（A ～ Z、a ～ z、0 ～ 9）、ハイフン、下線、ピリオド、空白文字。 無効：上記の英数字以外の文字（@ # $ % & * など）。
組織単位	部署など事業体に関連する名前（例： Kikakubu）。 有効：英数字（A ～ Z、a ～ z、0 ～ 9）、ハイフン、下線、ピリオド、空白文字。 無効：上記の英数字以外の文字（@ # $ % & * など）。
地域	組織が所在する都市その他の場所（例：Kawasaki、Shibuya）。 有効：英数字（A ～ Z、a ～ z、0 ～ 9）と空白文字。 無効：上記の英数字以外の文字（@ # $ % & * など）。
都道府県	証明書を申請している事業体の都道府県や地域例：Tokyo、Osaka、Kanagawa など）。 **メモ：** 略語は使用しないでください。 有効：英数字（大文字と小文字、0 ～ 9）と空白文字。 無効：上記の英数字以外の文字（@ # $ % & * など）。
国	証明書を申請している組織の所在国。
電子メール	会社の電子メールアドレス CSR と関連付ける任意の電子メールアドレスを入力できます。電子メールアドレスはアットマーク（@）を含む有効な電子メールアドレスでなければなりません (例： name@xyzcompany.com)。 **メモ：** この電子メールアドレスはオプションフィールドです。

サーバー証明書のアップロード

1. **SSL メインメニュー** ページで、**サーバー証明書のアップロード** を選択して **次へ** をクリックします。**証明書のアップロード** ページが表示されます。
2. テキストフィールドにファイルのパスを入力するか、参照 をクリックしてファイルを選択します。
3. 適用 をクリックします。証明書が無効の場合は、エラーメッセージが表示されます。

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

証明書のアップロード ページの内容を更新するには、更新をクリックします。

証明書のアップロード ページの内容を印刷するには、印刷をクリックします。

サーバー証明書の表示

SSL メインメニュー ページで、**サーバー証明書の表示** を選択して **次へ** をクリックします。**サーバー証明書の表示** ページが表示されます。

表5-28 に、**証明書** ウィンドウに表示されるフィールドと説明を示します。

表 5-28 証明書情報

フィールド	説明
シリアル	証明書のシリアル番号
タイトル	タイトルによって入力された証明書の属性
発行者	発行者によって返された証明書の属性
有効期限の開始日	証明書の発行日

有効期限の終了日	証明書の失効日

サーバー証明書の表示 ページの内容を更新するには、更新をクリックします。

サーバー証明書の表示 ページの内容を更新するには、印刷をクリックします。

セッションの管理

セッション ページにシャーシへの接続セッションをすべて表示し、どのアクティブ セッションを終了することもできます。

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

セッションを終了するには:

1. ウェブ経由で CMC にログインします。
2. **ネットワーク / セキュリティ** タブをクリックして、**セッション** サブタブをクリックします。
3. **セッション** ページで、終了するセッションを見つけ、ゴミ箱アイコンをクリックします。

セッションを管理するには:

1. CMC ウェブインタフェースにログインします。
2. システムツリーで **シャーシ** を選択します。
3. **ネットワーク / セキュリティ** タブをクリックします。
4. セッション サブタブをクリックします。セッション ページが表示されます。

表 5-29 セッションのプロパティ

プロパティ	説明
セッション ID	ログインの各インスタンスに生成される連番の ID 番号を表示します。
ユーザー名	ユーザーのログイン名が表示されます（ローカルユーザーまたは Active Directory ユーザー）。Active Directory ユーザー名の例として、name@domain.com、domain.com/name、domain.com\name などがあります。
IP アドレス	ユーザーの IP アドレスを表示します。
セッションの種類	セッションの種類（Telnet、シリアル、SSH、リモート RACADM、SMASH CLP、WSMAN、GUI セッション）が表示されます。
終了	表示されているセッションはどれでも終了できます（自分のセッションを除く）。関連するセッションを終了するには、ごみ箱のアイコン をクリックします。この欄は、**シャーシ設定システム管理者** 権限がある場合にのみ表示されます。

セッションを終了するには、セッションの説明行にあるゴミ箱アイコンをクリックします。

サービスの設定

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

メモ: リモート（RACADM）CLI ツールとウェブインタフェースはウェブサーバーを使用します。ウェブサーバーがアクティブではない場合、リモート RACDM とウェブインタフェースは動作しません。

メモ: 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。ウェブサーバーリセットは通常、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 を使って変更された、ウェブサーバーポートの設定がウェブインタフェースまたは RACADM を使って変更された、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などのイベントの結果引き起こされます。

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

CMC サービスを設定するには:

1. CMC ウェブインタフェースにログインします。
2. **ネットワーク / セキュリティ** タブをクリックします。
3. サービス サブタブをクリックします。サービス ページが表示されます。
4. 必要に応じて次のサービスを設定します。
   - CMC シリアルコンソール（表5-30）
   - ウェブサーバー（表5-31）
   - SSH（表5-32）
   - Telnet（表5-33）
   - リモート RACADM（表5-34）
   - SNMP（表5-35）
   - Syslog の削除（表5-36）
5. **適用** をクリックします。**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が更新されます。**

表 5-30 CMC シリアルコンソールの設定

設定	説明
有効	CMC の Telnet コンソールインタフェースを有効にします。 デフォルト: オフ（無効）
リダイレクト有効	CMC から シリアル/Telnet/SSH クライアント を使ってサーバーへのシリアル / テキスト コンソール リダイレクトを有効にします。CMC は、内部的にサーバーの COM2 ポートに接続する iDRAC に接続します。 設定オプション: オン（有効）、オフ（無効） デフォルト: チェック済み（有効）
アイドルタイムアウト	アイドル状態のシリアル セッションが自動的に切断されるまでの秒数を示します。タイムアウト 設定の変更は、次回のログインで有効になります。現在のセッションには影響しません。 タイムアウト範囲: 0 または 60 - 10800 秒。アイドルタイムアウト機能を無効にするには、0 を入力します。 デフォルト: 1800 秒
ボーレート	CMC の外部シリアルポートのデータ速度を示します。 有効な設定オプション: 9600、19200、28800、38400、57600、115200 bps デフォルト: 115200 bps
認証無効	CMC シリアルコンソールログイン認証を有効にします。 デフォルト: オフ（無効）
Esc キー	connect または racadm connect コマンドを使用するときにシリアル / テキストコンソール リダイレクトを終了する Escape キーの組み合わせを指定できます。 デフォルト: ^\ （<Ctrl> を押しながらバックスラッシュ (\) 文字を入力） **メモ:** キャレット文字 ^ は、<Ctrl> キーを表しています。 設定オプション: - 10 進値（例: 95） - 16 進値（例: 0x12） - 8 進値（例: 007） - ASCII 値（例: ^a）

	ASCII 値は以下のエスケープキーコードを使って表します。 • Esc の後に英字（a ～ z、A ～ Z） • Esc の後に特殊文字 [ ] \ ^ _ • 最大長：4
履歴バッファサイズ	シリアルコンソールに最後に書き込まれた文字を格納しているシリアル履歴バッファの最大サイズを示します。 デフォルト： 8192 文字
ログインコマンド	ユーザーが CMC シリアルコンソールインタフェースにログインするときに自動的に実行するシリアルコマンドを指定します。 例： connect server-1 デフォルト： [Null]

表 5-31 ウェブサーバーの設定

設定	説明
有効	CMC 用に Web Server サービスを有効にします（リモート RACADM と ウェブインタフェースからアクセス）。 デフォルト：オン（有効）
最大セッション数	シャーシで許可される同時ウェブユーザーインタフェースセッションの最大数を示します。最大セッション数 プロパティの変更は次回のログインで有効になります。現在のアクティブセッション（自分自身のセッションを含む）には影響しません。リモート RACADM はウェブサーバーの 最大セッション数 プロパティの影響は受けません。 許可範囲：1～4 デフォルト：4 **メモ：** 最大セッション数 プロパティを現在のアクティブ セッション数以下の値に変更してからログアウトした場合、他のセッションが終了するか期限切れになるまで再びログインできません。
アイドルタイムアウト	アイドル状態の Web ユーザーインタフェースセッションが自動的に切断されるまでの秒数を示します。タイムアウト 設定の変更は、次回のログインで有効になります。現在のセッションには影響しません。 タイムアウト範囲: 60 ～ 10800 秒です。 デフォルト：1800 秒
HTTP ポート番号	サーバー接続を受信待機中の CMC が使用するデフォルトポートを示します。 **メモ：** ブラウザで HTTP アドレスを入力すると、ウェブサーバーは自動的にリダイレクトして HTTPS を使用します。 デフォルト HTTPS ポート(80) を変更した場合は、ブラウザのアドレスフィールドのアドレスにポート番号を次のように入力する必要があります。 http://<IP アドレス>:<ポート番号> IP アドレス はシャーシの IP アドレスで、ポート番号 は、デフォルトの 80 以外の HTTP ポート番号です。 設定範囲：10～65535 デフォルト：80
HTTPS ポート番号	セキュアサーバー接続を受信待機中の CMC が使用するデフォルトポートを示します。 デフォルト HTTPS ポート番号 (443) を変更した場合は、ブラウザのアドレスフィールドのアドレスにポート番号を次のように入力する必要があります。 https://<IP アドレス>:<ポート番号> <IP アドレス> はシャーシの IP アドレスで、<ポート番号> はデフォルトの 443 以外の HTTPS ポート番号です。 設定範囲：10～65535 デフォルト：443

表 5-32 SSH の設定

設定	説明
有効	CMC で SSH を有効にします。

	デフォルト：オン（有効）
最大セッション数	シャーシで同時に実行できる SSH セッションの最大数。このプロパティの変更は、次のログインで有効になります。現在の アクティブセッション（自分のセッションを含む）には影響しません。 設定可能な範囲：1～4 デフォルト：4 **メモ：** 最大セッション数 プロパティを現在のアクティブ セッション数以下の値に変更してからログアウトした場合、他のセッションが終了するか期限切れになるまで再びログインできません。
アイドルタイムアウト	アイドル状態の SSH セッションが自動的に切断されるまでの秒数を示します。タイムアウト 設定の変更は、次回のログインで有効になります。現在のセッションには影響しません。 タイムアウト範囲: 0 または 60～10800 秒 アイドルタイムアウト機能を無効にするには、0 を入力します。 デフォルト：1800 秒
ポート番号	サーバーの接続を待機している CMC が使用するポート。 設定範囲：10～65535 デフォルト：22

表 5-33 Telnet の設定

設定	説明
有効	CMC の Telnet コンソールインタフェースを有効にします。 デフォルト：オフ（無効）
最大セッション数	シャーシで同時に実行できる Telnet セッションの最大数を示します。このプロパティの変更は、次のログインで有効になります。現在の アクティブセッション（自分のセッションを含む）には影響しません。 許可範囲：1～4 デフォルト：4 **メモ：** 最大セッション数 プロパティを現在のアクティブ セッション数以下の値に変更してからログアウトした場合、他のセッションが終了するか期限切れになるまで再びログインできません。
アイドルタイムアウト	アイドル状態の Telnet セッションが自動的に切断されるまでの秒数を示します。タイムアウト設定の変更は、次回のログインで有効になります。現在のセッションには影響しません。 タイムアウト範囲: 0 または 60～10800 秒 アイドルタイムアウト機能を無効にするには、0 を入力します。 デフォルト：1800 秒
ポート番号	サーバー接続を受信待機中の CMC が使用するポートを示します。 デフォルト：23

表 5-34 リモート RACADM の設定

設定	説明
有効	CMC へのリモート RACADM ユーティリティのアクセスを有効にします。 デフォルト：オン（有効）
最大セッション数	シャーシで同時に実行できる RACADM セッションの最大数を示します。このプロパティの変更は、次のログインで有効になります。現在の アクティブセッション（自分のセッションを含む）には影響しません。 許可範囲：1～4 デフォルト：4 **メモ：** 最大セッション数 プロパティを現在のアクティブ セッション数以下の値に変更してからログアウトした場合、他のセッションが終了するか期限切れになるまで再びログインできません。
アイドルタイムアウト	アイドル状態の racadm セッションが自動的に切断されるまでの秒数を示します。アイドルタイムアウト 設定の変更は、次回のログインで有効になります。現在のセッションには影響しません。アイドルタイムアウト 機能を無効にするには、0 を入力します。

	タイムアウト範囲: 0 または 10～1920 秒。アイドルタイムアウト機能を無効にするには、0 を入力します。 デフォルト：30 秒

表 5-35 SNMP 設定

設定	説明
有効	CMC で SNMP を有効にします。 **有効な値**：オン（有効）またはオフ（無効） **デフォルト**：オフ（無効）
コミュニティ名	CMC の SNMP デーモンからデータを取得するのに使うコミュニティ文字列を示します。

表 5-36 リモート Syslog 設定

設定	説明
有効	指定されたサーバー上でのシステムログの転送やリモート取り込みを有効にします。 **有効な値**：オン（有効）またはオフ（無効） **デフォルト**：オフ（無効）
Syslog サーバー 1	syslog のコピーをホストできる 3 つのサーバーのうちの最初の 1 つ。ホスト名、IPv6 アドレス、または IPv4 アドレスで指定します。
Syslog サーバー 2	syslog のコピーをホストできる 3 つのサーバーのうちの 2 番目。ホスト名、IPv6 アドレス、または IPv4 アドレスで指定します。
Syslog サーバー 3	syslog のコピーをホストできる 3 つのサーバーのうちの 3 番目。ホスト名、IPv6 アドレス、または IPv4 アドレスで指定します。
Syslog ポート番号	syslog のコピーを受信するために、リモートサーバー上のポート番号を指定します。3 つのサーバーすべてに対して、同じポート番号が使用されます。有効な syslog ポート番号は 10～65535 です。 **デフォルト**：514

電力バジェットの設定

CMC では、シャーシへの電力のバジェットを設定して電源を管理することができます。電源管理サービスは電力消費を最適化し、需要に基づいてさまざまなモジュールに電力を割り当て直します。

CMC を介して電源を設定する手順については、「電源の設定と管理」を参照してください。

CMC の電力管理サービスの詳細については、「Power Management を参照してください。

ファームウェアアップデートの管理

本項では、ウェブインタフェースを使って CMC ファームウェアをアップデートする方法を説明します。以下のコンポーネントは、GUI または RACADM コマンドを使用してアップデートすることができます。

- CMC - プライマリおよびスタンバイ
- iKVM
- iDRAC
- IOM インフラストラクチャデバイス

ファームウェアをアップデートする場合は、アップデートが失敗した場合にサービスが失われないように、推奨手順に従ってください。本セクションの手順を利用する前に、「CMC ファームウェアのインストールまたはアップデート」のガイドラインを確認してください。

現在のファームウェアバージョンの表示

アップデート ページには、アップデート可能なシャーシ内のすべてのコンポーネントの現行バージョンが表示されます。これには、iKVM ファームウェア、プライマリ CMC ファームウェア、（可能な場合）スタンドバイ CMC ファームウェア、iDRAC ファームウェア、および IOM インフラストラクチャ デバイスファームウェアが含まれます。詳細は、「IOM インフラストラクチャデバイスファームウェアのアップデート」を参照してください。デバイス名または すべて選択 / 選択解除 チェックボックスのいずれかをチェックし、更新の適用 ボタンを押すと、選択したデバイスの更新ページが表示されます。

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 CMC が iDRAC に破損したファームウェアがあることを検出した場合は、iDRAC も **更新可能なコンポーネント** ページに表示されます。CMC を使用して iDRAC ファームウェアを回復する手順については、「CMC を使用した iDRAC ファームウェア のリカバリ」を参照してください。

更新可能なコンポーネントを表示するには

1. ウェブインタフェースにログインします（「CMC ウェブインタフェースへのアクセス」を参照）。
2. システムツリーで **シャーシ** をクリックします。
3. アップデート タブをクリックします。アップデート可能なコンポーネント ページが表示されます。

ファームウェアのアップデート

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

メモ: ファームウェアのアップデートでは CMC と iKVM の現在の設定が維持されます。

メモ: システムコンポーネントのファームウェアをアップデートするためにウェブユーザーインタフェースのセッションを利用する場合、ファイル転送時間を十分に許容できるように**アイドルタイムアウト**時間を設定する必要があります。ファームウェアのファイル転送に 30 分までもかかることがあります。**アイドルタイムアウト値**を設定するには、「サービスの設定」を参照してください。

更新可能なコンポーネント ページには、一覧表示された各コンポーネントに対するファームウェアの現行バージョンが表示され、ファームウェアを最新バージョンに更新できます。デバイスファームウェアの基本的な更新手順:

- 更新するデバイスを選択します。
- グループ化の下にある適用ボタンをクリックします。
- 参照ボタンを押してファームウェアイメージを選択します。
- ファームウェア更新を開始するをクリックして更新処理を開始します。進捗ページの後に、ファイルイメージを転送中のメッセージが表示されます。

メモ: 必ずファームウェアの最新バージョンを用意してください。最新のファームウェアイメージファイルは、デルサポートサイトからダウンロードできます。

CMC ファームウェアのアップデート

メモ: サーバー上の CMC ファームウェアのアップデート中、シャーシ内の冷却ファンの一部または全部が全速回転します。これは正常な動作です。

メモ: ファームウェアが正常にアップロードされた後、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、スタンバイおよびアクティブの役割が置き換わります。スタンバイ（セカンダリ）CMC がアクティブ（プライマリ）CMC になります。アクティブ（プライマリ）CMC にのみアップデート適用した場合、リセットの完了後、プライマリ CMC ではアップデートされたイメージを利用しません。スタンバイ（セカンダリ）のみ、そのイメージが利用されます。

メモ: リセット中に他のユーザーが切断されないように、CMC にログインしている可能性のあるユーザーに通知し、**セッション** ページを表示して、アクティブなセッションを確認してください。セッション ページを開くには、ツリーで シャーシ を選択し、ネットワーク / セキュリティ タブをクリックして セッション サブタブをクリックします。そのページのヘルプには、ページの右上にある ヘルプ リンクからアクセスできます。

メモ: CMC との間でのファイルの転送中、ファイル転送アイコンが回転します。アイコンが回転しない場合は、ブラウザでアニメーションが有効になっているか確認してください。手順については、「34ページの「Internet Explorer でアニメーションの再生<?>」」を参照してください。

メモ: Internet Explorer を使って CMC からファイルをダウンロードするときに問題が起きた場合は、**暗号化されたページをディスクに保存しない** オプションを有効にしてください。手順については、「34ページの「Internet Explorer で CMC からファイルのダウンロード<?>」」を参照してください。

1. 更新可能コンポーネントページで、CMC のターゲットの更新チェックボックスを選択してCMC を選択して更新します。 両 CMC を同時にアップデートすることが可能です。
2. CMC コンポーネント リストの下の CMC の更新を実行するボタンをクリックします。

メモ: デフォルトの CMC ファームウェアイメージ名は、firmimg.cmc です。IOM インフラストラクチャデバイスのファームウェアをアップデートする前に、まず CMC ファームウェアをアップデートします。

3. ファームウェアイメージ フィールドに、管理ステーションまたは共有ネットワーク上のファームウェアのイメージファイルへのパスを入力するか、参照 をクリックし、ファイルの保存場所にナビゲートします。
4. ファームウェアアップデートを開始する をクリックします。ファームウェアアップデートの進行状況 セクションでは、ファームウェアアップデートのステータス情報を提供します。イメージファイルがアップロードされる間、ページにステータスインジケータが表示されます。ファイルの転送時間は、接続速度によって大きく異なります。内部アップデート処理が開始されると、ページは自動的に更新され、ファームウェアアップデートのタイマーが表示されます。その他の追記事項:
   - ファイル転送時に、更新 ボタンの利用、または他のページへ移動しないでください。
   - アップデートプロセスをキャンセルするには、ファイル転送およびアップデートのキャンセル をクリックします。このオプションは、ファイル転送時にのみ、利用可能です。
   - アップデート状態 フィールドにアップデートステータスが表示されます。このフィールドは、ファイル転送時に自動的に更新されます。

メモ: CMC のアップデートに数分かかる場合があります。

5. スタンバイ（セカンダリ）CMC の場合、アップデートが完了すると、アップデート状態フィールドに「完了」と表示されます。アクティブ（プライマリ）CMC の場合、ファームウェアのアップデート処理の最終フェーズでは、CMC とのブラウザセッションおよび接続は一時的に失われ、アクティブ（プライマリ）CMC はオフラインになります。アクティブ（プライマリ）CMC の再起動後、数分経過したら、再びログインする必要があります。

CMC がリセットすると、新しいファームウェアが アップデート可能なコンポーネント ページに表示されます。

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

iKVM ファームウェアのアップデート

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

1. CMC ウェブインタフェースに再びログインします。
2. システムツリーで シャーシ を選択します。
3. アップデート タブをクリックします。アップデート可能なコンポーネント ページが表示されます。
4. 対象となる iKVM のターゲットを更新するチェック ボックスを選択して、更新する iKVM を選択します。
5. iKVM コンポーネント リストの下の iKVM の更新を実行するボタンをクリックします。
6. 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。

メモ: iKVM ファームウェアイメージのデフォルト名は ikvm.bin です。この名前を変更することも可能です。

7. ファームウェアアップデートを開始する をクリックします。
8. はいをクリックして続行します。ファームウェアアップデートの進行状況 セクションでは、ファームウェアアップデートのステータス情報を提供します。イメージファイルがアップロードされる間、ページにステータスインジケータが表示されます。ファイルの転送時間は、接続速度によって大きく異なります。内部アップデート処理が開始されると、ページは自動的に更新され、ファームウェアアップデートのタイマーが表示されます。その他の追記事項:
   - ファイル転送時に、更新 ボタンの利用、または他のページへ移動しないでください。
   - アップデートプロセスをキャンセルするには、ファイル転送およびアップデートのキャンセル をクリックします。このオプションは、ファイル転送時にのみ、利用可能です。
   - アップデート状態 フィールドにアップデートステータスが表示されます。このフィールドは、ファイル転送時に自動的に更新されます。

メモ: iKVM のアップデートに 2 分までもかかる場合があります。

アップデートが完了すると、iKVM がリセットし、新しいファームウェアが アップデート可能なコンポーネント ページに表示されます。

IOM インフラストラクチャデバイスファームウェアのアップデート

この更新処理を実行すると、IOM デバイスのコンポーネントに対応するファームウェアが更新されます。IOM デバイス自体のファームウェアは更新されません。コンポーネントは、IOM デバイスと CMC の間を巡回するインタフェースです。コンポーネントの更新イメージは、CMC ファイルシステムに常駐し、そのコンポーネントは、コンポーネント上の現行バージョンと CMC のコンポーネント イ

メージが一致しない場合にのみ CMC ウェブ GUI に更新可能デバイスとして表示されます 。

1. CMC ウェブインタフェースに再びログインします。
2. システムツリーで シャーシ を選択します。
3. アップデート タブをクリックします。アップデート可能なコンポーネント ページが表示されます。
4. IOM デバイスに対応するターゲットを更新するチェックボックスを選択して、更新する IOM デバイスを選択します。
5. IOM コンポーネントリストの下の IOM の更新を実行するボタンをクリックします。

   メモ: 必要とするイメージは CMC 上に存在するため、IOM インフラストラクチャデバイス（IOMINK）の場合、**ファームウェアイメージ** フィールドは表示されません。IOMINF のファームウェアをアップデートする前に、まず CMC ファームウェアをアップデートします。

   IOMINF ファームウェアで CMC ファイルシステムに含まれているイメージが古いと判断された場合は、IOMINF をアップデートできます。最新の IOMINF ファームウェアを使用している場合は、IOMINF をアップデートすることはできません。最新の IOMINF デバイスはアップデート可能なデバイスとして一覧表示されます。

6. ファームウェアアップデートを開始する をクリックします。ファームウェアアップデートの進行状況 セクションでは、ファームウェアアップデートのステータス情報を提供します。イメージファイルがアップロードされる間、ページにステータスインジケータが表示されます。ファイルの転送時間は、接続速度によって大きく異なります。内部アップデート処理が開始されると、ページは自動的に更新され、ファームウェアアップデートのタイマーが表示されます。その他の追記事項:
   - ファイル転送時に、更新 ボタンの利用、または他のページへ移動しないでください。
   - アップデート状態 フィールドにアップデートステータスが表示されます。このフィールドは、ファイル転送時に自動的に更新されます。

メモ: IOMINF ファームウェアのアップデート時には、ファイル転送タイマーは表示されません。アップデートが完了すると、デバイスが再起動するため、IOM デバイスとの接続が一時的に失われます。

アップデートが完了すると、新しいファームウェアが アップデート可能なコンポーネント ページに表示され、アップデートされたシステムはそのページに表示されなくなります。

サーバー iDRAC ファームウェアのアップデート

メモ: ファームウェアがアップデートし、アップロードに成功すると、 iDRAC（サーバー上の）はリセットされ、一時的に利用不可になります。

メモ: iDRAC ファームウェアは iDRAC を搭載したサーバーではバージョン 1.4 以降、iDRAC6 Enterprise を搭載したサーバーではバージョン 2.0 以降である必要があります。

1. CMC ウェブインタフェースに再びログインします。
2. システムツリーで シャーシ を選択します。
3. アップデート タブをクリックします。アップデート可能なコンポーネント ページが表示されます。
4. 対象のデバイスのターゲットを更新するチェックボックスを選択して、更新する iDRAC を選択します。
5. iDRAC コンポーネント リストの下の iDRAC の更新を実行するボタンをクリックします。
6. 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。
7. ファームウェアアップデートを開始する をクリックします。ファームウェアアップデートの進行状況 セクションでは、ファームウェアアップデートのステータス情報を提供します。イメージファイルがアップロードされる間、ページにステータスインジケータが表示されます。ファイルの転送時間は、接続速度によって大きく異なります。内部更新処理が始まると、ページは自動的に更新され、ファームウェアアップデートのタイマーが表示されます。その他の追記事項:
   - ファイル転送時に、更新 ボタンを使用したり、他のページへ移動しないでください。
   - アップデートプロセスをキャンセルするには、ファイル転送およびアップデートのキャンセル をクリックします。このオプションは、ファイル転送時にのみ、利用可能です。
   - アップデート状態 フィールドにアップデートステータスが表示されます。このフィールドは、ファイル転送時に自動的に更新されます。

メモ: CMC またはサーバー のアップデートには数分かかる場合があります。

CMC を使用した iDRAC ファームウェア のリカバリ

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

初期世代のサーバーは、iDRAC ファームウェアの新規更新処理により破損したファームウェアを回復できます。CMC が iDRAC ファームウェアの破損を検知すると、**更新可能コンポーネント** ページにサーバーを一覧表示します。

iDRAC ファームウェアをアップデートするには、次の手順に従ってください。.

1. **support.dell.com** から管理コンピュータに最新の iDRAC ファームウェアをダウンロードします。
2. ウェブインタフェースにログインします（「CMC ウェブインタフェースへのアクセス」を参照）。
3. システムツリーで **シャーシ**をクリックします。
4. アップデートタブをクリックします。アップデート可能なコンポーネントページが表示されます。
5. 対象のデバイスのターゲットを更新するチェックボックスを選択して、更新対象と同じ型式の iDRAC を選択します。
6. iDRAC コンポーネント リストの下の iDRAC の更新を実行するボタンをクリックします。
7. **参照** をクリックして、ダウンロードした iDRAC ファームウェアイメージに移動し、**開く** をクリックします。

   メモ: デフォルトの iDRAC ファームウェアイメージ名は **firmimg.imc** です。

8. **ファームウェアアップデートを開 始する** をクリックします。その他の追記事項:
   - ファイル転送時に、更新 ボタンの利用、または他のページへ移動しないでください。
   - アップデートプロセスをキャンセルするには、ファイル転送およびアップデートのキャンセル をクリックします。このオプションは、ファイル転送時にのみ、利用可能です。
   - アップデート状態 フィールドにアップデートステータスが表示されます。このフィールドは、ファイル転送時に自動的に更新されます。

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

---

iDRAC の管理

CMC には、ユーザーがインストールされた、または新規に挿入されたサーバーの iDRAC ネットワークを設定できる iDRAC の配置ページがあります。このページで、ユーザーは、装着されている 1 つまたは複数の iDRAC デバイスを設定できます。また、ユーザーは、デフォルトの iDRAC ネットワーク設定と後でインストールする予定のサーバーのルートパスワードを設定できます。デフォルトは iDRAC QuickDeploy 設定です。

iDRAC の動作の詳細については、デルサポートサイト **support.dell.com** の『iDRAC ユーザーズガイド』を参照してください。

iDRAC QuickDeploy

iDRAC の配置ページの iDRAC QuickDeploy 選択には、新規に挿入されたサーバーに適用されるネットワーク設定が含まれます。この設定を使って QuickDeploy セクションの iDRAC ネットワーク設定 テーブルに値を自動入力できます。QuickDeploy を有効にすると、対象サーバーがインストールされたときに QuickDeploy の設定値をサーバーに適用します。

手順に従って、iDRAC QuickDeploy の設定を有効にし、設定します。

1. CMC ウェブインタフェースにログインします。
2. サーバー を選択します。
3. セットアップ タブをクリックします。 iDRAC の配置ページが表示されます。
4. 必要に応じて QuickDeploy を設定します。

表 5-37 QuickDeploy 設定

設定	説明
QuickDeploy を有効にする	新規に挿入されたサーバーに対してこのページで設定した iDRAC に自動的に表示する QuickDeploy 機能を有効 / 無効にします。自動設定は必ずローカルのLCD パネルで確認します。 **メモ:** これには、サーバー追加時に iDRAC ルート パスワードを設定する ボックスをチェックしたときのルートユーザーパスワードが含まれます。 デフォルト：オフ（無効）
サーバー挿入時に iDRAC ルートパスワードを設 定する	サーバーを挿入したとき、サーバーの iDRAC ルート パスワードを iDRAC ルートパスワード テキスト ボックスに表示される値に変更するかどうかを指定します。
iDRAC ルートパスワード	サーバー挿入時に iDRAC ルート パスワードを設定すると QuickDeploy を有効にするがチェックされていると、シャーシにサーバーが挿入されたとき

	に、このパスワードをサーバーの iDRAC ルート パスワードに割当てます。パスワードは、印刷可能な 1～20 文字(スペース含む)で指定します。
確認用 iDRAC ルート パスワード	iDRAC ルート パスワード フィールドに入力されたパスワードを確認します。
iDRAC LAN を有効にする	iDRAC LAN チャンネルを有効 / 無効にします。 デフォルト：オフ（無効）
iDRAC IPv4 を有効にする	iDRAC 上の IPv4 を有効にします。デフォルト設定は 有効 です。
IPMI over LAN を有効にする	シャーシに装備されている各 iDRAC の IPMI over LAN チャンネルを有効 / 無効にします。 デフォルト：オフ（無効）
iDRAC DHCP を有効にする	シャーシに装備されている各 iDRAC の DHCP を有効 / 無効にします。このオプションを有効にすると、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ます。DHCP は各 iDRAC の設定を自動割当するときに使用されるため、変更できません。 デフォルト：オフ（無効）
iDRAC IPv4 アドレス（スロット 1）を開始する	エンクロージャのスロット1に装備されているサーバーの iDRAC の固定 IP アドレスを指定します。各後続 iDRAC の IP アドレスは、スロットごとにスロット1の IP アドレスから 1 ずつ増加します。IP アドレスにスロット数を足した値がサブネットマスクより大きいと、エラー メッセージが表示されます。 **メモ：** サブネットマスクとゲートウェイは、IP アドレスのように増加しません。 たとえば、IP アドレスが 192.168.0.250 から始まり、サブネットマスクが 255.255.0.0 のとき、スロット 15 の QuickDeploy IP アドレスは 192.168.0.265 です。サブネットマスクが 255.255.255.0 のとき、QuickDeploy 設定の保存 または QuickDeploy 設定を使用して自動入力するボタンを選択すると、「QuickDeploy IP アドレス範囲は QuickDeploy サブネット内で完全でありません」というエラーメッセージが表示されます。
iDRAC IPv4 ネットマスク	新規に挿入されたすべてのサーバーに割当てられた QuickDeploy サブネットマスクを指定します。
iDRAC IPv4 ゲートウェイ	シャーシに装備されているすべての iDRAC に割り当てる QuickDeploy デフォルトゲートウェイを指定します。
iDRAC IPv6 を有効にする	IPv6 を使用できるシャーシに装備されている各 iDRAC の IPv6 アドレス指定を有効にします。
iDRAC IPv6 の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。デフォルト設定は 有効 です。
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。デフォルト設定は "::" 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。デフォルト設定は 64 です。

5. 選択を保存するには QuickDeploy 設定を保存するボタンをクリックします。iDRAC ネットワークの設定を変更した場合は、iDRAC ネットワークの設定を適用するボタンをクリックして、iDRAC への設定を適用します。
6. 表を前回保存した QuickDeploy 設定に更新して、インストールされた各サーバーの iDRAC ネットワーク設定を現在の値に回復するには、更新 ボタンをクリックします。

メモ： 更新ボタンをクリックすると、保存されていないすべての iDRAC QuickDeploy および iDRAC ネットワーク構成設定を削除します。

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

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

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

メモ： QuickDeploy フィールドの変更は即座に反映されますが、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 にコピーするには数分かかる場合があります。更新 ボタンを押すタイミングが早すぎると、 iDRAC サーバーのデータが部分的にしか正しく表示されない場合があります。

iDRAC ネットワーク設定

iDRAC の展開 ページの **iDRAC ネットワーク設定** セクションには、インストールされているすべてのサーバーの iDRAC IPv4 および IPv6 ネットワーク設定が一覧表示されます。この表を使用すると、インストールされている各サーバーの iDRAC ネットワーク設定を行うことができます。各フィールドに表示される初期値は、iDRAC から読み込まれた現在の値です。フィールドを変えて iDRAC ネットワーク設定を保存する をクリックすると、変更した iDRAC のフィールドが保存されます。この手順に従って、iDRAC ネットワーク設定の設定します。

1. CMC ウェブインタフェースにログインします。
2. サーバー を選択します。
3. セットアップ タブをクリックします。

iDRAC の配置ページが表示されます。

4. QuickDeploy を有効にするチェックボックスを選択して、 QuickDeploy 設定を有効にします。
5. 必要に応じて残りの iDRAC ネットワーク設定を設定します。

表 5-38 iDRAC ネットワーク設定

設定	説明
スロット	シャーシでサーバーが装着されているスロットを示します。スロット番号は 1～16（シャーシには使用できるスロットが 16 個あります）の連番 ID で、シャーシのサーバーの場所を識別します。 **メモ:** スロットに装着されているサーバーが 16 以下の場合は、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。
Name	各スロットに装着されているサーバーのサーバー名を表示します。デフォルトでは、スロットは SLOT-01 から SLOT-16 で表示されます。 **メモ:** スロット名に空白またはヌルは指定できません。
LAN を有効にする	LAN チャンネルを有効（チェック）または無効（チェックなし）にします。 **メモ:** LAN が選択されていない(無効)場合は、すべての別のネットワーク設定 (IPMI over LAN、DHCP、IP アドレス サブネット マスクおよび ゲートウェイ) は使用されません。このフィールドはアクセスできません。
ルートパスワードの変更	選択されている場合は、iDRAC ルートユーザーのパスワードの変更を許可できます。この操作を正しく行うためには、iDRAC ルート パスワードおよび確認用 iDRAC ルート パスワード フィールドが入力されている必要があります。
DHCP	選択した DHCP を使用して iDRAC IP アドレス、サブネット マスク、およびデフォルト ゲートウェイを取得します。それ以外のばあいは、iDRAC ネットワーク設定フィールドで定義された値を使います。このフィールドを設定するには、必ず LAN を有効にしてください。
IPMI オーバー LAN	IPMI LAN チャンネルを有効 (チェック) または無効 (チェックなし) にします。このフィールドを設定するには、必ず LAN を有効にしてください。
IP アドレス	静的 IPv4 または IPv6 アドレスがこのスロットにある iDRAC に割り当てられます。
サブネットマスク	このスロットに装着された iDRAC に割当てるサブネット マスクを指定します。
ゲートウェイ	このスロットに装着される iDRAC に割当てられるデフォルトのゲートウェイを指定します。
IPv4 を有効にする	スロット内の iDRAC がネットワーク上の IPv4 プロトコルを使用できるようにします。このオプションを有効にするには、**LAN を有効にする** オプションを選択する必要があります。デフォルト設定は 有効 です。
IPv6 を有効にする	スロット内の iDRAC がネットワーク上の IPv6 プロトコルを使用できるようにします。このオプションを有効にするには、**LAN を有効にする** オプションを選択し、**自動設定** オプションを選択解除する必要があります。デフォルト設定は 無効 です。 **メモ:** このオプションは、サーバーが IPv6 を使用できる場合にのみ利用できます。
自動設定	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。 **メモ:** このオプションは、サーバーが IPv6 を使用できる場合にのみ利用できます。
プレフィックス長	この iDRAC が属する IPv6 サブネットの長さをビット単位で指定します。

6. 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 ボタンを押します。QuickDeploy 設定に変更を加えても、変更内容は保存されます。
7. iDRAC ネットワーク設定をインストールされている各ブレードの現在の値に回復し、 QuickDeploy 表を前回保存した QuickDeploy 設定に更新するには、更新 ボタンを押します。

メモ: 更新 ボタンをクリックすると、保存されていないすべての iDRAC QuickDeploy および iDRAC ネットワーク構成設定が削除されます。

iDRAC ネットワーク設定表は、将来のネットワーク構成設定を反映するため、インストールされているブレード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 ネットワーク構成設定と一致しない場合もあります。更新ボタンを押すと、変更後の iDRAC ネットワーク構成設定で iDRAC の配置ページを更新します。

メモ: QuickDeploy フィールドの変更は即座に反映されますが、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 にコピーするには数分かかる場合があります。更新ボタンを押すタイミングが早すぎると、 象 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。

シングルサインオンを使って iDRAC を起動する

CMC は、サーバーなどの個別シャーシコンポーネントの制限付き管理を提供します。各個別コンポーネントを完全に管理するには、CMC の提供する、サーバーの管理コントローラ(iDRAC) ウェブベースのインタフェースを活用してください。

サーバーページから iDRAC 管理コンソールを起動するには、以下の操作を行います。

1. CMC ウェブインタフェースにログインします。
2. システムツリーで サーバー を選択します。サーバーステータス ページが表示されます。
3. 管理するサーバーに対する iDRAC GUI の起動アイコンをクリックします。

各サーバーに対する iDRAC 管理コンソールを起動するには、

1. CMC ウェブインタフェースにログインします。
2. システムツリーで拡張 サーバー を選択します。すべてのサーバー (1 ～16) が展開されたサーバーリストに表示されます。
3. 表示したいサーバーをクリックします。サーバーステータス ページが表示されます。
4. iDRAC GUI の起動アイコンをクリックします。

この機能は、シングル サインオンを採用しているため、2回目以降に iDRAC GUI を起動する際にユーザーがログインする必要はありません。シングルサインオンの詳細は以下をご覧ください。

- 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 にログインできます。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 に自動ログインできません。このユーザーが iDRAC GUI の起動ボタンをクリックすると、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。パスワードが一致しない同じログイン名を持つユーザーは、同じアカウントを持つと見なされません。

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。

メモ: サーバーがシャーシから取り外された、iDRAC IP アドレスを変更した、または iDRAC ネットワーク接続にエラーが発生した場合、iDRAC GUI の起動アイコン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。

FlexAddress

本項では、FlexAddress® のウェブインタフェース画面について説明します。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 をシャーシで提供される WWN/MAC ID に置き換えることを可能にします。

メモ: 設定画面にアクセスするには、FlexAddress のアップグレードを購入し、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し、インストールしていない場合は、ウェブインタフェース上に次のメッセージが表示されます。

> 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 アドレスの管理機能の詳細については、「Dell Chassis Management Controller ユーザーズガイド」を参照してください。

本機能をご購入になるには、www.dell.com で Dell にお問い合わせください。

FlexAddress ステータスの表示

FlexAddress ステータス情報を表示するには、ウェブインタフェースを使用できます。シャーシ全体または個別のサーバーのステータス情報を閲覧することができます。表示される情報には、以下が含まれます。

- ファブリック構成
- 有効/無効な FlexAddress
- スロット番号および名前
- シャーシ指定およびサーバー指定のアドレス
- 使用アドレス

メモ: コマンドラインインタフェースを使用して FlexAddress ステータスを表示することもできます。コマンドの詳細については、「FlexAddress の使用」 を参照してください。

シャーシ FlexAddress ステータスの表示

シャーシ全体の FlexAddress ステータス情報を表示することが可能です。ステータス情報には、機能が有効であるかどうか、そして各ブレードの FlexAddress ステータスの概要が含まれます。

シャーシにおいて、FlexAddress が有効であるか確認するには、次の手順に従います。

1. ウェブインタフェースにログインします（「CMC ウェブインタフェースへのアクセス」を参照）。
2. システムツリーで **シャーシ** をクリックします。
3. セットアップ タブをクリックします。一般セットアップ ページが表示されます。FlexAddress フィールドには、有効 または 無効 の値が表示されます。「有効」の値は、シャーシ上でこの機能がインストールされていることを意味します。「無効」は、シャーシ上にこの機能がインストールされておらず、利用もされていないことを意味します。

各サーバーモジュールの FlexAddress ステータス概要を表示するには、以下の手順に従います。

1. ウェブインタフェースにログインします（「CMC ウェブインタフェースへのアクセス」を参照）。
2. システムツリーで サーバー をクリックします。プロパティ タブ、 WWN/MAC サブタブを順にクリックします。
3. FlexAddress サマリ ページが表示されます。このページでは、シャーシ内のすべてのスロットの WWN 設定および MAC アドレスを確認することができます。

ステータスページでは、以下の情報を提供します。

ファブリック構成	ファブリック A、 ファブリック B および ファブリック C は、取り付けられている I/O ファブリックの種類を表示します。 **iDRAC** には、サーバー管理 MAC アドレスが表示されます。 **メモ:** ファブリック A を有効にすると、未使用スロットには、装着スロットで使用された場合にファブリックA および MAC のシャーシ指定 MAC アドレス、またはファブックB および Cの WWN 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。表示される情報には、以下が含まれます。 • iDRAC 管理コントローラはファブリックではありませんが、その FlexAddress はファブリックのように処理されます。 • スロット番号および位置 • FlexAddress の有効/無効ステータス • ファブリックタイプ • 使用されているサーバー指定およびシャーシ指定の 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（サーバー指定またはシャーシ指定）を示します。

4. 追加情報については、ヘルプ リンクをクリックし、「FlexAddress の使用」を参照してください。

サーバー FlexAddress ステータスの表示

各個別サーバーの FlexAddress ステータス情報も表示させることができます。サーバーレベル情報は、対象のブレードの FlexAddress ステータス概要を表示します。

FlexAddress サーバー情報を表示するには、次の手順に従います。

1. ウェブインタフェースにログインします（「CMC ウェブインタフェースへのアクセス」を参照）。
2. システムツリーで拡張 サーバー を選択します。すべてのサーバー (1 ～16) が展開されたサーバーリストに表示されます。
3. 表示したいサーバーをクリックします。サーバーステータス ページが表示されます。
4. セットアップ タブ、FlexAddress サブタブを順にクリックします。 FlexAddress ステータス ページが表示されます。このページでは、選択したサーバーの WWN 設定および MAC アドレスを確認することができます。

ステータスページでは、以下の情報を提供します。

有効化された FlexAddress	特定スロット上で FlexAddress 機能が有効または無効であるか表示します。
現在の状態	現在の FlexAddress 設定を表示します。 • シャーシ指定 - 選択したスロットのアドレスには、シャーシ指定の FlexAddress を使用しています。新しいサーバーがインストールされた場合でも、スロットベースの WWN/MAC アドレスは維持されます。

	• サーバー指定 - サーバーはコントローラハードウェアに埋め込まれたサーバー指定のアドレスまたはデフォルトアドレスを使用しています。		
電源状態	サーバーの現在の の電源状態（オン、電源投入中、電源切断中、オフおよび N/A）が表示されます。		
正常性		OK	FlexAddress が存在し、CMC にステータスを提示していることを意味します。CMC と FlexAddress 間で通信エラーが発生した場合には、CMC は FlexAddress の正常性状態を取得または表示できません。
		情報	正常性の状態（OK、警告、重大）に変化がない場合に FlexAddress についての情報を表示します。
		警告	警告アラートが発行されたこと、および対応処置を取る必要があることを示します。システム管理者が指定した時間内に対応処置を取らなかった場合は、サーバーの保全性に影響するような重要または重大なエラーを引き起こす可能性があります。
		重大	少なくとも 1 つのエラー警告が発行されたことを示します。重大な状態はサーバーのシステムエラーを示し、直ちに対応処置を取る必要があります。
		値なし	FlexAddress が不在の場合、正常性情報は提供されません。
iDRAC ファームウェア	現在サーバーにインストールされている iDRAC のバージョンを表示します。		
BIOS バージョン	サーバーモジュールの現在の BIOS バージョンを表示します。		
スロット	ファブリックの場所に関連付けられたサーバーのスロット番号。		
場所	シャーシ内の Input/Output（I/O） の位置をグループ番号（A、B、C）とスロット番号（1 または 2）で示します。スロット名：A1、A2、B1、B2、C1、C2		
ファブリック	ファブリックの種類を表示します。		
サーバー指定	サーバー指定 は、コントローラのハードウェアに埋め込まれたサーバー指定の WWN/MAC アドレスを表示します。		
シャーシ指定	シャーシ指定 は、特定のスロットで使用されるシャーシ指定の WWN/MAC アドレスを表示します。		

5. 追加情報については、ヘルプリンクをクリックし、「FlexAddress の使用」を参照してください。

FlexAddress の設定

FlexAddress をシャーシと一緒に購入された場合はインストール済みで、システムの電源を入れると有効になっています。FlexAddress を別途購入された場合は、『CMC セキュアデジタル (SD) カード技術仕様』に記載されている手順に従って、SD カードに格納されている機能をインストールする必要があります。このマニュアルについては、support.dell.com を参照してください。

設定を開始する前に、サーバーの電源を落とす必要があります。ファブリックごとに FlexAddress を有効または無効にすることができます。また、スロットごとに、機能を有効/無効にすることも可能です。ファブリックごとに機能の有効化を行う場合は、有効にするスロットを選択できます。たとえば、ファブリック-A で FlexAddress を有効にする場合、ファブリック-A のスロットのみが FlexAddress が有効になります。その他のファブリックは、サーバー上で工場で割り当てられた WWN/MAC を使用します。

FlexAddress が有効なスロットは、すべてのファブリックでも有効になります。たとえば、ファブリック-A および B を有効にし、ファブリック-A のスロット 1 で FlexAddress を有効にして、ファブリック-B のスロット 1 で無効にすることはできません。

メモ: コマンドラインインタフェースを使用して FlexAddress ステータスを表示することもできます。コマンドの詳細については、「FlexAddress の使用 を参照してください。

ファブリックおよびスロットのシャーシレベルの FlexAddress 設定

シャーシレベルで、FlexAddress 機能をファブリックおよびスロット上で有効または無効にすることができます。FlexAddress はファブリックごとに有効化を行い、その後にこの機能が有効になるスロットを選択します。FlexAddress を正しく設定するには、ファブリックおよびスロット上で有効にしなければなりません。

FlexAddress 機能をファブリックおよびスロット上で有効または無効にするには、次の手順に従います。

1. ウェブインタフェースにログオンします（「CMC ウェブインタフェースへのアクセス」を参照）。
2. システムツリーで **サーバー** をクリックします。
3. 設定 タブ → **FlexAddress** サブタブをクリックします。FlexAddress の展開 ページが表示されます。
4. シャーシ指定 WWN/MAC のファブリックの選択 に、ファブリック A、ファブリック B、ファブリック C、および iDRAC のチェックボックスを表示します。

5. FlexAddress を有効にしたい各ファブリックのチェックボックスをクリックします。ファブリックを無効にするには、チェックボックスをクリックし、選択をクリアにします。

メモ: ファブリックが選択されていない場合、選択されたスロットに対して FlexAddress は有効になりません。

シャーシ指定 WWN/MAC のスロットの選択 ページには、シャーシの各スロット（1-16）に対して有効 チェックボックスが表示されます。

6. FlexAddress を有効にしたい各スロットの 有効 チェックボックスをクリックします。すべてのスロットを選択したい場合は、すべて選択/ 選択解除 チェックボックスを利用します。スロットを無効にするには、有効 チェックボックスをクリックし、選択をクリアにします。

メモ: スロットにブレードが存在する場合、そのスロットで FlexAddress 機能を有効にする前に、ブレードの電源を落とす必要があります。

メモ: スロットが選択されていない場合、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。

7. 適用 をクリックして変更を保存します。

追加情報については、ヘルプ リンクをクリックし、「FlexAddress の使用」を参照してください。

スロットのサーバーレベルの FlexAddress 設定

サーバーレベルで、FlexAddress 機能を個別スロット上で有効または無効にすることができます。

個別のスロット上で FlexAddress 機能を有効または無効にするには、次の手順に従います。

1. ウェブインタフェースにログインします（「CMC ウェブインタフェースへのアクセス」を参照）。
2. システムツリーで拡張 サーバー を選択します。展開されたサーバーリストにすべてのサーバー（1～16）が表示されます。
3. 表示したいサーバーをクリックします。サーバーステータス ページが表示されます。
4. セットアップ タブ、FlexAddress サブタブを順にクリックします。 FlexAddress ステータス ページが表示されます。
5. FlexAddress 機能を有効にするには、FlexAddress の有効化 プルダウンメニューから はい を選択し、無効にするには いいえ を選択します。
6. 適用 をクリックして変更を保存します。追加情報については、ヘルプ リンクをクリックし、「FlexAddress の使用」を参照してください。

リモートファイル共有

リモート仮想メディアのファイル共有オプションは、CMC を使用して、ネットワーク上の共有ドライブ内のファイルを 1 つ以上のブレードにマッピングし、オペレーティングシステムを導入または更新します。接続が完了すると、リモートファイルはローカルシステムにある場合にアクセス可能です。サポートされている 2 つのメディアの種類はフロッピーディスクと CD/DVD ドライブです。

1. ウェブインタフェースにログインします（「CMC ウェブインタフェースへのアクセス」を参照）。
2. システムツリーで サーバー をクリックします。
3. 設定 タブ、リモートファイル共有 サブタブの順にクリックします。リモートファイル共有の導入 ページが表示されます。
4. リモートファイル共有設定を行います。

表 5-39 リモートファイル共有設定

設定	説明
イメージファイルパス	イメージファイルパスは接続および導入操作でのみ必要です。接続解除操作には適用されません。ネットワークドライブのパス名は、Windows SMB または Linux/Unix NFS プロトコルを使用してサーバーにマウントされます。 たとえば、CIFS に接続するには、//<CIFS ファイルシステムへの接続用 IP>/<ファイルパス>/<イメージ名> を入力します。 NFS に接続するには、：//<NFS ファイルシステムへの接続用 IP>:/<ファイルパス>/<イメージ名>を入力します。 末尾が **.img** のファイル名は仮想フロッピーとして接続されます。末尾が **.iso** のファイル名は仮想 CD/DVD として接続されます。最大文字数は 511 文字です。
ユーザー名	ユーザー名は接続および導入操作でのみ必要です。接続解除操作には適用されません。このフィールドで指定できる最大文字数は 40 です。
パスワード	パスワードは接続および導入操作でのみ必要です。接続解除操作には適用されません。このフィールドで指定できる最大文字数は 40 です。

スロット	スロットの場所を識別します。スロット番号は 1～16（シャーシには使用できるスロットが 16 個あります）の連番 ID です。
Name	スロットの名前を示します。スロットはシャーシ内の位置に応じて名前が付けられます。
Model	サーバーのモデル名を表示します。
電源状態	サーバーの電源状態を表示します。 **該当なし:** CMC はサーバーの電源状態を特定できていません。 **オフ** - サーバーまたはシャーシのどちらかの電源がオフです。 **オン** – シャーシおよびサーバーともに電源がオンです。 **電源投入中** - 電源オフおよび電源オンの間の一時的な状態です。操作が正常に完了すると、電源状態はオンになります。 **電源切断中** - 電源オンおよび電源オフの間の一時的な状態です。操作が正常に完了すると、電源状態はオフになります。
接続状態	リモートファイル共有接続状態を表示します。
すべて選択 / 選択解除	このオプションは、リモートファイル共有操作を行う前に選択します。リモートファイル共有操作には、接続、接続解除、導入の 3 つの操作があります。

5. **接続** をクリックすると、リモートファイル共有に接続されます。リモートファイル共有に接続するには、パス、ユーザー名、およびパスワードを入力する必要があります。操作を正常に完了すると、メディアにアクセスできます。

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

   導入 をクリックすると、メディアデバイスを導入できます。

   メモ: このアクションを行うとサーバーが再起動されるため、作業中のファイルをすべて保存してから、deploy コマンドを実行してください。

   このコマンドでは以下のアクションが実行されます。

   - 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用の最初の起動デバイスとして選択される。
   - サーバーが再起動される。
   - サーバーの電源が切れている場合は、電源がサーバーに投入される。

よくあるお問い合わせ（FAQ）

表5-40 は、よくあるお問い合わせとその回答です。

表 5-40 リモートシステムの管理と回復：よくあるお問い合わせ（FAQ）
よくあるお問い合わせ（FAQ）

質問	回答
CMC ウェブインタフェースにアクセスするとき、SSL 証明書のホスト名と CMC のホスト名が一致しないというセキュリティ警告が表示されます。	CMC には、ウェブインタフェースのネットワークセキュリティを保護するため、デフォルトの CMC サーバー証明書と、リモート RACADM 機能が含まれています。この証明書を使用する場合には、ウェブブラウザにはセキュリティ警告が表示されます。これは、デフォルトの証明書が CMC のホスト名を一致しない **CMC デフォルト証明書** に対して発行されるためです（例：IP アドレス）。 このセキュリティ問題に対応するには、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。証明書の発行に使用する証明書署名要求（CSR）を生成するとき、CSR のコモンネーム（CN）が CMC の IP アドレス（例：192.168.0.120）または登録済みの DNS CMC 名と一致することを確認してください。 CSR を登録されている DNS CMC 名と一致させるには： 1. **システムツリー**で **シャーシ** をクリックします。 2. **ネットワーク / セキュリティ** タブをクリックして**ネットワーク** タブをクリックします。**ネットワーク設定** ページが開きます。 3. **DNS への CMC の登録** チェックボックスを選択します。 4. **DNS CMC 名** フィールドに CMC 名を入力します。 5. **変更の適用** をクリックします。 CSR の生成と証明書の発行については、「SSL とデジタル証明書を使用した CMC 通信のセキュリティ確保」を参照してください。
プロパティを変更すると、リモート RACADM とウエブベースのサービスを使用できなくなる	CMC ウェブサーバーをリセットすると、リモート RACADM サービスとウエブインタフェースに再度アクセスできるようになるまで 1 分ほどかかる場合があります。

のはなぜですか?	次のような状況で CMC ウェブサーバーはリセットされます。 • CMC ウェブインタフェースを使用してネットワーク設定やネットワークセキュリティのプロパティの変更する場合 • **cfgRacTuneHttpsPort** プロパティが変更された（ config -f <設定ファイル> によって変更された場合を含む） • **racresetcfg** が使われた • CMC がリセットされたとき • 新しい SSL サーバー証明書がアップロードされた
DNS サーバーで CMC を登録できない理由は何ですか?	一部の DNS サーバーは 31 文字以内の名前しか登録しません。
CMC ウェブインタフェースにアクセスする場合に、SSL 証明書が信頼されていない認証局（CA）によって発行されまし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のネットワークセキュリティを保護するため、デフォルトの CMC サーバー証明書と、リモート RACADM 機能が含まれています。この証明書は、信頼される認証局から発行されていません。このセキュリティ問題に対応するには、信頼された認証局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ます（例：Thawte または Verisign）。証明書の発行の詳細については、「SSL とデジタル証明書を使用した CMC 通信のセキュリティ確保」を参照してください。

不明な理由で次のメッセージが表示されました。
 	
リモートアクセス：SNMP 認証エラー
 	
原因は何ですか?
	検出作業の一部として、IT Assistant はデバイスの get と set コミュニティ名の確認を試みます。IT Assistantには、get community name = public と set community name = private があります。CMCエージェントのデフォルトコミュニティ名は public です。IT Assistant が set リクエストを送信すると、CMC エージェントはコミュニティ = publicからのリクエストしか受け入れないため、SNMP 認証エラーが生成されます。
	
	RACADM を使用して、CMC のコミュニティ名を変更できます。
	
	CMC コミュニティ名を表示するには、次のコマンドを使用します。
	
	`racadm getconfig -g cfgOobSnmp`
	
	CMC コミュニティ名を設定するには、次のコマンドを使用します。
	
	`racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <コミュニティ名>`
	
	SNMP 認証トラップの生成を防ぐには、エージェントが受け入れるコミュニティ名を入力する必要があります。CMC は 1 つのコミュニティ名しか許可しないので、IT Assistant の検出設定と同じ get および set コミュニティ名を入力する必要があります。

CMC のトラブルシューティング

CMC ウェブインタフェースは、シャーシの識別、診断、およびトラブルシューティングツールを提供します。トラブルシューティングの詳細については、「トラブルシューティングとリカバリ」を参照してください。

目次ページに戻る