Cisco UCS E シリーズ M6 サーバーリリース 4.11.x CLI 設定ガイド

初版：2023 年 8 月 7 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

新機能および変更された機能に関する情報

次の表は、この最新リリースに関するガイドでの主な変更点の概要を示したものです。

表 *1 : Cisco Integrated Management Controller Software* リリース *4.11.1* の新機能

機能	説明	参照先
UCS E シリーズ M6 サーバー（UCS-E1100D-M6）のサポート。	UCS-E1100D-M6 サーバーを Cisco Catalyst 8300 エッジプラットフォームにインストールするためのサポートが追加されました。	Release Notes for Cisco UCS E-Series M6 Servers, Release 4.11.1

対象読者

このガイドは、次の 1 つ以上に責任を持つ、専門知識を備えたデータセンター管理者を主な対象にしています。

- サーバ管理
- ストレージ管理
- ネットワーク管理
- ネットワーク セキュリティ

マニュアルの構成

このマニュアルの構成は、次のとおりです。

章	タイトル	説明
第 1 章	概要	Cisco UCS E シリーズ M6 サーバーと CIMC の概要について説明します。
第 2 章	サーバーのオペレーティング システムのインストール	サーバー上のオペレーティング システム（OS）の設定方法を説明します。
第 3 章	サーバーの管理	サーバーのブートデバイスの順序、サーバーの電源、電力使用ポリシー、および BIOS の設定方法について説明します。
第 4 章	サーバーのプロパティの表示	サーバーの CPU、メモリ、電源、ストレージ、PCI アダプタおよび LOM のプロパティの表示方法について説明します。
第 5 章	サーバーのセンサーの表示	温度、電圧、ストレージのセンサーの表示方法について説明します。
第 6 章	リモートプレゼンスの管理	仮想 KVM、仮想メディア、および Serial over LAN 接続の設定方法を説明します。
第 7 章	ユーザーアカウントの管理	ユーザー アカウントの追加または変更方法、Active Directory によるユーザー認証の設定方法、ユーザー セッションの管理方法を説明します。
第 8 章	ネットワーク関連の設定	ネットワーク インターフェイス、ネットワーク設定、ネットワーク セキュリティ、NAM、および NTP の設定方法を説明します。
第 9 章	コミュニケーションサービスの設定	HTTP、SSH、Redfish、IPMI、および SNMP によるサーバー管理コミュニケーションの設定方法を説明します。
第 10 章	証明書の管理	サーバー証明書を生成、アップロード、および管理する方法を説明します。
第 11 章	プラットフォームイベントフィルタの設定	プラットフォーム イベント フィルタを設定および管理する方法を説明します。
第 12 章	ファームウェア管理	ファームウェアイメージを取得、インストール、およびアクティブにする方法を説明します。

章	タイトル	説明
第 13 章	障害およびログの表示	障害情報の表示方法、CIMC ログとシステムイベントログメッセージの表示、エクスポート、およびクリア方法を説明します。
第 14 章	サーバーユーティリティ	サポートデータのエクスポート方法、サーバー設定のエクスポート方法とインポート方法、サーバー設定を出荷時デフォルトにリセットする方法、管理インターフェイスのリブート方法を説明します。

表記法

テキストのタイプ	説明
GUI 要素	タブの見出し、領域名、フィールド ラベルなどの GUI 要素は、イタリック体（**italic**）で示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトルなどのメイン タイトルは、ボールド体（**bold**）で示しています。
ユーザー入力	表示どおりにユーザーが入力するテキストやユーザーが押すキーは、このフォント（例：**`this font`**）で示しています。
マニュアルのタイトル	マニュアルのタイトルは、イタリック体（*italic*）で示しています。
システム出力	システムが表示するターミナル セッションおよび情報は、`courier` フォントで示しています。
CLI コマンド	CLI コマンドのキーワードは、**this font**で示しています。 CLI コマンドの引数は、このフォント（例：*this font*）で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。

テキストのタイプ	説明
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

ヒント 「問題解決に役立つ情報」です。ヒントには、トラブルシューティングや操作方法ではなく、ワンポイントアドバイスと同様に知っておくと役立つ情報が記述される場合もあります。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ワンポイント アドバイス 「時間の節約に役立つ操作」です。ここに紹介している方法で作業を行うと、時間を短縮できます。

警告 安全上の重要な注意事項

この警告マークは「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。

SAVE THESE INSTRUCTIONS

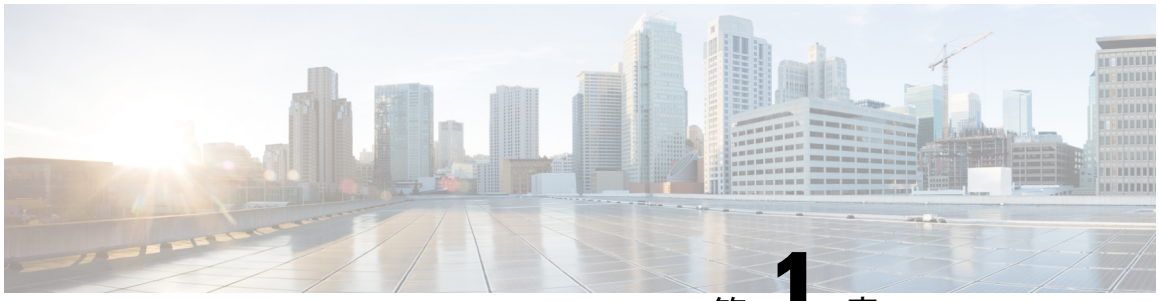
関連資料

『Documentation Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine』にはすべての製品ドキュメントへのリンクが示されています。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカルサポート、その他の有用な情報について、毎月更新される『What's New in Cisco Product Documentation』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

『更新情報』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。



第 1 章

概要

Cisco UCS E シリーズ M6 サーバーの概要

Cisco UCS E シリーズ M6 サーバーは、Cisco Catalyst 8300 シリーズ エッジ プラットフォーム内に収容される、サイズ、重量、電力効率の高いブレードサーバーです。これらのサーバーは、Linux などのオペレーティングシステム上のベアメタルとして、または VMware vSphere Hypervisor などのハイパーバイザー上の仮想マシンとして展開されるブランチオフィス アプリケーションに汎用コンピューティング プラットフォームを提供します。

UCS E シリーズ M6 サーバーは、汎用コンピューティング用の強力な Intel IceLake-D プロセッサを使用して専用に構築されています。ダブル幅のフォームファクタで提供され、2 つの SM スロットに収まります。

（注） E シリーズ M6 サーバー、およびルータごとにインストールできるサーバーの最大数については、『*Hardware Requirements Guide for Cisco UCS E-Series M6 Servers*』の「Hardware Requirements」の項を参照してください。 .

サーバー ソフトウェア

UCS E シリーズ M6 サーバーには、次の 3 つの主要なソフトウェアシステムが必要です。

• CIMC ファームウェア

• BIOS ファームウェア

- オペレーティング システムまたはハイパーバイザ

CIMC ファームウェア

Cisco Integrated Management Controller（CIMC）は、E シリーズ M6 サーバーのマザーボードに組み込まれた個別の管理モジュールです。専用のプロセッサが（メインサーバー CPU から独立して）CIMC ファームウェアを実行します。システムには、現行バージョンの CIMC ファームウェアが付属しています。CIMC ファームウェアは更新可能ですが、初期インストールは必要ありません。

CIMC は E シリーズ M6 サーバー用の管理サービスです。Web ベースの GUI または SSH ベースの CLI を使用して、サーバーにアクセスし、サーバーを設定、管理、モニターできます。

BIOS ファームウェア

BIOS は、システム内のハードウェアを初期化し、ブート可能なデバイスを検出し、それらを指定された順序でブートします。オペレーティング システムを起動したり、オペレーティング システムが使用するハードウェアを設定したりします。使いやすい BIOS 管理機能により、ハードウェアを操作したり、使用したりできます。さらに、BIOS には、システムを設定し、ファームウェアを管理するためのオプションが用意されています。

システムには、現行バージョンの BIOS ファームウェアが付属しています。BIOS ファームウェアを更新できますが、初期インストールは必要ありません。

オペレーティング システムまたはハイパーバイザ

メインサーバー CPU は Linux などのオペレーティングシステム上で、またはハイパーバイザ上で動作します。オペレーティングシステムまたはハイパーバイザがプレインストールされた E シリーズ M6 サーバーを購入することも、独自のプラットフォームをインストールすることもできます。

（注） E シリーズ M6 サーバーで使用可能なプラットフォームの詳細については、『*Release Notes for Cisco UCS E-Series M6 Servers*』の「Software Requirements」の項を参照してください。

CIMC の概要

Cisco Integrated Management Controller（CIMC）は、E シリーズ M6 サーバー用の管理サービスです。CIMC はサーバー内で動作します。Web ベースの GUI または SSH ベースの CLI を使用して、サーバーにアクセスし、サーバーを設定、管理、モニターできます。

CIMC を使用すると次のサーバー管理タスクを実行できます。

- サーバーの電源のオン、電源のオフ、電源再投入、リセット、およびシャットダウンします。
- サーバーのブート順を設定します。

- サーバーのプロパティ、ルータ情報、およびシャーシのステータスを表示します。
- リモートプレゼンスを管理します。
- ローカルユーザーアカウントを作成して管理し、Active Directory によるリモートユーザーの認証をイネーブルにする
- NIC プロパティ、IPv4、VLAN、ネットワークセキュリティなど、ネットワーク関連の設定を行います。
- HTTP、SSH、IPMI over LAN、SNMP、Redfish などの通信サービスを設定します。
- 証明書を管理します。
- プラットフォーム イベント フィルタを設定します。
- 電源、ファン、温度、電圧、電流、LED、ストレージセンサーを監視します。
- CIMC ファームウェアを更新します。
- BIOS ファームウェアを更新します。
- 内部リポジトリからホストイメージをインストールします。
- 障害、アラーム、およびサーバーのステータスをモニターします。
- タイムゾーンを設定しローカルタイムを表示します。
- サーバー障害の発生時にテクニカルサポートデータを収集します。

ほとんどのタスクは、GUI インターフェイスと CLI インターフェイスのいずれでも実行できます。また、一方のインターフェイスで実行されたタスクの結果は、もう一方のインターフェイスにも表示されます。ただし、以下のことは実行できません。

- CIMC GUI を使用して CIMC CLI を呼び出します。
- CIMC CLI で呼び出したコマンドを CIMC GUI に表示します。
- CIMC GUI から CIMC CLI 出力を生成します。

CIMC CLI

CIMC CLI は、E シリーズ M6 サーバー用のコマンドライン管理インターフェイスです。CIMC CLI は、次の方法で起動できます。

- シリアル ポートを使用する。
- SSH を介してネットワーク上で。
- ルータから。次のコマンドを使用します。
  - **hw-module subslot** *slot/subslot* **session imc**：Cisco Catalyst 8300 Edge シリーズ プラットフォームにインストールされた E シリーズ M6 サーバーに使用します。

CLI ユーザには、admin、user（コントロールはできるが設定はできない）、および read-only のいずれかのロールが与えられます。

コマンド モード

CLI のコマンド モードは階層構造になっており、EXEC モードがこの階層の最高レベルとなります。高いレベルのモードは、低いレベルのモードに分岐します。scope コマンドを使用すると、高いレベルのモードから 1 つ低いレベルのモードに移動し、exit コマンドを使用すると、モード階層内の 1 つ高いレベルに移動します。top コマンドを実行すると、EXEC モードに戻ります。

（注） ほとんどのコマンド モードは、管理対象オブジェクトに関連付けられています。**scope** コマンドを実行すると、管理対象オブジェクトは作成されず、管理対象オブジェクトがすでに存在するモードにアクセスできるだけです。

各モードには、そのモードで入力できるコマンドのセットが含まれています。各モードで使用できるほとんどのコマンドは、関連付けられた管理対象オブジェクトに関係しています。割り当てられているロールによっては、あるモードで使用できるコマンドのサブセットにしかアクセスできない場合があります。アクセスできないコマンドは非表示になります。

各モードの CLI プロンプトには、モード階層における現在のモードまでのフルパスが表示されます。これにより、コマンド モード階層での現在位置がわかりやすくなります。また、階層内を移動する必要がある場合には、非常に便利な機能です。

コマンド モード表

次の表に、最初の 4 レベルのコマンド モード、各モードへのアクセスに使用するコマンド、および各モードに関連付けられている CLI プロンプトを示します。

モード名	アクセスするコマンド	モード プロンプト
EXEC	任意のモードから **top** コマンド	#
bios	EXEC モードから scope bios コマンド	/bios #
certificate	EXEC モードから scope certificate コマンド	/certificate #
chassis	EXEC モードから **scope chassis** コマンド	/chassis #
cimc	EXEC モードから scope cimc コマンド	/cimc #

モード名	アクセスするコマンド	モード プロンプト
fault	EXEC モードから scope fault コマンド	/fault #
host-image-mapping	EXEC モードからの **scope host-image-mapping** コマンド	/host-image-mapping#
http	EXEC モードから scope http コマンド	/http #
ipmi	EXEC モードから scope ipmi コマンド	/ipmi #
kvm	EXEC モードから scope kvm コマンド	/kvm #
ldap	EXEC モードから scope ldap コマンド	/ldap #
sel	EXEC モードから scope sel コマンド	/sel #
sensor	EXEC モードから scope sensor コマンド	/sensor #
snmp	EXEC モードから scope snmp コマンド	/snmp #
sol	EXEC モードから scope sol コマンド	/sol #
ssh	EXEC モードから scope ssh コマンド	/ssh #
tacacs+	EXEC モードからの **scope tacacs+** コマンド	/tacacs
user	EXEC モードから **scope user** *user-number* コマンド	/user #
user-policy	EXEC モードからの **scope user-policy** *policy-number* コマンド	/user-policy #
user-session	EXEC モードから **scope user-session** *session-number* コマンド	/user-session #

モード名	アクセスするコマンド	モード プロンプト
vmedia	EXEC モードから scope vmedia コマンド	/vmedia #

コマンドの完了または終了

任意のモードでTabキーを使用すると、コマンドを実行できます。コマンド名の一部を入力してTabを押すと、コマンド全体が表示されるか、または別のキーワードを選択するか引数値を入力する必要があるところまで表示されます。

スコープ内にある場合、**exit** コマンドで 1 レベル上位に移動できます。たとえばスコープが **/chassis/dimm-summary** のときに **exit** を入力した場合、スコープは 1 レベル上位の **/chassis** まで移動します。

コマンド履歴

CLIでは、現在のセッションで使用したすべてのコマンドが保存されます。上矢印キーまたは下矢印キーを使用すると、これまでに使用したコマンドを1つずつ表示できます。上矢印キーを押すと履歴内の直前のコマンドが、下矢印キーを押すと履歴内の次のコマンドが表示されます。履歴の最後に到達すると、下矢印キーを押しても次のコマンドが表示されなくなります。

履歴内のすべてのコマンドは、履歴を1つずつ表示し、目的のコマンドを再度呼び出し、Enterを押すだけでもう一度実行することができます。このコマンドは手動で入力したように表示されます。また、コマンドを再度呼び出した後、実行する前にコマンドを変更することもできます。

保留コマンドのコミット、廃棄、および表示

CLIでコンフィギュレーション コマンドを入力する場合、commit コマンドを入力するまで、そのコマンドは適用されません。コミットされるまで、コンフィギュレーションコマンドは保留状態となり、discardコマンドを入力して廃棄できます。保留中のコマンドについては、アスタリスク（*）がコマンドプロンプトの前に表示されます。この例に示すように、commitコマンドを入力するとそのアスタリスクは消えます。

```
Server# scope kvm
Server /kvm # set enabled yes
Server /kvm *# commit
Server /kvm #
```

複数のコマンド モードで保留中の変更を積み重ね、commit コマンド 1 つでまとめて適用できます。任意のコマンド モードで show configuration pending コマンドを入力して、保留中のコマンドを表示できます。

（注） 複数のコマンドをまとめてコミットするのは、アトミック操作ではありません。失敗したコマンドがあっても、成功したコマンドは適用されます。失敗したコマンドはエラーメッセージで報告されます。

注意 同じスコープの中で行った変更をコミットするには、**commit** コマンドを使用しなければなりません。**commit** コマンドを使用して、別のスコープで行った変更の送信を試みると、エラーが返されます。これらの変更は再実行し、再コミットする必要があります。

コマンド出力形式

ほとんどの CLI **show** コマンドでは、オプションの **detail** キーワードを指定でき、出力情報は表ではなくリスト形式で表示されます。

出力情報を **detail** コマンドで表示する方法に応じて、次のコマンドのいずれかを使用します。

- **set cli output default**：見やすいデフォルト形式。コマンド出力は、コンパクトなリストで表示されます。

  次に、デフォルト形式のコマンド出力例を示します。

```
Server /chassis # set cli output default
Server /chassis # show hdd detail
Name HDD_01_STATUS:
    Status : present
Name HDD_02_STATUS:
    Status : present
Name HDD_03_STATUS:
    Status : present

Server /chassis #
```

- **set cli output yaml**：スクリプトによって簡単に解析できる YAML 形式。コマンド出力は、定義された文字列で区切られた YAML Ain't Markup Language（YAML）データ シリアル化言語で表示されます。

  次に、YAML 形式のコマンド出力例を示します。

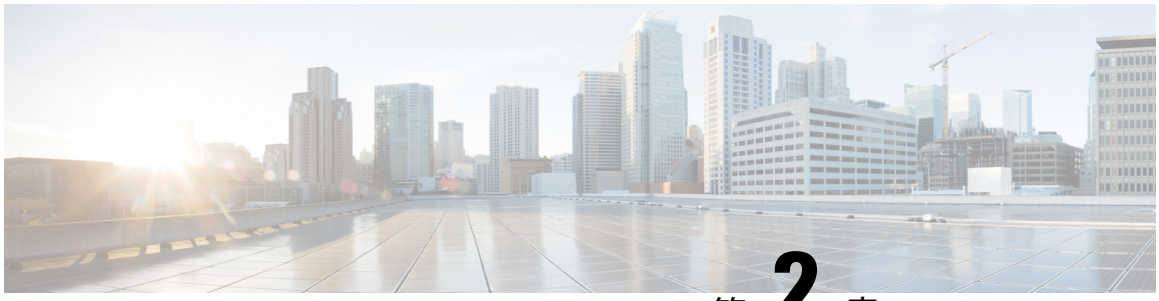
```
Server /chassis # set cli output yaml
Server /chassis # show hdd detail
---
    name: HDD_01_STATUS
    hdd-status: present

---
    name: HDD_02_STATUS
    hdd-status: present

---
    name: HDD_03_STATUS
    hdd-status: present
```

```
...
Server /chassis #
```

YAML の詳細については、http://www.yaml.org/about.html を参照してください。

CLI に関するオンラインヘルプ

いつでも **?** 文字を入力して、コマンド構文の現在の状態で使用可能なオプションを表示することができます。プロンプトに何も入力せずに「?」を入力すると、現在のモードで使用できるコマンドがすべて表示されます。コマンドの一部を入力して「?」を入力すると、その時点のコマンド構文内の位置で使用可能なキーワードと引数がすべて表示されます。



第 2 章

サーバーのオペレーティング システムまたはハイパーバイザのインストール

オペレーティング システムまたはハイパーバイザのインストール方法

UCS E シリーズ M6 サーバーは、複数のオペレーティングシステムとハイパーバイザをサポートします。インストールされるプラットフォームに関係なく、次のいずれかのツールを使用してサーバーにインストールできます。

- KVM コンソール
- PXE インストール サーバー
- ホスト イメージ マッピング

⚠

注意 仮想ドライブをマップするには 1 種類だけを使用する必要があります。たとえば、KVM コンソールまたは Host Image Mapping のいずれかを使用します。組み合わせて使用すると、サーバーが未定義の状態になります。

KVM コンソール

KVM コンソールはCIMCからアクセス可能なインターフェイスであり、サーバーへのキーボード、ビデオ、マウスの直接接続をエミュレートします。KVMコンソールを使用すると、リモートの場所からサーバーに接続できます。サーバーに物理的に接続された CD/DVD ドライブを使用する代わりに、KVM コンソールは仮想メディアを使用します。これは、仮想 CD/DVD ドライブにマップされる実際のディスクドライブまたはディスクイメージファイルです。次のいずれでも仮想ドライブにマップできます。

- お使いのコンピュータ上の CD/DVD
- コンピュータ上のディスク イメージ ファイル（ISO または IMG ファイル）
- コンピュータ上の USB フラッシュ ドライブ

KVM コンソールを使用して、サーバーにオペレーティング システムまたはハイパーバイザをインストールし、次の作業を行うことができます。

- 起動中に F2 を押して、BIOS セットアップ メニューにアクセスします。
- 起動中に F8 を押して、CIMC 設定ユーティリティにアクセスします。

KVMコンソールを使用したオペレーティングシステムまたはハイパーバイザのインストール

KVM コンソールは GUI を介してのみ動作するため、CLI を使用してオペレーティング システムまたはハイパーバイザをインストールすることはできません。KVM コンソールを使用してプラットフォームをインストールするには、『*GUI Configuration Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine*』の『Installing an Operating System or Hypervisor Using the KVM Console』セクションの説明に従ってください。.

PXE インストール サーバー

Preboot Execution Environment（PXE）インストール サーバーを使用すると、クライアントはリモートの場所からオペレーティング システムまたはハイパーバイザをブートおよびインストールできます。この方法を使用するには、PXE環境が設定されていて、VLAN（通常は専用のプロビジョニングVLAN）で使用できるようになっている必要があります。さらに、サーバーがネットワークからブートするように設定されている必要があります。サーバーは、ブートすると、PXE 要求をネットワーク経由で送信します。PXE インストールサーバーは、この要求に応答確認し、サーバーにオペレーティングシステムまたはハイパーバイザをインストールするイベントのシーケンスを開始します。

PXEサーバーは、インストールディスク、ディスクイメージ、またはスクリプトを使用して、オペレーティング システムまたはハイパーバイザをインストールできます。また、独自のディ

スクイメージを使用して、プラットフォーム、追加コンポーネント、またはアプリケーションをインストールすることもできます。

（注） PXEインストールは、多数のサーバーにプラットフォームをインストールする場合に効率のよい方法です。ただし、この方法を使用するにはPXE環境をセットアップする必要があることを考えると、他のインストール方法を使用する方が簡単な場合があります。

PXEインストールサーバーを使用したオペレーティングシステムまたはハイパーバイザのインストール

始める前に

VLAN 経由でサーバーに到達できることを確認します。

ステップ1 ブート順を [PXE] に設定します。

ブート順の設定の詳細については、「UEFIマップとUEFIOSを使用したサーバーのブート順の設定」の項を参照してください。

ステップ2 サーバーをリブートします。

注意 共有 LOM インターフェイスを使用して CIMC にアクセスしている場合は、サーバーのリブート プロセス中に CIMC GUI を使用しないでください。CIMC GUI を使用すると、イーサネット ポートに設定されていた IP アドレスがブート エージェントによってオーバーライドされるため、PXE のインストール中に GUI の接続が解除されます。

VLAN で PXE インストール サーバを使用できる場合は、サーバが再起動するとインストール プロセスが開始します。通常、PXE インストールは自動化されており、追加のユーザ入力を必要としません。残りのインストールプロセスについては、インストールしているオペレーティング システムまたはハイパーバイザのインストレーション ガイドを参照してください。

次のタスク

インストールが完了したら、LAN のブート順を元の設定にリセットします。

ホスト イメージ マッピング

ホストイメージマッピング機能を使用すると、ホストイメージのダウンロード、マッピング、マッピング解除、または削除を行うことができます。Linux や VMware などのホストイメージをリモート FTP または HTTP サーバーから CIMC 内部リポジトリにダウンロードし、そのイ

メージを E シリーズ M6 サーバーの USB コントローラの仮想ドライブにマッピングします。イメージをマップした後は、イメージをマウントした仮想ドライブが最初のブートデバイスになるようにブート順序を設定してから、サーバーをリブートします。ホストイメージのファイル拡張子は必ず .iso になります。

ホスト イメージのマッピング

始める前に

- admin 権限を持つユーザーとして CIMC にログインします。
- 適切なサードパーティからホスト イメージ ファイルを取得します。

（注） アップデートがすでに処理中であるときにイメージアップデートを開始すると、どちらのアップデートも失敗します。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope host-image-mapping**	remote install コマンド モードを開始します。
ステップ 2	Server /host-image-mapping # **download-image** {**ftp** | **ftps** | **http** | **https** | **scp**} *server-ip-address path / filename* [**username** *username* **password** *password*]	指定したリモート サーバーから CIMC 内部リポジトリにイメージをダウンロードします。ホストイメージのファイル拡張子は必ず .iso になります。リモートサーバーには、FTP、FTPS、SCP、HTTP、または HTTPS サーバーを使用できます。リモート サーバーでユーザー認証が必要な場合は、リモート サーバーのユーザー名とパスワードを追加する必要があります。 （注） イメージ ファイルがサイズ制限を超えると、エラー メッセージが表示されます。 （注） HTTP サーバーはユーザー認証をサポートしていません。FTP だけがユーザー認証をサポートしています。
ステップ 3	（オプション）Server /host-image-mapping # **show detail**	イメージダウンロードのステータスを表示します。
ステップ 4	Server /host-image-mapping # **map-image** *image_name.iso*	USB コントローラの仮想ドライブにイメージをマウントします。仮想ドライブには、次のいずれかを使用できます。

	コマンドまたはアクション	目的
		• HDD：ハード ディスク ドライブ • CDROM：ブート可能 CD-ROM
ステップ 5	（オプション）Server /host-image-mapping # **show detail**	ホスト イメージ マッピングのステータスを表示します。

例

次の例は、ホストイメージをマッピングする方法を示しています。

```
Server /host-image-mapping # download-image http 10.126.254.155 /download/image_name.iso
Username:
Password:
Image download has started.
Please check the status using "show detail".
Current Mapped Image: None
Host Image Status: "Downloading ..Please wait: 8.1%"

Server /host-image-mapping # show detail
Current Mapped Image: None
Host Image Status: Image Downloaded and Processed Successfully
Server /host-image-mapping # map-image
Please check the status using "show detail".

Server /host-image-mapping # show detail
Current Mapped Image: image_name.iso
Host Image Status: Image mapped successfully, set HDD as the Boot device.
Server /host-image-mapping #
```

次のタスク

1. イメージがインストールされている仮想ドライブが最初にブートされるデバイスになるように、ブート順を設定します。「UEFI マップと UEFIOS を使用したサーバーのブート順の設定」を参照してください。
2. サーバーをリブートします。イメージにアンサー ファイルが含まれている場合は、オペレーティング システムのインストールは自動化され、イメージがインストールされます。それ以外の場合は、インストール ウィザードが表示されます。ウィザードの手順に従って、イメージをインストールします。
3. オペレーティング システムまたはハイパーバイザをインストールした後にディスク ドライブが表示されない場合は、ドライバをインストールする必要があります。詳細については「CIMC ファームウェアの概要」を参照してください。
4. インストールが完了したら、仮想メディアのブート順を元の設定にリセットします。

ホスト イメージのマッピング解除

始める前に

admin 権限を持つユーザーとして CIMC にログインします。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope host-image-mapping**	remote install コマンド モードを開始します。
ステップ 2	Server /host-image-mapping # **unmap-image**	USB コントローラの仮想ドライブからイメージをマウント解除します。
ステップ 3	Server /host-image-mapping # **show detail**	（任意）ホストのイメージのマッピング解除に関するステータスを表示します。

例

次に、ホストイメージのマップを解除する例を示します。

```
Server /host-image-mapping # unmap-image
Please check the status using "show detail".
Server /host-image-mapping # show detail
Current Mapped Image: None
Host Image Status: Unmap Successful!!
Server /host-image-mapping #
```

ホスト イメージの削除

始める前に

admin 権限を持つユーザーとして CIMC にログインします。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope host-image-mapping**	リモートのインストール モードを開始します。
ステップ 2	Server /host-image-mapping # **delete-image**	CIMC 内部リポジトリからイメージを削除します。

例

次に、ホストのイメージを削除する例を示します。

```
Server# scope host-image-mapping
Server /host-image-mapping # delete-image
```

MGF（TE1）インターフェイスによるESXネットワーク接続の設定

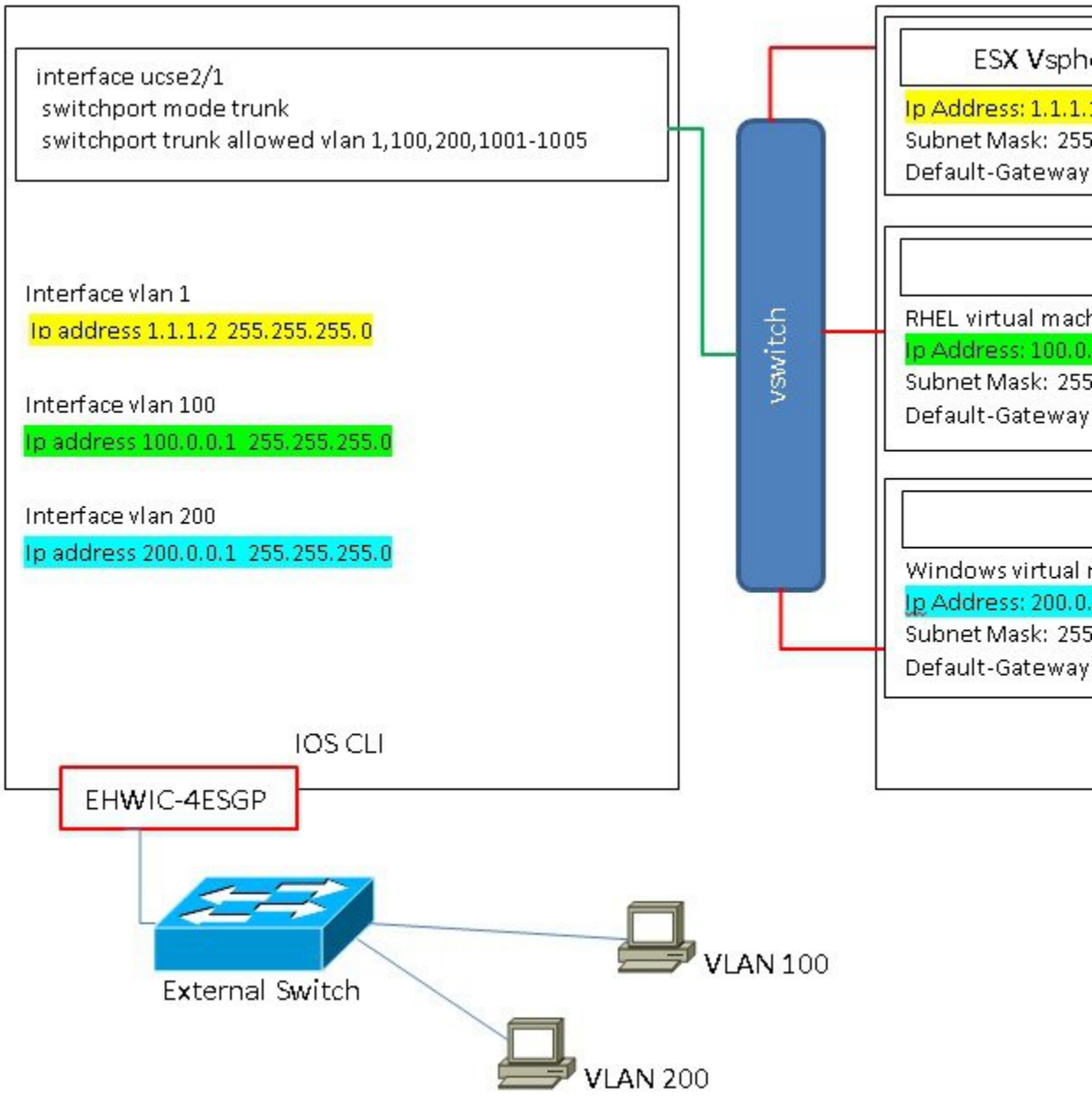
E シリーズ M6 サーバーでは、MGF (TE1) インターフェイスはバックプレーンを介してイーサネット スイッチ モジュールに内部接続します。この項では、UCS E シリーズ ホストと外部ネットワーク間の通信リンクの設定方法について説明します。

MGF (TE1) インターフェイスを介して ESX ネットワーク接続を設定できるシナリオは 2 つあります。

- L2 ネットワーキング：ホストと VM が同じサブネット内にある
- L3 ネットワーキング：ホストと VM が異なるネットワークにある
- L3 ネットワーキング：ホストと VM が同じネットワーク内にある

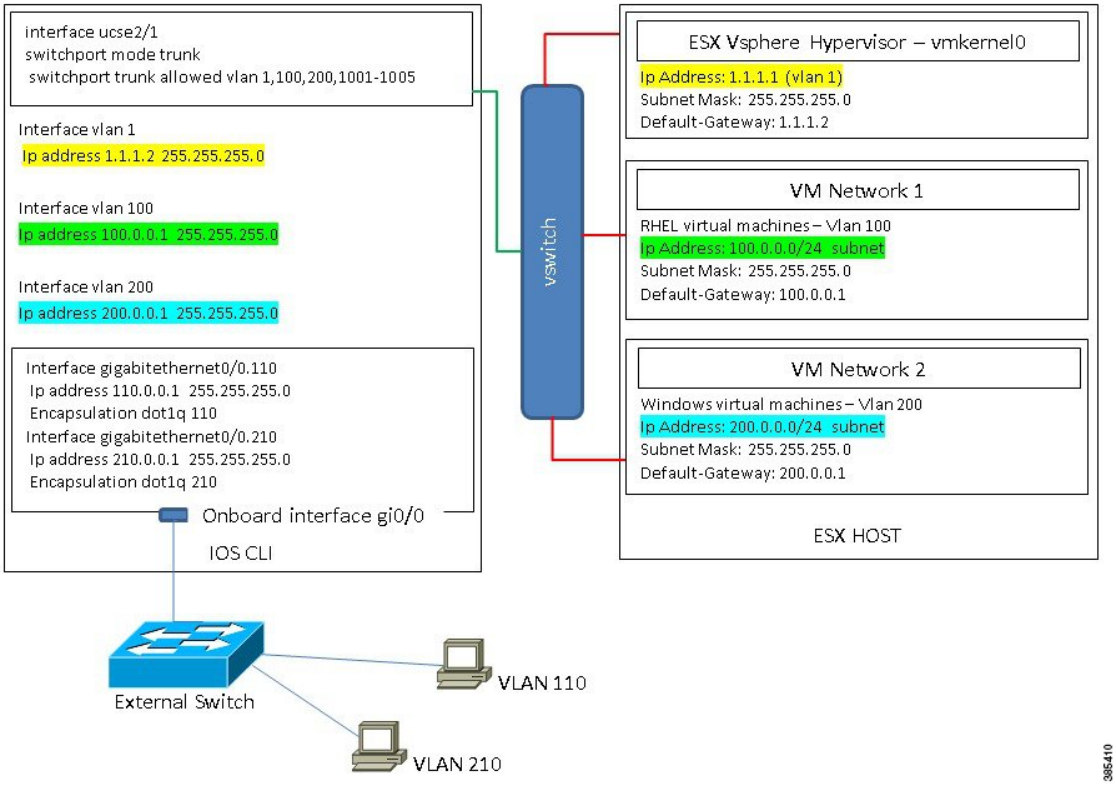
L2 ネットワーキング：ホストと VM が同じサブネット内にある

このシナリオでは、UCS E シリーズ M6 サーバーは VLAN 100 および 200 で VMS をホストしています。トラフィックはルータに入り、UCSE2/1/GE1 インターフェイスを通過し、EHWIC モジュールによって物理ホストに切り替わります。



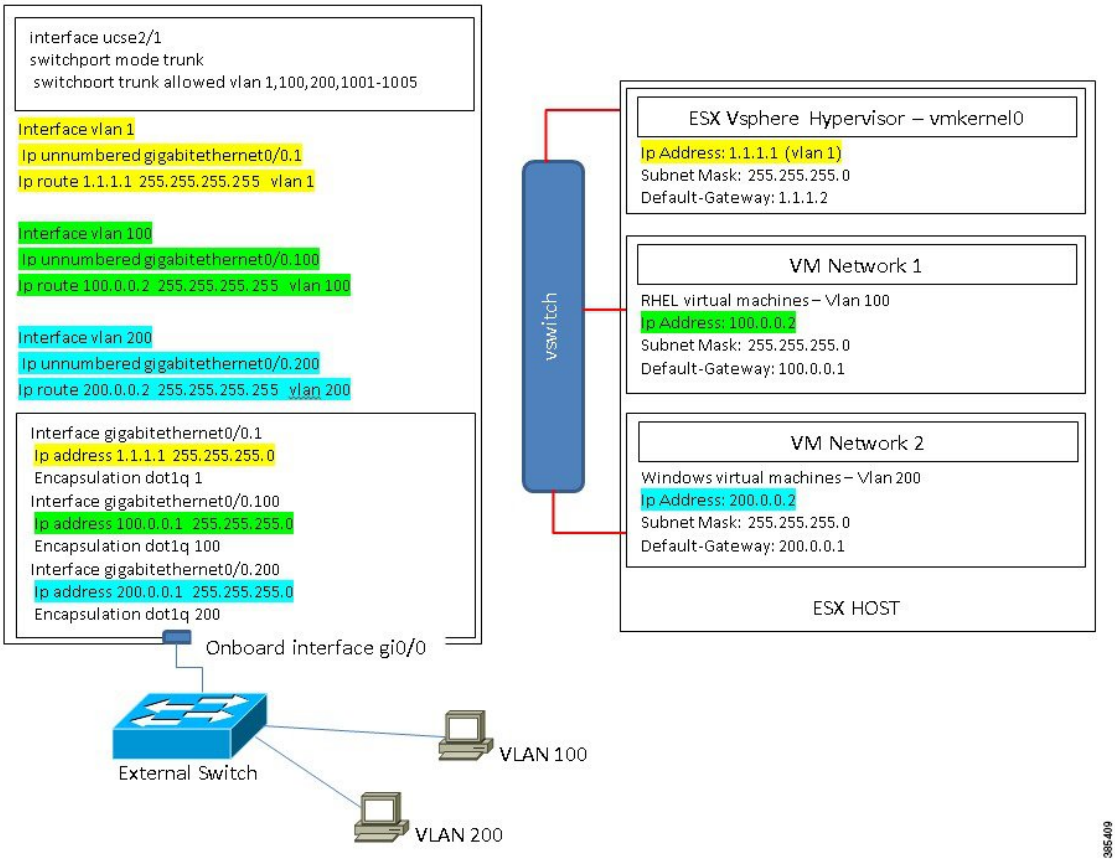
L3 ネットワーキング：ホストと VM が異なるネットワークにある

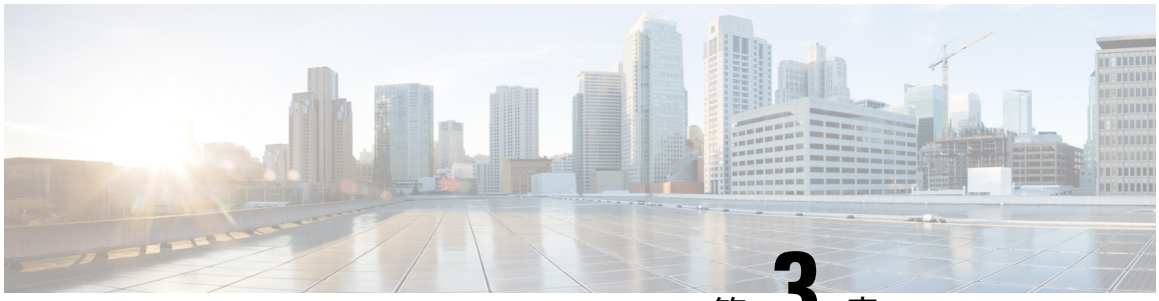
このシナリオでは、VM は UCSE1/0/1 経由でルータにトラフィックを送信することにより、異なるサブネット内のホストと通信します。ルータ上では、トラフィックは VLAN インターフェイスに到達し、Catalyst 8300 シリーズ エッジ プラットフォームによってルーティングされる L3 を取得します。



L3 ネットワーキング：ホストと VM が同じネットワーク内にある

このシナリオでは、物理ホストはVMと同じサブネット内にあります。次の設定により物理ホストをオンボードL3インターフェイスに接続し、VMと物理ホスト間の通信を有効にできます。


interface ucse2/1
switchport mode trunk
switchport trunk allowed vlan 1,100,200,1001-1005
Interface vlan 1
Ip unnumbered gigabitethernet0/0.1
Ip route 1.1.1.1 255.255.255.255 vlan 1
Interface vlan 100
Ip unnumbered gigabitethernet0/0.100
Ip route 100.0.0.2 255.255.255.255 vlan 100
Interface vlan 200
Ip unnumbered gigabitethernet0/0.200
Ip route 200.0.0.2 255.255.255.255 vlan 200
Interface gigabitethernet0/0.1
Ip address 1.1.1.1 255.255.255.0
Encapsulation dot1q 1
Interface gigabitethernet0/0.100
Ip address 100.0.0.1 255.255.255.0
Encapsulation dot1q 100
Interface gigabitethernet0/0.200
Ip address 200.0.0.1 255.255.255.0
Encapsulation dot1q 200
Onboard interface gi0/0
External Switch
VLAN 100
VLAN 200
vswitch
ESX Vsphere Hypervisor – vmkernel0
Ip Address: 1.1.1.1 (vlan 1)
Subnet Mask: 255.255.255.0
Default-Gateway: 1.1.1.2
VM Network 1
RHEL virtual machines – Vlan 100
Ip Address: 100.0.0.2
Subnet Mask: 255.255.255.0
Default-Gateway: 100.0.0.1
VM Network 2
Windows virtual machines – Vlan 200
Ip Address: 200.0.0.2
Subnet Mask: 255.255.255.0
Default-Gateway: 200.0.0.1
ESX HOST
385409



第 3 章

サーバの管理

サーバーのブート順の設定

（注） ホストが BIOS 電源投入時自己診断テスト（POST）を実行している間は、ブート順を変更しないでください。

始める前に

このタスクを実行するには、user または admin 権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **set boot-order** *device1, device2, device3....*	ブート デバイス オプションと順序を指定します。 （注） オプションでは、大文字と小文字は区別されません。

	コマンドまたはアクション	目的
		次の 1 つ以上を選択できます。 • uefimap • uefios • uefipxeTE0/TE1/TE3/TE4 • uefipxeGE2
ステップ 3	Server /bios # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 4	（任意）Server /bios # **show detail**	サーバーのブート順を表示します。

次回の BIOS ブートでは、新しいブート順が使用されます。

例

次に、ブート順を設定し、トランザクションをコミットする例を示します。

```
server /bios # set boot-order uefimap,uefios
To manage boot-order:
- Reboot server to have your boot-order settings take place
- Do not disable boot options via BIOS screens
- If a specified device type is not seen by the BIOS, it will be removed
from the boot order configured on the BMC
- Your boot order sequence will be applied subject to the previous rule.
The configured list will be appended by the additional device types
seen by the BIOS
- Legacy Boot Order configuration will disable all the active Boot Devices which will
hide them from BIOS

server /bios *# commit
Changes to BIOS set-up parameters will require a reboot.
Do you want to reboot the system?[y|N]y
A system reboot has been initiated.

server /bios # show detail
BIOS:
BIOS Version: UCSEDM6_1.08
BIOS Flash: 1
Backup BIOS Version: UCSEDM6_1.08
Backup BIOS Flash: 0
BIOS Post Complete: 0
Boot Order: UEFIMAP,UEFIOS
FW Update Status: Done, OK
Password: ******
server /bios #
```

サーバーのリセット

始める前に

このタスクを実行するには、user または admin 権限でログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **power hard-reset**	確認プロンプトの後に、サーバーがリセットされます。 （注） サーバーの電源の再投入は、x86 サーバーの電源をオフにしてからオンにすることと同じです。 （注） 電源のハードリセットは、サーバーの実際のリセット ボタンを押す動作と同じです。

例

次に、サーバをリセットする例を示します。

```
Server# scope chassis
Server /chassis # power hard-reset
This operation will change the server's power state.
Continue?[y|N]y
```

サーバーのシャットダウン

始める前に

このタスクを実行するには、user または admin 権限でログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	Server /chassis # **power shutdown**	確認プロンプトの後で、サーバーをシャットダウンします。

例

次に、サーバーをシャットダウンする例を示します。

```
Server# scope chassis
Server /chassis # power shutdown

This operation will change the server's power state.
Do you want to continue?[y|N]y
```

Cisco IOS CLI 設定変更のロック

Cisco IOS CLI を使用して設定変更が行われないようにするには、この手順を実行します。

始める前に

このタスクを実行するには、user または admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **show detail**	（任意）サーバーのプロパティを表示します。IOS ロック アウトの現在のステータス（ロックまたはロック解除されているかどうか）を決定することができます。
ステップ 3	Server /chassis # **set ios-lockout locked**	設定変更が Cisco IOS CLI を使用して行われないようにします。
ステップ 4	Server /chassis* # **commit**	変更をコミットします。
ステップ 5	Server /chassis # **show detail**	（任意）サーバーのプロパティを表示します。IOS ロック アウトの現在のステータス（ロックまたはロック解除されているかどうか）を決定することができます。

例

次に、設定変更が Cisco IOS CLI を使用して行われないようにする例を示します。

```
Server /chassis # show detail
Chassis:
Power: off
    IOS Lockout: unlocked
    Power Button: unlocked
    Reset Button: unlocked
    Serial Number: FOC26285Q4B
    Product Name: UCS E1100D M6
    PID: UCS-E1100D-M6
    UUID: 1CD1E026-089C-0000-E822-D9826168E8F8
    Description:
    Asset Tag: Unknown
    FPGA Version: 3.4.2
    Uptime: 22 hours, 54 minutes
    SBFPGA Version: 1.0.2
    MCU Version: 240.10
    AIKIDO Version: 2711-270
    Last Reboot Reason: Flash Reset
Server /chassis # set ios-lockout locked
Server /chassis *# commit
Server /chassis # show detail
Chassis:
    Power: off
    IOS Lockout: locked
    Power Button: unlocked
    Reset Button: unlocked
    Serial Number: FOC26285Q4B
    Product Name: UCS E1100D M6
    PID : UCS-E1100D-M6
    UUID: 1CD1E026-089C-0000-E822-D9826168E8F8
    Description:
    Asset Tag: Unknown
    FPGA Version: 3.4.2
    Uptime: 22 hours, 54 minutes
    SBFPGA Version: 1.0.2
    MCU Version: 240.10
    AIKIDO Version: 2711-270
    Last Reboot Reason: Flash Reset
```

Cisco IOS CLI 設定変更のロック解除

この手順を使用して、Cisco IOS CLI を使用した設定変更を許可します。

始める前に

このタスクを実行するには、user または admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **show detail**	（任意）サーバーのプロパティを表示します。IOS ロック アウトの現在のステータス（ロックまたはロック解除されているかどうか）を決定することができます。
ステップ 3	Server /chassis # **set ios-lockout unlocked**	Cisco IOS CLI を使用した設定変更を許可します。
ステップ 4	Server /chassis* # **commit**	変更をコミットします。
ステップ 5	Server /chassis # **show detail**	（任意）サーバーのプロパティを表示します。IOS ロック アウトの現在のステータス（ロックまたはロック解除されているかどうか）を決定することができます。

例

次に、Cisco IOS CLI を使用した設定変更を許可する例を示します。

```
Server /chassis # show detail
Chassis:
    Power: off
    IOS Lockout: locked
    Power Button: unlocked
    Reset Button: unlocked
    Serial Number: FOC26285Q4B
    Product Name: UCS E1100D M6
    PID : UCS-E1100D-M6
    UUID: 1CD1E026-089C-0000-E822-D9826168E8F8
    Description:
    Asset Tag: Unknown
    FPGA Version: 3.4.2
    Uptime: 22 hours, 54 minutes
    SBFPGA Version: 1.0.2
    MCU Version: 240.10
    AIKIDO Version: 2711-270
    Last Reboot Reason: Flash Reset
Server /chassis # set ios-lockout unlocked
Server /chassis *# commit
Server /chassis # show detail
Chassis:
    Power: off
    IOS Lockout: unlocked
    Power Button: unlocked
    Reset Button: unlocked
    Serial Number: FOC26285Q4B
    Product Name: UCS E1100D M6
    PID : UCS-E1100D-M6
    UUID: 1CD1E026-089C-0000-E822-D9826168E8F8
    Description:
    Asset Tag: Unknown
    FPGA Version: 3.4.2
```

```
    Uptime: 22 hours, 54 minutes
    SBFPGA Version: 1.0.2
    MCU Version: 240.10
    AIKIDO Version: 2711-270
    Last Reboot Reason: Flash Reset
Server /chassis #
```

サーバーの電源管理

サーバーの電源投入

（注） サーバーの電源がCIMC経由以外の何らかの方法でオフにされた場合、サーバーは電源をオンにしてもすぐにはアクティブになりません。この場合、CIMC が初期化を完了するまで、サーバーはスタンバイ モードに入ります。

始める前に

このタスクを実行するには、user または admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **power on**	確認のプロンプトが表示されたら、サーバーの電源をオンにします。

例

次に、サーバーの電源をオンにする例を示します。

```
Server /chassis # power on
This operation will change the server's power state.
Do you want to continue?[y|N]y
Server /chassis # show
Power   Serial Number    Product Name      PID    UUID
----- --------------- ----------------- -----------------  ----------------------------
on      FOC26071VZY      UCS E1100D M6     UCS-E1100D-M6    1CD1E026-0311-0000-
0F12-FC9ABB95AA0A

Server /chassis #
```

サーバーの電源オフ

始める前に

このタスクを実行するには、user または admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **power off**	サーバーの電源をオフにします。

例

次に、サーバーの電源をオフにする例を示します。

```
Server# scope chassis
Server /chassis # power off
This operation will change the server's power state.
Do you want to continue?[y|N]y
Server /chassis # show
Power  Serial Number  Product Name    PID   UUID
----- ------------- ---------------- ------------- --------------------------
off   FOC26071VZY    UCS E1100D M6   UCS-E1100D-M6  1CD1E026-0311-0000-0F12-FC9ABB95AA0A

Server /chassis #
```

サーバー電源の再投入

始める前に

このタスクを実行するには、user または admin 権限でログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **power cycle**	確認のプロンプトが表示されたら、サーバーの電源を再投入します。

	コマンドまたはアクション	目的
		（注） • サーバーの電源の再投入は、x86 サーバーの電源をオフにしてからオンにすることと同じです。 • 電源のハードリセットは、サーバーの実際のリセット ボタンを押す動作と同じです。

例

次に、サーバ電源を再投入する例を示します。

```
Server# scope chassis
Server /chassis # power cycle

This operation will change the server's power state.
Continue?[y|N]y
```

電力復元ポリシーの設定

電力復元ポリシーによって、シャーシの電力供給が失われた後、サーバーに電力を復元する方法が決定されます。

始める前に

このタスクを実行するには、user または admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc #**scope power-restore-policy**	電力復元ポリシー コマンドを入力します。
ステップ 3	Server /cimc/power-restore-policy # **set policy** {**power-off** | **power-on** | **restore-last-state**}	シャーシの電源が復旧した場合に実行するアクションを指定します。次のいずれかを選択します。 • **power-off**：サーバーの電源は、手動で投入されるまでオフのままになります。 • **power-on**：サーバーの電源は、シャーシの電源が回復したときにオンになります。

	コマンドまたはアクション	目的
		• **restore-last-state**：サーバーを電源損失前と同じ電源状態（オフまたはオン）に復元します。これがデフォルトのアクションになります。
ステップ 4	Server /cimc/power-restore-policy# **commit**	トランザクションをシステムの設定にコミットします。

例

次の例では、電力復元ポリシーを power-onに設定して、トランザクションをコミットします。

```
Server# scope CIMC
Server /CIMC # scope power-restore-policy
Server /CIMC/power-restore-policy # set policy power-on
Server /CIMC/power-restore-policy *# commit
Server /CIMC/power-restore-policy #  show detail
Power Restore Policy:
    Power Restore Policy: power-on

Server /CIMC/power-restore-policy #
```

サーバーの前面パネルの電源ボタンのロック

物理サーバーの前面パネルにある物理電源ボタンをディセーブルにするには、この手順を使用します。電源ボタンがディセーブルになると、前面パネルの電源ボタンを使用してサーバーの電源をオンまたはオフにすることはできません。

始める前に

このタスクを実行するには、user または admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **show detail**	（任意）サーバーのプロパティが表示されます。電源ボタンの現在のステータス（ロックまたはロック解除されているかどうか）を決定することができます。
ステップ 3	Server /chassis # **set power-button locked**	電源ボタンをディセーブルにします。前面パネルの電源ボタンを使用して、サーバーの電源をオンまたはオフにすることはできません。

	コマンドまたはアクション	目的
ステップ 4	Server /chassis* # **commit**	変更をコミットします。
ステップ 5	Server /chassis # **show detail**	（任意）サーバーのプロパティが表示されます。電源ボタンの現在のステータス（ロックまたはロック解除されているかどうか）を決定することができます。

例

次に、物理サーバーの前面パネルにあるサーバーの物理的な電源ボタンをディセーブルにする例を示します。

```
Server# scope chassis
Server /chassis # show detail
Chassis:
    Power: off
    IOS Lockout: unlocked
    Power Button: unlocked
    Reset Button: unlocked
    Serial Number: FOC26285PBW
    Product Name: UCS E1100D M6
    PID : UCS-E1100D-M6
    UUID: 1CD1E026-05DC-0000-88E4-3E11AF0AA302
    Description:
    Asset Tag: Unknown
    FPGA Version: 3.4.2
    Uptime: 4 hours, 22 minutes
    SBFPGA Version: 1.0.2
    MCU Version: 240.9
    AIKIDO Version: 271e-270
    Last Reboot Reason: Flash Reset
Server /chassis # set power-button locked
Server /chassis *# commit
Server /chassis # show detail
Chassis:
    Power: off
    IOS Lockout: unlocked
    Power Button: locked
    Reset Button: unlocked
    Serial Number: FOC26285PBW
    Product Name: UCS E1100D M6
    PID : UCS-E1100D-M6
    UUID: 1CD1E026-05DC-0000-88E4-3E11AF0AA302
    Description:
    Asset Tag: Unknown
    FPGA Version: 3.4.2
    Uptime: 4 hours, 22 minutes
    SBFPGA Version: 1.0.2
    MCU Version: 240.9
    AIKIDO Version: 271e-270
    Last Reboot Reason: Flash Reset
Server /chassis #
```

サーバーの前面パネルにある電源ボタンのロック解除

物理サーバーの前面パネルにある実際の電源ボタンを有効にするには、この手順を使用します。電源ボタンが有効になっていると、前面パネルの電源ボタンを使用してサーバーの電源をオンまたはオフにすることができます。

始める前に

このタスクを実行するには、user または admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **show detail**	（任意）サーバーのプロパティが表示されます。電源ボタンの現在のステータス（ロックまたはロック解除されているかどうか）を決定することができます。
ステップ 3	Server /chassis # **set power-button unlocked**	電源ボタンをイネーブルにします。サーバーの電源をオンまたはオフにするには、前面パネルの電源ボタンを使用できます。
ステップ 4	Server /chassis* # **commit**	変更をコミットします。
ステップ 5	Server /chassis # **show detail**	（任意）サーバーのプロパティが表示されます。電源ボタンの現在のステータス（ロックまたはロック解除されているかどうか）を決定することができます。

例

次に、物理サーバーの前面パネルにあるサーバーの物理的な電源ボタンを有効にする例を示します。

```
server /chassis # set power-button unlocked
server /chassis *# commit
server /chassis # show detail
Chassis:
    Power: off
    IOS Lockout: unlocked
    Power Button: unlocked
    Reset Button: unlocked
    Serial Number: FOC26285PBW
    Product Name: UCS E1100D M6
    PID : UCS-E1100D-M6
    UUID: 1CD1E026-05DC-0000-88E4-3E11AF0AA302
    Description:
```

```
    Asset Tag: Unknown
    FPGA Version: 3.4.2
    Uptime: 4 hours, 22 minutes
    SBFPGA Version: 1.0.2
    MCU Version: 240.9
    AIKIDO Version: 271e-270
    Last Reboot Reason: Flash Reset
server /chassis #
```

ブート順の設定

UEFI マップと UEFIOS を使用したサーバーのブート順の設定

（注） ホストが BIOS 電源投入時自己診断テスト（POST）を実行している間は、ブート順を変更しないでください。

始める前に

このタスクを実行するには、user または admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **set boot-order** {*uefimap, uefios, uefipxeTE0, uefipxeTE1, uefipxeTE3, uefipxeTE4, uefipxeGE2*}	Server/bios # **set boot-order** *uefimap,uefios* ブート デバイス オプションと順序を指定します。 （注） オプションでは、大文字と小文字は区別されません。 次の 1 つ以上を選択できます。 • uefimap：UEFI 仮想マップブートオプション • uefios：UEFI オペレーティングシステム • uefipxe：PXE ブート • TE0 • TE1 • TE3 • TE4

	コマンドまたはアクション	目的
		• GE2
ステップ 3	Server /bios # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 4	（任意）Server /bios # **show detail**	サーバーのブート順を表示します。

新しいブート順は、次回の BIOS ブート時に使用されます。

例

次に、ブート順を設定し、トランザクションをコミットする例を示します。

```
server /bios # set boot-order uefimap,uefios
To manage boot-order:
- Reboot server to have your boot-order settings take place
- Do not disable boot options via BIOS screens
- If a specified device type is not seen by the BIOS, it will be removed
from the boot order configured on the BMC
- Your boot order sequence will be applied subject to the previous rule.
The configured list will be appended by the additional device types
seen by the BIOS
- Legacy Boot Order configuration will disable all the active Boot Devices which will
hide them from BIOS

server /bios *# commit
Changes to BIOS set-up parameters will require a reboot.
Do you want to reboot the system?[y|N]y
A system reboot has been initiated.

server /bios # show detail
BIOS:
BIOS Version: UCSEDM6_1.08
BIOS Flash: 1
Backup BIOS Version: UCSEDM6_1.08
Backup BIOS Flash: 0
BIOS Post Complete: 0
Boot Order: UEFIMAP,UEFIOS
FW Update Status: Done, OK
Password: ******
server /bios #
```

（注） UEFI セキュアブートを有効にすると、UEFI オプション（uefimap および uefios）のみを使用できますさらに、UEFIセキュアブートを設定します。これにより、平均ブート時間が約 45 ー 50 秒短縮されます。

BIOS の設定

BIOS ステータスの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **show detail**	BIOS ステータスの詳細を表示します。

BIOS ステータス情報には、次のフィールドが含まれます。

名前	説明
BIOS Version	実行中の BIOS のバージョン文字列。
Boot Order	サーバーが使用を試行する、ブート可能なターゲット タイプの順序。
FW Update/Recovery Status	保留中のファームウェア アップデートまたは回復アクションのステータス。
FW Update/Recovery Progress	直近のファームウェア アップデートまたは回復アクションの完了率。

例

次に、BIOS ステータスを表示する例を示します。

```
SERVER /bios # show detail
BIOS:
    BIOS Version: UCSEDM6_1.08
    BIOS Flash: 1
    Backup BIOS Version: UCSEDM6_1.08
    Backup BIOS Flash: 0
    BIOS Post Complete: 0
    Boot Order: (none)
    FW Update Status: Done, OK
    Password: ******
```

サーバー管理 BIOS の設定

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **scope server-management**	サーバー管理 BIOS 設定コマンド モードを開始します。
ステップ 3	BIOS 設定を設定します。	CLI コマンド、説明、および各 BIOS 設定のオプションに関する情報については、セクション「サーバー管理 BIOS 設定 （38 ページ）」を参照してください。
ステップ 4	Server /bios/server-management # **commit**	トランザクションをシステムの設定にコミットします。 変更内容は次のサーバーのリブート時に適用されます。サーバーの電源が投入されている場合、すぐにリブートするかどうかを質問されます。

例

次に、ボー レートを 9.6k に設定する例を示します。

```
SERVER /bios #
SERVER /bios # scope server-management
SERVER /bios/server-management # set BaudRate
<VALUE> 115.2k* | 19.2k | 38.4k | 57.6k | 9.6k
SERVER /bios/server-management # set BaudRate 9.6k
SERVER /bios/server-management *# commit
Your changes will be reflected in BIOS on next boot.
SERVER /bios/server-management #
```

BIOS CMOS のクリア

非常に珍しいケースですが、サーバーのトラブルシューティング時に、サーバーの BIOS CMOS メモリのクリアが必要になることがあります。この手順は、通常のサーバー メンテナンスには含まれません。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **clear-cmos**	確認を求めるプロンプトの後に、CMOS メモリがクリアされます。

例

次に、BIOS CMOS メモリをクリアする例を示します。

```
Server# scope bios
Server /bios # clear-cmos

This operation will clear the BIOS CMOS.
Note: Server should be in powered off state to clear CMOS.
Continue?[y|N] y
```

BIOS パスワードの設定

手順

	コマンドまたはアクション	目的
ステップ 1	Server/bios# **set password**	BIOS パスワードを設定します。

例

次に、BIOS パスワードを設定する例を示します。

```
Server/bios# set password
Warning:

Strong Password Policy is enabled!


For CIMC protection your password must meet the following requirements:
The password must have a minimum of 8 and a maximum of 20 characters. The password must
 not contain the User's Name.
The password must contain characters from three of the following four categories.
English uppercase characters (A through Z) English lowercase characters (a through z)
Base 10 digits (0 through 9)
Non-alphabetic characters (!, @, #, $, %, ^, &, *, -, _, +, =)
```

BIOS パスワードのクリア

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **clear-bios-password**	BIOS パスワードをクリアします。パスワードのクリア処理を有効にするには、サーバーをリブートする必要があります。サーバーがリブートすると、新しいパスワードを作成するように求められます。

例

次に、BIOS パスワードをクリアする例を示します。

```
Server# scope bios
Server /bios # clear-bios-password

This operation will clear the BIOS Password.
Note: Server should be rebooted to clear BIOS password.
Continue?[y|N]y
```

BIOS デフォルトの復元

始める前に

このタスクを実行するには、admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **bios-setup-default**	BIOS のデフォルト設定を復元します。このコマンドでは、リブートが開始されます。

例

次の例は、BIOS デフォルト設定を復元します。

```
Server# scope bios
Server /bios # bios-setup-default

This operation will reset the BIOS set-up tokens to factory defaults. All your
configuration will be lost.
Changes to BIOS set-up parameters will initiate a reboot.
Continue?[y|N]y
```

サーバー BIOS 設定

次の各表に、表示および設定が可能なサーバー BIOS 設定を示します。

（注） お使いのサーバーでの BIOS 設定のサポート状況を確認することを推奨します。搭載されているハードウェアによっては、一部の設定がサポートされていない場合があります。

詳細：プロセッサ BIOS 設定

名前	説明
Package C State Limit	アイドル時にサーバ コンポーネントが使用できる電力量。次のいずれかになります。 • サーバーは、すべてのサーバーコンポーネントに全電力を常時提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • システムレベルの調整が進行中であるため、消費電力が高くなります。調整が完了するまで、パフォーマンス上の問題が発生する可能性があります。 • CPU がアイドル状態の場合、システムは C3 オプションを使用した場合よりも消費電力をさらに削減します。このオプションでは、節約される電力が C0 または C2 よりも多くなりますが、サーバーがフルパワーに戻るまで、パフォーマンス上の問題が発生する可能性があります。 • CPU がアイドル状態の場合、サーバーはコンポーネントに最小限の電力を供給します。このオプションでは、節約される電力量が最大になりますが、サーバーがハイ パフォーマンス モードに戻るのに要する時間も最も長くなります。 • サーバは、使用可能な任意の C 状態に入ります。 （注） このオプションは [CPU C ステート（CPU C State）] が有効の場合にのみ使用されます。

詳細：**USB BIOS** 設定

名前	説明
USB ポート 0	USB ポート 0（KVM コネクタ）のステータス。次のいずれかになります。 • [無効（Disabled）]：USB ポート 0 は無効です。 • [有効（Enabled）]：USB ポート 0 は有効です。
USB ポート 1	USB ポート 1（物理ポート）のステータス。次のいずれかになります。 • [無効（Disabled）]：USB ポート 1 は無効です。 • [有効（Enabled）]：USB ポート 1 は有効です。

サーバー管理 BIOS 設定

名前	説明
FRB2 有効	POST 中にシステムがハングした場合に、システムを回復するために CIMC によって FRB2 タイマーが使用されるかどうか。次のいずれかになります。 • [Disabled]：FRB2 タイマーは使用されません。 • [Enabled]：POST 中に FRB2 タイマーが開始され、必要に応じてシステムの回復に使用されます。

名前	説明
Console Redirection	POST および BIOS のブート中に、シリアル ポートをコンソール リダイレクションに使用できるようにします。BIOS のブートが完了し、オペレーティング システムがサーバを担当すると、コンソール リダイレクションは関連がなくなり、無効になります。次のいずれかになります。 • [Disabled]：POST 中にコンソール リダイレクションは実行されません。 • [有効（Enabled）]：POST 中にシリアル ポート A をコンソールリダイレクション用にイネーブルにします。[シリアルポートA（Serial Port A）] オプションを選択する場合は、[詳細（Advanced）] メニューの [Serial Port A] もイネーブルにする必要があります。 （注） このオプションを有効にする場合は、POST 中に表示される Quiet Boot のロゴ画面を無効にします。
Flow Control	フロー制御にハンドシェイク プロトコルを使用するかどうか。送信要求/クリア ツーセンド（RTS/CTS）は、隠れ端末の問題によって生じる可能性のあるフレーム衝突を減らすのに役立ちます。次のいずれかになります。 • [None]：フロー制御は使用されません。 • [RTS-CTS]：RTS/CTS がフロー制御に使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。

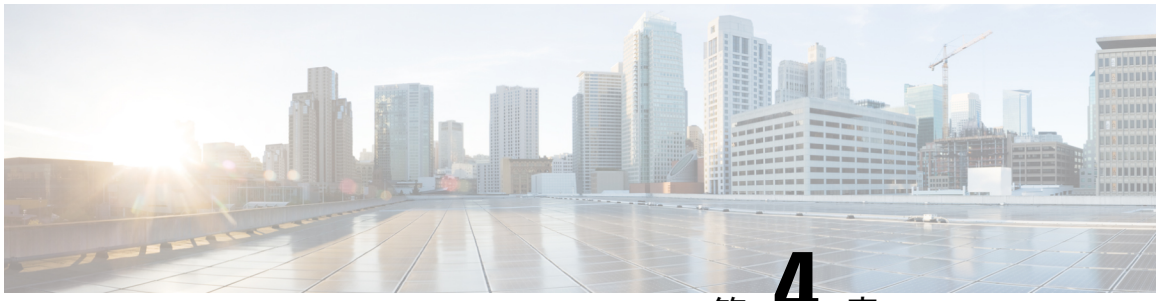
名前	説明
ボー レート	シリアル ポートの伝送速度として使用されるボー レート。[Console Redirection] を無効にする場合は、このオプションを使用できません。次のいずれかになります。 • [9.6k]：9600 ボー レートが使用されます。 • [19.2k]：19200 ボー レートが使用されます。 • [38.4k]：38400 ボー レートが使用されます。 • [57.6k]：57600 ボー レートが使用されます。 • [115.2k]：115200 ボー レートが使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。
Terminal Type	コンソール リダイレクションに使用される文字フォーマットのタイプ。次のいずれかになります。 • [PC-ANSI]：PC-ANSI 端末フォントが使用されます。 • [VT100]：サポートされている VT100 ビデオ端末とその文字セットが使用されます。 • [VT100-PLUS]：サポートされている VT100-plus ビデオ端末とその文字セットが使用されます。 • [VT-UTF8]：UTF-8 文字セットのビデオ端末が使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。

名前	説明
OS Boot Watchdog Timer	BIOS が指定されたタイムアウト値でウォッチドッグ タイマーをプログラムするかどうか。タイマーが切れる前にオペレーティング システムのブートを完了しない場合、CIMC はシステムをリセットし、エラーがログに記録されます。次のいずれかになります。 • [Disabled]：サーバーのブートにかかる時間をトラッキングするためにウォッチドッグ タイマーは使用されません。 • [Enabled]：サーバーのブートにかかる時間をウォッチドッグ タイマーでトラッキングします。指定された時間内にサーバーが起動しない場合
OS Boot Watchdog Timer Policy	ウォッチドッグ タイマーが切れたときにシステムで実行されるアクション。次のいずれかになります。 • [Do Nothing]：OS のブート中にウォッチドッグ タイマーが切れたときに、サーバーの電源状態は変化しません。 • [Power Down]：OS のブート中にウォッチドッグ タイマーが切れた場合、サーバーの電源はオフになります。 • [Reset]：OS のブート中にウォッチドッグ タイマーが切れた場合、サーバーはリセットされます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にする場合にのみ適用されます。

次に、BIOS サーバー管理設定の例を示します。

```
server /bios/server-management # set

BaudRate     Baud rate
BootOrderRules     Boot Order Rules
cli          CLI options
ConsoleRedir       Console redirection
FlowCtrl     Flow Control
FRB-2        FRB 2 Timer
OSBootWatchdogTimer      OS Watchdog Timer
OSBootWatchdogTimerPolicy      OS Watchdog Timer Policy
OSBootWatchdogTimerTimeout     OS Watchdog Timer Timeout
```

```
TerminalType       Terminal type

server /bios/server-management # show detail

Set-up parameters:
Baud rate: 115.2k
Boot Order Rules: CIMC-config
Console redirection: Disabled
FRB 2 Timer: Enabled
Flow Control: None
OS Watchdog Timer: Disabled
OS Watchdog Timer Policy: Reset
OS Watchdog Timer Timeout: 10 minutes
Terminal type: PC-ANSI
```



第 4 章

サーバのプロパティの表示

サーバーのプロパティの表示

始める前に

サーバーの電源をオンにする必要があります。そうしないと、プロパティが表示されません。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **show detail**	サーバーのプロパティを表示します。

例

次に、サーバーのプロパティを表示する例を示します。

```
SERVER# scope chassis
SERVER /chassis # show detail
Power: on
    IOS Lockout: unlocked
    Power Button: unlocked
```

```
    Reset Button: unlocked
    Serial Number: FOC26285PD2
    Product Name: UCS E1100D M6
    PID : UCS-E1100D-M6
    UUID: 1CD1E026-05D1-0000-2C68-107B2C231D4A
    Description:
    Asset Tag: Unknown
    FPGA Version: 2.0.2
    Uptime: 3 hours, 15 minutes
    SBFPGA Version: 22.11.8
    MCU Version: 240.10
    AIKIDO Version: 2711-270
    Last Reboot Reason: Flash Reset
SERVER /chassis #
```

実際のブート順の表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **show actual-boot-order**	BIOS ステータスの詳細を表示します。

例

次の例は、実際のブート順序を表示します。

```
Server# scope bios
Server /bios # show actual-boot-order
Boot Order   Type     Boot Device
-----------  -------------------- ----------------------------------
1    UEFI Image Map      UEFI Image Map
2    Internal EFI Shell  Internal EFI Shell
3    UEFI PXE TE3 IPv4   UEFI PXE TE3 IPv4
4    UEFI PXE TE4 IPv4   UEFI PXE TE4 IPv4
5    UEFI PXE GE2 IPv4   UEFI PXE GE2 IPv4
6    UEFI PXE TE0 IPv4   UEFI PXE TE0 IPv4
7    UEFI PXE TE1 IPv4   UEFI PXE TE1 IPv4
```

CIMC 情報の表示

始める前に

CIMC ファームウェアをサーバーにインストールします。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **show** [**detail**]	CIMC ファームウェア、現在時刻およびブートローダ バージョンを表示します。

例

次に、CIMC に関する情報の例を示します。

```
server /cimc # show detail
Cisco IMC:
    Firmware Version: 4.11(0)73
    Current Time: Fri Mar 10 12:22:46 2023
    Boot-loader Version: 4.11(0)73
    Local Time: Fri Mar 10 17:52:46 2023 IST +0530 (NTP)
    Timezone: Asia/Kolkata
    Reset Reason: graceful-rebootE1100D-FOC26071VZY /cimc #
```

CPU のプロパティの表示

始める前に

サーバーの電源をオンにする必要があります。そうしないと、プロパティが表示されません。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **show cpu** [**detail**]	CPU のプロパティを表示します。

例

次に、CPU のプロパティを表示する例を示します。

```
server # scope chassis
server /chassis # show cpu
Name         Cores    Version
------------ -------- --------------------------------------------------
CPU0         10       Intel(R) Xeon(R) D-1749NT CPU @ 3.00GHz

server /chassis #
```

メモリのプロパティの表示

始める前に

サーバーの電源をオンにする必要があります。そうしないと、プロパティが表示されません。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **show dimm** [**detail**]	メモリのプロパティを表示します。

例

次に、メモリのプロパティを表示する例を示します。

```
Server# scope chassis
Server /chassis # show dimm
Name                  Capacity        Channel Speed (MHz) Channel Type
--------------------- --------------- ------------------- ----------------
CPU0_DIMM_A1          Not Installed   Unknown             Unknown
CPU0_DIMM_A2          Not Installed   Unknown             Unknown
CPU0_DIMM_B1          32768 MB        2400                DDR4
CPU0_DIMM_B2          32768 MB        2400                DDR4
Server /chassis #
```

次に、メモリのプロパティに関する詳細情報を表示する例を示します。

```
Server# scope chassis
Server /chassis # show dimm detail

Name CPU0_DIMM_A1:
    Capacity: Not Installed
    Channel Speed (MHz): NA
    Channel Type: NA
    Memory Type Detail: NA
    Bank Locator: NA
    Visibility: NA
    Operability: NA
    Manufacturer: NA
    Part Number: NA
    Serial Number: NA
    Asset Tag: NA
    Data Width: NA

Name CPU0_DIMM_A2:
    Capacity: Not Installed
    Channel Speed (MHz): NA
    Channel Type: NA
    Memory Type Detail: NA
    Bank Locator: NA
    Visibility: NA
    Operability: NA
    Manufacturer: NA
```

```
    Part Number: NA
    Serial Number: NA
    Asset Tag: NA
    Data Width: NA

Name CPU0_DIMM_B1:
    Capacity: 32768 MB
    Channel Speed (MHz): 2400
    Channel Type: DDR4
    Memory Type Detail: Synchronous Registered (Buffered)
    Bank Locator: NODE 0
    Visibility: Yes
    Operability: Operable
    Manufacturer: Hynix
    Part Number: HMAA4GR8AMR4N-UH
    Serial Number: 32657137
    Asset Tag: CPU0_DIMM_B1_AssetTag
    Data Width: 64 bits

Name CPU0_DIMM_B2:
    Capacity: 32768 MB
    Channel Speed (MHz): 2400
    Channel Type: DDR4
    Memory Type Detail: Synchronous Registered (Buffered)
    Bank Locator: NODE 0
    Visibility: Yes
    Operability: Operable
    Manufacturer: Hynix
    Part Number: HMAA4GR8AMR4N-UH
    Serial Number: 32657031
    Asset Tag: CPU0_DIMM_B2_AssetTag
    Data Width: 64 bits
```

ハード ドライブのプレゼンスの表示

始める前に

サーバーの電源をオンにする必要があります。そうしないと、プロパティが表示されません。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **show hdd**	ハード ドライブを表示します。

例

次に、電源のプロパティを表示する例を示します。

```
Server# scope chassis
Server /chassis # show hdd
Name            Status
```

```
-----------          -------
HDD1_STATUS          present
HDD2_STATUS          present
HDD3_STATUS          present
HDD4_STATUS          present
```

次に、ハードディスクの存在と詳細を表示する例を示します。

```
server /chassis/hdd # show detail
    Name HDD1_STATUS:
    Status :  present
    Name HDD2_STATUS:
    Status :  present
    Name HDD3_STATUS:
    Status :  present
   Name HDD4_STATUS:
    Status :  present
```

インターフェイスの MAC アドレスの表示

システムで定義されたインターフェイスの名前、各ホストインターフェイスに割り当てられた MAC アドレスを表示できます。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope network**	ネットワーク コマンド モードを開始します。
ステップ 3	Server /cimc/network # **show lom-mac-list** [**detail**]	システムで定義されたインターフェイスの名前、各ホスト インターフェイスに割り当てられた MAC アドレスを表示します。

例

次に、システムで定義されたインターフェイスの名前、各ホストインターフェイスに割り当てられた MAC アドレスを表示する例を示します。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # show lom-mac-list
Interface                      MAC Address
------------------------------ --------------------
Console                        1C:D1:E0:26:03:12
TE1                            1C:D1:E0:26:03:13
GE2                            1C:D1:E0:26:03:16
TE3                            1C:D1:E0:26:03:14
TE4                            1C:D1:E0:26:03:15
Server /cimc/network #
```

CIMC ネットワーク接続の状態の表示

始める前に

CIMC ネットワーク接続のステータスを表示するには、管理者権限を持つユーザーとしてログインする必要があります。

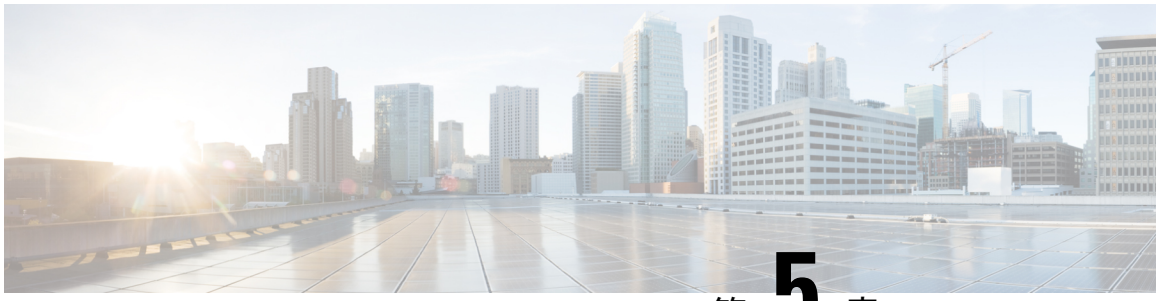
手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope network**	CIMC ネットワーク コマンド モードを開始します。
ステップ 3	Server /cimc/network # **show link state [detail]**	CIMC ネットワーク接続の状態が表示されます（リンクが検出されたかどうか、つまり物理ケーブルがネットワーク インターフェイスに接続されているかどうか）。

例

次に、CIMC ネットワーク接続の状態を表示する例を示します。

```
Server /cimc/network # show link-state detail
Interface                     State
----------------------------- --------------------
Console                       Link Detected
TE1                           No Link Detected
GE2                           Link Detected
TE3                           No Link Detected
TE4                           No Link Detected
Dedicated                     No Link Detected
Server /cimc/network #
```



第 5 章

サーバのセンサーの表示

温度センサーの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope sensor**	センサー コマンド モードを開始します。
ステップ 2	Server /sensor # **show temperature** [**detail**]	サーバーの温度センサーの統計情報を表示します。

例

次に、温度センサーの統計情報を表示する例を示します。

```
Server# scope sensor
Server /sensor # show temperature
Name              Sensor Status  Reading    Units  Critical  Min Critical Max
Non-Recoverable Min  Non-Recoverable Max
--------------   -------------- ---------- ------ --------  ----------------
-------------------- ---------------------
TEMP_SENS_FRONT   Normal         23.0       C       N/A          60.0          N/A
             70.0
TEMP_SENS_REAR    Normal         29.0       C       N/A          75.0          N/A
             85.0


Server /sensor #
```

電圧センサーの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope sensor**	センサー コマンド モードを開始します。
ステップ 2	Server /sensor # **show voltage** [**detail**]	サーバーの電圧センサーの統計情報を表示します。

例

次に、電圧センサーの統計情報を表示する例を示します。

```
Server# scope sensor
Server /sensor # show voltage
Name     Sensor Status   Reading  Units  Critical Min  Critical Max  Non-Recoverable Min
  Non-Recoverable Max
-------------------------------------------------------------------------------------------------
P12V       Normal        12.803      V        11.151       13.806       11.151
      13.806
P0V6_SB_BMC      Normal        0.601      V        0.569        0.632        0.569
           0.632
P5V_SB           Normal        5.031      V        4.493        5.499        4.493
           5.499
P2V5_SB          Normal        2.516      V        2.375        2.621        2.375
           2.621
P3V3_SB          Normal        3.350      V        2.970        3.634        2.970
           3.634
P0V86_SB_C827    Normal        0.858      V        0.819        0.905        0.819
           0.905
P2V5_SB_ABC      Normal        2.492      V        2.375        2.750        2.375
           2.750
P1V8_VCCIN       Normal        1.790      V        1.615        2.071        1.615
           2.071
P1V8_SB          Normal        1.802      V        1.622        1.981        1.622
           1.981
P1V1_SB_BMC      Normal        1.100      V        1.022        1.209        1.022
           1.209
P1V2_DDR4_VDD    Normal        1.225      V        1.076        1.318        1.076
           1.318
P1V8_SB_NACDELAY Normal        1.802      V        1.622        1.981        1.622
           1.981
P1V2_SB          Normal        1.193      V        1.139        1.264        1.139
           1.264
P1V_PCIE4        Normal        0.998      V        0.897        1.100        0.897
           1.100
P1V05_SB         Normal        1.061      V        0.952        1.162        0.952
           1.162
P0V74_SB_VNN     Normal        0.850      V        0.608        1.209        0.608
           1.209
P1V8_SB_PHY      Normal        1.786      V        1.622        1.981        1.622
           1.981
P1V_SB           Normal        0.991      V        0.952        1.053        0.952
           1.053
P0V6_DDR4_ABC    Normal        0.605      V        0.538        0.659        0.538
           0.659
```

```
P3V3_SB_MCU      Normal        3.318      V        2.812        3.792        2.812
          3.792
Server /sensor #
```

LED センサーの表示

始める前に

サーバーの電源をオンにする必要があります。そうしないと、情報が表示されません。

手順

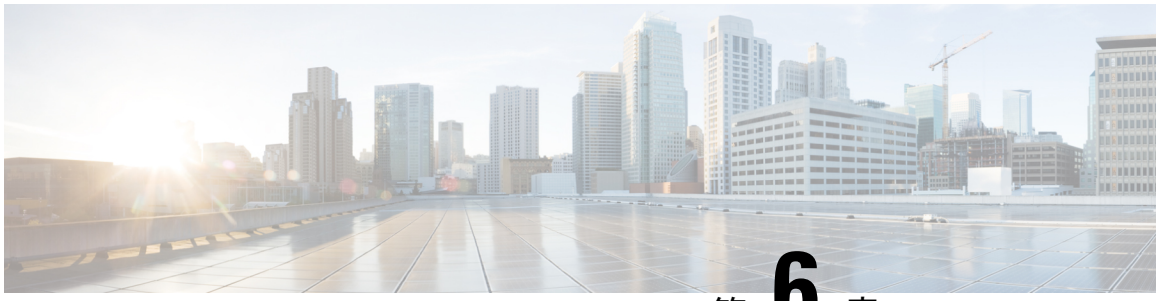
	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **show led** [**detail**]	外部 LED の名前、状態、および色が表示されます。

例

次に、外部の LED に関する情報を表示する例を示します。

```
Server# scope chassis
Server /chassis # show led
LED Name                  LED State  LED Color
------------------------- ---------- --------
LED_PWR_BTN               ON         GREEN
LED_HLTH_STATUS           ON         GREEN
LED_SYS                   ON         GREEN
LED_BMC_ACT               ON         GREEN
OVERALL_DIMM_STATUS       ON         GREEN

Server /chassis # show led detail
LEDs:
    LED Name: LED_PWR_BTN
    LED State: ON
    LED Color: GREEN

LEDs:
    LED Name: LED_HLTH_STATUS
    LED State: ON
    LED Color: GREEN

LEDs:
    LED Name: LED_SYS
    LED State: ON
    LED Color: GREEN

LEDs:
    LED Name: LED_BMC_ACT
    LED State: ON
    LED Color: GREEN

LEDs:
    LED Name: OVERALL_DIMM_STATUS
```

```
LED State: ON
LED Color: GREEN
```



第 6 章

リモート プレゼンスの管理

仮想 KVM の管理

KVM コンソール

KVM コンソールはCIMCからアクセス可能なインターフェイスであり、サーバーへのキーボード、ビデオ、マウスの直接接続をエミュレートします。KVM コンソールを使用すると、リモートの場所からサーバーに接続できます。サーバーに物理的に接続された CD/DVD ドライブを使用する代わりに、KVM コンソールは仮想メディアを使用します。これは、仮想 CD/DVD ドライブにマップされる実際のディスクドライブまたはディスクイメージファイルです。次のいずれでも仮想ドライブにマップできます。

- お使いのコンピュータ上の CD/DVD
- コンピュータ上のディスク イメージ ファイル（ISO または IMG ファイル）
- コンピュータ上の USB フラッシュ ドライブ

KVM コンソールを使用して、サーバーにオペレーティング システムまたはハイパーバイザをインストールし、次の作業を行うことができます。

- ブートアップ中に **F2** を押して、BIOS セットアップ メニューにアクセスします。
- 起動中に [F6] を押して、[BIOSブート（BIOS Boot ）] メニューにアクセスします。
- ブートアップ中に **F8** を押して、CIMC Configuration Utility にアクセスします。

仮想 KVM の設定

始める前に

仮想 KVM を設定するには、admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope kvm**	KVM コマンド モードを開始します。
ステップ 2	Server /kvm # **set enabled** {**yes** | **no**}	仮想 KVM をイネーブルまたはディセーブルにします。
ステップ 3	Server /kvm # **set kvm-port** *port*	KVM通信に使用するポートを指定します。
ステップ 4	Server /kvm # **set local-video** {**yes** | **no**}	ローカル ビデオが [yes] である場合、KVM セッションはサーバーに接続されているすべてのモニターにも表示されます。
ステップ 5	Server /kvm # **set max-sessions** *sessions*	許可されている KVM の同時セッションの最大数を指定します。*sessions* 引数の値は、1 ～ 4 の範囲の整数になります。
ステップ 6	Server /kvm # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 7	Server /kvm # **show** [**detail**]	（任意）仮想 KVM の設定を表示します。

例

次に、仮想 KVM を設定し、その設定を表示する例を示します。

```
Server# scope kvm
Server /kvm # set enabled yes
Server /kvm *# set kvm-port 2068
Server /kvm *# set max-sessions 4
Server /kvm *# set local-video yes
Server /kvm *# commit
Server /kvm # show detail
KVM Settings:
    Max Sessions: 4
    Local Video: yes
    Active Sessions: 0
    Enabled: yes
    KVM Port: 2068

Server /kvm #
```

次のタスク

GUI から仮想 KVM を起動します。

仮想 KVM のイネーブル化

始める前に

仮想 KVM をイネーブルにするには、admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope kvm**	KVM コマンド モードを開始します。
ステップ 2	Server /kvm # **set enabled yes**	仮想 KVM をイネーブルにします。
ステップ 3	Server /kvm # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 4	Server /kvm # **show** [**detail**]	（任意）仮想 KVM の設定を表示します。

例

次に、仮想 KVM をイネーブルにする例を示します。

```
Server# scope kvm
Server /kvm # set enabled yes
Server /kvm *# commit
Server /kvm # show
Local Video        Active Sessions    Enabled       VM Port
------------------ ----------------- --------------- -------
yes                 0                 yes           2068

Server /kvm #
```

仮想 KVM のディセーブル化

始める前に

仮想 KVM をディセーブルにするには、admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope kvm**	KVM コマンド モードを開始します。
ステップ 2	Server /kvm # **set enabled no**	仮想 KVM をディセーブルにします。 （注） 仮想 KVM をディセーブルにすると仮想メディア機能へのアクセスがディセーブルになりますが、仮想メディアがイネーブルであれば仮想メディア デバイスは切断されません。
ステップ 3	Server /kvm # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 4	Server /kvm # **show** [**detail**]	（任意）仮想 KVM の設定を表示します。

例

次に、仮想 KVM をディセーブルにする例を示します。

```
Server# scope kvm
Server /kvm # set enabled no
Server /kvm *# commit
Server /kvm # show
Local Video      Active Sessions   Enabled   KVM Port
---------------- ---------------   -------   --------
yes              0                 no        2068

Server /kvm #
```

Serial over LAN の管理

Serial over LAN

Serial over LAN（SoL）は、IP を介した SSH セッションを利用して、管理対象システムのシリアルポートの入力と出力をリダイレクトできるようにするメカニズムです。SoL は、CIMC 経由でホスト コンソールに到達するための手段となります。

Serial Over LAN に関するガイドラインおよび制約事項

SoL にリダイレクトするには、サーバー コンソールに次の設定が含まれている必要があります。

- シリアル ポート A へのコンソール リダイレクション

- フロー制御なし
- ボー レートを SoL と同様に設定
- VT-100 terminal type
- レガシー OS リダイレクションをディセーブル

SoL セッションは、ブートメッセージなどの行指向の情報や、BIOS 設定メニューなどの文字指向の画面メニューを表示します。サーバーで Windows などのビットマップ指向表示のオペレーティングシステムやアプリケーションが起動されると、SoLセッションによる表示はなくなります。サーバーで Linux などのコマンドライン指向のオペレーティング システム（OS）が起動された場合、SoL セッションで適切に表示するために OS の追加設定が必要になることがあります。

SoL セッションでは、ファンクション キー F2 を除くキーストロークはコンソールに送信されます。F2 をコンソールに送信するには、Escape キーを押してから 2 を押します。

Serial over LAN の設定

始める前に

SoL を設定するには、admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope sol**	SoL コマンド モードを開始します。
ステップ 2	Server /sol # **set enabled** {**yes** | **no**}	サーバーで SoL をイネーブルまたはディセーブルにします。
ステップ 3	Server /sol # **set baud-rate** {**9600** | **19200** | **38400** | **57600** | **115200**}	システムが SoL 通信に使用するシリアル ボー レートを設定します。 （注） このボー レートは、サーバーのシリアル コンソールで設定したボー レートと一致する必要があります。
ステップ 4	Server /sol # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 5	Server /sol # **show** [**detail**]	（任意）SoL の設定を表示します。

例

次に、SoL を設定する例を示します。

```
Server# scope sol
Server /sol # set enabled yes
Server /sol *# set baud-rate 115200
Server /sol *# commit
Server /sol # show
Enabled     Baud Rate(bps)   Com Port  SOL SSH Port
-------     ---------------  --------  -------------
yes         115200           com0      2400

Server /sol #
```

Serial Over LAN の起動

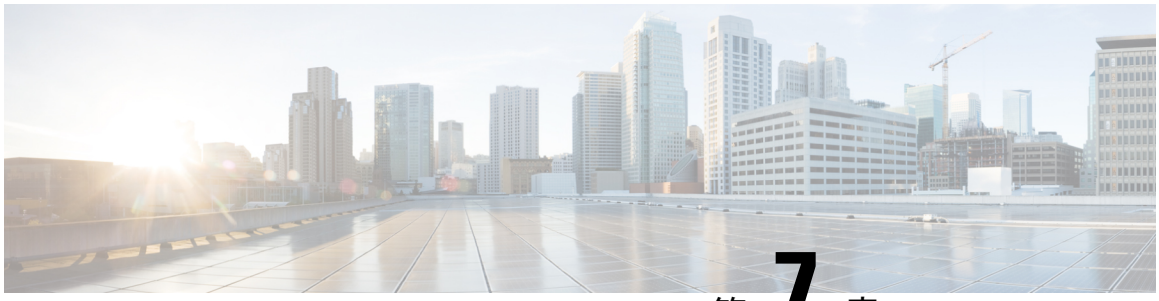
手順

	コマンドまたはアクション	目的
ステップ 1	Server# **connect host**	リダイレクトされたサーバー コンソール ポートへの SoL 接続を開始します。このコマンドは、どのコマンド モードでも入力できます。

次のタスク

Ctrl キーと **X** キーを押して SoL から切断し、CLI セッションに戻ります。

（注） SoL をイネーブルにすると、シリアル ポートからの出力がリダイレクトされます。このため、Cisco IOS CLI を使用してホストのセッションに入ろうとすると、出力は表示されません。



第 7 章

ユーザ アカウントの管理

ローカル ユーザーの設定

始める前に

ローカルユーザーアカウントを設定または変更するには、admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope user** *usernumber*	ユーザー番号のユーザーコマンドモードを入力します。
ステップ 2	Server /user # **set enabled** {**yes** |**no**\\	CIMC でユーザー アカウントをイネーブルまたはディセーブルにします。
ステップ 3	Server /user # **set name** *username*	ユーザーのユーザー名を指定します。
ステップ 4	Server /user # **set password**	ユーザーのパスワードを指定します。パスワードを 2 回入力するように求められます。
ステップ 5	Server /user # **set role** {**readonly** |**user** |**admin**\\	ユーザーに割り当てるロールを指定します。ロールは次のいずれかです。

	コマンドまたはアクション	目的
		• readonly：このユーザーは情報を表示できますが、変更することはできません。 • user：このユーザーは、次の操作を実行できます。 • すべての情報を表示する • 電源のオン、電源再投入、電源のオフなどの電力制御オプションを管理する • KVM コンソールと仮想メディアを起動する • すべてのログをクリアする • ロケータ LED を切り替える • admin：このユーザーは、GUI、CLI、IPMI で可能なすべての処理を実行できます。
ステップ 6	Server /user # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、ユーザー 5 を admin として設定する例を示します。

```
Server# scope user 5
Server /user # set enabled yes
Server /user *# set name john
Server /user *# set password
Please enter password:
Please confirm password:
Server /user *# set role readonly
Server /user *# commit
Server /user #  show
User   Name             Role      Enabled   SSH Key Count
------ ---------------- --------  ---------  --------------
5      user             readonly  yes       (n/a)
```

LDAP サーバ（Active Directory）

CIMC では、情報をディレクトリ内で編成してこの情報へのアクセスを管理するディレクトリ サービスがサポートされます。CIMC は、ネットワークでディレクトリ情報を保管および保持する Lightweight Directory Access Protocol（LDAP）をサポートします。さらに、CIMC は Microsoft Active Directory（AD）もサポートします。Active Directory はさまざまなネットワーク サービ

スを提供するテクノロジーであり、LDAP と同様のディレクトリ サービス、Kerberos ベースの認証、DNS ベースの名前付けなどが含まれます。CIMC は LDAP での Kerberos ベースの認証サービスを利用します。

CIMC で LDAP がイネーブルになっている場合、ローカル ユーザー データベース内に見つからないユーザー アカウントに関するユーザー認証とロール許可は、LDAP サーバーによって実行されます。LDAP ユーザー認証の形式は username@domain.com です。

[LDAP Settings] 領域で [Enable Encryption] チェックボックスをオンにすることで、LDAP サーバーへの送信データを暗号化するようサーバーに要求できます。

LDAP サーバの設定

CIMC を設定して、LDAP をユーザーの認証と許可に使用できます。LDAP を使用するには、CIMC のユーザー ロールとロケールを保持する属性を使用してユーザーを設定します。CIMC のユーザーロールとロケールにマップされた既存の LDAP 属性を使用できます。または、LDAP スキーマを変更して、属性 ID 1.3.6.1.4.1.9.287247.1 を持つ Cisco AVPair 属性などの新しいカスタム属性を追加できます。

重要 スキーマの変更の詳細については、http://technet.microsoft.com/en-us/library/bb727064.aspx の記事を参照してください。

（注） この例では Cisco AVPair という名前のカスタム属性を作成しますが、CIMC のユーザーロールとロケールにマップされた既存の LDAP 属性を使用することもできます。

LDAP サーバーに対して次の手順を実行する必要があります。

ステップ 1 LDAP スキーマ スナップインがインストールされていることを確認します。

ステップ 2 スキーマ スナップインを使用して、次のプロパティを持つ新しい属性を追加します。

プロパティ	値
Common Name	CiscoAVPair
LDAP Display Name	CiscoAVPair
Unique X500 Object ID	1.3.6.1.4.1.9.287247.1
説明	CiscoAVPair
構文	Case Sensitive String

ステップ 3 スナップインを使用して、ユーザ クラスに CiscoAVPair 属性を追加します。

1. 左ペインで [クラス（Classes）] ノードを展開し、u を入力してユーザークラスを選択します。
2. [Attributes] タブをクリックして、[Add] をクリックします。
3. c を入力して CiscoAVPair 属性を選択します。
4. [OK] をクリックします。

ステップ 4 CIMC にアクセスできるようにするユーザーに対し、次のユーザー ロール値を CiscoAVPair 属性に追加します。

ロール	Cisco-AV-Pair 属性の値
admin	`shell:roles="admin"`
user	`shell:roles="user"`
read-only	`shell:roles="read-only"`

（注） 属性に値を追加する方法の詳細については、http://technet.microsoft.com/en-us/library/bb727064.aspx の記事を参照してください。

次のタスク

CIMC を使用して LDAP サーバーを設定します。

CIMC での LDAP の設定

ローカル ユーザーの認証と許可に LDAP サーバーを使用するには、CIMC で LDAP を設定します。

始める前に

このタスクを実行するには、admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope ldap**	LDAP コマンドモードを入力します。
ステップ 2	Server /ldap # **set enabled** {**yes** |**no**\\	LDAP セキュリティをイネーブルまたはディセーブルにします。LDAP セキュリティがイネーブルの場合、ローカル ユーザー データベースにないユーザー アカウントに対し、ユーザー認証とロール許可が LDAP によって実行されます。
ステップ 3	Server /ldap # **set domain** *LDAP domain name*	LDAP ドメイン名を指定します。

	コマンドまたはアクション	目的
ステップ 4	Server /ldap # **set timeout** *seconds*	LDAP検索操作がタイムアウトするまでCIMCが待機する秒数を指定します。0 ～ 1800 秒の間隔を指定する必要があります。
ステップ 5	Server /ldap # **set encrypted** {**yes** |**no**\\	暗号化がイネーブルである場合、サーバーはADに送信されるすべての情報を暗号化します。
ステップ 6	Server /ldap # **set base-dn** *domain-name*	LDAP サーバーで検索するベース DN を指定します。
ステップ 7	Server /ldap # **set attribute** 名	ユーザーのロールとロケール情報を保持するLDAP属性を指定します。このプロパティは、常に、名前と値のペアで指定されます。システムは、ユーザーレコードで、この属性名と一致する値を検索します。 CIMC ユーザー ロールおよびロケールにマップされた既存の LDAP 属性を使用するか、CiscoAVPair 属性など、次の属性 ID を持つカスタム属性を作成できます。 `1.3.6.1.4.1.9.287247.1` （注） このプロパティを指定しない場合、ユーザー アクセスが拒否されます。
ステップ 8	Server /ldap # **set filter-attribute**	アカウント名属性を指定します。Active Directoryを使用している場合は、このフィールドに**sAMAccountName** を指定します。
ステップ 9	Server /ldap # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 10	Server /ldap # **show** [**detail**]	（任意）LDAP の設定を表示します。

例

次に、CiscoAVPair 属性を使用して LDAP を設定する例を示します。

```
Server# scope ldap
Server /ldap # set enabled yes
Server /ldap *# set domain sample-domain
Server /ldap *# set timeout 60
Server /ldap *# set base-dn example.com
Server /ldap *# set attribute CiscoAVPair
Server /ldap *# set filter-attribute sAMAccountName
Server /ldap *# commit
Server /ldap # show detail
LDAP Settings:
    Enabled: yes
```

```
    Domain: sample-domain
    BaseDN: example.com
    Timeout (for each server): 60
    Filter-Attribute: sAMAccountName
    Attribute: CiscoAvPair
Server /ldap #
```

次のタスク

グループ承認用に LDAP グループを使用する場合は、CIMC での LDAP グループの設定 を参照してください。

CIMC での LDAP グループの設定

（注） Active Directory（AD）グループ許可をイネーブルにして設定すると、ローカル ユーザー データベースにないユーザーや、Active Directory で CIMC の使用を許可されていないユーザーに対するグループ レベルでのユーザー認証も行われます。

始める前に

- このタスクを実行するには、admin 権限を持つユーザーとしてログインする必要があります。
- Active Directory（または LDAP）をイネーブルにして、設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope ldap**	LDAP コマンド モードを開始して、AD を設定します。
ステップ 2	Server /ldap# **scope ldap-group-rule**	LDAP グループ ルール コマンド モードを開始して、AD を設定します。
ステップ 3	Server /ldap/ldap-group-rule # **set group-auth** {**yes** |**no**}	LDAP グループ許可をイネーブルまたはディセーブルにします。
ステップ 4	Server /ldap # **scope role-group** *index*	設定に使用可能なグループ プロファイルのいずれかを選択します。ここで、*index* は 1 から 28 までの数字です。
ステップ 5	Server /ldap/role-group # **set name** *group-name*	サーバーへのアクセスが許可されているグループの名前を AD データベースに指定します。
ステップ 6	Server /ldap/role-group # **set domain** *domain-name*	グループが存在する必要がある AD ドメインを指定します。

	コマンドまたはアクション	目的

ステップ 7	Server /ldap/role-group # **set role** {**admin** | **user** | **readonly**}	この AD グループのすべてのユーザーに割り当てられる権限レベル（ロール）を指定します。次のいずれかになります。
		• **admin**：ユーザーは使用可能なすべてのアクションを実行できます。
		• **user**：ユーザーは、次のタスクを実行できます。
		  • すべての情報を表示する
		  • 電源のオン、電源再投入、電源のオフなどの電力制御オプションを管理する
		  • KVM コンソールと仮想メディアを起動する
		  • すべてのログをクリアする
		  • ロケータ LED を切り替える
		• **readonly**：ユーザーは情報を表示できますが、変更することはできません。

ステップ 8	Server /ldap/role-group # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、LDAP グループの許可を設定する例を示します。

```
Server# scope ldap
Server /ldap # scope ldap-group-rule
Server /ldap/ldap-group-rule # set group-auth yes
Server /ldap *# scope role-group 5
Server /ldap/role-group # set name Training
Server /ldap/role-group* # set domain example.com
Server /ldap/role-group* # set role readonly
Server /ldap/role-group* # commit
ucs-c250-M2 /ldap # show role-group
Group  Group Name       Domain Name      Assigned Role
------ -----------     --------------   --------------
1      (n/a)            (n/a)            admin
2      (n/a)            (n/a)            user
3      (n/a)            (n/a)            readonly
4      (n/a)            (n/a)            (n/a)
5      Training         example.com      readonly

Server /ldap/role-group #
```

TACACS+ サーバー

TACACS+は、ユーザーによるルータまたはネットワーク アクセス サーバーへのアクセス試行の集中的な確認を可能にするセキュリティプロトコルです。TACACS+サービスは、TACACS+サーバー上のデータベースで維持されます。ネットワーク アクセス サーバーで TACACS+ 機能を設定し、使用可能にするには、TACACS+ サーバーを設定しておく必要があります。

TACACS+ サーバーで、Cisco Integrated Management Controller（CIMC）サービスの Cisco 属性値（AV）ペア権限レベル（priv-lvl）が管理者とオペレータの最小権限レベルに設定されていることを確認します。

CIMC の TACACS+ サポートの制約事項

- CIMC は、最大 6 台の TACACS+ サーバーへの接続をサポートします。
- ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。
- TACACS+ および LDAP の設定は排他的であり、一度に 1 つの設定のみが有効になります。
- デフォルトの時間は 5 秒です。
- デフォルトの TCP ポート接続は 49 です。
- デフォルトのログインは PAP ログインであり、ユーザーが入力した詳細データの代わりに、ユーザー名とパスワードが PAP プロトコルパケットでネットワーク アクセス サーバーに到着します。
- IPv4 だけがサポートされます。
- 事前共有キー（PSK）のサイズは 32 文字です。
- 共有秘密キーでサポートされる特殊文字は次の通りです：**! @% ^ * - _ .**

TACACS+ の動作

始める前に

ユーザーが TACACS+ を使用して CIMC に認証して単純な ASCII ログインを試行すると、次のオプションが提供されます。

CIMC は最終的に、TACACS+ サーバーから次のいずれかの応答を受信します。

- ACCEPT：ユーザは認証され、サービスを開始できます。CIMC が許可を要求するように設定されている場合は、この時点で許可のプロセスが開始されます。

- REJECT：ユーザは認証に失敗しました。ユーザは、今後のアクセスを拒否されるか、または、TACACS+ サーバによっては、ログイン シーケンスを再試行するプロンプトが表示されます。
- CONTINUE：ユーザーは、さらに認証情報の入力を求められます。

次のタスク

認証後、CIMC は承認要求を TACACS+ サーバーに送信します。承認結果に基づいて、CIMC はユーザーのロールを割り当てます。

TACACS+ サーバーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope tacacs+**	TACACS+ コンフィギュレーション モードを入力します。
ステップ 2	Server /tacacs+ # **set enabled** [**yes** | **no**]	TACACS+ ベースの認証を有効または無効にします。
ステップ 3	Server /tacacs+ # **fallback-only-on-no-connectivity** [**yes** | **no**]	他の認証優先順位へのフォールバックをイネーブルまたはディセーブルにします。
ステップ 4	Server /tacacs+/tacacs-server # **scope tacacs-server 1**	Enters tacacs-server 1 configuration mode.
ステップ 5	Server /tacacs+/tacacs-server # **set tacacs-server** *ip-address*	TACACS サーバーの IP アドレスを設定します。
ステップ 6	Server / tacacs+/tacacs-server # **set tacacs-port** *port*	TACACS ポートを設定します。
ステップ 7	Server /tacacs+/tacacs-server # **set tacacs-key** *key-string*	サーバーとの認証を開始するための事前共有キーを設定します。キーの最大長は 32 文字です。
ステップ 8	Server /tacacs+/tacacs-server # **scope tacacs-server 1**	Enters tacacs-server 1 configuration mode.
ステップ 9	Server /tacacs+/tacacs-server # **set tacacs-server** *ip-address*	TACACS サーバーの IP アドレスを設定します。
ステップ 10	Server / tacacs+/tacacs-server # port **set tacacs-port**	TACACS ポートを設定します。
ステップ 11	Server /tacacs+/tacacs-server # **set tacacs-key***key-string*	サーバーとの認証を開始するための事前共有キーを設定します。キーの最大長は 32 文字です。
ステップ 12	Server /tacacs # **commit**	トランザクションをシステムの設定にコミットします。

	コマンドまたはアクション	目的
ステップ 13	Server /tacacs # **show** [**detail**]	（任意）TACACS+ サーバーの設定を表示します。

例

次に、TACACS サーバーを設定する例を示します。

```
Server /# scope tacacs+
Server /tacacs+ #set enabled yes
Server /tacacs+ *#set fallback-only-on-no-connectivity no
Server /tacacs+ *#commit
Server /tacacs+ #scope tacacs-server 1
Server /tacacs+/tacacs-server #set tacacs-server 10.126.254.174
Server /tacacs+/tacacs-server *#set tacacs-port 49
Server /tacacs+/tacacs-server *#set tacacs-key
Please enter tacacs-key: _Abcded_abcde_123_abcd12_zxy123_
Please confirm tacacs-key: _Abcded_abcde_123_abcd12_zxy123_
Server /tacacs+/tacacs-server #commit
```

次に、TACACS+ サーバー設定を確認する例を示します。

```
Server /tacacs+/tacacs-server #show  detail
Server Id 1:
Server IP address/Hostname: 10.126.254.174
Server Key: ******
Server Port: 49
```

ユーザー セッションの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **show user-session**	現在のユーザー セッションの情報を表示します。

コマンドの出力には、現在のユーザー セッションに関する次の情報が表示されます。

名前	説明
[セッション ID（Session ID）] カラム	セッションの固有識別情報。
[Username] カラム	ユーザーのユーザー名。
[IP Address] カラム	ユーザーがサーバーにアクセスした IP アドレス。
[Type] カラム	ユーザーがサーバーにアクセスした方法。たとえば、CLI、vKVM などです。

名前	説明
[Action] カラム	ユーザー アカウントに**admin** ユーザー ロールが割り当てられている場合、関連付けられたユーザー セッションを強制的に終了できるときはこのカラムに [Terminate] と表示されます。それ以外の場合は、N/A と表示されます。 （注） このタブから現在のセッションを終了することはできません。

例

次に、現在のユーザ セッションに関する情報を表示する例を示します。

```
Server# show user-session
ID     Name             IP Address        Type         Killable
------ ---------------- ----------------- ------------ --------
15     admin            10.20.30.138      CLI          yes

Server /user #
```

ユーザー セッションの終了

始める前に

ユーザーセッションを終了するには、admin 権限を持つユーザーとしてログインする必要があります。

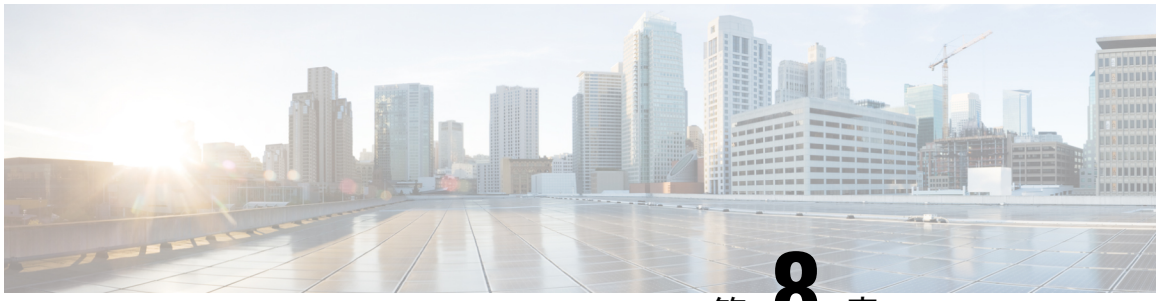
手順

	コマンドまたはアクション	目的
ステップ 1	Server # **show user-session**	現在のユーザーセッションの情報を表示します。終了するユーザーセッションは、終了可能（killable）であり、独自のセッションではないことが必要です。
ステップ 2	Server /user-session # **scope user-session** *session-number*	終了する番号付きのユーザー セッションに対してユーザーセッション コマンドモードを開始します。
ステップ 3	Server /user-session # **terminate**	ユーザー セッションを終了します。

例

次に、ユーザー セッション 10 の admin がユーザー セッション 15 を終了する例を示します。

```
Server# show user-session
ID     Name             IP Address        Type         Killable
------ ---------------- ----------------- ------------ --------
10     admin            10.20.41.234      CLI          yes
15     admin            10.20.30.138      CLI          yes

Server# scope user-session 15
Server /user-session # terminate
User session 15 terminated.

Server /user-session #
```



第 8 章

ネットワーク関連の設定

CIMC NIC の設定

CIMC NIC

CIMC への接続には、2 種類の NIC モードを使用できます。

NIC モード

- [Dedicated]：CIMC への接続は、管理イーサネット ポートを経由して使用できます。
- Shared LOM：CIMC への接続は、マザーボードのオンボード LAN（LOM）イーサネット ホスト ポート経由およびルータの PCIe と MGF インターフェイス経由で使用できます。

（注） Shared LOM モードでは、すべてのホスト ポートが同じサブネットに属している必要があります。

次の例は、リンク状態を示しています。

```
server /cimc/network # show link-state detail
Interface                     State
----------------------------- --------------------
Console                       Link Detected
```

```
TE1                             No Link Detected
GE2                             No Link Detected
TE3                             No Link Detected
TE4                             No Link Detected
Dedicated                       Link Detected
```

次の例は、LOM MAC リストを示しています。

```
Server /cimc/network # show lom-mac-list
Interface                       MAC Address
------------------------------- -------------------
Console                         1C:D1:E0:26:05:A6
TE1                             1C:D1:E0:26:05:A7
GE2                             1C:D1:E0:26:05:AA
TE3                             1C:D1:E0:26:05:A8
TE4                             1C:D1:E0:26:05:A9
```

CIMC NIC の設定

NIC モードとインターフェイスを設定するには、次の手順を実行します。

始める前に

NIC を設定するには、admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope network**	CIMC ネットワーク コマンドモードを開始します。
ステップ 3	Server /cimc/network # **set mode** {**dedicated** |**shared_lom**}	NIC モードを次のいずれかに設定します。 • **dedicated**：CIMC へのアクセスに管理イーサネットポートを使用します。 • **shared LOM mode**：CIMC へのアクセスに LAN On Motherboard（LOM）イーサネットホストポートを使用します。 （注） Shared LOM モードでは、すべてのホスト ポートが同じサブネットに属している必要があります。
ステップ 4	Server /cimc/network # **set interface** {**console** | **te1** | **ge2** | **te3** | **te4**}	NIC インターフェイスを次のいずれかに設定します。 • **console**：内部インターフェイスで、ルータの PCIe インターフェイスを E シリーズ サーバーに接続するために使用されます。

	コマンドまたはアクション	目的
		• **te1**：高速バックプレーンスイッチでCIMCにアクセスするために使用される内部インターフェイス。 • **ge2**：プライマリインターフェイスまたはバックアップインターフェイスとして使用できる外部インターフェイス。 • **te3**：プライマリインターフェイスまたはバックアップインターフェイスとして使用できる外部インターフェイス。 • **te4**：プライマリインターフェイスまたはバックアップインターフェイスとして使用できる外部インターフェイス。
ステップ 5	Server /cimc/network # **commit**	トランザクションをシステムの設定にコミットします。 （注） 使用可能な NIC モードおよび NIC 冗長モードのオプションは、お使いのプラットフォームによって異なります。サーバーでサポートされていないモードを選択すると、変更を保存するときにエラーメッセージが表示されます。

例

次に、CIMC ネットワーク インターフェイスを設定する例を示します。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set mode shared_lom
WARNING: Changing this configuration may cause the Router network configuration to be
out of sync.
You may still commit your changes, but it is recommended that changes be done on the
Router.
Server /cimc/network *# set interface ge2
WARNING: Changing this configuration may cause the Router network configuration to be
out of sync.
You may still commit your changes, but it is recommended that changes be done on the
Router.
Server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network #
```

共通プロパティの設定

サーバーを説明するには、共通プロパティを使用します。

始める前に

共通プロパティを設定するには、admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope network**	CIMC ネットワーク コマンドモードを開始します。
ステップ 3	Server /cimc/network # **set hostname** *host-name*	ホストの名前を指定します。
ステップ 4	Server /cimc/network # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、コマンドのプロパティを設定する例を示します。

```
Server# scope cimc
Server /cimc # scope network
server /cimc/network # set hostname Server
WARNING: Changing this configuration may cause the Router network configuration to be
out of sync.
You may still commit your changes, but it is recommended that changes be done on the
Router.
server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network #
```

IPv4 の設定

始める前に

IPv4 ネットワークの設定を実行するには、admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope network**	CIMC ネットワーク コマンドモードを開始します。
ステップ 3	Server /cimc/network # **set dhcp-enabled** {**yes** |**no**}	CIMC で DHCP を使用するかどうかを選択します。 （注） DHCP がイネーブルである場合は、CIMC 用に 1 つの IP アドレスを予約するように DHCP サーバーを設定することを推奨します。サーバーの複数のポートを通じて CIMC に到達できる場合、それらのポートの全範囲の MAC アドレスに対して 1 つの IP アドレスを予約する必要があります。
ステップ 4	Server /cimc/network # **set v4-addr** *ipv4-address*	CIMC の IP アドレスを指定します。
ステップ 5	Server /cimc/network # **set v4-netmask** *ipv4-netmask*	IP アドレスのサブネット マスクを指定します。
ステップ 6	Server /cimc/network # **set v4-gateway** *gateway-ipv4-address*	IP アドレスのゲートウェイを指定します。
ステップ 7	Server /cimc/network # **set dns-use-dhcp** {**yes** |**no**}	CIMC が DNS サーバー アドレスを DHCP から取得するかどうかを選択します。
ステップ 8	Server /cimc/network # **set preferred-dns-server** *dns1-ipv4-address*	プライマリ DNS サーバーの IP アドレスを指定します。
ステップ 9	Server /cimc/network # **set alternate-dns-server** *dns2-ipv4-address*	セカンダリ DNS サーバーの IP アドレスを指定します。
ステップ 10	Server /cimc/network # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 11	Server /cimc/network # **show** [**detail**]	（任意）IPv4 ネットワークの設定を表示します。

例

次に、IPv4 ネットワークの設定を実行し、表示する例を示します。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set dns-use-dhcp no
WARNING: Changing this configuration may cause the Router network configuration to be
out of sync.
You may still commit your changes, but it is recommended that changes be done on the
Router.
Server /cimc/network *# set dhcp-enabled no
```

```
WARNING: Changing this configuration may cause the Router network configuration to be
out of sync.
You may still commit your changes, but it is recommended that changes be done on the
Router.
Server /cimc/network *# set v4-addr 10.20.30.11
WARNING: Changing this configuration may cause the Router network configuration to be
out of sync.
You may still commit your changes, but it is recommended that changes be done on the
Router.
Server /cimc/network *# set v4-gateway 10.20.30.1
WARNING: Changing this configuration may cause the Router network configuration to be
out of sync.
You may still commit your changes, but it is recommended that changes be done on the
Router.
Server /cimc/network *# set v4-netmask 255.255.248.0
WARNING: Changing this configuration may cause the Router network configuration to be
out of sync.
You may still commit your changes, but it is recommended that changes be done on the
Router.
Server /cimc/network *# set preferred-dns-server 192.168.30.31
WARNING: Changing this configuration may cause the Router network configuration to be
out of sync.
You may still commit your changes, but it is recommended that changes be done on the
Router.
Server /cimc/network *# set alternate-dns-server 192.168.30.32
WARNING: Changing this configuration may cause the Router network configuration to be
out of sync.
You may still commit your changes, but it is recommended that changes be done on the
Router.
Server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network #

Server /cimc/network # show detail
Network Setting:
IPv4 Enabled: yes
IPv4 Address: 10.20.30.11
IPv4 Netmask: 255.255.248.0
IPv4 Gateway: 10.20.30.1
DHCP Enabled: no
DDNS Enabled: yes
DDNS Update Domain:
DDNS Refresh Interval(0-8736 Hr): 0
Obtain DNS Server by DHCP: no
Preferred DNS: 192.168.30.31
Alternate DNS: 192.168.30.32
IPv6 Enabled: no
IPv6 Address: ::
IPv6 Prefix: 64
IPv6 Gateway: ::
IPv6 Link Local: ::
IPv6 SLAAC Address: ::
IPV6 DHCP Enabled: no
IPV6 Obtain DNS Server by DHCP: no
IPV6 Preferred DNS: ::
IPV6 Alternate DNS: ::
VLAN Enabled: no
VLAN ID: 1
VLAN Priority: 0
Port Profile:
Hostname: Server
MAC Address: 1C:D1:E0:26:0F:81
```

```
NIC Mode: shared_lom
NIC Redundancy: none
NIC Interface: ge2
VIC Slot: 0
```

（注） この設定が **show detail** コマンドに反映されるまでに数分かかることがあります。

IPv6 の設定

始める前に

IPv6 ネットワークの設定を実行するには、admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope network**	CIMC ネットワーク コマンド モードを開始します。
ステップ 3	Server /cimc/network # **set v6-dhcp no**	DHCP をディセーブルにします。
ステップ 4	Server /cimc/network # **set v6-enabled yes**	IPv6 アドレッシングをイネーブルにします。
ステップ 5	Server /cimc/network # **set v6-addr** *ipv6-address*	CIMC の IP アドレスを指定します。
ステップ 6	Server /cimc/network # **set v6-gateway** *gateway-ipv6address*	IP アドレスのゲートウェイを指定します。
ステップ 7	Server /cimc/network # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 8	Server /cimc/network # **show** [**detail**]	（任意）IPv4 と IPv6 ネットワークの設定を表示します。

例

次に、IPv6 ネットワークの設定を実行し、表示する例を示します。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set v6-dhcp-enabled no
WARNING: Changing this configuration may cause the Router network configuration to be
out of sync.
You may still commit your changes, but it is recommended that changes be done on the
Router.
```

```
Please set "v6-enabled" to "yes" before you commit
Otherwise your setting for "v6-dhcp-enabled" will not be reflected
Server /cimc/network *# set v6-enabled yes
WARNING: Changing this configuration may cause the Router network configuration to be
out of sync.
You may still commit your changes, but it is recommended that changes be done on the
Router.
Warning: You have chosen to change IPv6 property without a valid IPv6 address.
Server /cimc/network *# set v6-addr 2001:db8:101:f101:f2f7::14
WARNING: Changing this configuration may cause the Router network configuration to be
out of sync.
You may still commit your changes, but it is recommended that changes be done on the
Router.
Server /cimc/network *# set v6-gateway 2001:db8:101:f101:f2f7::1
WARNING: Changing this configuration may cause the Router network configuration to be
out of sync.
You may still commit your changes, but it is recommended that changes be done on the
Router.
Server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network #

Server /cimc/network # show detail
Network Setting:
IPv4 Enabled: yes
IPv4 Address: 10.20.30.11
IPv4 Netmask: 255.255.248.0
IPv4 Gateway: 10.20.30.1
DHCP Enabled: no
DDNS Enabled: yes
DDNS Update Domain:
DDNS Refresh Interval(0-8736 Hr): 0
Obtain DNS Server by DHCP: no
Preferred DNS: 192.168.30.31
Alternate DNS: 192.168.30.32
IPv6 Enabled: yes
IPv6 Address: 2001:db8:101:f101:f2f7::14
IPv6 Prefix: 64
IPv6 Gateway: 2001:db8:101:f101:f2f7::1
IPv6 Link Local: fe80::1ed1:e0ff:fe26:f81
IPv6 SLAAC Address: 6666:1000::1ed1:e0ff:fe26:f81
IPV6 DHCP Enabled: no
IPV6 Obtain DNS Server by DHCP: no
IPV6 Preferred DNS: ::
IPV6 Alternate DNS: ::
VLAN Enabled: no
VLAN ID: 1
VLAN Priority: 0
Port Profile:
Hostname: Server
MAC Address: 1C:D1:E0:26:0F:81
NIC Mode: shared_lom
NIC Redundancy: none
NIC Interface: ge2
VIC Slot: 0
Server /cimc/network #
```

サーバー VLAN の設定

始める前に

サーバー VLAN を設定するには、admin としてログインしている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope network**	CIMC ネットワーク コマンド モードを開始します。
ステップ 3	Server /cimc/network # **set vlan-enabled** {**yes** |**no**}	CIMC を VLAN に接続するかどうかを選択します。
ステップ 4	Server /cimc/network # **set vlan-id** *id*	VLAN 番号を指定します。
ステップ 5	Server /cimc/network # **set vlan-priority** *priority*	VLAN でのこのシステムのプライオリティを指定します。
ステップ 6	Server /cimc/network # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 7	Server /cimc/network # **show** [**detail**]	（任意）ネットワークの設定を表示します。

例

次に、サーバー VLAN を設定する例を示します。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set vlan-enabled yes Server /cimc/network *# set vlan-id 10 Server
 /cimc/network *# set vlan-priority 32 Server /cimc/network *# commit
Server /cimc/network # show detail
Network Setting:
    IPv4 Enabled: yes
     IPv4 Address: 10.20.30.11
     IPv4 Netmask: 255.255.248.0
     IPv4 Gateway: 10.20.30.1
     DHCP Enabled: no
     DDNS Enabled: yes
     DDNS Update Domain:
     DDNS Refresh Interval(0-8736 Hr): 0
     Obtain DNS Server by DHCP: no
     Preferred DNS: 0.0.0.0
     Alternate DNS: 0.0.0.0
     IPv6 Enabled: no
     IPv6 Address: ::
     IPv6 Prefix: 64
     IPv6 Gateway: ::
     IPv6 Link Local: ::
     IPv6 SLAAC Address: ::
```

```
        IPV6 DHCP Enabled: no
        IPV6 Obtain DNS Server by DHCP: no
        IPV6 Preferred DNS: ::
        IPV6 Alternate DNS: ::
        VLAN Enabled: yes
        VLAN ID: 10
        VLAN Priority: 32
        Port Profile:
        Hostname: Server
        MAC Address: 1C:D1:E0:26:05:A5
        NIC Mode: dedicated
        NIC Redundancy: none
        NIC Interface:
        VIC Slot: 0
Server /cimc/network #
```

ネットワーク セキュリティの設定

ネットワーク セキュリティ

CIMC は、IP ブロッキングをネットワーク セキュリティとして使用します。IP ブロッキングは、サーバーまたは Web サイトと、特定の IP アドレスまたはアドレス範囲との間の接続を防ぎます。IP ブロッキングは、これらのコンピュータから Web サイト、メール サーバー、またはその他のインターネット サーバーへの不要な接続を効果的に禁止します。

禁止 IP の設定は、一般的に、サービス拒絶（DoS）攻撃から保護するために使用されます。CIMC は、IP ブロッキングの失敗回数を設定して、IP アドレスを禁止します。

ネットワーク セキュリティの設定

IP ブロッキングの失敗回数を設定する場合は、ネットワーク セキュリティを設定します。

始める前に

ネットワーク セキュリティを設定するには、admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope network**	CIMC ネットワーク コマンドモードを開始します。
ステップ 3	Server /cimc/network # **scope ipblocking**	コマンド モードの妨げになる IP を入力します。
ステップ 4	Server /cimc/network/ipblocking # **set enabled** {**yes** | **no**}	IP ブロッキングをイネーブルまたはディセーブルにします。

	コマンドまたはアクション	目的
ステップ 5	Server /cimc/network/ipblocking # **set fail-count** *fail-count*	指定された時間ユーザーがロックアウトされる前に、ユーザーが試行できるログインの失敗回数を設定します。 この回数のログイン試行失敗は、[IP Blocking Fail Window] フィールドで指定されている期間内に発生する必要があります。 3 ～ 10 の範囲の整数を入力します。
ステップ 6	Server /cimc/network/ipblocking # **set fail-window** *fail-seconds*	ユーザーをロックアウトするためにログイン試行の失敗が発生する必要のある期間（秒数）を設定します。 60 ～ 120 の範囲の整数を入力します。
ステップ 7	Server /cimc/network/ipblocking # **set penalty-time** *penalty-seconds*	ユーザーが指定されている期間内にログイン試行の最大回数を超えた場合に、ユーザーがロックアウトされている秒数を設定します。 300 ～ 900 の範囲の整数を入力します。
ステップ 8	Server /cimc/network/ipblocking # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、IP ブロッキングを設定する例を示します。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # scope ipblocking
Server /cimc/network/ipblocking # set enabled yes
Server /cimc/network/ipblocking *# set fail-count 5
Server /cimc/network/ipblocking *# set fail-window 90
Server /cimc/network/ipblocking *# set penalty-time 600
Server /cimc/network/ipblocking *# commit
Server /cimc/network/ipblocking #
```

IPS フィルタリングの設定

始める前に

このタスクを実行するには、admin 権限でログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope network**	CIMC ネットワーク コマンドモードを開始します。
ステップ 3	Server /cimc/network # **scope ipfiltering**	IP フィルタリング コマンド モードを開始します。
ステップ 4	Server /cimc/network/ipfiltering # **set enabled** {**yes** | **no**}	IP フィルタリングをイネーブルまたはディセーブルにします。プロンプトに **y** を入力して IP フィルタリングをイネーブルにします。
ステップ 5	Server /cimc/network/ipfiltering # **set filter-1** *IPv4* または *IPv6* アドレスまたは一定範囲の *IP* アドレス	20 つの IP フィルタを設定できます。IPv4 または IPv6 IP アドレスまたは IP アドレス範囲を割り当てることができます。
ステップ 6	Server /cimc/network/ipfiltering # **commit**	トランザクションをシステム設定にコミットします。
ステップ 7	Server /cimc/network/nam # **showdetail**	（任意）IP フィルタリングのステータスを表示します。

例

次に、IP フィルタリングを設定する例を示します。

```
Server /cimc/network # scope ipfiltering
Server /cimc/network/ipfiltering # set enabled yes
This will enable IP Filtering
Do you wish to continue? [y/N] y
Server /cimc/network/ipfiltering *# commit
Changes to the ipfiltering will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network/ipfiltering # set filter-1 1.1.1.1-255.255.255.255
Server /cimc/network/ipfiltering *# set filter-2 10.10.10.10
Server /cimc/network/ipfiltering *# set filter-3 2001:db8:101:f101:f2f7::15
Server /cimc/network/ipfiltering *# commit
Changes to the ipfiltering will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network/ipfiltering #

Server /cimc/network/ipfiltering # show detail
IP Filter Service Settings:
Enabled: yes
Filter 1: 1.1.1.1-255.255.255.255
Filter 2: 10.10.10.10
Filter 3: 2001:db8:101:f101:f2f7::15
Filter 4:
Filter 5:
Filter 6:
Filter 7:
Filter 8:
```

```
Filter 9:
Filter 10:
Filter 11:
Filter 12:
Filter 13:
Filter 14:
Filter 15:
Filter 16:
Filter 17:
Filter 18:
Filter 19:
Filter 20:
Server /cimc/network/ipfiltering #
```

NTP 設定の構成

NTP 設定

デフォルトでは、CIMC がリセットされると、ホストと時刻が同期されます。Network Time Protocol（NTP）サービスを導入すると、CIMC を設定して NTP サーバーと時刻を同期できます。デフォルトでは、NTP サーバーは CIMC で動作しません。NTP サーバーまたは時刻源サーバーとして機能するサーバー（少なくとも 1 台、最大 4 台）の IP アドレスまたは DNS アドレスを指定し、NTP サービスをイネーブルにして設定する必要があります。NTP サービスをイネーブルにすると、CIMC は設定された NTP サーバーと時刻を同期します。NTP サービスは CIMC でのみ変更できます。

（注） NTP サービスを有効にするには、DNS アドレスではなくサーバーの IP アドレスを指定することをお勧めします。

NTP 設定の構成

始める前に

このタスクを実行するには、admin 権限でログインする必要があります。

手順

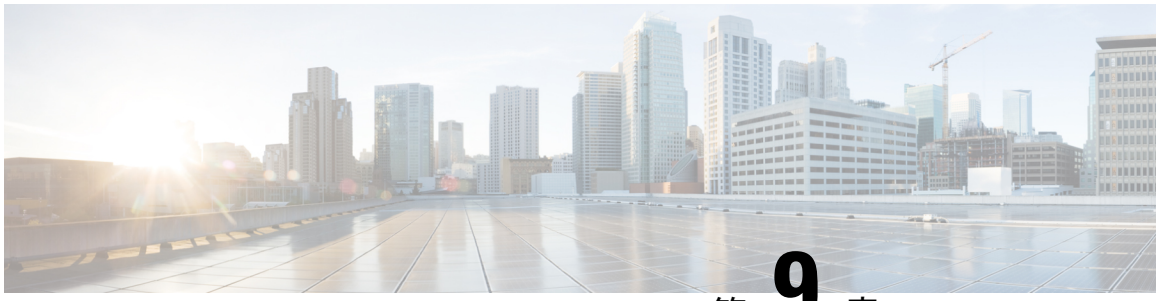
	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope network**	CIMC ネットワーク コマンド モードを開始します。
ステップ 3	Server /cimc/network # **scope ntp**	NTP コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	Server /cimc/network/ntp # **set enabled** {**yes** | **no**}	NTP サービスをイネーブルまたはディセーブルにします。
ステップ 5	Server /cimc/network/ntp # **set** [**server-1** | **server-2** | **server-3** | **server-4**] *ip-address or domain-name*	NTP サーバーまたはタイムソース サーバーとして動作する特定のサーバーの IP アドレスまたはドメイン名を設定します。 最大 4 つのサーバーを設定できます。
ステップ 6	Server /cimc/network/ntp # **show detail**	（任意）NTP サービスがイネーブルになっているかどうか、および NTP サーバーの IP アドレスまたはドメイン名を表示します。

例

次の例は、NTP の設定を示しています。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # scope ntp
Server /cimc/network/ntp # set enabled yes
Warning: IPMI Set SEL Time command will be disabled if NTP is enabled.
Do you wish to continue? [y/N] y
Server /cimc/network/ntp *# set server-1 10.50.171.9
Server /cimc/network/ntp *# set server-2 time.cisco.com
Server /cimc/network/ntp *# commit
Server /cimc/network/ntp #

Server /cimc/network/ntp # show detail
NTP Service Settings:
Enabled: yes
Server 1: 10.50.171.9
Server 2: time.cisco.com
Server 3:
Server 4:
Status: unsynchronised
Server /cimc/network/ntp #
```



第 9 章

コミュニケーション サービスの設定

HTTP の設定

始める前に

HTTP を設定するには、admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope http**	HTTP コマンドモードを入力します。
ステップ 2	Server /http # **set enabled** {**yes** | **no**}	CIMC で HTTP および HTTPS サービスをイネーブルまたはディセーブルにします。
ステップ 3	Server /http # **set http-port** *number*	HTTP 通信に使用するポートを設定します。デフォルトは 80 です。
ステップ 4	Server /http # **set https-port** *number*	HTTPS 通信に使用するポートを設定します。デフォルトは 443 です。
ステップ 5	Server /http # **set timeout** *seconds*	HTTP 要求の間、CIMC がタイムアウトしてセッションを終了するまで待機する秒数を設定します。

	コマンドまたはアクション	目的
		60 ～ 10,800 の範囲の整数を入力します。デフォルトは 1,800 秒です。
ステップ 6	Server /http # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、CIMC に HTTP を設定する例を示します。

```
Server#
Server# scope http
Server /http # set http-enabled yes
Server /http *# set http-port 80
Server /http *# set http-redirect yes
Server /http *# set https-enabled yes
Server /http *# set https-port 443
Server /http *# set timeout 1800
Server /http *# commit
Server /http # show
HTTP Port  HTTPS Port Timeout  Active Sessions HTTPS Enabled HTTP Redirected  HTTP Enabled
---------- ---------- -------- --------------- ------------- -----------------
-----------------
80          443        1800     0               yes           yes              yes

Server /http #
```

SSH の設定

始める前に

SSH を設定するには、admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ssh**	SSH コマンドモードを入力します。
ステップ 2	Server /ssh # **set enabled** {**yes** | **no**}	CIMC で SSH をイネーブルまたはディセーブルにします。
ステップ 3	Server /ssh # **set ssh-port** *number*	セキュア シェル アクセスに使用するポートを設定します。デフォルトは 22 です。
ステップ 4	Server /ssh # **set timeout** *seconds*	SSH要求がタイムアウトしたものとシステムが判断するまで待機する秒数を設定します。

	コマンドまたはアクション	目的
		60 ～ 10,800 の範囲の整数を入力します。デフォルトは 300 秒です。
ステップ 5	Server /ssh # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 6	Server /ssh # **show** [**detail**]	（任意）SSH の設定を表示します。

例

次に、CIMC に SSH を設定する例を示します。

```
Server# scope ssh
Server /ssh # set enabled yes
Server /ssh *# set ssh-port 22
Server /ssh *# set timeout 600
Server /ssh *# commit
Server /ssh # show detail

SSH Port Timeout   Active Sessions   Enabled
---------     --------   ---------------   ---------
22       600  1           yes

Server /ssh #
```

Redfish のイネーブル化

始める前に

このタスクを実行するには、admin 権限を持つユーザーとしてログインする必要があります。

手順の概要

1. Server # **scope redfish**
2. Server /redfish # **set enabled** {**yes** |**no**}
3. Server /redfish* # **commit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Server # **scope redfish**	redfish コマンド モード を開始します。
ステップ 2	Server /redfish # **set enabled** {**yes** |**no**}	Cisco IMC の redfish 制御を有効または無効にします。
ステップ 3	Server /redfish* # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、Cisco IMC の redfish 制御を有効にし、トランザクションをコミットする例を示します。

```
Server# scope redfish
Server /redfish # set enabled yes
Server /redfish *# commit
Server /redfish # show detail
REDFISH Settings:
 Enabled: yes
 Active Sessions: 0
 Max Sessions: 4

Server /redfish #
```

詳細については、『Cisco UCS C-Series Servers REST API Programmer's Guide, Release 3.0』を参照してください。

XML API の設定

CIMC の XML API

Cisco CIMC XML Application Programming Interface (API) は、E-Series M6 サーバー 対応の CIMC に対するプログラマチック インターフェイスです。この API は、HTTP または HTTPS 経由で XML ドキュメントを受け取ります。

XML API の詳細については、「CIMC XML API Programmer's Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine」を参照してください。

XML API のイネーブル化

始める前に

このタスクを実行するには、admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope xmlapi**	XML API コマンド モードを開始します。
ステップ 2	Server /xmlapi # **set enabled** {**yes** | **no**}	CIMC の XML API 制御をイネーブルまたはディセーブルにします。
ステップ 3	Server /xmlapi *# **commit**	トランザクションをシステムの設定にコミットします。

例

次に、CIMC の XML API 制御を有効にし、トランザクションをコミットする例を示します。

```
Server# scope xmlapi
Server /xmlapi # set enabled yes
Server /xmlapi *# commit
Server /xmlapi # show detail
XMLAPI Settings:
    Enabled: yes
    Active Sessions: 0
    Max Sessions: 4
```

IPMI の設定

IPMI over LAN

インテリジェント プラットフォーム管理インターフェイス（IPMI）では、サーバ プラットフォームに組み込まれているサービス プロセッサとのインターフェイスのためのプロトコルを定義しています。このサービス プロセッサはベースボード管理コントローラ（BMC）と呼ばれ、サーバのマザーボードに存在します。BMC は、メイン プロセッサおよびボード上の他の要素に、簡単なシリアル バスを使用してリンクします。

通常動作の間、IPMI は、サーバのオペレーティング システムがシステム ヘルスについての情報を取得し、システムのハードウェアを制御できるようにします。たとえば、IPMI を使用すると、温度、ファンの速度、および電圧などのセンサーをモニターして、問題を事前に検出できます。サーバーの温度が指定されているレベルより高くなった場合、サーバーのオペレーティング システムは BMC に対して、ファンの速度を上げたり、プロセッサの速度を下げたりして問題に対処するよう指示できます。

IPMI over LAN の設定

IPMI over LAN は、CIMC を IPMI メッセージで管理する場合に設定します。

始める前に

このタスクを実行するには、admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope ipmi**	IPMI コマンド モードを開始します。
ステップ 2	Server /ipmi # **set enabled** {**yes** | **no**}	このサーバーで IPMI アクセスをイネーブルまたはディセーブルにします。

	コマンドまたはアクション	目的
ステップ 3	Server /ipmi # **set privilege-level** {**readonly** | **user** | **admin**}	このサーバーで IPMI セッションに割り当て可能な最高特権レベルを指定します。ここに表示される値は次のとおりです。 • **readonly** ：IPMI ユーザーは情報を表示できますが、変更することはできません。このオプションを選択した場合、「Administrator」、「Operator」、または「User」ユーザー ロールを持つ IPMI ユーザーが作成できるのは、読み取り専用の IPMI セッションだけです。それ以外に所持している IPMI 特権は関係ありません。 • **user** ：IPMI ユーザーは一部の機能を実行できますが、管理タスクは実行できません。このオプションを選択した場合、「Administrator」または「Operator」ユーザー ロールを持つ IPMI ユーザーがこのサーバーで作成できるのは、ユーザーセッションと読み取り専用セッションだけです。 • **admin** ：IPMI ユーザーは使用可能なすべてのアクションを実行できます。このオプションを選択した場合、「Administrator」ユーザー ロールを持つ IPMI ユーザーは、管理者、ユーザー、および読み取り専用セッションをこのサーバーで作成できます。
ステップ 4	Server /ipmi # **set encryption-key** *key*	IPMI 通信に使用する IPMI 暗号キーを設定します。キーの値は、40 個の 16 進数であることが必要です。
ステップ 5	Server /ipmi # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、CIMC に IPMI over LAN を設定する例を示します。

```
Server# scope ipmi
Server /ipmi # set enabled yes
Server /ipmi *# set privilege-level admin
Server /ipmi *# set encryption-key abcdef01234567890abcdef01234567890abcdef
Server /ipmi *# commit
Server /ipmi # show

Enabled     Encryption Key                           Privilege Level Limit
--------    ---------------------------------------    ------------------------
yes   abcdef01234567890abcdef01234567890abcdef     admin
```

```
Server /ipmi #
```

SNMP の設定

SNMP

Cisco UCS E シリーズ M6 サーバーは、サーバーの設定とステータスを表示し、SNMP トラップによって障害とアラート情報を送信するための簡易ネットワーク管理プロトコル（SNMP）をサポートしています。CIMC でサポートされている Management Information Base（MIB）ファイルの詳細については、『MIB Quick Reference for Cisco UCS』を参照してください。

SNMP プロパティの設定

始める前に

このタスクを実行するには、admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope snmp**	SNMP コマンド モードを開始します。
ステップ 2	Server /snmp # **set enabled** {**yes** | **no**}	SNMP をイネーブルまたはディセーブルにします。 （注） 追加の SNMP コンフィギュレーション コマンドが受け入れられる前には、SNMP をイネーブルにして保存する必要があります。
ステップ 3	Server /snmp # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 4	Server /snmp # **set community-str** コミュニティ	CIMC が SNMP ホストに送信するトラップ メッセージに含まれるデフォルトの SNMP v1 または v2c コミュニティ名を指定します。名前には最大 18 文字を使用できます。
ステップ 5	Server /snmp # **setcommunity-access**	次のいずれかになります。 • ディセーブル • 制限あり • 全二重

	コマンドまたはアクション	目的
ステップ 6	Server /snmp # **settrap-community-str**	トラップ情報が送信される SNMP コミュニティ グループを指定します。名前には最大 18 文字を使用できます。
ステップ 7	Server /snmp # **set sys-contact** 連絡先	SNMP の実装を担当する、システムの連絡先を指定します。連絡先情報には、電子メールアドレス、名前と電話番号などを最大 254 文字で指定できます。スペースが含まれている値を入力するには、エントリを引用符で囲む必要があります。
ステップ 8	Server /snmp # **set sys-location** 場所	SNMP エージェント（サーバー）が実行されるホストの場所を指定します。ロケーション情報には最大 254 文字を使用できます。スペースが含まれている値を入力するには、エントリを引用符で囲む必要があります。
ステップ 9	Server /snmp # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、SNMP プロパティを設定し、トランザクションをコミットする例を示します。

```
Server# scope snmp
Server /snmp # set enabled yes
Server /snmp *# commit
Server /snmp # set community-str cimcpublic
Server /snmp # set community-access Full

Server /snmp # set trap-community-str public
Server /snmp *# set sys-contact "User Name <username@example.com> +1-408-555-1212"
Server /snmp *# set sys-location "San Jose, California"
Server /snmp *# commit Server /snmp # show detail

SNMP Settings:
 Enabled: yes
 SNMP Port: 161
 System Contact: User Name <username@example.com> +1-408-555-1212
 System Location: unknown
 SNMP v2 Enabled: yes
 Access Community String: cimcpublic
 Trap Community String: public
 SNMP Community access: full
 SNMP v3 Enabled: no
 User Input EngineID:
 SNMP Engine ID: 80 00 1F 88 80 40 EB F5 32 B7 C9 EC 63
 Serial Number Enabled: no

Server /snmp #
```

次のタスク

「SNMP トラップ設定の指定 （95 ページ）」セクションに従って SNMP トラップ設定を設定します。

SNMP トラップ設定の指定

始める前に

このタスクを実行するには、admin 権限を持つユーザーとしてログインする必要があります。

トラップの設定を実行する前に、SNMP をイネーブルにして保存する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope snmp**	SNMP コマンド モードを開始します。
ステップ 2	Server /snmp # **scope trap-destinations** *number*	指定した宛先に対して SNMP トラップ宛先コマンド モードを開始します。4 つの SNMP トラップ宛先を使用できます。宛先の *number* は、1 ～ 15 の範囲の整数です。
ステップ 3	Server /snmp/trap-destinations # **set enabled** {**yes** | **no**}	SNMP トラップ宛先をイネーブルまたはディセーブルにします。
ステップ 4	Server /snmp/trap-destinations # **set version** {**1** | **2** | **3**}	必要なトラップ メッセージの SNMP バージョンを指定します。 （注） SNMPv3 トラップは SNMPv3 ユーザーおよびキー値が正しく設定されている場所だけに配信されます。
ステップ 5	Server /snmp/trap-destinations # **set type** {**trap** | **inform**}	SNMP 通知メッセージを単純なトラップとして送信するのか、レシーバによる確認応答が必要なインフォーム要求として送信するかを指定します。 （注） 通知オプションは V2 ユーザーに対してのみ選択できます。
ステップ 6	Server /snmp/trap-destinations # **set user** *user*	
ステップ 7	Server /snmp/trap-destination # **set v4-addr** *ip-address*	SNMP トラップ情報を送信する宛先 IP アドレスを指定します。
ステップ 8	Server /snmp/trap-destination # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、汎用の SNMP トラップとトラップの宛先番号 1 を設定し、トランザクションをコミットする例を示します。

```
Server# scope snmp
Server /snmp # Scope trap-destinations 1
Server /snmp/trap-destination *# set enabled yes
Server /snmp/trap-destination *# set version 2
Server /snmp/trap-destination *# set type inform
Server /snmp/trap-destination *# set user user1
Server /snmp/trap-destination *# set trap-addr 192.2.3.4
Server /snmp/trap-destination *# commit
Server /snmp/trap-destination # show detail
Trap Destination 1:
    Enabled: yes
    SNMP version: 2
    Trap type: inform
    SNMP user: unknown
    Trap Address(IPv4/IPv6/FQDN): 10.197.82.5
    Trap Port: 162
    Delete Trap: no
    Trap Community String: public
```

テスト SNMP トラップ メッセージの送信

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope snmp**	SNMP コマンド モードを開始します。
ステップ 2	Server /snmp # **sendSNMPtrap**	イネーブルにされている設定済みの SNMP トラップ宛先に SNMP テスト トラップを送信します。 （注） テスト メッセージを送信するために、トラップは設定済みで、イネーブルにされている必要があります。

例

次に、イネーブルにされているすべての SNMP トラップ宛先にテスト メッセージを送信する例を示します。

```
Server# scope snmp
Server /snmp # sendSNMPtrap
SNMP Test Trap sent to the destination.
Server /snmp #
```

SNMPv3 ユーザーの設定

始める前に

このタスクを実行するには、admin 権限を持つユーザーとしてログインする必要があります。

これらのコンフィギュレーション コマンドが受け入れられる前には、SNMP をイネーブルにして保存する必要があります。

手順

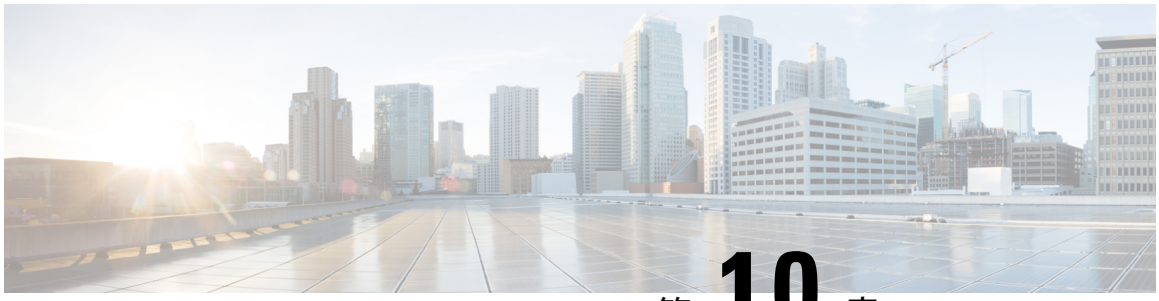
	コマンドまたはアクション	目的
ステップ 1	Server # **scope snmp**	SNMP コマンド モードを開始します。
ステップ 2	Server /snmp # **scope v3users** *number*	指定したユーザー番号の SNMPv3 ユーザーのコマンド モードを開始します。
ステップ 3	サーバー/snmp/v3users # **set v3add** {**yes** |**no**}	SNMPv3 ユーザーを追加または削除します。 • **yes**：このユーザーは SNMPv3 ユーザーとしてイネーブルになり、SNMP OID ツリーにアクセスできます。 （注） セキュリティ名とセキュリティ レベルがこの時点で設定されていないと、ユーザーの追加に失敗します。 • **no**：このユーザー設定は削除されます。
ステップ 4	Server /snmp/v3users # **set v3security-name** *security-name*	このユーザーの SNMP ユーザー名を入力します。
ステップ 5	Server /snmp/v3users # **set v3security-level** {**noauthnopriv** |**authnopriv** |**authpriv**}	このユーザーのセキュリティ レベルを選択します。次のいずれかになります。 • **noauthnopriv**：このユーザーには、許可パスワードもプライバシー パスワードも必要ありません。 • **authnopriv**：このユーザーには許可パスワードが必要ですが、プライバシー パスワードは不要です。このオプションを選択した場合は、認証キーを設定する必要があります。 • **authpriv**：このユーザーには、許可パスワードとプライバシーパスワードの両方が必要です。このオプションを選択した場合は、認証キーおよび秘密暗号キーを設定する必要があります。

	コマンドまたはアクション	目的
ステップ 6	Server /snmp/v3users # **set v3proto** {**MD5** |**SHA**}	このユーザーの認証プロトコルを選択します。
ステップ 7	Server /snmp/v3users # **set v3auth-key** *auth-key*	このユーザーの許可パスワードを入力します。
ステップ 8	Server /snmp/v3users # **set v3priv-proto** {**DES** |**AES**}	このユーザーの暗号化プロトコルを選択します。
ステップ 9	Server /snmp/v3users # **set v3priv-auth-key** *priv-auth-key*	このユーザーの秘密暗号キー（プライバシー パスワード）を入力します。
ステップ 10	Server /snmp/v3users # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、SNMPv3 ユーザー番号 2 を設定し、トランザクションをコミットする例を示します。

```
Server# scope snmp
Server /snmp # scope v3users 2
Server /snmp/v3users # set v3add yes
Server /snmp/v3users *# set v3security-name ucsSNMPV3user
Server /snmp/v3users *# set v3security-level authpriv
Server /snmp/v3users *# set v3proto SHA
Server /snmp/v3users *# set v3auth-key
Please enter v3auth-key:ex4mp1ek3y
Please confirm v3auth-key:ex4mp1ek3y
Server /snmp/v3users *# set v3priv-proto AES
Server /snmp/v3users *# set v3priv-auth-key
Please enter v3priv-auth-key:!1@2#3$4%5^6&7*8
Please confirm v3priv-auth-key:!1@2#3$4%5^6&7*8
Server /snmp/v3users *# commit
Settings are being applied ... allow a few minutes for the process to complete
Server /snmp/v3users # show detail
User 2:
 Add User: yes
 Security Name: ucsSNMPV3user
 Security Level: authpriv
 Auth Type: SHA
 Auth Key: ******
 Encryption: AES
 Private Key: ******

Server /snmp/v3users #
```



第 10 章

証明書の管理

サーバ証明書の管理

ステップ 1 CIMC から CSR を生成します。

ステップ 2 証明書の発行と署名を行う認証局に CSR ファイルを送信します。組織で独自の自己署名証明書を生成している場合は、CSR ファイルを使用して自己署名証明書を生成できます。

ステップ 3 新しい証明書を CIMC にアップロードします。

（注） アップロードされた証明書は、CIMC によって生成された CSR から作成される必要があります。この方法で作成されていない証明書はアップロードしないでください。

証明書署名要求の生成

始める前に

証明書を設定するには、admin 権限を持つユーザーとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope certificate**	証明書コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	Server /certificate # **generate-csr**	証明書署名要求（CSR）の生成に関するダイアログを起動します。

証明書署名要求に関して、次の情報の入力を求めるプロンプトが表示されます。

Common Name（CN）	CIMC の完全修飾ホスト名
Organization Name (O)	証明書を要求している組織。
Organization Unit (OU)	組織ユニット
Locality（L）	証明書を要求している会社の本社が存在する市または町。
StateName (S)	証明書を要求している会社の本社が存在する州または行政区分。
Country Code (CC)	会社の本社が存在する国を示す 2 文字の ISO 国コード。
Email	会社の管理用電子メールの連絡先。

要求された情報を入力すると、証明書署名要求が生成され、コンソール出力に表示されます。CSR ファイルは作成されませんが、コンソール出力から CSR 情報をコピーして、テキストファイルに貼り付けることができます。

例

次に、証明書署名要求を生成する例を示します。

```
Server /certificate # generate-csr
Common Name (CN): test.example.com
Organization Name (O): Example, Inc.
Organization Unit (OU): Test Department
Locality (L): San Jose
StateName (S): CA
Country Code (CC): US
Email: user@example.com
[Supported Algorithms: sha1, sha256, sha384, sha512 (Default sha384)]
Signature Algorithm: sha384
Do you want to set Challenge Password ? [y|n] (Default y)n
String Encoding utf8only/nombstr/pkix/default (Enter to skip):
Do you want to enter Subject Alternative Name parameters?[y|n]n
Continue to generate CSR?[y|N]y
Do you want self sign CSR and overwrite the current certificate?
All HTTPS and SSH sessions will be disconnected. [y|N]y

Server /certificate # show detail
Certificate Information:
    Serial Number: 3FA8AF325A18359FAFB29C518838A542D945F0EB
    Subject Country Code (CC): US
    Subject State (S): CA
    Subject Locality (L): San Jose
    Subject Organization (O): "Example
    Subject Organizational Unit (OU): Test Department
```

```
Subject Common Name (CN): test.example.com
Issuer Country Code (CC): US
Issuer State (S): CA
Issuer Locality (L): San Jose
Issuer Organization (O): "Example
Issuer Organizational Unit (OU): Test Department
Issuer Common Name (CN): test.example.com
Valid From: Mar 24 04:32:34 2023 GMT
Valid To: Jun 26 04:32:34 2025 GMT
```

次のタスク

次のいずれかの作業を実行します。

- 公共の認証局から証明書を取得したくない場合に、組織が独自の認証局を運用していなければ、CSRから自己署名証明書を内部生成し、すぐにサーバーにアップロードするよう、CIMC を設定できます。この処理を行うには、この例では最後のプロンプトの後に **y** と入力します。
- 組織が自己署名証明書を生成するための独自の証明書サーバーを運用している場合は、「-----BEGIN ...」から「END CERTIFICATE REQUEST-----」までのコマンド出力をコピーして、csr.txt というファイルに貼り付けます。CSR ファイルを証明書サーバーに入力して、自己署名証明書を生成します。
- 公共の認証局から証明書を取得する場合は、「-----BEGIN ...」から「END CERTIFICATE REQUEST-----」までのコマンド出力をコピーして、csr.txt というファイルに貼り付けます。CSR ファイルを認証局に提出して、署名付き証明書を取得します。

CIMC によって自己署名証明書を内部生成し、アップロードする最初のオプションを使用しない場合は、証明書コマンド モードで **upload** コマンドを使用して新しい証明書をアップロードする必要があります。

自己署名証明書の作成

パブリック認証局（CA）を使用してサーバー証明書の生成と署名を行う代わりに、独自のCAを運用して独自の証明書に署名することができます。このセクションでは、Linux で実行されている OpenSSL 証明書サーバを使用して CA を作成するコマンドおよびサーバ証明書を生成するコマンドについて説明します。OpenSSL の詳細については「http://www.openssl.org」を参照してください。

（注） これらのコマンドは、CIMC ではなく、OpenSSL パッケージを使用している Linux サーバーで入力します。

始める前に

組織内のサーバーで、証明書サーバーのソフトウェアパッケージを取得してインストールします。

手順

	コマンドまたはアクション	目的
ステップ 1	**openssl genrsa -out***CA_keyfilenamekeysize* 例： `# openssl genrsa -out ca.key 1024`	このコマンドは、CA によって使用される RSA 秘密キーを生成します。 （注） ユーザ入力なしで CA がキーにアクセスできるように、このコマンドに -des3 オプションは使用しないでください。 指定されたファイル名には、指定されたサイズの RSA キーが含まれています。
ステップ 2	**openssl req -new -x509 -days** *numdays* **-key***CA_keyfilename* **-out***CA_certfilename* 例： `# openssl req -new -x509 -days 365 -key ca.key -out ca.crt`	このコマンドは、指定されたキーを使用して、CA の自己署名証明書を新規に作成します。証明書は指定された期間有効になります。このコマンドは、ユーザに証明書の追加情報を求めるプロンプトを表示します。 証明書サーバーは、アクティブな CA です。
ステップ 3	**echo "nsCertType = server" > openssl.conf** 例： `# echo "nsCertType = server" > openssl.conf`	このコマンドは、証明書がサーバー限定の証明書であることを指定する行を OpenSSL 設定ファイルに追加します。この指定により、認証されたクライアントがサーバになりすます man-in-the-middle 攻撃を防御できます。 OpenSSL 設定ファイル openssl.conf には、"nsCertType = server" という文が含まれています。
ステップ 4	**openssl x509 -text -noout -in ca.crt** 例： `# openssl x509 -text -noout -in ca.crt`	このコマンドは証明書を表示します。

例

この例は、CA の作成方法、および新規に作成された CA が署名するサーバー証明書の生成方法を示します。これらのコマンドは、OpenSSL を実行している Linux サーバーで入力します。

```
[root@localhost ~]# openssl genrsa -out ca.key 1024
Generating RSA private key, 1024 bit long modulus (2 primes)
...........+++++
......+++++
e is 65537 (0x010001)
[root@localhost ~]# openssl req -new -x509 -days 365 -key ca.key -out ca.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
```

```
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:CA
Locality Name (eg, city) [Default City]:San Jose
Organization Name (eg, company) [Default Company Ltd]:Example
Organizational Unit Name (eg, section) []:Test Department
Common Name (eg, your name or your server's hostname) []:test.example.com
Email Address []:user@example.com
[root@localhost ~]#
[root@localhost ~]# echo "nsCertType = server" > openssl.conf
[root@localhost ~]# openssl x509 -text -noout -in ca.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            33:52:14:5a:12:8d:12:9c:c1:fa:77:13:a5:0c:eb:af:83:bd:6b:68
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = CA, L = San Jose, O = Example, OU = Test Department, CN =
test.example.com, emailAddress = user@example.com
        Validity
            Not Before: Mar 28 23:15:11 2023 GMT
            Not After : Mar 27 23:15:11 2024 GMT
        Subject: C = US, ST = CA, L = San Jose, O = Example, OU = Test Department, CN =
 test.example.com, emailAddress = user@example.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (1024 bit)
                Modulus:
                    00:b9:a6:16:7d:bf:74:d0:10:e2:61:af:56:55:ee:
                    60:e6:57:c0:74:bd:b0:0b:7d:64:54:75:74:d8:f8:
                    7b:3e:1a:5b:cf:d4:76:6d:fb:01:92:07:d0:3b:45:
                    9c:49:22:7d:22:55:75:05:d9:94:d2:f2:7d:4b:14:
                    96:5e:fc:26:12:30:6f:1f:54:a8:40:25:e2:1a:62:
                    f8:ec:f8:be:e2:b0:fc:85:21:9b:cb:78:f7:6d:0e:
                    00:01:50:a9:07:e8:de:c2:b5:44:c5:41:c1:3a:0b:
                    93:4f:e9:94:c6:82:df:76:15:de:42:1f:b3:86:de:
                    96:0c:52:27:10:25:25:75:8d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                71:84:61:C4:AF:E7:57:2C:B4:BB:19:22:D7:DC:7A:7F:80:E8:58:A3
            X509v3 Authority Key Identifier:
                keyid:71:84:61:C4:AF:E7:57:2C:B4:BB:19:22:D7:DC:7A:7F:80:E8:58:A3

            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
         89:6d:7f:72:89:29:4e:8b:da:74:ec:8b:10:78:ca:86:68:be:
         88:c2:25:79:cd:a1:dc:7d:ac:32:18:be:7d:54:6e:12:c9:53:
         de:c3:dc:b3:e7:52:1e:14:c5:1c:10:95:3f:e3:df:04:82:27:
         19:56:55:c6:96:e1:0c:cc:0a:81:05:aa:3f:a3:29:52:b3:bb:
         66:78:55:2b:b0:c5:f9:f7:bc:fb:e4:fd:30:f2:16:73:65:88:
         38:ea:6f:dc:34:44:50:ef:3b:a8:ac:22:98:34:11:bb:e8:27:
         6d:da:5d:ff:18:b9:e4:4f:22:54:b9:ab:51:1f:41:51:00:4e:
         25:f6
[root@localhost ~]#
```

次のタスク

新しい証明書を CIMC にアップロードします。

サーバー証明書のアップロード

始める前に

証明書をアップロードするには、admin 権限を持つユーザーとしてログインする必要があります。

アップロードする証明書は、読み取り可能テキストとして使用できる必要があります。アップロード手順で、証明書テキストをコピーして CLI に貼り付けます。

（注） 最初に、CIMC 証明書管理 CSR の生成手順を使用して CSR を生成し、その CSR を使用してアップロード用の証明書を取得する必要があります。この方法で取得されていない証明書はアップロードしないでください。

（注） 新しいサーバー証明書がアップロードされると、現在の HTTPS および SSH セッションはすべて切断されます。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope certificate**	証明書コマンド モードを開始します。
ステップ 2	Server /certificate # **upload**	新しいサーバー証明書を入力してアップロードするためのダイアログが起動します。

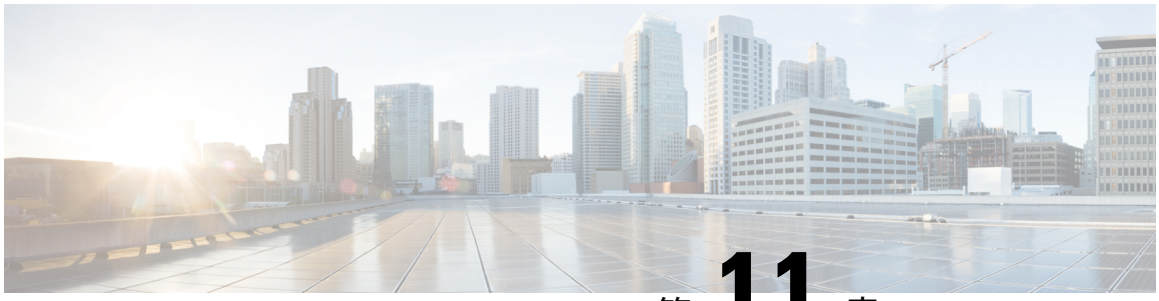
プロンプトが表示されたら、証明書テキストをコピーしてコンソールに貼り付け、CTRL を押した状態で D を押して証明書をアップロードします。

例

次に、新しい証明書をサーバーにアップロードする例を示します。

```
Server# scope certificate
Server /certificate # upload
Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
ZgAMivyCsKgb/6CjQtsofvzxmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
```

```
gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
-----END CERTIFICATE-----
<CTRL+D>
```



第 11 章

プラットフォーム イベント フィルタの設定

プラットフォーム イベント フィルタ

プラットフォームイベントフィルタ（PEF）は、ハードウェア関連の重要なイベントが発生したときに、アクションをトリガーしたりアラートを生成したりできます。PEF ごとに、プラットフォームイベントが発生したときに実行するアクション（またはアクションを実行しないこと）を選択できます。また、プラットフォームイベントが発生したときにアラートを生成して送信することもできます。アラートはSNMP トラップとして送信されるので、アラートを送信するには、先に SNMP トラップの宛先を設定する必要があります。

プラットフォーム イベント アラートの生成はグローバルにイネーブルまたはディセーブルにできます。ディセーブルにすると、PEF がアラートを送信するように設定されていても、アラートは送信されません。

プラットフォーム イベント アラートのイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope fault**	障害コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	Server /fault # **set platform-event-enabled** {**yes** | **no**}	プラットフォーム イベント アラートを有効または無効にします。 プロンプトで**y**と入力して、プラットフォームイベント アラートを有効にします。
ステップ 3	Server /fault # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 4	Server /fault # **show** [**detail**]	（任意）プラットフォーム イベント アラートの設定を表示します。

例

次に、プラットフォーム イベント アラートをイネーブルにする例を示します。

```
Server# scope fault
Server /fault # set platform-event-enabled yes
Server /fault *# commit
Server /fault # show Platform Event
Enabled
yes

Server /fault #
```

プラットフォーム イベント アラートのディセーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope fault**	障害コマンド モードを開始します。
ステップ 2	Server /fault # **set platform-event-enabled** {**yes** | **no**}	プラットフォーム イベント アラートを有効または無効にします。 プロンプトで**n**と入力して、プラットフォームイベント アラートを無効にします。
ステップ 3	Server /fault # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 4	Server /fault # **show** [**detail**]	（任意）プラットフォーム イベント アラートの設定を表示します。

プラットフォーム イベント フィルタの設定

例

次に、プラットフォーム イベント アラートをディセーブルにする例を示します。

```
Server# scope fault
Server /fault # set platform-event-enabled no
Server /fault *# commit
Server /fault # show Platform Event
Enabled
no

Server /fault #
```

プラットフォーム イベント フィルタの設定

次のプラットフォーム イベント フィルタに対する処理とアラートを設定できます。

ID	プラットフォーム イベント フィルタ
1	温度緊急アサート フィルタ
2	温度警告アサート フィルタ
3	電圧緊急アサート フィルタ
4	プロセッサ アサート フィルタ
5	メモリ緊急アサート フィルタ
6	ドライブ スロット アサート フィルタ
7	LSI 緊急アサート フィルタ
8	LSI 警告アサート フィルタ

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope fault**	障害コマンド モードを開始します。
ステップ 2	Server /fault # **scope pef** *id*	指定したイベントに対してプラットフォームイベント フィルタ コマンド モードを開始します。 イベント ID 番号に対応するプラットフォーム イベント フィルタの表を参照してください。
ステップ 3	Server /fault/pef # **set action** {**none** | **reboot** | **power-cycle** | **power-off**}	このイベントが発生した場合に必要なシステムの処理を選択します。次のいずれかの処理を選択できます。

	コマンドまたはアクション	目的
		• **none** ：システム アクションは実行されません。 • **reboot** ：サーバーがリブートされます。 • **power-cycle** ：サーバーに電源が再投入されます。 • **power-off** ：サーバーの電源がオフになります。
ステップ 4	Server /fault/pef # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、イベントに対するプラットフォーム イベント アラートを設定します。

```
Server# scope fault
Server /fault # scope pef 1
Server /fault/pef # set action reboot Server /fault/pef *# commit
Server /fault/pef # show

Platform Event Filter      Event                              Action
----------------------    ----------------------------------    ----------
  1                  Temperature Critical Assert Filter    reboot
Server /fault/pef #
```

次のタスク

PEF を設定してアラートを送信する場合は、次のタスクを完了させます。

- プラットフォーム イベント アラートのイネーブル化
- SNMP トラップ設定の実行

プラットフォーム イベント トラップの解釈

SNMP トラップとして送信された CIMC プラットフォーム イベント アラートには、エンタープライズ オブジェクト ID（OID）が `1.3.6.1.4.1.3183.1.1.0.event` の形式で含まれています。OID の最初の 10 個のフィールドは、
`iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).wired_for_management(3183).PET(1).version(1).version(0)`
を表し、IPMI プラットフォーム イベント トラップ（PET）バージョン 1.0 メッセージであることを示しています。最後のフィールドはイベント番号であり、通知されている特定の状態またはアラートを示しています。

プラットフォーム イベント トラップの説明

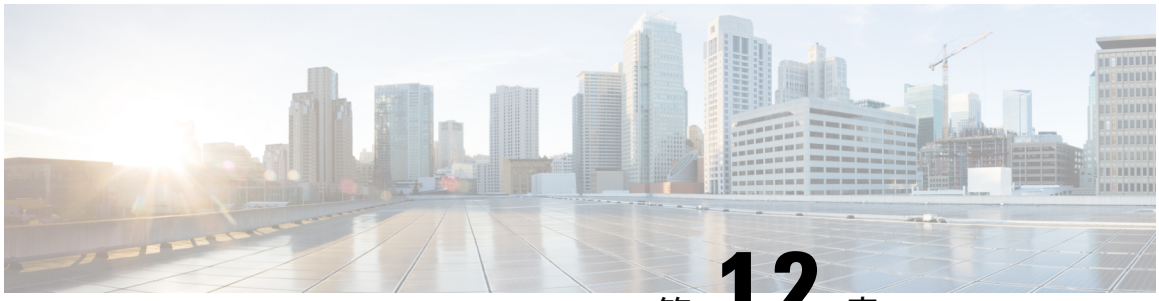
次の表に、プラットフォーム イベント トラップ メッセージで通知されるイベントの説明を示します。これらは、トラップ OID のイベント番号に基づいています。

イベント番号		プラットフォーム イベントの説明
0	0h	テスト トラップ
65799	010107h	温度に関する警告
65801	010109h	温度が重大な状態
131330	020102h	電圧不足、緊急
131337	020109h	電圧が重大な状態
196871	030107h	電流に関する警告
262402	040102h	ファンが重大な状態
459776	070400h	プロセッサ関連（IOH-Thermalert/Caterr センサー）：予測障害非アサート
459777	070401h	プロセッサ関連（IOH-Thermalert/Caterr センサー）：予測障害アサート
460032	070500h	プロセッサ電力警告：制限未超過
460033	070501h	プロセッサ電力警告：制限超過
524533	0800F5h	電源が重大な状態
524551	080107h	電源に関する警告
525313	080401h	個々の電源に関する警告
527105	080B01h	電源冗長性の損失
527106	080B02h	電源冗長性復元
552704	086F00h	電源挿入済み
552705	086F01h	電源モジュール障害
552707	086F03h	電源 AC の損失

イベント番号		プラットフォーム イベントの説明
786433	0C0001h	修正可能な ECC メモリエラー、リリース 1.3(1) 以降のリリース、すべての読み取りタイプを受け入れるように設定されたフィルタ
786439	0C0007h	DDR3_INFO センサー LED：RED ビットアサート（DIMM での ECC エラーの可能性が高い）、汎用センサー
786689	0C0101h	修正可能な ECC メモリ エラー、リリース 1.3(1) 以降のリリース
818945	0C7F01h	修正可能な ECC メモリ エラー、リリース 1.2(x) 以前のリリース
818951	0C7F07h	DDR3_INFO センサー LED：RED ビットアサート（DIMM での ECC エラーの可能性が高い）、1.2(x) 以前のリリース
851968	0D0000h	HDD センサーでは障害がないことが示されています。汎用センサー
851972	0D0004h	HDD センサーでは障害があることが示されています。汎用センサー
854016	0D0800h	HDD が存在しない、汎用センサー
854017	0D0801h	HDD が存在する、汎用センサー
880384	0D6F00h	HDD あり、障害の兆候なし
880385	0D6F01h	HDD の障害
880512	0D6F80h	HDD が存在しない
880513	0D6F81h	HDD がアサート解除されたが障害状態ではない

イベント番号		プラットフォーム イベントの説明
884480	0D7F00h	ドライブ スロット LED オフ
884481	0D7F01h	ドライブ スロット LED オン
884482	0D7F02h	ドライブ スロット LED 高速で点滅
884483	0D7F03h	ドライブ スロット LED 低速で点滅
884484	0D7F04h	ドライブ スロット LED 緑
884485	0D7F05h	ドライブ スロット LED オレンジ
884486	0D7F01h	ドライブ スロット LED 青
884487	0D7F01h	ドライブ スロット LED 読み取り
884488	0D7F08h	ドライブ スロット オンライン
884489	0D7F09h	ドライブ スロット低下

（注） すべての読み取りタイプを受け入れるようにイベント フィルタが設定された場合は、16 進のイベント番号のビット 15:8 は 0 にマスクされます。たとえば、イベント番号 786689（0C0101h）は 786433（0C0001h）になります。



第 12 章

ファームウェア管理

CIMC ファームウェアの概要

UCS E シリーズ M6 サーバーは、使用しているサーバーモデルに固有のシスコ認定ファームウェアを使用します。すべてのサポート対象サーバーモデルのファームウェアの新しいリリースは、Cisco.com からダウンロードできます。

潜在的な問題を回避するには、Host Upgrade Utility（HUU）を使用することを強く推奨します。このユーティリティは、CIMC、BIOS、およびその他のファームウェア コンポーネントを互換性のあるレベルにアップグレードします。

（注） 一致する CIMC ファームウェアをアクティブ化するまでは、新しい BIOS ファームウェアをインストールしないでください。インストールすると、サーバーがブートしなくなります。

CIMC ファームウェアの更新プロセスは、次の段階に分けられます。これは、サーバーがオフラインになる時間を最小限にするためです。

- **インストール**：この段階では、CIMC は、選択した CIMC ファームウェアをサーバーの非アクティブまたはバックアップ スロットにインストールします。
- **アクティベーション**：この段階では、CIMC は非アクティブ ファームウェア バージョンをアクティブとして設定してサーバーをリブートします。これにより、サービスが中断さ

れます。サーバーをリブートすると、新規のアクティブスロット内のファームウェアが、実行中のバージョンになります。

CIMC ファームウェアをアクティブ化した後は、BIOS ファームウェアを更新できます。サーバーは、BIOS アップデートプロセス全体を通して、電源をオフにする必要があります。CIMC がリブートを完了すると、サーバーの電源をオンにして、サービスに戻すことができます。

（注） 古いファームウェアバージョンを新しいものにアップグレードしたり、新しいファームウェアバージョンを古いものにダウングレードしたりできます。

ファームウェアのアップグレードのオプション

Cisco Host Upgrade Utility（HUU）を使用して、ファームウェア コンポーネントをアップグレードできます。

HUU：すべてのファームウェア コンポーネントのアップグレードにCIMC、BIOSおよびFPGAファームウェアを含むHUU ISO ファイルを使用することを推奨します。 HUU ISO パッケージを使用してすべてのファームウェアをアップグレードすることをお勧めします。

（注） 最新バージョンの CIMC または BIOS ファームウェアを古いバージョンの他のファームウェアとともに使用すると、予期しない動作が発生する可能性があります。

シスコからのソフトウェアの取得

BIOS および CIMC ファームウェアをダウンロードするには、次の手順を使用します。

ステップ 1 http://www.cisco.com/ を参照します。

ステップ 2 まだログインしていない場合は、ページの右上隅にある [Log In] をクリックし、Cisco.com の資格情報を使用してログインします。

ステップ 3 上部のメニュー バーで、[Support] をクリックします。

ロールダウン メニューが表示されます。

ステップ 4 [Downloads]（中央）ペインから、[All Downloads]（右下隅）をクリックします。

[Download Software] ページが表示されます。

ステップ 5 左ペインから、[Products] をクリックします。

ステップ 6 中央ペインから、[Unified Computing and Servers] をクリックします。

ステップ 7 右ペインから、[Cisco UCS E-Series Software] をクリックします。

ステップ 8 右ペインから、ダウンロードするソフトウェアのサーバー モデルの名前をクリックします。

[Download Software] ページは次のカテゴリで表示されます。

- [Unified Computing System (UCSE) Server Firmware]：ホスト アップグレード ユーティリティが含まれています。

ステップ 9 適切なソフトウェア カテゴリ リンクをクリックします。

ステップ 10 ダウンロードするソフトウェア イメージに関連付けられている [Download] ボタンをクリックします。

[End User License Agreement] ダイアログボックスが表示されます。

ステップ 11 （任意）複数のソフトウェア イメージをダウンロードするには、次を実行します。

a) ダウンロードするソフトウェア イメージに関連付けられている [Add to cart] ボタンをクリックします。

b) 右上にある [Download Cart] ボタンをクリックします。

カートに追加したすべてのイメージが表示されます。

c) 右下隅にある [Download All] をクリックして、すべてのイメージをダウンロードします。

[End User License Agreement] ダイアログボックスが表示されます。

ステップ 12 [Accept License Agreement] をクリックします。

ステップ 13 必要に応じて、次のいずれかを実行します。

- ソフトウェア イメージ ファイルをローカル ドライブに保存します。
- ソフトウェア イメージを TFTP サーバーからインストールする場合は、使用する TFTP サーバーにファイルをコピーします。

サーバーは、TFTP サーバー上の宛先フォルダに対する読み取り権限を持っていることが必要です。

次のタスク

ソフトウェア イメージをインストールします。

リモート サーバーからの CIMC ファームウェアのインストール

潜在的な問題を回避するには、Host Upgrade Utility（HUU）を使用することを強く推奨します。このユーティリティは、CIMC、BIOS、およびその他のファームウェア コンポーネントを互換性のあるレベルにアップグレードします。

（注） 一致する CIMC ファームウェアをアクティブ化するまでは、新しい BIOS ファームウェアをインストールしないでください。インストールすると、サーバーがブートしなくなります。

始める前に

- admin 権限を持つユーザーとして CIMC にログインします。
- シスコから CIMC ファームウェア ファイルを取得します。

（注） アップデートがすでに処理中であるときにアップデートを開始すると、どちらのアップデートも失敗します。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope firmware**	CIMC ファームウェア コマンド モードを開始します。
ステップ 3	Server /cimc/firmware # **update** *protocol ip-address path*	プロトコル、リモート サーバーの IP アドレス、サーバー上のファームウェア ファイルへのファイル パスを指定します。プロトコルは次のいずれかになります。 • **tftp** • **ftp** • **sftp** • **scp** • **http**
ステップ 4	Server /cimc # **show detail**	（任意）BIOS ファームウェアアップデートの進捗状況を表示します。

例

次に、ファームウェアをアップデートする例を示します。

```
Server# scope cimc
Server /cimc # scope firmware
Server /cimc/firmware # update tftp 10.20.34.56 test/dnld-ucs-k9-bundle.1.0.2h.bin
```

```
<CR> Press Enter key Firmware update has started.

Please check the status using "show detail"

Server /cimc #
```

次のタスク

新しいファームウェアをアクティブにします。

インストールした CIMC ファームウェアのアクティブ化

始める前に

CIMC ファームウェアをサーバーにインストールします。

重要 アクティブ化の進行中は、次のことを行わないでください。

- サーバーのリセット、電源切断、シャットダウン。
- CIMC をリブートまたはリセットします。
- 他のすべてのファームウェアをアクティブ化します。
- テクニカル サポート データまたは設定データをエクスポートします。

（注） アップデートの処理中にアクティブ化を開始すると、アクティブ化に失敗します。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope firmware**	CIMC ファームウェア コマンド モードを開始します。
ステップ 3	Server /cimc/firmware # **show** [**detail**]	使用可能なファームウェア イメージおよびステータスを表示します。
ステップ 4	Server /cimc # **activate**	選択したイメージをアクティブにします。イメージ番号が指定されていない場合、サーバーは現在非アクティブのイメージをアクティブにします。

例

この例では、ファームウェアイメージをアクティブ化します。

```
Server /cimc/firmware # show detail
Firmware Image Information:
    Update Stage: NONE
    Update Progress: 0%
    Current FW Version: 4.11(0)73
    FW Image 1 Version: 4.1-suthandy-030223-111138
    FW Image 1 State: BACKUP INACTIVATED
    FW Image 2 Version: 4.11(0)73
    FW Image 2 State: RUNNING ACTIVATED
    Boot-loader Version: 4.11(0)73
    Secure Boot: ENABLED

Server /cimc #
Server /cimc # activate
```

パスワードの保存形式の変更

この手順では、パスワードストレージの形式を変更する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **change-password-storage**	パスワードストレージの形式を変更します。形式を変更する前にプロンプトが表示されます。

例

次に、形式を変更する例を示します。

```
Server# scope cimc
Server /cimc # change-password-storage

This operation will change the user password storage form to be SHA512 with salt.
Note that, once you start this operation:
1. You cannot change the password storage format back.
2. The IPMI over LAN feature will stop working.
3. You need to change the passwords of all local users to have them stored in the new
format.
Are you sure you want to continue?[y|N]

Press Y to change the format.
```

TFTP サーバーからの BIOS ファームウェアのインストール

潜在的な問題を回避するには、Host Upgrade Utility（HUU）を使用することを強く推奨します。このユーティリティーは、CIMC、BIOS、およびその他のファームウェア コンポーネントを互換性のあるレベルにアップグレードします。

HUU を使用する代わりに CIMC および BIOS ファームウェアを手動でアップグレードする場合、まず CIMC ファームウェアを更新してから、BIOS ファームウェアを更新します。一致する CIMC ファームウェアをアクティブ化するまでは、新しい BIOS ファームウェアをインストールしないでください。インストールすると、サーバーがブートしなくなります。

（注） アップデートがすでに処理中であるときにアップデートを開始すると、どちらのアップデートも失敗します。

（注） BIOS ファームウェアを更新する前に、サーバーの電源を切り、モジュールをメンテナンスモードにします。

始める前に

シスコから CIMC ファームウェア ファイルを取得します。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **update protocol** *ip-address path-and-filename*	BIOS ファームウェアのアップデートを開始します。サーバーは、指定の IP アドレスにある TFTP サーバーから、指定のパスとファイル名のアップデート ファームウェアを取得します。
ステップ 3	Server /bios # **show detail**	（オプション）BIOS ファームウェアアップデートの進捗状況を表示します。
ステップ 4	Server /bios # **activate**	インストールされている BIOS ファームウェアをアクティブ化します。

例

次に、BIOS ファームウェアをアップデートする例を示します。

```
Server# scope bios
Server /bios # update 10.20.34.56 //test/dnld-ucs-k9-bundle.1.0.2h.bin
<CR> Press Enter key
Firmware update has started.
Please check the status using "show detail"
Server /bios #
```

UCS E シリーズ M6 サーバーアクセス問題のトラブルシューティング

E シリーズ M6 サーバーへのアクセスに問題がある場合は、CIMC ファームウェアイメージが破損しているか、ファイルシステムが破損しているか、CIMC ファームウェアのインストールが正常に完了しなかった可能性があります。必要に応じて、次のいずれかを実行します。

- CIMC ファームウェア イメージが破損している場合は、破損した CIMC ファームウェア イメージからの回復 （122 ページ）を参照してください。
- ファイルシステムが破損している場合は、破損ファイルシステムの回復 （124ページ）を参照してください。
- CIMCファームウェアのインストールが正常に終了しなかった場合は、CIMCファームウェアを再インストールします。

重要 セキュリティ上の観点から、**boot backup** コマンドはディセーブルです。

破損した CIMC ファームウェア イメージからの回復

始める前に

- サーバを PC に接続します。シリアルケーブルの一端を E シリーズ サーバーのシリアルポートに接続し、もう一端を PC に接続します。
- ユーザが指定したインターフェイス オプションに応じて、次のいずれかを実行します。
  - 専用：イーサネットケーブルを E シリーズ M6 サーバーの管理（専用）ポートに接続します。
  - Shared-Lom-GE2：イーサネットケーブルを E シリーズ M6 サーバーの外部 GE2 インターフェイスに接続します。

- Shared-Lom-Console：Cisco IOS CLI を使用して、E シリーズ M6 サーバーの内部コンソールインターフェイスを設定します。

- シリアル出力を表示するには、Minicom を起動します。
- 通信設定は、9600 ボー、8 ビット、パリティなし、および 1 ストップ ビットに設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	Router # **hw-module subslot** *slot* **stop**	指定した E シリーズ M6 サーバーへの電源をシャットダウンします。
ステップ 2	Router # **hw-module subslot** *slot* **start**	指定した E シリーズ M6 サーバーの電源を再起動します。
ステップ 3	***	Minicom から、*** コマンドを入力してブートローダプロンプトを入力します。
ステップ 4	ucse-cimc > boot current recovery	現在のイメージから E シリーズ M6 サーバーをブートします。
ステップ 5	Recovery-shell # **interface** [**dedicated** | **shared-lom-console** | **shared-lom-ge1** | **shared-lom-ge2** | **shared-lom-ge3**] *interface-ip-address* **netmask** *gateway-ip-address*	指定したインターフェイスの IP アドレス、サブネットマスク、ゲートウェイ IP アドレスを指定します。
ステップ 6	Recovery-shell # **ping** *tftp-ip-address*	CIMC ファームウェアが保存されているリモートの TFTP サーバーに ping を送信し、ネットワーク接続を確認します。
ステップ 7	Recovery-shell # **update** *tftp-ip-address image-filename*	CIMC ファームウェアイメージをインストールします。このイメージはリモートの TFTP サーバーに保存されています。
ステップ 8	Recovery-shell # **reboot**	CIMC をリブートします。

例

この例では、E シリーズ M6 サーバーの CIMC ファームウェアイメージを回復します。

```
Router# hw-module subslot 2/0 stop
Router# hw-module subslot 2/0 start

***

ucse-cimc > boot current recovery
recovery-shell# interface shared-lom-ge2 192.168.0.138 255.255.255.0 192.168.0.1
Network configuration:
```

```
IP config: addr: 192.168.0.138 Mask: 255.255.255.0
Gateway: 192.168.0.1
recovery-shell# ping 10.20.34.56
PING 10.20.34.56 (10.20.34.56): 56 data bytes
64 bytes from 10.20.34.56: seq=0 ttl=60 time=10.000 ms
64 bytes from 10.20.34.56: seq=1 ttl=60 time=0.000 ms
--- 10.20.34.56 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss round-trip min/avg/max =
0.000/1.000/10.000 ms
recovery-shell# update 10.20.34.56 update_pkg-cimc.combined.bin
downloading firmware image "update_pkg-cimc.combined.bin" from " 10.20.34.56 "
download firmware image done, size in bytes: 22384144
installing firmware image, please wait ... activating installed image
done
Stage: NONE
Status: SUCCESS

Error: Success
recovery-shell# reboot
```

破損ファイル システムの回復

この手順は、CIMC ブート ログ ファイルに次のエラー メッセージが表示された場合に使用します。

```
UNEXPECTED INCONSISTENCY; RUN fsck MANUALLY
```

始める前に

- サーバを PC に接続します。シリアルケーブルの一端を E シリーズ サーバーのシリアル ポートに接続し、もう一端を PC に接続します。
- ユーザが指定したインターフェイス オプションに応じて、次のいずれかを実行します。
  - 専用：イーサネットケーブルを E シリーズ M6 サーバーの管理（専用）ポートに接続します。
  - Shared-Lom-GE2：イーサネットケーブルを E シリーズ M6 サーバーの外部 GE2 インターフェイスに接続します。
  - Shared-Lom-Console：Cisco IOS CLI を使用して、E シリーズ M6 サーバーの内部コンソールインターフェイスを設定します。
- シリアル出力を表示するには、Minicom を起動します。
- 通信設定は、9600 ボー、8 ビット、パリティなし、および 1 ストップ ビットに設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	Router # **hw-module subslot** *slot* **stop**	指定した E シリーズ M6 サーバーへの電源をシャットダウンします。

	コマンドまたはアクション	目的
ステップ 2	Router # **hw-module subslot** *slot* **start**	指定したEシリーズM6サーバーの電源を再起動します。
ステップ 3	***	Minicomから、*** コマンドを入力してブートローダプロンプトを入力します。
ステップ 4	ucse-cimc > boot current recovery	現在のイメージからEシリーズM6サーバーをブートします。
ステップ 5	Recovery-shell # **fs-check** [**p3** | **p4**]	特定のパーティションのファイルシステムをチェックし、破損したファイルシステムを復元します。 （注） このコマンドでは、p3 および p4 パーティションだけを使用できます。このコマンドは破損したパーティションで使用します。破損したパーティションは、CIMC ブート アップ時に**run fsk** エラーメッセージを表示するパーティションです。 • コマンド出力に **clean** が表示される場合は、破損したファイルが回復されていることを示します。**reboot** コマンドを入力して、CIMC を再起動します。以降の手順を省略します。 • コマンド出力に **clean** が表示されない場合は、ステップ 6 に進みます。
ステップ 6	Recovery-shell # **reboot**	（任意）破損したファイルシステムが **fs-check [p3 | p4]** コマンドによって復元されず、出力に **clean** が表示されない場合は、**reboot** コマンドを入力してパーティションをフォーマットします。 以降の手順を省略します。 （注） p3 パーティションをフォーマットすると、CIMC 設定は失われます。
ステップ 7	Recovery-shell # **interface** [**dedicated** | **shared-lom-console** | **shared-lom-ge1** | **shared-lom-ge2** | **shared-lom-ge3**] *interface-ip-address* **netmask** *gateway-ip-address*	指定したインターフェイスのIPアドレス、サブネットマスク、ゲートウェイIPアドレスを指定します。
ステップ 8	Recovery-shell # **ping** *tftp-ip-address*	CIMCファームウェアが保存されているリモートのTFTPサーバーにpingを送信し、ネットワーク接続を確認します。

	コマンドまたはアクション	目的
ステップ 9	Recovery-shell # **update** *tftp-ip-address image-filename*	CIMC ファームウェアイメージをインストールします。このイメージはリモートの TFTP サーバーに保存されています。
ステップ 10	Recovery-shell # **reboot**	CIMC をリブートします。

例

この例は、E シリーズ M6 サーバーで **fs-check p3** コマンドを使用して、現在のイメージから CIMC ファームウェアを回復します。

```
Router# hw-module subslot 1/0 stop
Router# hw-module subslot 1/0 start

***

ucse-cimc > boot current recovery
recovery-shell# fs-check p3
e2fsck 1.41.14 (22-Dec-2010)
/dev/mmcblk0p3: recovering journal
/dev/mmcblk0p3: clean, 429/7840 files, 3331/31296 blocks
recovery-shell# fs-check p4
e2fsck 1.41.14 (22-Dec-2010)
/dev/mmcblk0p4: clean, 51/506912 files, 1880262/2025296 blocks
recovery-shell# reboot
```

Recovery Shell コマンド

Recovery Shell コマンド	**Description**
Recovery-shell # **dedicated-interface** *interface-ip-address netmask gateway-ip-address*	専用インターフェイスの IP アドレス、サブネットマスク、ゲートウェイ IP アドレスを指定します。
Recovery-shell # **dedicated-interface (DEPRECATED)**	専用ポートの現在の設定を表示します。
Recovery-shell # **interface [dedicated | shared-lom-console | shared-lom-ge1 | shared-lom-ge2 | shared-lom-ge3]** *interface-ip-address netmask gateway-ip-address*	指定したインターフェイスの IP アドレス、サブネットマスク、ゲートウェイ IP アドレスを指定します。
Recovery-shell # **interface**	インターフェイスの設定を表示します。
Recovery-shell # **ping** *tftp-ip-address*	CIMC ファームウェアが保存されているリモートの TFTP サーバーに ping を送信し、ネットワーク接続を確認します。

Recovery-shell # **update** *tftp-ip-address image-filename*	CIMC ファームウェアイメージをインストールします。このイメージはリモートの TFTP サーバーに保存されています。
Recovery-shell # **fs-check [p3 | p4]**	特定のパーティションのファイル システムをチェックし、破損したファイル システムを復元します。
Recovery-shell # **active image**	CIMC が実行されている現在のアクティブなイメージを表示します（イメージ 1 またはイメージ 2）。
Recovery-shell # **active image [1 | 2]**	アクティブなイメージを 1 または 2 に変更します。指定したイメージがすでにアクティブになっている場合は、メッセージが表示されます。それ以外の場合は、指定したイメージがアクティブになります。 active image コマンドを使用した後は、**reboot** コマンドを使用して、新たに設定したイメージを有効にします。
Recovery-shell # **reboot**	CIMC ファームウェアをリブートします。

パスワードの復旧

始める前に

- サーバを PC に接続します。シリアルケーブルの一端を E シリーズ サーバーのシリアル ポートに接続し、もう一端を PC に接続します。
- ユーザが指定したインターフェイス オプションに応じて、次のいずれかを実行します。
  - 専用：イーサネットケーブルを E シリーズ M6 サーバーの管理（専用）ポートに接続します。
  - Shared-Lom-GE2：イーサネットケーブルを E シリーズ M6 サーバーの外部 GE2 インターフェイスに接続します。
  - Shared-Lom-Console：Cisco IOS CLI を使用して、E シリーズ M6 サーバーの内部コンソール インターフェイスを設定します。
- シリアル出力を表示するには、Minicom を起動します。
- 通信設定は、9600 ボー、8 ビット、パリティなし、および 1 ストップ ビットに設定します。

ステップ 1 Router # **hw-module subslot** *1/0* **oir power-cycle**

E シリーズ M6 サーバーの電源が再投入されます。

ステップ 2 「***」と入力して Autoboot: 0 を停止します

プロンプトの後に「****」と入力します。

ステップ 3 ucse-cimc > **boot current recovery**

boot current recovery と入力して、リカバリモードで起動します。

ステップ 4 Recovery-shell #

```
Recovery-shell は、メニュー方式の限定機能インターフェイスです。

主なオプション：

1. configure interface
   2. show interfaces
   3. ping
   4. cimc image options
   5. emmc options
   6. admin password reset
   7. enter debug shell
   8. exit and reboot
```

ステップ 5 Recovery-shell（選択内容を入力）# **emmc format p3**

パスワードを含む設定をクリアする EMMC カードの p3 パーティションをフォーマットします。

（注） EMMC をパーティション分割すると、CIMC 設定、ISO ファイル、パスワードなどの EMMC カードの内容が失われるか、クリアされます。

```
ACT2 リセットが完了しました。システムを再起動し、デフォルトのパスワードでログインしてください。Recovery-shell は、
メニュー方式の限定機能インターフェイスのメインオプションです：

1. configure interface
  2. show interfaces
  3. ping
  4. cimc image options
  5. emmc options
  6. admin password reset
  7. enter debug shell
  8. exit and reboot
```

ステップ 6 Recovery-shell（選択内容を入力）# **8**

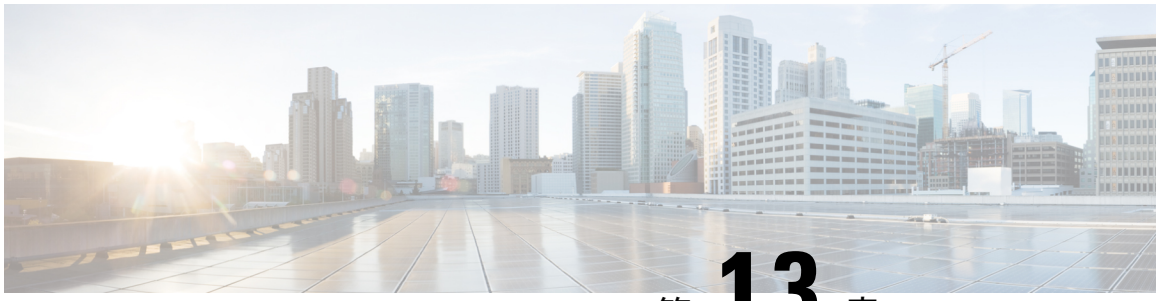
8 を押して終了し、デバイスを再起動します。

例

この例では、CMIC パスワードを覚えていない場合にパスワードを回復します。

```
server # login: admin
Password:
****************WARNING!*****************
```

```
Default credentials were used for login.
   Administrator password needs to be
     changed for security purposes.
**************************************
Enter current password: password
Please change the password...
Enter new password: <strong-password>
Re-enter new password: <strong-password>
Updating password...
Password updated successfully.
```



第 13 章

障害およびログの表示

障害

障害サマリーの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope fault**	障害コマンド モードを開始します。
ステップ 2	Server /fault # **show discrete-alarm** [**detail**]	個々のセンサーからの障害の要約を表示します。
ステップ 3	Server /fault # **show threshold-alarm** [**detail**]	しきい値センサーからの障害の要約を表示します。
ステップ 4	Server /fault # **show pef** [**detail**]	（任意）プラットフォーム イベント フィルタの要約を表示します。

例

この例では、個別のセンサーからの障害の要約を表示します。

```
Server# scope fault
Server /fault # show discrete-alarm
Name             Reading          Sensor Status
-------------    -----------      ----------------
PSU2_STATUS      absent           Critical

Server /fault #
```

システム イベント ログ

システム イベント ログの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope sel**	システム イベント ログ（SEL）コマンド モードを開始します。
ステップ 2	Server /sel # **show entries** [**details**]	（任意）システムイベントについて、イムスタンプ、イベントのシビラティ（重大度）、およびイベントの説明を表示します。**detail** キーワードを指定すると、表形式ではなくリスト形式で情報が表示されます。

例

次に、システム イベント ログを表示する例を示します。

```
Server# scope sel
Server /sel # show entries
Time                        Severity          Description
-----------------------     -------------     ----------------------------------------
2023-06-30 21:17:53 UTC     Informational     "LED_BMC_ACT: Platform sensor, "
2023-06-30 21:17:53 UTC     Informational     "LED_BMC_ACT: Platform sensor, "
2023-06-30 21:17:52 UTC     Informational     "LED_SYS: Platform sensor, "
2023-06-30 21:17:52 UTC     Informational     "LED_SYS: Platform sensor, "
2023-06-30 21:17:51 UTC     Informational     "LED_HLTH_STATUS: Platform sensor, "
2023-06-30 21:17:51 UTC     Informational     "LED_HLTH_STATUS: Platform sensor, "
2023-06-30 21:17:50 UTC     Informational     "LED_PWR_BTN: Platform sensor, "
2023-06-30 21:17:50 UTC     Informational     "LED_PWR_BTN: Platform sensor, "
2023-06-30 21:17:50 UTC    Normal           "P1_PRESENT: Presence sensor, Device Removed
 / Device Absent was asserted"
2023-06-30 21:17:50 UTC     Normal            "BIOS_POST_CMPLT: Presence sensor, Device
 Removed / Device Absent was asserted"
2023-06-30 21:17:50 UTC     Normal           "MINI_STORAGE_PRS: Presence sensor, Device
 Removed / Device Absent was asserted"
2023-06-30 21:17:50 UTC     Normal            "MAIN_POWER_PRS: Presence sensor, Device
Inserted / Device Present was asserted"
2023-06-30 21:17:50 UTC     Normal            "HDD4_STATUS: Drive Slot sensor, Drive
Presence was asserted"
sence was asserted" UTC     Normal            "HDD3_STATUS: Drive Slot sensor, Drive
Pre--More--
2023-06-30 21:17:50 UTC     Normal            "HDD2_STATUS: Drive Slot sensor, Drive
Presence was asserted"
2023-06-30 21:17:50 UTC     Normal            "HDD1_STATUS: Drive Slot sensor, Drive
Presence was asserted"
2023-06-30 21:17:50 UTC     Normal            "RISER3_PRESENT: Presence sensor, Device
Removed / Device Absent was asserted"
2023-06-30 21:17:50 UTC     Normal            "RISER2_PRESENT: Presence sensor, Device
```

```
Removed / Device Absent was asserted"
2023-06-30 21:17:50 UTC     Normal           "RISER1_PRESENT: Presence sensor, Device
Removed / Device Absent was asserted"
```

システム イベント ログのクリア

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope sel**	システム イベント ログ コマンド モードを開始します。
ステップ 2	Server /sel # **clear**	処理の確認を求めるプロンプトが表示されます。プロンプトに **y** と入力すると、システム イベント ログはクリアされます。

例

次に、システム イベント ログをクリアする例を示します。

```
Server# scope sel
Server /sel # clear
This operation will clear the whole sel.
Continue?[y|N]y
```

Cisco IMC Log

CIMC ログの表示

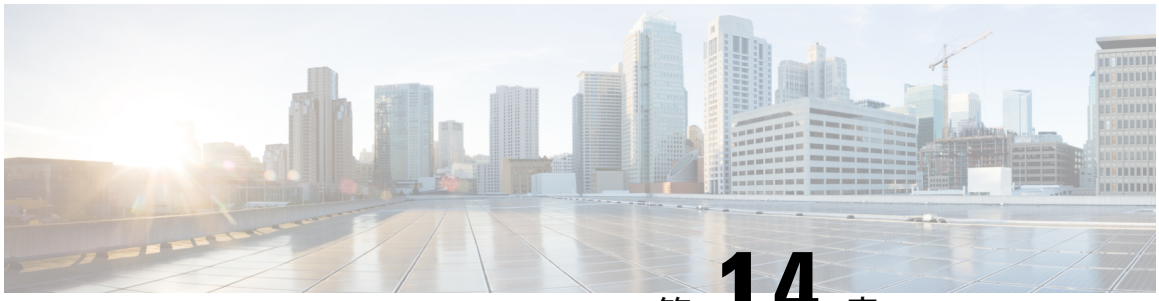
手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope log**	CIMC ログ コマンド モードを開始します。
ステップ 3	Server /cimc/log # **show entries** [**detail**]	（任意）CIMC イベントをタイムスタンプ、イベントを記録したソフトウェアモジュール、およびイベントの説明とともに表示します。

例

次に、CIMC イベントのログを表示する例を示します。

Recovery-shell# **fs-check [p3| p4]**	特定のパーティションのファイル システムをチェックし、破損したファイル システムを復元します。
Recovery-shell# **active image**	CIMC が実行されている現在のアクティブなイメージを表示します（イメージ 1 またはイメージ 2）。
Recovery-shell# **active image [1 | 2]**	アクティブなイメージを 1 または 2 に変更します。指定したイメージがすでにアクティブになっている場合は、メッセージが表示されます。 それ以外の場合は、指定したイメージがアクティブになります。 active image コマンドを使用した後は、**reboot** コマンドを使用して、新たに設定したイメージを有効にします。
Recovery-shell# **reboot**	CIMC ファームウェアをリブートします。



第 14 章

サーバ ユーティリティ

リモート サーバーへのテクニカル サポート データのエクスポート

このタスクは、Cisco Technical Assistance Center（TAC）から要求された場合に実行します。このユーティリティは、TACが技術上の問題をトラブルシューティングおよび解決する際に役立つ設定情報、ログ、および診断データが含まれる要約レポートを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope tech-support**	tech-support コマンド モードになります。
ステップ 3	Server /cimc/tech-support # **set remote-ip** *ip-address*	サポート データ ファイルを保存する必要のあるリモート サーバーの IP アドレスを指定します。
ステップ 4	Server /cimc/tech-support # **set remote-path** *path/filename*	サーバー上に保存するサポート データ ファイルの名前を指定します。この名前を入力するときは、ファイルの相対パスを、サーバー ツリーの最上位から目的の場所まで含めてください。
ステップ 5	Server /cimc/tech-support # **set remote-protocol** *protocol-type*	リモート サーバーのプロトコルを指定します。リモート サーバーのプロトコルは次のいずれかになります。

	コマンドまたはアクション	目的
		• **tftp** • **ftp** • **sftp** • **scp** • **http**
ステップ 6	Server /cimc/tech-support # **set remote-username** *username*	（任意）システムがリモート サーバーへのログインに使用する必要のあるユーザー名。 （注） ユーザー名は、リモート サーバーが TFTP または HTTP の場合は適用されません。
ステップ 7	Server /cimc/tech-support # **set remote-password** *password*	（任意）リモート ユーザー名のパスワード。 （注） パスワードは、リモート サーバーが TFTP または HTTP の場合は適用されません。
ステップ 8	Server /cimc/tech-support # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 9	Server /cimc/tech-support # **start**	リモート サーバーへのサポート データ ファイルの転送を開始します。
ステップ 10	Server /cimc/tech-support # **show detail**	ファイルのアップロードのステータスを表示します。
ステップ 11	Server /cimc/tech-support # **cancel**	（任意）リモート サーバーへのサポート データ ファイルの転送を取り消します。

例

次に、サポート データ ファイルを作成し、そのファイルを TFTP サーバーに転送する例を示します。

```
Server# scope cimc
Server /cimc # scope tech-support
Server /cimc/tech-support # set remote-ip 10.20.30.41
Server /cimc/tech-support *# set remote-path /user/user1/supportfile
Server /cimc/tech-support *# set remote-protocol tftp
Server /cimc/tech-support *# commit
Server /cimc/tech-support # start
 Tech Support upload started.
Server /cimc/tech-support # show detail
Tech Support:
    Server Address: 10.20.30.41
```

```
    Path: /user/user1/supportfile Protocol: tftp
    Username:
    Password: ******
    Progress(%): 0
    Status: COLLECTING

Server /cimc/tech-support # show detail
Tech Support:
    Server Address: 10.20.30.41
    Path: /user/user1/supportfile
    Protocol: tftp
    Username:
    Password: ******
    Progress(%): 85
    Status: COLLECTING

Server /cimc/tech-support # show detail
Tech Support:
    Server Address: 10.20.30.41
    Path: /user/user1/supportfile
    Protocol: tftp
    Username:
    Password: ******
    Progress(%): 100
    Status: COMPLETED
```

次のタスク

生成されたレポート ファイルを Cisco TAC に提供します。

CIMC の再起動

現在実行されているファームウェアで問題が発生した場合など、非常に珍しいケースですが、サーバーのトラブルシューティング時に、CIMC の再起動が必要になることがあります。この手順は、通常のサーバー メンテナンスには含まれません。CIMC を再起動した後にログオフすると、CIMC は数分間使用できません。

（注） サーバーが電源投入時自己診断テスト（POST）を実行しているとき、またはExtensible Firmware Interface（EFI）シェルを操作しているときにCIMCを再起動すると、サーバーの電源は、CIMCの再起動が完了するまでオフになります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **reboot**	確認のプロンプトが表示されたら、CIMC を再起動します。

例

次に、CIMC を再起動する例を示します。

```
Server# scope cimc
Server /cimc # reboot
This operation will reboot the CIMC.
Continue?[y|N]y
```

CIMC の出荷時デフォルトへのリセット

現在実行されているファームウェアで問題が発生した場合など、非常に珍しいケースですが、サーバーのトラブルシューティング時に、CIMC の出荷時デフォルトへのリセットが必要になることがあります。これを行うと、ユーザーが設定可能なすべての設定がリセットされます。

この手順は、通常のサーバーメンテナンスには含まれません。CIMC をリセットした後は、ログオフしてから再びログインする必要があります。また、接続が失われ、ネットワーク設定を再び指定する必要がある場合もあります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **factory-default**	確認プロンプトの後に、CIMC が出荷時デフォルトにリセットされます。

CIMC の出荷時デフォルトには、次の条件が含まれます。

- CIMC CLI へのアクセス用に、SSH がイネーブルになっている。
- CIMC GUI へのアクセス用に、HTTPS がイネーブルになっている。
- 単一ユーザーアカウントが存在している（ユーザー名は **admin**、パスワードは **password** です）。
- 管理ポートで DHCP がイネーブルになっている。
- ブート順が CDROM、PXE（LoM を使用）、FDD、HDD になっている。
- KVM と vMedia がイネーブルになっている。
- USB がイネーブルになっている。
- SoL がディセーブルになっている。

例

次に、CIMC を出荷時デフォルトにリセットする例を示します。

```
Server# scope cimc
Server /cimc # factory-default
This operation will reset the CIMC configuration to factory default.
All your configuration will be lost.
Continue?[y|N]
```

CIMC 設定のエクスポートとインポート

CIMC 設定のエクスポートとインポート

CIMC 設定のバックアップを実行するには、システム設定のスナップショットを作成し、生成されたCIMC設定ファイルをネットワーク上の場所にエクスポートできます。エクスポート操作で保存されるのは、管理プレーンからの情報だけです。サーバー上のデータはバックアップされません。ユーザーアカウントやサーバー証明書など、機密情報の設定はエクスポートされません。

エクスポートされたCIMC設定ファイルは、同じシステムで復元したり、別のCIMCシステムにインポートしたりできます。ただし、インポートするシステムのソフトウェアバージョンとエクスポートするシステムのソフトウェアバージョンが同じであるか、両者の設定に互換性があることが前提となります。設定ファイルを設定テンプレートとして他のシステムにインポートする場合は、IPアドレスやホスト名などシステム固有の設定を変更する必要があります。インポート操作によって情報が変更されるのは、管理プレーンだけです。

CIMC 設定ファイルは XML テキスト ファイルで、その構造と要素は CIMC コマンド モードに対応しています。

エクスポートまたはインポート操作を実行する場合は、次のガイドラインを考慮してください。

- エクスポートまたはインポートは、システムがアップ状態で、稼働しているときに実行できます。エクスポート操作によるサーバまたはネットワーク トラフィックへの影響はありませんが、インポート操作によって IP アドレスなどが変更されると、トラフィックが中断されたりサーバがリブートされたりすることがあります。
- エクスポートとインポートを同時に実行することはできません。

CIMC 設定のエクスポート

（注） セキュリティ上の理由から、この操作でユーザーアカウントやサーバー証明書をエクスポートしないでください。

始める前に

- バックアップ TFTP サーバーの IP アドレスを取得します。
- コンフィギュレーション ファイルのインポート時に SNMP の設定情報を復元する場合は、コンフィギュレーション ファイルを作成する前に、このサーバーで SNMP がイネーブルになっていることを確認します。コンフィギュレーションをエクスポートするときに SNMP がディセーブルになっていると、CIMC は、ファイルのインポート時に SNMP の値を適用しません。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope import-export**	import-export コマンド モードを開始します。
ステップ 3	Server /cimc/import-export # **export-config** *tftp-ip-address path-and-filename*	バックアップ操作を開始します。コンフィギュレーション ファイルは、指定した IP アドレスの TFTP サーバで指定されたパスとファイル名で保存されます。

エクスポート操作が正常に完了したかどうかを確認するには、 **show detail** コマンドを使用します。操作を中止するには、CTRL+C を入力します。

例

次に、CIMC コンフィギュレーション ファイルをバックアップする例を示します。

```
Server# scope cimc
Server /cimc # scope import-export
Server /cimc/import-export # export-config 192.0.2.34 /ucs/backups/cimc5.xml
Export config started. Please check the status using "show detail".
Server /cimc/import-export # show detail
Import Export: Operation: EXPORT Status: COMPLETED
Error Code: 100 (No Error) Diagnostic Message: NONE

Server /cimc/import-export #
```

CIMC 設定のインポート

始める前に

コンフィギュレーション ファイルのインポート時に SNMP 設定情報を復元する場合は、インポートを行う前にこのサーバーで SNMP がディセーブルになっていることを確認します。インポート時に SNMP がイネーブルになっていると、CIMC は現在の値をコンフィギュレーション ファイルに保存されている値で上書きしません。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope import-export**	import-export コマンド モードを開始します。
ステップ 3	Server /cimc/import-export # **import-config** *tftp-ip-address path-and-filename*	インポート操作を開始します。指定した IP アドレスの TFTP サーバーで指定されたパスとファイル名で、コンフィギュレーション ファイルはインポートされます。

インポート操作が正常に完了したかどうかを確認するには、 **show detail** コマンドを使用します。操作を中止するには、CTRL+C を入力します。

例

次に、CIMC コンフィギュレーションをインポートする方法を示します。

```
Server /cimc/import-export # import-config tftp 192.0.2.34 /ucs/backups/cimc5.xml
Passphrase:
Import config started. Please check the status using "show detail".

Server /cimc/import-export # show detail
Import Export:
Operation: IMPORT
Status: TRANSFERING
Error Code: 0 (No Error)
Diagnostic Message: NONE
Server /cimc/import-export #
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。