Cisco UCS E シリーズ サーバと Cisco UCS E シリーズ ネットワーク コンピュートエンジンの統合管理コントローラ リリース 3.2.x CLI コンフィギュレーション ガイド

初版：2017 年 7 月 31 日

最終更新：2017 年 7 月 31 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/

目 次

はじめに

この前書きは、次の項で構成されています。

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 *3.2.1* の新機能と重要な動作の変更

機能	説明	参照先
UCS-E180D-M3/K9 および UCS-E1120D-M3/K9 サーバをサポートします。	Cisco ISR 4000 シリーズへの UCS-E180D-M3/K9 および UCS-E1120D-M3/K9 の取り付けに対するサポートが追加されました。	概要 （1 ページ）

表 *2 : Cisco Integrated Management Controller Software* リリース *3.1.1* の新機能と重要な動作の変更

機能	説明	参照先
UCS-E160S-M3/K9 サーバをサポートします。	Cisco ISR 4000 シリーズに UCS-E160S-M3/K9 の取り付けに対するサポートが追加されました。	概要 （1 ページ）

表 *3 : Cisco Integrated Management Controller Software* リリース *3.0.1* の新機能と重要な動作の変更

機能	説明	参照先
NIM E シリーズ ネットワーク コンピュート エンジン サポート	NIM E シリーズ ネットワーク コンピュート エンジン（NIM E シリーズ NCE）のサポート。	概要 （1 ページ）
障害およびログ		障害およびログの表示 （173 ページ）
ネットワーク解析モジュール（NAM）および Network Time Protocol（NTP）の設定	NAM 機能と NTP サービスを有効にするためのサポートが追加されました。	ネットワーク関連の設定 （109 ページ）

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-Series Servers、Cisco UCS E シリーズ ネットワーク コンピュート エンジン、および CIMC の概要を紹介します。
第 2 章	サーバのオペレーティング システムのインストール	サーバ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	サーバの管理	サーバのブート デバイスの順序、サーバの電源、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。

章	タイトル	説明
第 4 章	RAID を使用したストレージの管理	RAID を設定および管理する手順について説明します。 （注） RAID 機能はE シリーズ サーバおよび SM E シリーズ NCE に適用されます。RAID 機能は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。
第 5 章	サーバのプロパティの表示	サーバの 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 6 章	サーバのセンサーの表示	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 7 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 8 章	ユーザアカウントの管理	ユーザアカウントの追加または変更方法、Active Directory によるユーザ認証の設定方法、ユーザセッションの管理方法を説明します。
第 9 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 10 章	コミュニケーションサービスの設定	HTTP、SSH、IPMI、および SNMP によるサーバ管理コミュニケーションの設定方法を説明します。
第 11 章	証明書の管理	サーバ証明書を生成、アップロード、および管理する方法を説明します。
第 12 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 13 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。
第 14 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 15 章	サーバユーティリティ	サポートデータのエクスポート方法、サーバ設定のエクスポート方法とインポート方法、サーバ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。

章	タイトル	説明
第 16 章	診断テスト	診断テストの実行方法を説明します。

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。
ユーザ入力	表示どおりにユーザが入力するテキストやユーザが押すキーは、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、角かっこで囲み、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。
[ ]	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。ここで説明しているアクションを実行すると、時間を節減できます。
警告	安全上の重要な注意事項 「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。Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. これらの注意事項を保存しておいてください

関連資料

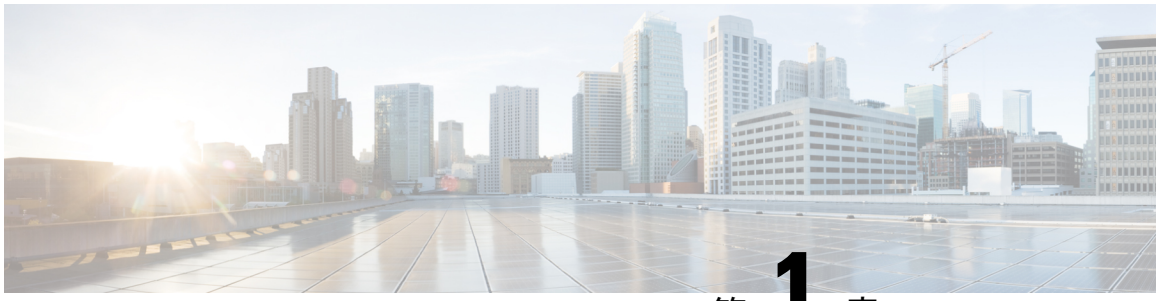
『Documentation Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine』にはすべての製品ドキュメントへのリンクが示されています。

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。

『*What's New in Cisco Product Documentation*』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。

ドキュメントの更新通知を受け取るには、Cisco UCS Docs on Twitter をフォローしてください。



第 1 章

概要

この章は、次の項で構成されています。

Cisco UCS E シリーズ サーバおよび Cisco UCS E シリーズ ネットワーク コンピュート エンジンの概要

Cisco UCS E-Series Servers（E シリーズ サーバ）およびCisco UCS E シリーズ ネットワーク コンピュート エンジン（NCE）はサイズ、重量、電力の効率にすぐれたブレード サーバのファミリで、第 2 世代の Cisco サービス統合型ルータ（Cisco ISR G2）および Cisco ISR 4000 シリーズに搭載されています。 これらのサーバは、オペレーティング システム（Microsoft Windows や Linux など）上でベアメタルとして、あるいはハイパーバイザ（VMware vSphere Hypervisor、Microsoft Hyper-V、Citrix XenServer など）上で仮想マシンとして導入される、ブランチオフィス アプリケーション向けの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。

E シリーズ サーバは、汎用コンピューティングの強力な Intel Xeon プロセッサ用に特別に作られています。 また、シングル幅とダブル幅の 2 種類のフォーム ファクタがあります。 シングル幅のE シリーズ サーバは単一のサービス モジュール（SM）スロットに適しており、ダブル幅のE シリーズ サーバは 2 つの SM スロットに適しています。

NCEは価格と性能の点で最適化されたモジュールで、シスコのネットワーク アプリケーションおよび他の軽量な汎用アプリケーションをホストするようにビルドされています。これらは、SM、NIM、および EHWIC の 3 つのフォーム ファクタで提供されます。SM E シリーズ NCE は 1 つの SM スロットに、NIM E シリーズ NCE は 1 つの NIM スロットに、EHWIC E シリーズ NCE は 2 つの EHWIC スロットに収納できます。

（注）
- EHWIC E シリーズ NCE は Cisco ISR G2 のみに設置できます。
- NIM E シリーズ NCE は Cisco ISR 4000 シリーズにのみ設置できます。
- Cisco ISR 4331 には SM スロットが 1 つあります。Cisco ISR 4321 および Cisco ISR 4431 には SM スロットがありません。
- Citrix XenServer は E シリーズ サーバでのみサポートされます。
- Cisco UCS-E160S-M3/K9、UCS-E180D-M3/K9、および UCS-E1120D-M3/K9 サーバは、ISR 4000 シリーズでのみサポートされます。
- CIMC 3.2.x は EHWIC NCE ではサポートされていません。

（注） サポートされているEシリーズ サーバおよびNCEについて、また 1 つのルータあたりにインストール可能なサーバの最大数については、『*Hardware Installation Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine*』の「Hardware Requirements」の項を参照してください。

サーバ ソフトウェア

E シリーズ サーバとNCEには、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 サーバまたはNCEのマザーボードに組み込まれている別の管理モジュールです。専用の ARM ベースのプロセッサが（メインサーバ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 サーバおよびNCE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、サーバにアクセスし、サーバを設定、管理、モニタできます。

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。他にも BIOS では、システムを設定したり、ファームウェアを管理したり、BIOS エラー レポートを作成したりすることもできます。

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 ファームウェアは更新可能ですが、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 CPU は Microsoft Windows や 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。Microsoft Windows Server または VMware vSphere Hypervisor が事前にインストールされているE シリーズ サーバまたはNCE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 サーバまたはNCEでテストされたプラットフォームについては、『『*Release Notes for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine*』』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 サーバおよび NCE 用の管理サービスです。CIMC はサーバ内で動作します。Web ベースの GUI または SSH ベースの CLI を使用して、サーバにアクセスし、サーバを設定、管理、モニタできます。

CIMC を使用すると次のサーバ管理タスクを実行できます。

- サーバの電源のオン、電源のオフ、電源再投入、リセット、およびシャットダウンを行う
- サーバのブート順を設定する
- RAID レベルを管理する

  （注） RAID 機能は E シリーズ サーバおよび SM E シリーズ NCE に適用できます。RAID 機能は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

- サーバのプロパティとセンサーを表示する
- リモート プレゼンスを管理する
- ローカル ユーザ アカウントを作成して管理し、Active Directory によるリモート ユーザの認証をイネーブルにする
- NIC プロパティ、IPv4、IPv6、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う

- HTTP、SSH、IPMI over LAN、SNMP、Redfish などのコミュニケーション サービスを設定する
- 証明書を管理する
- プラットフォーム イベント フィルタを設定する
- CIMC ファームウェアを更新する
- BIOS ファームウェアを更新する
- 内部リポジトリからホスト イメージをインストールする
- 障害、アラーム、およびサーバのステータスをモニタする
- サーバ障害の発生時にテクニカル サポート データを収集する

ほとんどすべてのタスクは、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 を呼び出すことはできない
- CIMC CLI で呼び出したコマンドを CIMC GUI に表示することはできない
- CIMC GUI から CIMC CLI 出力を生成することはできない

CIMC CLI

CIMC CLI は、E シリーズ サーバおよびNCE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。必要に応じて次のコマンドのいずれかを使用します。
  - **ucse** *slot* **session imc**：Cisco ISR G2 にインストールされている E シリーズ サーバおよび SM E シリーズ NCE で使用。Cisco IOS Release 15.2(4)M 〜15.4(2)T で適用可能。
  - **ucse subslot** *slot/subslot* **session imc**：Cisco ISR G2 にインストールされている E シリーズ サーバ、SM E シリーズ NCE、および EHWIC E シリーズ NCEで使用。Cisco IOS Release 15.4(3)M で適用可能。
  - **hw-module subslot** *slot/subslot* **session imc**：Cisco ISR 4000 シリーズにインストールされている E シリーズ サーバ および NIM E シリーズ NCE で使用。

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 #
advanced	BIOS モードから scope advanced コマンド	/bios/advanced #
main	BIOS モードから scope main コマンド	/bios/main #
server-management	BIOS モードから scope server-management コマンド	/bios/server-management #
certificate	EXEC モードから scope certificate コマンド	/certificate #

モード名	アクセスするコマンド	モード プロンプト
chassis	EXEC モードから **scope chassis** コマンド	/chassis #
storageadapter （注） このコマンドモードはEHWIC E シリーズNCEおよびNIM E シリーズNCEには適用されません。	シャーシ モードから **scope storageadapter** *slot* コマンド	/chassis/storageadapter #
physical-drive （注） このコマンドモードはEHWIC E シリーズNCEおよびNIM E シリーズNCEには適用されません。	storageadapter モードから **scope physical-drive** *drive-number* コマンド	/chassis/storageadapter /physical-drive #
virtual-drive （注） このコマンドモードはEHWIC E シリーズNCEおよびNIM E シリーズNCEには適用されません。	storageadapter モードから **scope virtual-drive** *drive-number* コマンド	/chassis/storageadapter /virtual-drive #
cimc	EXEC モードから scope cimc コマンド	/cimc #
import-export	cimc モードから scope import-export コマンド	/cimc/import-export #
log	cimc モードから scope log コマンド	/cimc/log #
server	ログ モードから **scope server** *index* コマンド	/cimc/log/server #
network	cimc モードから scope network コマンド	/cimc/network #
ipblocking	ネットワーク モードから scope ipblocking コマンド	/cimc/network/ipblocking #
tech-support	cimc モードから scope tech-support コマンド	/cimc/tech-support #

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 #
pef	障害モードから scope pef コマンド	/fault/pef #
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 #
power-cap	EXEC モードから scope power-cap コマンド	/power-cap #
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 #
trap-destination	snmp モードから **scope trap-destination** コマンド	/snmp/trap-destination #
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 #
user	EXEC モードから **scope user** *user-number* コマンド	/user #
user-session	EXEC モードから **scope user-session** *session-number* コマンド	/user-session #
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。

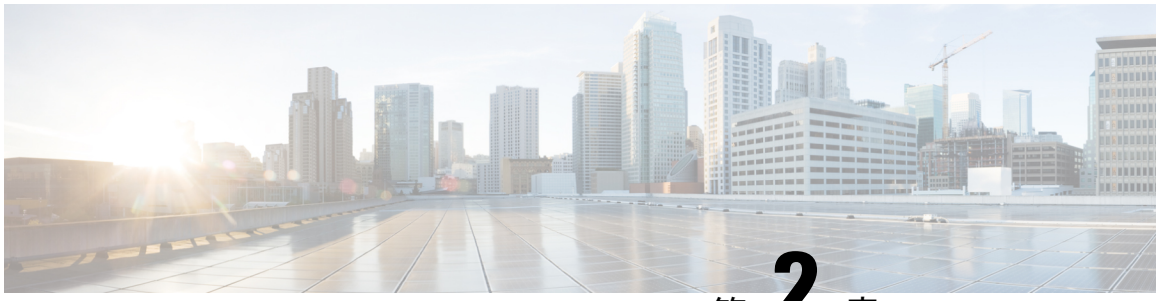
  次に、YAML 形式のコマンド出力例を示します。

```
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

この章は、次の項で構成されています。

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

E シリーズ サーバおよびNCE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
- 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に接続できます。サーバに物理的に接続された CD/DVD ドライブまたはフロッピー 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 ドライブまたはフロッピー 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。

- コンピュータ上の CD/DVD またはフロッピー ドライブ
- 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。

（注） CIMC Configuration Utility は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

- Cisco UCS M1 および M2 サーバの場合は、ブートアップ中に **Ctrl+H** を押し、WebBIOS にアクセスして RAID を設定します。

  Cisco UCS M3 サーバの場合は、ブートアップ中に **Ctrl+R** を押し、MegaRAID コントローラにアクセスして RAID を設定します。

（注） RAID は EHWIC E シリーズ NCE および NIM E シリーズ NCE ではサポートされていません。これらの SKU では、**Ctrl+H** および **Ctrl+R** は機能しません。

KVM コンソールを起動するための Java 要件

KVM コンソールを起動するためには、システムにリリース 1.6 以降の Java をインストールしておく必要があります。

証明書が Java で取り消しされたために KVM コンソールが起動しない場合は、Java の設定を変更する必要があります。次の手順を実行します。

1. Java コントロール パネルにアクセスします。

2. [Advanced] タブをクリックします。
3. [Perform certificate revocation on] で、[Do not check (not recommended)] ラジオ ボタンを選択します。詳細については、http://www.java.com/en/download/help/revocation_options.xmlを参照してください。

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手順については、『*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」の項を参照してください。

PXE インストール サーバ

Preboot Execution Environment（PXE）インストール サーバを使用すると、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 サーバは、この要求に応答確認し、サーバ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。

ステップ 2 サーバをリブートします。

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。Microsoft Windows、Linux、VMware などのホスト イメージを、リモート FTP または HTTP サーバから CIMC 内部リポジトリにダウンロードしてから、E シリーズ サーバまたはNCE内の USB コントローラの仮想ドライブにマップします。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、サーバをリブートします。ホストイメージはファイル拡張子として .iso または .img がなければなりません。

また、ホスト イメージ マッピング機能により、診断イメージをダウンロードし、マウントできます。診断イメージのファイル拡張子は必ず .diag 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**} *server-ip-address path / filename* [**username** *username* **password** *password*]	指定したリモート サーバから 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 サーバには、FTP、FTPS、HTTP、または HTTPS サーバを指定できます。リモート サーバでユーザ認証が必要な場合は、リモート サーバのユーザ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 サーバはユーザ認証をサポートしていません。FTP だけがユーザ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**	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。 • HDD：ハード ディスク ドライブ • FDD：フロッピー 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

次に、ホストのイメージをマッピングする例を示します。

```
Server# scope host-image-mapping
Server /host-image-mapping # download-image ftp 10.20.34.56 pub/hostimage.iso
---
Server /host-image-mapping # show detail
Host Image Info:
  Name: HostImage.iso
  Size: 6626848
  Last Modified Time: Fri, 12 Aug 2011 21:13:27 GMT
  Host Image Status: Download Successful!!
Server /host-image-mapping # map-image
---
status: ok
---
Server /host-image-mapping # show detail
Host Image Info:
  Name: HostImage.iso
  Size: 6626848
  Last Modified Time: Fri, 12 Aug 2011 21:13:27 GMT
  Host Image Status: Image mapped successfully!!
```

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。サーバのブート順の設定 （23 ページ）を参照してください。
2. サーバをリブートします。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。Microsoft Windows Server へのドライバのインストール手順については、Microsoft Windows Server 用のドライバのインストール （16 ページ）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。

Microsoft Windows Server 用のドライバのインストール

（注） E シリーズ サーバ または NCE オプション 1（オペレーティング システムやハイパーバイザが事前にインストールされていない E シリーズ サーバ または NCE）を購入し、Microsoft Windows Server の独自のバージョンをインストールした場合は、ドライバをインストールする必要があります。

Microsoft Windows オペレーティング システムでは、次のドライバをインストールする必要があります。

- Windows 2008 R2 用のオンボード ネットワーク ドライバ
- Windows 2008 R2 用の LSI ドライバ（オンボード ハードウェア RAID コントローラ）

- Windows 2008 R2 用の Intel ドライバ
- Windows 用の Intel サーバ チップセット ドライバ
- Windows Server 2012 R2 用の Intel ネットワーク アダプタ ドライバ

（注） 「Windows Server 2012 R2 用の Intel ネットワーク アダプタ ドライバ」ドライバは、次のサーバにのみ適用できます。

- UCS-E160S-M3 サーバ
- UCS-EN140N-M2 サーバ
- UCS-EN120E-M2 サーバ
- UCS-E180D-M3/K9 サーバ
- UCS-E1120D-M3/K9 サーバ

（注） 追加ドライバは Windows 2012 には必要ではありません。

10 ギガビット アドオン カードを購入した場合は、Windows 2008 R2 用の 10G PCIe ネットワーク ドライバもインストールする必要があります。

ステップ 1 ドライバを Cisco.com からダウンロードします。シスコからのソフトウェアの取得（152 ページ）を参照してください。

ステップ 2 ドライバ ファイルを USB フラッシュ ドライブにコピーします。

ステップ 3 使用する Microsoft Windows Server をインストールします。

インストール プロセスの途中で、LSI ドライバを要求されます。

ステップ 4 USB フラッシュ ドライブを E シリーズ サーバ の USB スロットに差し込み、LSI ドライバをインストールします。

この手順は E シリーズ サーバおよび SM E シリーズ NCE に適用されます。この手順は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

ステップ 5 Microsoft Windows Server のインストールが完了したら、オンボード ネットワーク ドライバ（Broadcom）と Intel ドライバをインストールします。

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、ホストのイメージのマッピングを解除する例を示します。

```
Server# scope host-image-mapping
Server /host-image-mapping # unmap-image
Server /host-image-mapping # show detail
Host Image Info:
  Name: HostImage.iso
  Size: 6626848
  Last Modified Time: Fri, 12 Aug 2011 21:13:27 GMT
  Host Image Status: Image unmapped successfully!!
```

ホスト イメージの削除

始める前に

admin 権限を持つユーザとして 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（GE1）インターフェイスによるESXネットワーク接続の設定

UCS E シリーズ サーバでは、MGF（GE1）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。

（注） この機能は、ISR G2 シリーズ ルータの EHWIC 4ESGP に対応している UCS E シリーズ サーバでのみサポートされます。

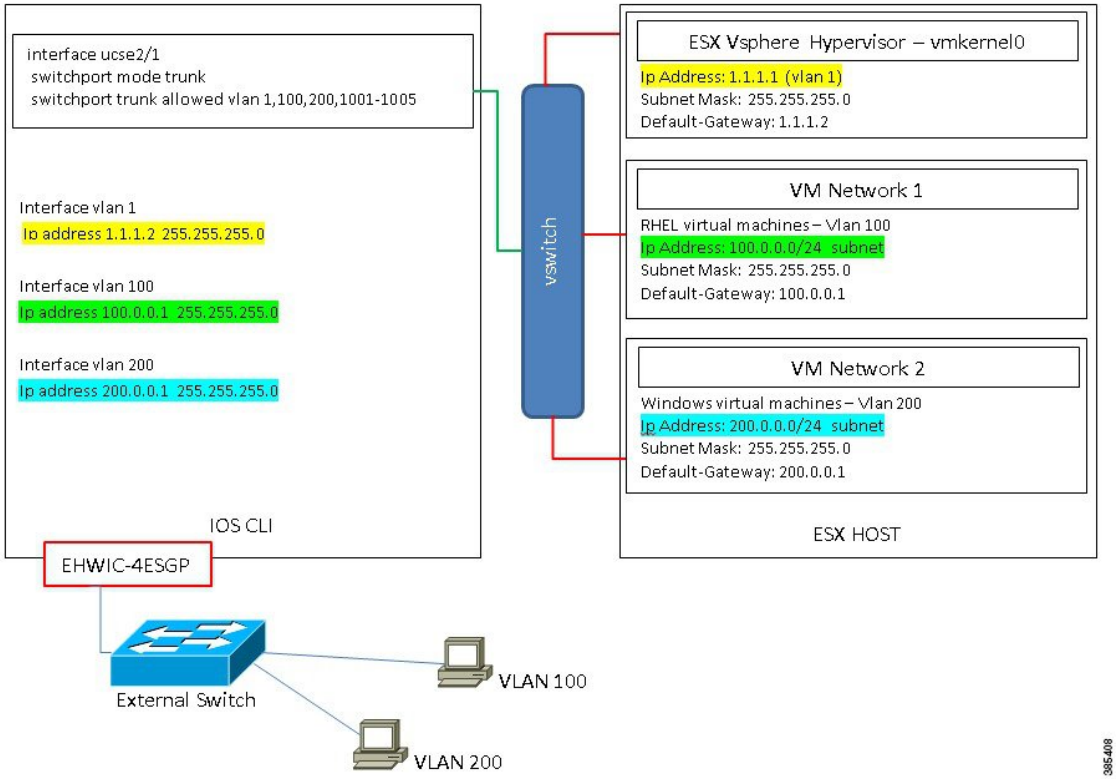
次の 3 つのシナリオにより、MGF（GE1）インターフェイスによる ESX ネットワーク接続を設定できます。

- 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

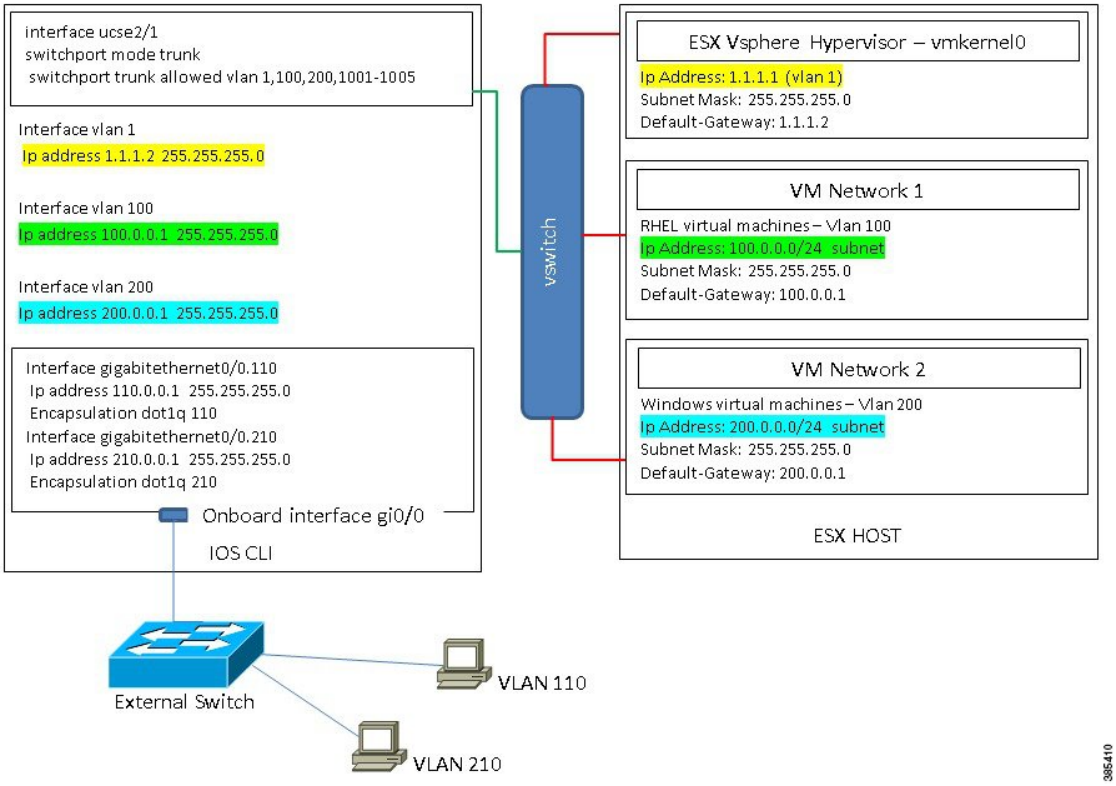
このシナリオでは、UCS E シリーズ ブレードは VLAN 100 および 200 で VM をホストします。トラフィックは MGF/UCSE2/1/ GE1 インターフェイスを介してルータに到着し、EHWIC モジュールによって物理ホストに切り替えられます。

次の設定は、（同じ VLAN 内の）VM と物理ホストが通信するしくみを示しています。



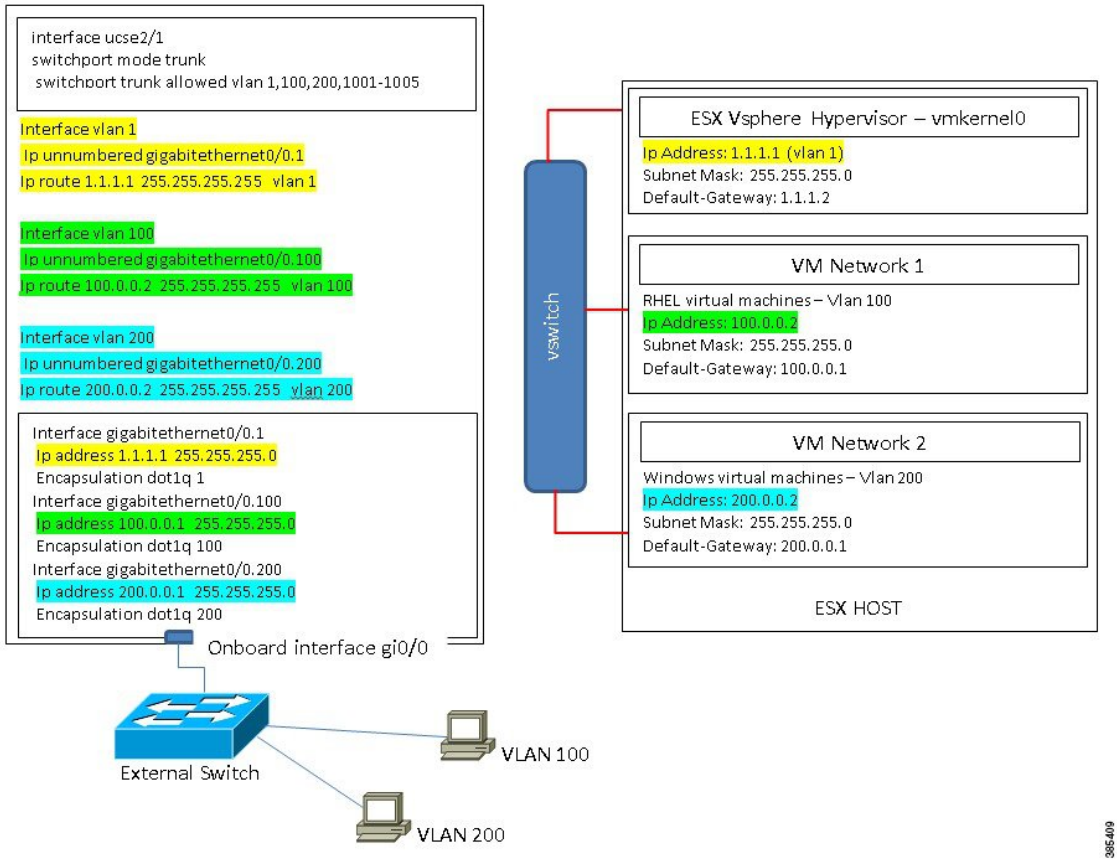
L3 ネットワーキング：ホストと VM が異なるネットワークにある

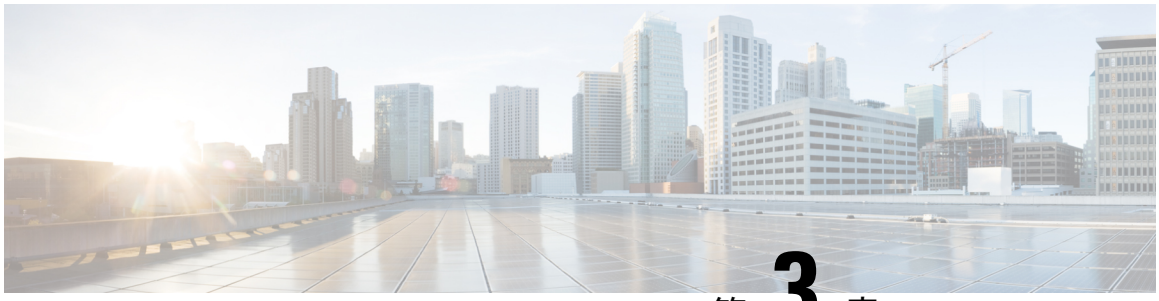
このシナリオでは、VM は、UCSE2/1 を介してルータにトラフィックを送信することにより、別のサブネット内のホストと通信します。ルータ上で、トラフィックは VLAN インターフェイスに到着し、ISRG2 により L3 ルーティングされます。



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が、ルータに EHWIC がありません。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

この章は、次の項で構成されています。

サーバのブート順の設定

（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** *category:device1*[,*category:device2*[,*category:device3*[,*category:device4*[,*category:device5*]]]]	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。 • cdrom：ブート可能な CD-ROM • 仮想 CD • fdd：フロッピーディスク ドライブ • 仮想フロッピー • hdd：ハード ディスク ドライブ • RAID • キプロス • 仮想 HiFd • pxe：PXE ブート • GigEth0 • GigEth1 • GigEth2 • GigEth3 • efi：Extensible Firmware Interface
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**	サーバのブート順を表示します。

新規のブート順は、次の BIOS のブートで使用されます。

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# scope bios
Server /bios # set boot-order cdrom:Virtual-CD,hdd:raid,efi
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
Server /bios *# commit
Server /bios #
Server /bios # show detail
```

```
BIOS:
    BIOS Version: "UCSES.1.5.0.1 (Build Date: 02/14/2013)"
    Boot Order: CDROM:Virtual-CD,HDD:RAID,EFI
    FW Update/Recovery Status: None, OK
    Active BIOS: main
```

サーバのリセット

始める前に

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

手順の概要

1. Server# **scope chassis**
2. Server /chassis # **power hard-reset**

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 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、サーバがリセットされます。 （注） • サーバ電源の再投入は、サーバの物理的な電源ボタンを押して電源をオフにした後に、電源をオンにする動作と同じです。 • 電源のハード リセットは、サーバの実際のリセット 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]
```

サーバのシャットダウン

始める前に

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

手順の概要

1. Server# **scope chassis**
2. Server /chassis # **power shutdown**

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 chassis**	シャーシ モードを開始します。
ステップ 2	Server /chassis # **power shutdown**	確認プロンプトの後で、サーバをシャットダウンします。 （注） NIM E シリーズ NCE のシャットダウンには最大 60 秒かかります。シャットダウンを 2、3 回試しても NIM E シリーズ NCE がシャットダウンしない場合は、ルータから次のコマンドを入力します。 1. Router # **hw-module subslot 0/***NIM-slot-number* **stop** 2. Router # **hw-module subslot 0/***NIM-slot-number* **start**

例

次に、サーバ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 権限を持つユーザとしてログインする必要があります。

手順の概要

1. Server# **scope chassis**
2. Server /chassis # **show detail**
3. Server /chassis # **set ios-lockout locked**
4. Server /chassis* # **commit**
5. Server /chassis # **show detail**

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 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# scope chassis
Server /chassis # show detail
 Chassis:
  Power: on
  Power Button: unlocked
  IOS Lockout: unlocked
  Serial Number: FHH16150031
  Product Name: E160DP
  PID : UCS-E160DP-M1/K9
  UUID: 0024C4F4-89F2-0000-A7D1-770BCA4B8924
  Description
Server /chassis # set ios-lockout locked
Server /chassis* # commit
Server /chassis # show detail
```

```
Chassis:
 Power: on
 Power Button: unlocked
 IOS Lockout: locked
 Serial Number: FHH16150031
 Product Name: E160DP
 PID : UCS-E160DP-M1/K9
 UUID: 0024C4F4-89F2-0000-A7D1-770BCA4B8924
 Description
```

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 権限を持つユーザとしてログインする必要があります。

手順の概要

1. Server# **scope chassis**
2. Server /chassis # **show detail**
3. Server /chassis # **set ios-lockout unlocked**
4. Server /chassis* # **commit**
5. Server /chassis # **show detail**

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 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# scope chassis
Server /chassis # show detail
 Chassis:
  Power: on
  Power Button: unlocked
  IOS Lockout: locked
  Serial Number: FHH16150031
  Product Name: E160DP
  PID : UCS-E160DP-M1/K9
  UUID: 0024C4F4-89F2-0000-A7D1-770BCA4B8924
  Description
Server /chassis # set ios-lockout unlocked
Server /chassis* # commit
Server /chassis # show detail
 Chassis:
  Power: on
  Power Button: unlocked
  IOS Lockout: unlocked
  Serial Number: FHH16150031
  Product Name: E160DP
  PID : UCS-E160DP-M1/K9
  UUID: 0024C4F4-89F2-0000-A7D1-770BCA4B8924
  Description
```

サーバの電源管理

サーバの電源投入

（注） サーバの電源が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 権限を持つユーザとしてログインする必要があります。

手順の概要

1. Server# **scope chassis**
2. Server /chassis # **power on**

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 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、サーバの電源をオンにします。

例

次に、サーバの電源をオンにする例を示します。

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

Server /chassis # show
Power Serial Number Product Name   PID            UUID
----- ------------- -------------  -------------  ------------------------------------
on    FOC16161F1P   E160D          UCS-E160D-M... 1255F7F0-9F17-0000-E312-94B74999D9E7
```

サーバの電源オフ

（注） この手順は NIM E シリーズ NCE には適用されません。

始める前に

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

手順の概要

1. Server# **scope chassis**
2. Server /chassis # **power off**

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 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**	サーバの電源をオフにします。

	コマンドまたはアクション	目的
		（注） NIM E シリーズ NCE では、**power shutdown** コマンドを使用することをお勧めします。電源を切る必要がある場合は、ルータで次のコマンドを使用します。 1. Router # **hw-module subslot 0/***NIM-slot-number* **stop** 2. Router # **hw-module subslot 0/***NIM-slot-number* **start**

例

次に、サーバ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.
Continue?[y|N]y

Server /chassis # show
Power Serial Number Product Name   PID            UUID
----- ------------- -------------  -------------  ------------------------------------
off    FOC16161F1P   E160D          UCS-E160D-M... 1255F7F0-9F17-0000-E312-94B74999D9E7
```

サーバ電源の再投入

（注） この手順は NIM E シリーズ NCE には適用されません。

始める前に

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

手順の概要

1. Server# **scope chassis**
2. Server /chassis # **power cycle**

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 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 cycle**	確認のプロンプトが表示されたら、サーバの電源を再投入します。 （注） • サーバ電源の再投入は、サーバの物理的な電源ボタンを押して電源をオフにした後に、電源をオンにする動作と同じです。 • 電源のハード リセットは、サーバの実際のリセット ボタンを押す動作と同じです。 （注） NIM E シリーズ NCE では、**power shutdown** コマンドを使用することをお勧めします。電源を再投入する必要がある場合は、ルータで次のいずれかのコマンドを使用します。 • **1.** Router # **hw-module subslot 0/***NIM-slot-number* **stop** **2.** Router # **hw-module subslot 0/***NIM-slot-number* **start** • Router # **hw-module subslot 0/***NIM-slot-number* **reload** （注） このコマンドにより、モジュールの電源が再投入されます。CIMC とサーバがリブートします。

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、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。

（注） これらのコマンドは、ISR 4K ルータでのみサポートされます。ISR G2 ではサポートされません。ISR G2 の場合は、CIMC の BIOS 設定を参照してください。

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。 • **restore-last-state**：サーバ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

ISRG2 上のモジュール

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 BIOS
Server /BIOS # scope server-management
Server /BIOS/server-management # set ResumeOnACPowerLoss power-on
Server /BIOS/server-management # commit
Server /BIOS/server-management #  show detail
```

```
Power Restore Policy:
    Power Restore Policy: power-on

Server /BIOS/server-management #
```

（注） CLI で変更された設定を確認できますが、設定を有効にするにはサーバをリブートする必要があります。

ISR4K 上のモジュール

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 #
```

サーバの前面パネルの電源ボタンのロック

（注） この手順はE シリーズ サーバおよび SM E シリーズ NCE に適用されます。この手順は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

物理サーバ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 権限を持つユーザとしてログインする必要があります。

手順の概要

1. Server# **scope chassis**
2. Server /chassis # **show detail**
3. Server /chassis # **set power-button locked**
4. Server /chassis* # **commit**
5. Server /chassis # **show detail**

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 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、サーバの電源をオンまたはオフにすることはできません。
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、物理サーバの前面パネルにあるサーバ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: on
  Power Button: unlocked
  IOS Lockout: unlocked
  Serial Number: FHH16150031
  Product Name: E160DP
  PID : UCS-E160DP-M1/K9
  UUID: 0024C4F4-89F2-0000-A7D1-770BCA4B8924
  Description
Server /chassis # set power-button locked
Server /chassis* # commit
Server /chassis # show detail
 Chassis:
  Power: on
  Power Button: locked
  IOS Lockout: unlocked
  Serial Number: FHH16150031
  Product Name: E160DP
  PID : UCS-E160DP-M1/K9
  UUID: 0024C4F4-89F2-0000-A7D1-770BCA4B8924
  Description
```

サーバの前面パネルにある電源ボタンのロック解除

（注） この手順はE シリーズ サーバおよび SM E シリーズ NCE に適用されます。この手順は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

物理サーバ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 権限を持つユーザとしてログインする必要があります。

手順の概要

1. Server# **scope chassis**
2. Server /chassis # **show detail**
3. Server /chassis # **set power-button unlocked**
4. Server /chassis* # **commit**
5. Server /chassis # **show detail**

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

```
Server# scope chassis
Server /chassis # show detail
 Chassis:
  Power: on
  Power Button: locked
  IOS Lockout: unlocked
  Serial Number: FHH16150031
  Product Name: E160DP
  PID : UCS-E160DP-M1/K9
  UUID: 0024C4F4-89F2-0000-A7D1-770BCA4B8924
  Description
Server /chassis # set power-button unlocked
Server /chassis* # commit
Server /chassis # show detail
 Chassis:
  Power: on
  Power Button: unlocked
  IOS Lockout: unlocked
  Serial Number: FHH16150031
  Product Name: E160DP
  PID : UCS-E160DP-M1/K9
  UUID: 0024C4F4-89F2-0000-A7D1-770BCA4B8924
  Description
```

BIOS の設定

BIOS ステータスの表示

手順の概要

1. Server# **scope bios**
2. Server /bios # **show detail**

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 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。

名前	説明
Boot Order	サーバが使用を試行する、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# scope bios
Server /bios # show detail
    BIOS Version: "C460M1.1.2.2a.0 (Build Date: 01/12/2011)"
    Boot Order: EFI,CDROM,HDD
    FW Update/Recovery Status: NONE
    FW Update/Recovery Progress: 100

Server /bios #
```

BIOS の詳細設定

（注） 搭載されているハードウェアによっては、このトピックで説明されている一部の設定オプションが表示されない場合があります。

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 advanced**	高度な 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 コマンドに関する各 BIOS 設定のオプションの詳細については、次のトピックを参照してください。 • 詳細：プロセッサ BIOS 設定 （42 ページ） • 詳細：メモリ BIOS 設定 （50 ページ）

	コマンドまたはアクション	目的
		• 詳細：シリアル ポート BIOS 設定 （50 ページ） • 詳細：USB BIOS 設定 （51 ページ）
ステップ 4	Server /bios/advanced # **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のリブート時に適用されます。サーバ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、Intel Virtualization Technology をイネーブルにする例を示します。

```
Server# scope bios
Server /bios # scope advanced
Server /bios/advanced # set IntelVTD Enabled
Server /bios/advanced *# commit
Changes to BIOS set-up parameters will require a reboot.
Do you want to reboot the system?[y|N] n
Changes will be applied on next reboot.
Server /bios/advanced #
```

サーバ管理 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 コマンドに関する各 BIOS 設定のオプションの詳細については、次のトピックを参照してください。 • サーバ管理 BIOS 設定 （51 ページ）
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。

	コマンドまたはアクション	目的
		変更内容は次のサーバのリブート時に適用されます。サーバ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# scope bios
Server /bios # scope server-management
Server /bios/server-management # set BaudRate 9.6k
Server /bios/server-management *# commit
Changes to BIOS set-up parameters will require a reboot.
Do you want to reboot the system?[y|N] n
Changes will be applied on next reboot.
Server /bios/server-management #
```

BIOS CMOS のクリア

非常に珍しいケースですが、サーバのトラブルシューティング時に、サーバの 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、通常のサーバメンテナンスには含まれません。

手順の概要

1. Server# **scope bios**
2. Server /bios # **clear-cmos**

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 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。 （注） Cisco UCS-E160S-M3/K9 サーバ（UCS E M3 サーバ）で **clear-cmos** コマンドを実行すると、CPU が一時的なデフォルト状態になるため、次回サーバに電源を投入したときにブート時間が非常に長くなります（35 ～ 40 分）。この問題を回避するには、ブート時に 1 ～ 2 分待ってからサーバの電源を入れ直します。ブート時間が正常に戻ります。

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 パスワードのクリア

手順の概要

1. Server# **scope bios**
2. Server /bios # **clear-bios-password**

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 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、サーバをリブートする必要があります。サーバがリブートすると、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 権限を持つユーザとしてログインする必要があります。

手順の概要

1. Server# **scope bios**
2. Server /bios # **bios-setup-default**

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 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 BIOS 設定

次の各表に、表示および設定が可能なサーバ BIOS 設定を示します。

（注） お使いのサーバでの 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
[Intel Turbo Boost Technology] [Intel Turbo Boost Technology]	プロセッサでインテル ターボ ブーストテクノロジーを使用するかどうか。このテクノロジーでは、仕様よりも低い電力、温度、または電圧でプロセッサが動作していると、自動的にそのプロセッサの周波数が上がります。次のいずれかになります。 • [Disabled]：プロセッサの周波数は自動的には上がりません。 • [Enabled]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。

名前	説明
[Enhanced Intel Speedstep Technology]	プロセッサで拡張版 Intel SpeedStep テクノロジーを使用するかどうか。このテクノロジーでは、プロセッサの電圧やコア周波数をシステムが動的に調整できます。このテクノロジーにより、平均電力消費量と平均熱発生量が減少する可能性があります。次のいずれかになります。 • [Disabled]：プロセッサの電圧または周波数を動的に調整しません。 • [Enabled]：プロセッサで Enhanced Intel SpeedStep Technology が使用され、サポートされているすべてのスリープ状態でさらに電力を節約することが可能になります。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。
[Intel Hyper-Threading Technology]	プロセッサでインテルハイパースレッディングテクノロジーを使用するかどうか。このテクノロジーでは、マルチスレッド ソフトウェア アプリケーションのスレッドを各プロセッサ内で並列に実行できます。次のいずれかになります。 • [Disabled]：プロセッサでのハイパースレッディングを禁止します。 • [Enabled]：プロセッサでの複数スレッドの並列実行を許可します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。

名前	説明
[Number of Enabled Cores]	パッケージ内の論理プロセッサ コアの状態を設定します。この設定をディセーブルにすると、ハイパースレッディングもディセーブルになります。次のいずれかになります。 • [All]：すべての論理プロセッサ コアでマルチ プロセッシングをイネーブルにします。 • [1] ～ [*n*]：サーバ上で動作できる論理プロセッサ コアの数を指定します。マルチ プロセッシングをディセーブルにし、サーバ上で動作する論理プロセッサ コアを1つだけにするには、[**1**] を選択します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。
[Execute Disable]	アプリケーション コードを実行できる場所を指定するために、サーバのメモリ領域を分類します。この分類の結果、悪意のあるワームがバッファにコードを挿入しようとした場合、プロセッサでコードの実行を無効にします。この設定は、損害、ワームの増殖、および特定クラスの悪意のあるバッファ オーバーフロー攻撃を防止するのに役立ちます。次のいずれかになります。 • [Disabled]：プロセッサでメモリ領域を分類しません。 • [Enabled]：プロセッサでメモリ領域を分類します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。

名前	説明
[Intel Virtualization Technology]	プロセッサで Intel Virtualization Technology（VT）を使用するかどうか。このテクノロジーでは、1つのプラットフォームで、複数のオペレーティング システムとアプリケーションをそれぞれ独立したパーティション内で実行できます。次のいずれかになります。 • [Disabled]：プロセッサでの仮想化を禁止します。 • [Enabled]：プロセッサで、複数のオペレーティング システムをそれぞれ独立したパーティション内で実行できます。 （注） このオプションを変更した場合は、設定を有効にするためにサーバの電源を再投入する必要があります。
[Intel VT for Directed IO]	Intel Virtualization Technology for Directed I/O（VT-d）をプロセッサで使用するかどうか。次のいずれかになります。 • [Disabled]：プロセッサで仮想化テクノロジーを使用しません。 • [Enabled]：プロセッサで仮想化テクノロジーを使用します。
[Intel VT-d Interrupt Remapping]	プロセッサで Intel VT-d Interrupt Remapping をサポートするかどうか。次のいずれかになります。 • [Disabled]：プロセッサでリマッピングをサポートしません。 • [Enabled]：プロセッサで VT-d Interrupt Remapping を必要に応じて使用します。
[Intel VT-d Coherency Support]	プロセッサで Intel VT-d Coherency をサポートするかどうか。次のいずれかになります。 • [Disabled]：プロセッサでコヒーレンシをサポートしません。 • [Enabled]：プロセッサで VT-d Coherency を必要に応じて使用します。

名前	説明
[Intel VT-d Address Translation Services]	プロセッサで Intel VT-d Address Translation Services（ATS）をサポートするかどうか。次のいずれかになります。 • [Disabled]：プロセッサで ATS をサポートしません。 • [Enabled]：プロセッサで VT-d ATS を必要に応じて使用します。
[Intel VT-d PassThrough DMA]	プロセッサで Intel VT-d Pass-through DMA をサポートするかどうか。次のいずれかになります。 • [Disabled]：プロセッサでパススルー DMA をサポートしません。 • [Enabled]：プロセッサで VT-d Pass-through DMA を必要に応じて使用します。
[Direct Cache Access]	プロセッサで、データを I/O デバイスから直接プロセッサ キャッシュに入れることにより、I/O パフォーマンスを向上させることができます。この設定はキャッシュミスを減らすのに役立ちます。次のいずれかになります。 • [Disabled]：データは I/O デバイスから直接プロセッサ キャッシュには入れられません。 • [Enabled]：データは I/O デバイスから直接プロセッサ キャッシュに入れられます。
[Processor C3 Report]	プロセッサからオペレーティング システムに C3 レポートを送信するかどうか。次のいずれかになります。 • [Disabled]：プロセッサから C3 レポートを送信しません。 • [ACPI C2][ACPI_C2]：C2 フォーマットを使用してプロセッサから C3 レポートを送信します。 • [ACPI C3][ACPI_C3]：C3 フォーマットを使用してプロセッサから C3 レポートを送信します。

名前	説明
[Processor C6 Report]	プロセッサからオペレーティングシステムにC6 レポートを送信するかどうか。次のいずれかになります。 • [Disabled]：プロセッサから C6 レポートを送信しません。 • [Enabled]：プロセッサからC6 レポートを送信します。
[Hardware Prefetcher]	プロセッサで、インテルハードウェアプリフェッチャが必要に応じてデータおよび命令ストリームをメモリから取得し、統合 2 次キャッシュに入れることを許可するかどうか。次のいずれかになります。 • [Disabled]：ハードウェアプリフェッチャは使用しません。 • [Enabled]：プロセッサで、キャッシュの問題が検出されたときにプリフェッチャを使用します。 （注） この値を設定するには、で[Custom] を選択する必要があります。[Custom] 以外の値の場合は、このオプションよりも、選択されたCPU パフォーマンスプロファイルの設定が優先されます。
[Adjacent Cache-Line Prefetch]	プロセッサで、Intel Adjacent Cache-Line Prefetch メカニズムを使用して必要に応じてデータを取得するかどうか。次のいずれかになります。 • [Disabled]：Adjacent Cache-Line Prefetch メカニズムは使用しません。 • [Enabled]：キャッシュの問題が検出されたときに Adjacent Cache-Line Prefetch メカニズムを使用します。 （注） この値を設定するには、で[Custom] を選択する必要があります。[Custom] 以外の値の場合は、このオプションよりも、選択されたCPU パフォーマンスプロファイルの設定が優先されます。

名前	説明
[Boot Option Rom]	ROM の種類を設定します。次のいずれかになります。 • Legacy：サーバはレガシー オプション ROM を起動します。 • UEFI：サーバはレガシー UEFI ROM を起動します。 • Disabled：オプション ROM は使用できません。
[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。 • [C0 state][C0_state]：サーバはすべてのサーバコンポーネントに常にフルパワーを提供します。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。 • [C2 state][C2_state]：システムレベルの調整が進行中のため、電力消費が多くなります。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。 • [C6 state][C6_state]：CPUのアイドル時に、システムはC3オプションの場合よりもさらに電力消費を減らします。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。 • [C7 state][C7_state]：CPUのアイドル時に、サーバはコンポーネントが使用できる電力量を最小にします。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。 • [No Limit][No_Limit]：サーバは、使用可能な任意のCステートに入ることがあります。 （注） このオプションは [CPU C State] がイネーブルの場合にのみ使用されます。

名前	説明
[Boot Order Rules]	CIMC で指定されたブート順と BIOS セットアップ ユーティリティで指定されたブート順のどちらに従ってシステムがブートするか。次のいずれかになります。 • [Strict]：システムは CIMC で指定されたブート順に従ってブートします。 • [Loose]：システムは BIOS セットアップ ユーティリティで指定されたブート順に従ってブートします。
[Patrol Scrub]	システムがサーバ上のメモリの未使用部分でも単一ビット メモリ エラーをアクティブに探して訂正するかどうか。次のいずれかになります。 • [Disabled]：CPU がメモリ アドレスの読み取りまたは書き込みを行うときのみ、システムはメモリの ECC エラーをチェックします。 • [Enabled]：システムは定期的にメモリを読み書きして ECC エラーを探します。エラーが見つかると、システムは修正を試みます。このオプションにより、単一ビット エラーは複数ビット エラーになる前に修正される場合がありますが、パトロール スクラブの実行時にパフォーマンスが低下する場合もあります。
[Demand Scrub]	システムがオンデマンドでのメモリのスクラビング処理を許可するかどうか。次のいずれかになります。 • **[Disabled]**：システムはオンデマンドでのメモリのスクラビング処理を許可しません。 • **[Enabled]**：システムはオンデマンドでのメモリのスクラビング処理を許可します。エラーが発生した場合、システムは修正を試みるか、読み込めないというマークを付けます。このプロセスは、システムを少数のデータ処理エラーにより迅速に実行します。

名前	説明
[Device Tagging]	システムが、説明、アドレス、名前を含むさまざまな情報に基づいた、デバイスとインターフェイスのグループ化を許可するかどうか。次のいずれかになります。 • **[Disabled]**：システムはデバイスとインターフェイスのグループ化を許可しません。 • **[Enabled]**：システムはデバイスとインターフェイスのグループ化を許可します。

詳細：メモリ BIOS 設定

名前	説明
[Select Memory RAS]	サーバに対するメモリの信頼性、可用性および機密性（RAS）の設定方法。次のいずれかになります。 • [Maximum Performance][Maximum_Performance]：システムのパフォーマンスが最適化されます。 • [Mirroring]：システムのメモリの半分をバックアップとして使用することにより、システムの信頼性が最適化されます。 • [Sparing]：一定のメモリ冗長性でシステムの信頼性を強化しながら、ミラーリングの場合よりも多くのメモリをオペレーティング システムが使用できるようにします。

詳細：シリアル ポート BIOS 設定

名前	説明
[Serial A Enable]	シリアル ポート A を有効にするか無効にするか。次のいずれかになります。 • [Disabled]：シリアル ポートは無効になります。 • [Enabled]：シリアル ポートは有効になります。

詳細：USB BIOS 設定

名前	説明
[USB Port 0]	プロセッサで USB ポート 0 を使用するかどうか。次のいずれかになります。 • [Disabled]：サーバで USB ポート 0 を使用しません。 • [Enabled]：プロセッサで USB ポート 0 を使用します。
[USB Port 1]	プロセッサで USB ポート 1 を使用するかどうか。次のいずれかになります。 • [Disabled]：サーバで USB ポート 1 を使用しません。 • [Enabled]：プロセッサで USB ポート 1 を使用します。

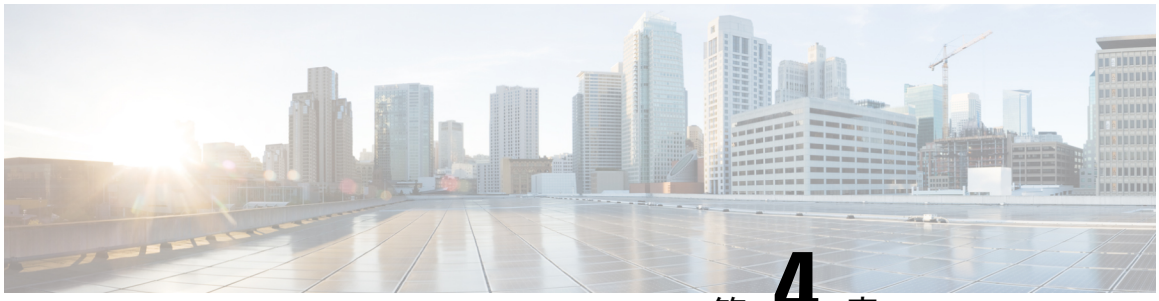
サーバ管理 BIOS 設定

名前	説明
[Assert NMI on SERR]	システム エラー（SERR）の発生時に、BIOS がマスク不能割り込み（NMI）を生成し、エラーをログに記録するかどうか。次のいずれかになります。 • [Disabled]：SERR の発生時に、BIOS は NMI を生成することもエラーをログに記録することもしません。 • [Enabled]：SERR の発生時に、BIOS は NMI を生成し、エラーをログに記録します。[Assert NMI on PERR] を有効にする場合は、この設定を有効にする必要があります。
[Assert NMI on PERR]	プロセッサ バス パリティ エラー（PERR）の発生時に、BIOS がマスク不能割り込み（NMI）を生成し、エラーをログに記録するかどうか。次のいずれかになります。 • [Disabled]：PERR の発生時に、BIOS は NMI を生成することもエラーをログに記録することもしません。 • [Enabled]：PERR の発生時に、BIOS は NMI を生成し、エラーをログに記録します。この設定を使用するには、[Assert NMI on SERR] をイネーブルにする必要があります。

名前	説明
[FRB2 Enable]	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。
[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発生しません。 • [Serial Port A][Serial_Port_A]：POST中のコンソール リダイレクション用にシリアル ポート A をイネーブルにします。このオプションはブレード サーバおよびラックマウント サーバに対して有効です。[Serial Port A] オプションを選択する場合は、[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
[Baud Rate]	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。サーバが [OS Boot Watchdog Timer Timeout] フィールドに指定された時間内にブートしない場合、CIMC はエラーをログに記録し、[OS Boot Watchdog Policy] フィールドに指定されたアクションを実行します。**set OSBootWatchdogTimerTimeout** コマンドで指定された時間内にブートしない場合、CIMC はエラーをログに記録し、**set OSBootWatchdogTimerPolicy** コマンドで指定されたアクションを実行します。
[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。



第 4 章

RAID を使用したストレージの管理

（注） RAID 機能は E シリーズ サーバおよび SM E シリーズ NCE に適用できます。RAID 機能は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

この章は、次の項で構成されています。

RAID オプション

（注） RAID 機能は E シリーズ サーバおよび SM E シリーズ NCE に適用できます。RAID 機能は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

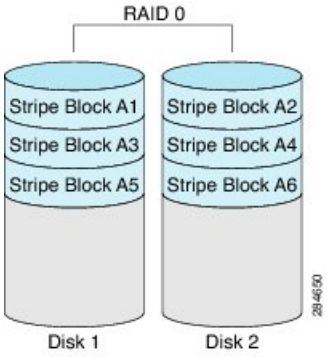
E シリーズ サーバのデータ ファイルは、ローカルの Redundant Array of Inexpensive Disks（RAID）に保存することもできます。次の RAID レベルがサポートされています。

- シングルワイドの E シリーズ サーバでは、RAID 0 と RAID 1 レベルがサポートされます。
- ダブルワイドの E シリーズ サーバでは、RAID 0、RAID 1、および RAID 5 レベルがサポートされます。
- PCIe オプションを搭載したダブルワイドの E シリーズ サーバ では、RAID 0 と RAID 1 レベルがサポートされます。

RAID 0

RAID 0 では、データは 1 台以上のディスク ドライブにわたるストライプ ブロックに冗長性（ミラーリング）なしで均等に保存されます。すべてのディスク ドライブのデータは異なります。

図 *1 : RAID 0*



RAID 1 と比較すると、RAID 0 では両方のディスク ドライブがデータの保存に使用されるため、記憶域が増加します。2 台のディスク ドライブ内で読み取り操作と書き込み操作が並行して発生するため、パフォーマンスが向上します。

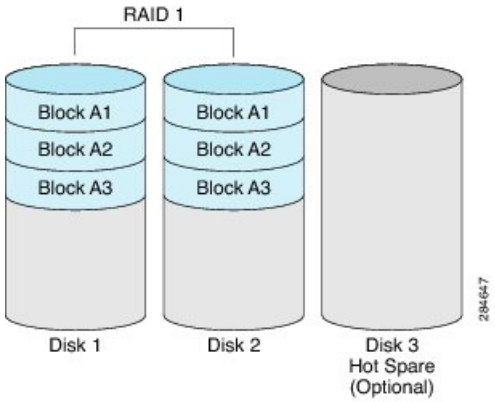
ただし、耐障害性、エラー チェック、ホット スペア、ホットスワップはありません。一方のディスク ドライブで障害が発生した場合は、アレイ全体のデータが破壊されます。エラー チェックやホットスワップの機能がないため、アレイは回復不能なエラーの影響を受けやすくなります。

RAID 1

RAID 1 は、ディスク ドライブの両方でデータが同一であるミラーリングされた一連のディスク ドライブを作成し、冗長性とハイ アベイラビリティを提供します。一方のディスク ドライブで障害が発生した場合は、他方のディスク ドライブが引き継ぎ、データは保持されます。

RAID 1 では、ホット スペア ディスク ドライブを使用することもできます。ホット スペア ドライブは、常にアクティブであり、フェールオーバー時のホット スタンバイ ドライブとして待機しています。

図 *2 : RAID 1*



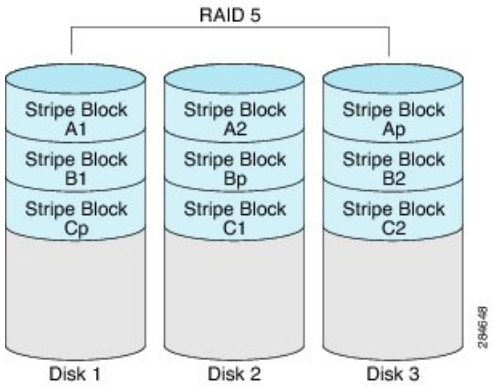
RAID 1 では、耐障害性とホットスワップがサポートされます。1 台のディスク ドライブで障害が発生した場合は、障害のあるディスク ドライブを取り外して新しいディスク ドライブに交換することができます。

ただし、RAID 0 と比較すると、潜在的な合計ディスク領域の半分しか保存に使用できないため記憶域が減少します。また、パフォーマンスにも影響があります。

RAID 5

RAID 5 では、データがすべてのディスク ドライブにわたって保存され、各ドライブにパリティ データが分散されます。それにより、低コストで冗長性が実現されます。

図 *3 : RAID 5*



RAID 5 は、RAID 1 よりも大きいデータ ストレージ容量と、RAID 0 よりも優れたデータ保護を提供します。さらに、ホット スワップもサポートしています。ただし、パフォーマンスは RAID 1 の方が優れています。

RAID 10

RAID 0 と RAID 1 の組み合わせである RAID 10 は、ミラーリングされたスパンにまたがってストライピングされたデータで構成されます。RAID 10 ドライブ グループは、ミラーリングされた一連のドライブからストライピングされたセットを作成する、スパンされたドライブ グ

ループです。RAID 10 では、最大 8 つのスパンを使用できます。スパンに含まれる各 RAID 仮想ドライブには、偶数のドライブを使用する必要があります。RAID 1 仮想ドライブは、ストライプ サイズが同一である必要があります。RAID 10 は、高いデータ スループットと完全なデータ冗長性を提供しますが、より多くのスパンを使用します。

（注） RAID 10 はダブル幅 M3 サーバでサポートされています。

非 RAID

コンピュータのディスク ドライブが RAID として設定されていない場合、コンピュータは非 RAID モードです。非 RAID モードは、Just a Bunch of Disks または Just a Bunch of Drives（JBOD）とも呼ばれます。非RAIDモードでは、耐障害性、エラーチェック、ホットスワップ、ホットスペア、冗長性はサポートされません。

RAID オプションの概要

RAID オプション	Description	利点	欠点
RAID 0	冗長性なしでストライプブロックに均等に保存されるデータ	• 優れたストレージ効率 • パフォーマンスの向上	• エラー チェックなし • 耐障害性なし • ホットスワップなし • 冗長性なし • ホット スペアなし
RAID 1	ディスク ドライブのミラーセットとオプションのホット スペア ディスク ドライブ	• ハイ アベイラビリティ • 耐障害性 • ホット スペア • ホットスワップ	• ストレージの減少 • パフォーマンス上の影響

RAID 5	すべてのディスク ドライブにわたってストライプブロックに保存されるデータと分散されたパリティ データ	• RAID 1 よりも優れたストレージ効率 • RAID 0 よりも優れた耐障害性 • 低コストの冗長性 • ホットスワップ	• 低いパフォーマンス
非 RAID	RAID が設定されていないディスク ドライブ JBOD とも呼ばれます	• ポータブル	• エラー チェックなし • 耐障害性なし • ホットスワップなし • 冗長性なし • ホット スペアなし

RAID の設定

（注） RAID 機能は E シリーズ サーバおよび SM E シリーズ NCE に適用できます。RAID 機能は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

仮想ドライブの RAID レベル、ストリップ サイズ、ホスト アクセス権限、ドライブ キャッシング、および初期化パラメータを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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 storageadapter**	インストールされているストレージ カードに関する情報を表示します。この情報を使用して、ストレージ カードが装着されているスロットを判別できます。
ステップ 3	Server /chassis # **scope storageadapter SLOT-5**	装着されているストレージ カードに対してコマンド 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 /chassis/storageadapter # **show physical-drive**	物理ディスク ドライブを表示します。この情報を使用して、物理ドライブのステータスを確認することができます。 （注） RAID を設定するには、物理ドライブのステータスが **unconfigured good** である必要があります。物理ドライブのステータスを変更するには、「物理ドライブの状態の変更」を参照してください。
ステップ 5	Server /chassis/storageadapter # **create-virtualdrive** {**-r0** | **-r1** | **-r5**} *physical-drive-numbers* [**QuickInit** | **FullInit** | **NoInit**] [**RW** | **RO** | **Blocked**] [**DiskCacheUnchanged** | **DiskCacheEnable** | **DiskCacheDisable**] [**-strpsz64** | **-strpsz32** | **-strpsz16** | **-strpsz8**]	物理ドライブに指定されている RAID レベルで仮想ドライブを作成します。次のオプションを指定することもできます。 （注） オプションでは、大文字と小文字は区別されません。 • （任意）初期化のオプション • **QuickInit**：コントローラがドライブを即時に初期化します。数秒以内に、仮想ドライブへのデータ書き込みを開始できます。これがデフォルトのオプションです。 • **FullInit**：コントローラは新しいコンフィギュレーションの完全な初期化を行います。初期化が完了するまで、仮想ドライブにデータを書き込むことはできません。ドライブのサイズが大きい場合、この処理に長時間かかることがあります。 • **NoInit**：コントローラはドライブの初期化を行いません。 • （任意）アクセス ポリシーのオプション • **RW**：ホストにドライブへのフル アクセス権があります。これがデフォルトのオプションです。 • **RO**：ホストはドライブからのデータ読み取りのみを行えます。 • [Blocked]：ホストはドライブにアクセスできません。 • （任意）ドライブのキャッシュ オプション

	コマンドまたはアクション	目的
		• **DriveCacheDisable**：物理ドライブでキャッシュがディセーブルになります。 （注） これがデフォルトであり、推奨オプションです。 • **DriveCacheUnchanged**：コントローラは物理ドライブに指定されたキャッシュ ポリシーを使用します。これがデフォルトのオプションです。 • **DriveCacheEnable**：物理ドライブでキャッシュがイネーブルになります。 • （任意）ストリップ サイズのオプション • **-strpsz64**：これがデフォルトのオプションです。 • **-strpsz32** • **-strpsz16** • **-strpsz8** **注意** ストリップ サイズを小さく設定した場合の VMware vSphere Hypervisor™ インストールに関する既知の問題があるため、vSphere プラットフォームをインストールするときは、**strpsz64** オプションを使用することをお勧めします。
ステップ 6	Server /chassis/storageadapter # **show virtual-drive**	（任意）ストレージカード用の仮想ドライブの情報を表示します。この情報を使用して、RAID 設定を確認することができます。

例

次に、RAID を設定する例を示します。

```
Server# scope chassis
Server /chassis # show storageadapter

PCI Slot Product      Name    Serial Number  Firmware Package Build   Product ID Cache
Memory Size
-------- ------------------------------ -------------- ------------------------
-------------- ---
SLOT-5   LSI MegaRAID SAS     2004 ROMB      20.10.1-0092             LSI Logic   0 MB
```

```
Server /chassis # scope storageadapter SLOT-5

Server /chassis /storageadapter# show physical-drive

Slot Number  Controller Status              Manufacturer   Model        Drive  Firmware
 Coerced Size   Type
-----------  ---------- ---------------------------------- -------------- --------------
 -------------- ---
1             SLOT-5     unconfigured good    TOSHIBA        MBF2600RC    5704   571250
MB          HDD
2             SLOT-5     unconfigured good    ATA            ST9500620NS  SN01   475883
MB          HDD

Server /chassis /storageadapter # create-virtualdrive -r0 1 FullInit RW DiskCacheEnable
 -strpsz32
---
status: ok
----------------------
Server /chassis /storageadapter # show virtual-drive
Virtual Drive  Status               Name                     Size       RAID Level
-------------- -------------------- ------------------------ ---------- ----------
0              Optimal                                       571250 MB  RAID 0
```

次のタスク

ディスク ドライブをブート可能にします。「ディスク ドライブのブート可能化」を参照してください。

物理ドライブの状態の変更

（注） RAID 機能は E シリーズ サーバおよび SM E シリーズ NCE に適用できます。RAID 機能は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

物理ドライブの状態を変更するには、次の手順を実行します。[hotspare]、[jbod]、または [unconfigured good] を選択できます。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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 storageadapter**	インストールされているストレージ カードに関する情報を表示します。この情報を使用して、ストレージ カードが装着されているスロットを判別できます。

	コマンドまたはアクション	目的
ステップ 3	Server /chassis # **scope storageadapter SLOT-5**	装着されているストレージカードに対してコマンドモードを開始します。
ステップ 4	Server /chassis/storageadapter # **show physical-drive**	物理ディスク ドライブを表示します。
ステップ 5	Server /chassis/storageadapter # **scope physical-drive** *slot-number*	指定された物理ドライブのコマンドモードを開始します。
ステップ 6	Server /chassis/storageadapter /physical-drive # **show detail**	指定された物理ドライブに関する情報を表示します。
ステップ 7	Server /chassis/storageadapter /physical-drive # **set state {unconfiguredgood | jbod | hotspare}**	物理ドライブの状態を変更します。[hotspare]、[jbod]、または [unconfigured good] を選択できます。
ステップ 8	Server /chassis/storageadapter /physical-drive* # **commit**	変更をコミットします。
ステップ 9	Server /chassis/storageadapter /physical-drive # **show detail**	指定された物理ドライブに関する情報を表示します。

例

次に、物理ドライブの状態を変更する例を示します。

```
Server# scope chassis
Server /chassis # show storageadapter

PCI Slot Product      Name    Serial Number  Firmware Package Build   Product ID Cache
Memory Size
-------- ------------------------------ -------------- ------------------------
-------------- ---
SLOT-5   LSI MegaRAID SAS     2004 ROMB      20.10.1-0092             LSI Logic   0 MB


Server /chassis# scope storageadapter SLOT-5
Server /chassis /storageadapter# show physical-drive

Slot Number  Controller Status              Manufacturer   Model        Drive  Firmware
 Coerced Size   Type
-----------  ----------  ------------------------------------ -------------- --------------
 -------------- -----
1             SLOT-5     system               TOSHIBA        MBF2600RC    5704   571250
MB           HDD
2             SLOT-5     unconfigured good    ATA            ST9500620NS  SN01   475883
MB           HDD

Server /chassis /storageadapter# scope physical-drive 1
Server /chassis /storageadapter/physical-drive# show detail

Slot Number 1:
    Controller: SLOT-5
    Status: system
    Manufacturer: TOSHIBA
    Model: MBF2600RC
    Drive Firmware: 5704
```

```
    Coerced Size: 571250 MB
    Type: HDD

Server /chassis /storageadapter/physical-drive# set state hotspare
Server /chassis /storageadapter/physical-drive*# commit
Server /chassis /storageadapter/physical-drive# show detail

Slot Number 1:
    Controller: SLOT-5
    Status: hotspare
    Manufacturer: TOSHIBA
    Model: MBF2600RC
    Drive Firmware: 5704
    Coerced Size: 571250 MB
    Type: HDD
```

仮想ドライブの削除

（注） RAID 機能は E シリーズ サーバおよび SM E シリーズ NCE に適用できます。RAID 機能は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

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 # **scope storageadapter SLOT-5**	装着されているストレージカードに対してコマンド モードを開始します。
ステップ 3	Server /chassis/storageadapter # **scope virtual-drive 0**	仮想ドライブを削除するために必要な仮想ドライブ番号を含む仮想ドライブ情報を表示します。
ステップ 4	Server /chassis/storageadapter/virtual-drive # **delete virtual-drive**	指定した仮想ドライブが削除されます。

例

次の例は、仮想ドライブの削除方法を示します。

```
Server /chassis# scope storageadapter SLOT-5
Server /chassis /storageadapter # show virtual-drive
Virtual Drive  Status               Name                    Size       RAID Level
-------------- -------------------- ----------------------- ---------- ----------
0              Optimal                                      571250 MB  RAID 0

Server /chassis /storageadapter # delete virtual-drive 0
VD 0 is the boot drive.  It is hosting the server's operating system.
All data on the drive will be lost.
Are you sure you want to delete this virtual drive?
```

```
Enter 'yes' to confirm -> yes

Server /chassis /storageadapter *# commit
```

仮想ドライブの再構築のオプション

（注） RAID 機能は E シリーズ サーバおよび SM E シリーズ NCE に適用できます。RAID 機能は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

新しい RAID レベルに仮想ドライブを移行（再構築）するには、物理ドライブを追加または削除する必要があります。物理ドライブを追加または削除するとき、仮想ドライブのサイズは維持または増加されます。

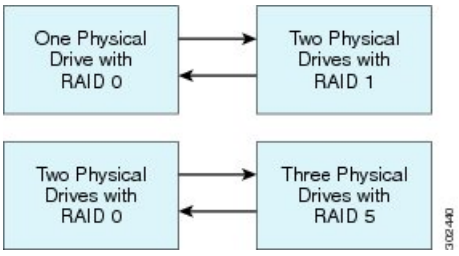
仮想ドライブのサイズは維持または増加させることはできますが、減少させることはできません。たとえば、RAID 0 で 2 台の物理ドライブがある場合、同じ台数のドライブで RAID 1 に移行することはできません。これは、RAID 1 では、仮想ドライブのサイズを以前の半分に減らした、ミラーリングされた一連のディスク ドライブが作成されるためです。これはサポートされていません。

（注） 仮想ドライブの再構築プロセスは、完了までに数時間かかることがあります。再構築プロセス中も、システムを引き続き使用できます。

仮想ドライブのサイズを保持するオプション

仮想ドライブを新しい RAID レベルに移行した際に仮想ドライブのサイズが維持されるオプションについては、次の図とその後に続く表を参照してください。

図 *4*:仮想ドライブ サイズが維持されるオプション



次の表に、仮想ドライブのサイズが維持されるオプションの一覧と、仮想ドライブを特定の RAID レベルに移行する際に追加または削除しなければならない物理ドライブの台数に関する情報を示します。

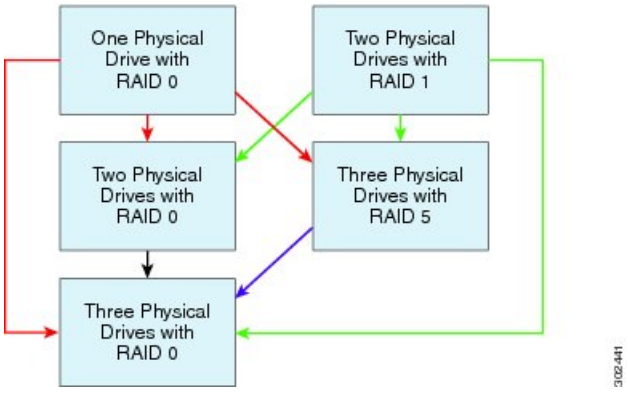
表 *4:* 仮想ドライブ サイズの維持

変更前：	移行後：	ディスクの追加または削除
RAID 0 で物理ドライブが 1 台	RAID 1 で物理ドライブが 2 台	ディスクを 1 台追加します。
RAID 1 で物理ドライブが 2 台	RAID 0 で物理ドライブが 1 台	ディスクを 1 台削除します。
RAID 0 で物理ドライブが 2 台	RAID 5 で物理ドライブが 3 台	ディスクを 1 台追加します。
RAID 5 で物理ドライブが 3 台	RAID 0 で物理ドライブが 2 台	ディスクを 1 台削除します。

仮想ドライブのサイズを増やすためのオプション

仮想ドライブを新しい RAID レベルに移行したときに仮想ドライブのサイズが増加するオプションについては、次の図とその後に続く表を参照してください。

図 *5:* 仮想ドライブ サイズが増加するオプション



次の表に、仮想ドライブのサイズが増加するオプションの一覧と、仮想ドライブを特定のRAIDレベルに移行する際に追加または削除しなければならない物理ドライブの台数に関する情報を示します。

表 *5:* 仮想ドライブ サイズの増加

変更前：	移行後：	ディスクの追加または削除
RAID 0 で物理ドライブが 1 台 図中の**赤色**の矢印を参照してください。	RAID 0 で物理ドライブが 2 台	ディスクを 1 台追加します。
	RAID 5 で物理ドライブが 3 台	ディスクを 2 台追加します。
	RAID 0 で物理ドライブが 3 台	ディスクを 2 台追加します。
RAID 1 で物理ドライブが 2 台 図中の**緑色**の矢印を参照してください。	RAID 0 で物理ドライブが 2 台	—
	RAID 5 で物理ドライブが 3 台	ディスクを 1 台追加します。
	RAID 0 で物理ドライブが 3 台	ディスクを 1 台追加します。
RAID 0 で物理ドライブが 2 台 図中の**黒色**の矢印を参照してください。	RAID 0 で物理ドライブが 3 台	ディスクを 1 台追加します。
RAID 5 で物理ドライブが 3 台 図中の**紫色**の矢印を参照してください。	RAID 0 で物理ドライブが 3 台	—

仮想ドライブの再構築

（注） RAID 機能は E シリーズ サーバおよび SM E シリーズ NCE に適用できます。RAID 機能は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

指定された RAID レベルに仮想ドライブを移行するために、物理ドライブを追加または削除するには、この手順を使用します。

始める前に

仮想ドライブの再構築のオプション （65 ページ）を参照してください。

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 storageadapter**	インストールされているストレージカードに関する情報を表示します。この情報を使用して、ストレージ カードが装着されているスロットを判別できます。
ステップ 3	Server /chassis # **scope storageadapter SLOT-5**	装着されているストレージカードに対してコマンド モードを開始します。
ステップ 4	Server /chassis/storageadapter # **scope virtual-drive** ドライブ番号	指定された仮想ドライブのコマンドモードを開始します。
ステップ 5	Server /chassis/storageadapter /virtual-drive # **reconstruct** {**-r0 | -r1 | -r5**} [**-add | -rmv**] *new-physical-drive-slot-number(s)*	新しい指定 RAID レベルに仮想ドライブを移行するために物理ドライブを追加または削除します。 • **-r0 | -r1 | -r5**：使用可能な RAID レベルは RAID 0、RAID 1、または RAID 5 です。 • **- add | - rmv**：物理ドライブを追加または削除します。
ステップ 6	Server /chassis/storageadapter /virtual-drive # **show detail**	指定された仮想ドライブに関する情報を表示します。

例

次に、最初に RAID 1 として設定されていた 2 台のディスクのうち 1 台を RAID 0 に移行する例を示します。

```
Server# scope chassis
Server /chassis # show storageadapter

PCI Slot Product      Name    Serial Number  Firmware Package Build   Product ID Cache
Memory Size
-------- ------------------------------ -------------- ------------------------
-------------- ---
SLOT-5   LSI MegaRAID SAS     2004 ROMB      20.10.1-0092             LSI Logic   0 MB


Server /chassis# scope storageadapter SLOT-5
Server /chassis /storageadapter# scope virtual-drive 0
Server /chassis /storageadapter/virtual-drive# reconstruct -r0 -rmv 1
---
status: ok
...
Server /chassis /storageadapter/virtual-drive# show detail
Status: Optimal
    Status: Optimal
    Name:
```

```
Size: 475883 MB
RAID Level: RAID 1
Target ID: 0
Stripe Size: 64 KB
Drives Per Span: 2
Span Depth: 1
Access Policy: Read-Write
Disk Cache Policy: Unchanged
Write Cache Policy: Write Through
Cache Policy: Direct
Read Ahead Policy: None
Auto Snapshot: false
Auto Delete Oldest: true
Allow Background Init: true
ReConstruct Progress: 0 %
ReConstruct Elapsed Seconds: 3 s
```

ディスク ドライブのブート可能化

（注） RAID 機能は E シリーズ サーバおよび SM E シリーズ NCE に適用できます。RAID 機能は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

RAIDの設定後、ディスク ドライブをブート可能にする必要があります。ディスク ドライブをブート可能にするには、次の手順を実行します。

始める前に

ディスク ドライブに RAID を設定します。

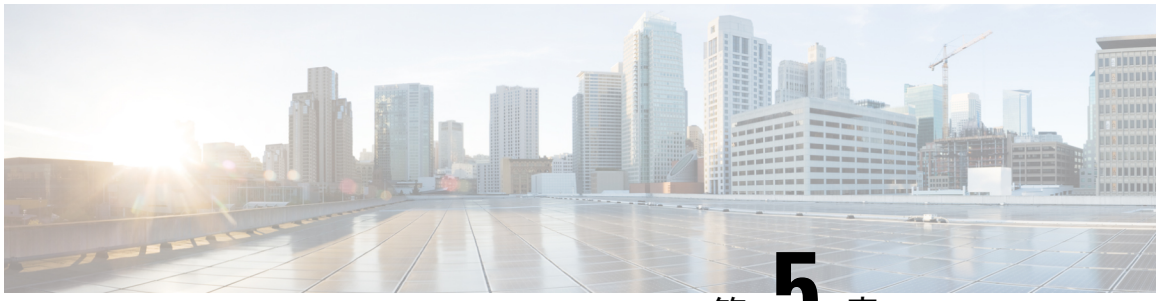
手順

	コマンドまたはアクション	目的
ステップ 1	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 # **scope storageadapter SLOT-5**	装着されているストレージ カードに対してコマンド モードを開始します。
ステップ 3	Server /chassis # **scope storageadapter SLOT-5**	装着されているストレージ カードに対してコマンド モードを開始します。
ステップ 4	Server /chassis/storageadapter # **scope virtual-drive 0**	仮想ドライブを設定するために必要な仮想ドライブ番号を含む仮想ドライブ情報を表示します。
ステップ 5	Server /chassis/storageadapter /virtual-drive# **set boot-drive**	ディスク ドライブをブート可能にします。

例

次に、CIMC CLI を使用してディスク ドライブをブート可能にする例を示します。

```
Server /chassis# scope storageadapter SLOT-5
Server /chassis /storageadapter# show physical-drive

Slot Number  Controller Status              Manufacturer   Model        Drive  Firmware
 Coerced Size   Type
----------- ---------- ----------------------------------- -------------- --------------
 -------------- -----
1            SLOT-5     system               TOSHIBA        MBF2600RC    5704   571250
MB           HDD
2            SLOT-5     unconfigured good    ATA            ST9500620NS  SN01   475883
MB           HDD

   Server /chassis /storageadapter# set boot-drive 0
Are you sure you want to set virtual drive 0 as the boot drive?
Enter 'yes' to confirm -> yes
```



第 5 章

サーバのプロパティの表示

この章は、次の項で構成されています。

サーバのプロパティの表示

始める前に

サーバ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**	サーバのプロパティを表示します。

例

次に、サーバのプロパティを表示する例を示します。

```
Server# scope chassis
Server /chassis # show detail
Chassis:
    Power: on
    Power Button: unlocked
    IOS Lockout: unlocked
    Serial Number: FOC16161F1P
    Product Name: E160D
    PID : UCS-E160D-M1/K9
    UUID: 1255F7F0-9F17-0000-E312-94B74999D9E7
    Description
```

実際のブート順の表示

手順の概要

1. Server# **scope bios**
2. Server /bios # **show actual-boot-order**

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 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。

```
E160S/bios# scope bios
Server /bios # show actual-boot-order
Boot Order   Type                      Boot Device
------------ ------------------------- ----------------------------------
1            Internal EFI Shell        Internal EFI Shell
2            CD/DVD                    Cisco vKVM-Mapped vDVD1.22
3            CD/DVD                    Cisco CIMC-Mapped vDVD1.22
4            Network Device (PXE)      TE2 - 10G Port 2
5            Network Device (PXE)      TE3 - 10G Port 3
6            Network Device (PXE)      GE0 - 1G Internal Port 0
7            Network Device (PXE)      GE1 - 1G Internal Port 1
8            FDD                       Internal Flash
9            FDD                       Cisco vKVM-Mapped vFDD1.22
10           HDD                       Cisco vKVM-Mapped vHDD1.22
11           HDD                       Cisco CIMC-Mapped vHDD1.22
12           HDD                       RAID Adapter
```

```
E1120D/bios# scope bios
Server /bios # show actual-boot-order
Boot Order   Type                      Boot Device
------------ ------------------------- ----------------------------------
1            CD/DVD                    Cisco vKVM-Mapped vDVD1.22
2            CD/DVD                    Cisco CIMC-Mapped vDVD1.22
3            HDD                       RAID Adapter
4            HDD                       Cisco
5            HDD                       Cisco vKVM-Mapped vHDD1.22
6            HDD                       Cisco CIMC-Mapped vHDD1.22
7            FDD                       Cisco vKVM-Mapped vFDD1.22
8            Network Device (PXE)      IBA XE Slot 0300 v2358
9            Network Device (PXE)      IBA XE Slot 0301 v2358
10           Network Device (PXE)      BRCM MBA Slot 0500 v15.2.7
11           Network Device (PXE)      BRCM MBA Slot 0501 v15.2.7
12           Internal EFI Shell        Internal EFI Shell
```

CIMC 情報の表示

始める前に

CIMC ファームウェアをサーバにインストールします。

手順の概要

1. Server# **scope cimc**
2. Server /cimc # **show** [**detail**]

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 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# scope cimc
Server /cimc # show detail
CIMC:
    Firmware Version: 1.0(1.20120417172632)
    Current Time: Thu Apr 26 12:11:44 2012
    Boot-loader Version: 1.0(1.20120417172632).16
```

SD カード情報の表示

始める前に

CIMC ファームウェアをサーバにインストールします。

（注） .

SD カードは、M3 モジュール（UCS-E160S-M3、UCS-E180D-M3、および UCS-E1120D-M3）ではサポートされていません。

手順の概要

1. Server# **scope cimc**
2. Server /cimc # **show sd detail**

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 cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **show sd detail**	SD カードに関する情報（製造元とアプリケーション ID、シリアル番号、ハードウェアとファームウェアのバージョン、製造年月日、SD カードが検出されたかどうか）が表示されます。カード検出ステータスが **yes** の場合は、SD カードが搭載されており、機能しています。

例

次に、CIMC に関する情報の例を示します。

```
Server# scope cimc
Server /cimc # show sd detail
Manufacturer ID: Unigen 0x000045
    OEM/Application ID: 0x0024
    Serial Number: 0x39500025
    Hardware Revision: 0x2
    Firmware Revision: 0x0
    Manufacture Date: 06/2013
    Card Detected: yes
```

CPU のプロパティの表示

始める前に

サーバ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
------------ -------- --------------------------------------------------
CPU1         4        Intel(R) Xeon(R) CPU     E5-2418L 0 @ 2.00GHz

Server /chassis #
```

メモリのプロパティの表示

始める前に

サーバ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
-------------------- --------------- ------------------- ---------------

Node0_Dimm0          8192 MB         1333                DDR3
Node0_Dimm1          8192 MB         1333                DDR3
Node0_Dimm2          8192 MB         1333                DDR3
```

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 Node0_Dimm0:
 Capacity: 8192 MB
 Channel Speed (MHz): 1333
 Channel Type: DDR3
 Memory Type Detail: Registered (Buffered)
 Bank Locator: Node0_Bank0
 Visibility: Yes
 Operability: Operable
 Manufacturer: Samsung
 Part Number: M393B1K70DH0-
 Serial Number: 86A7D514
 Asset Tag: Dimm0_AssetTag
 Data Width: 64 bits
 Name Node0_Dimm1:
 Capacity: 8192 MB
```

電源のプロパティの表示

始める前に

サーバ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。

（注） Power-cap は ISR44XX ではサポートされていません。これは、ISR-G2 でのみサポートされています。

手順の概要

1. Server# **scope power-cap**
2. Server /power-cap # **show** [**detail**]

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 power-cap**	電力制限コマンド モードを開始します。
ステップ 2	Server /power-cap # **show** [**detail**]	サーバ電力使用量の情報を表示します。

例

この例では、シングル幅の E シリーズ サーバの詳細な電源プロパティを表示します。

```
Server# scope power-cap
Server /power-cap # show detail
 Cur Consumption (W): 36.10 W
 Max Consumption (W): 075
 Min Consumption (W): 36.10 W
Server /power-cap #
```

この例では、倍幅の E シリーズ サーバの詳細な電源プロパティを表示します。

```
Server# scope power-cap
Server /power-cap # show detail
 Cur Consumption (W): 43.1 W
 Max Consumption (W): 160
 Min Consumption (W): 43.1 W
Server /power-cap #
```

ストレージのプロパティの表示

ストレージ アダプタのプロパティの表示

（注） この手順はE シリーズ サーバおよび SM E シリーズ NCE に適用されます。この手順は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

始める前に

サーバ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 storageadapter** [*slot*] [**detail**]	インストールされているストレージ カードを表示します。

	コマンドまたはアクション	目的
		（注） このコマンドは、CIMC 経由で管理できるサーバの MegaRAID のすべてのコントローラを表示します。インストールされているコントローラまたはストレージ デバイスが表示されない場合、CIMC 経由で管理できません。
ステップ 3	Server /chassis # **scope storageadapter SLOT-5**	装着されているストレージ カードに対してコマンド モードを開始します。
ステップ 4	Server /chassis/storageadapter # **show capabilites** [**detail**]	ストレージ カードでサポートされる RAID レベルを表示します。
ステップ 5	Server /chassis/storageadapter # **show error-counters** [**detail**]	ストレージ カードによって認識されたエラーの数を表示します。
ステップ 6	Server /chassis/storageadapter # **show firmware-versions** [**detail**]	ストレージ カードのファームウェア バージョン情報を表示します。
ステップ 7	Server /chassis/storageadapter # **show hw-config** [**detail**]	ストレージ カードのハードウェア情報を表示します。
ステップ 8	Server /chassis/storageadapter # **show pci-info** [**detail**]	ストレージ カードのディスプレイ アダプタの PCI 情報が表示されます。
ステップ 9	Server /chassis/storageadapter # **show running-firmware-images** [**detail**]	ストレージ カードの実行中のファームウェアの情報を表示します。
ステップ 10	Server /chassis/storageadapter # **show settings** [**detail**]	ストレージ カードのアダプタ ファームウェアの設定を表示します。

例

次に、ストレージのプロパティを表示する例を示します。

```
Server# scope chassis
Server /chassis # show storageadapter

Controller Product Name              Firmware Package Build Product ID     Cache Memory
 Size
---------- --------------------------- ---------------------- --------------
-----------------
SLOT-5     LSI MegaRAID SAS 2004 ROMB  20.10.1-0092           LSI Logic      0 MB
```

物理ドライブのプロパティの表示

（注） この手順はE シリーズ サーバおよび SM E シリーズ NCE に適用されます。この手順は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

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 # **scope storageadapter SLOT-5**	装着されているストレージ カードに対してコマンド モードを開始します。
ステップ 3	Server /chassis/storageadapter # **show physical-drive** [*slot-number*] [**detail**]	ストレージ カードの物理ドライブの情報を表示します。
ステップ 4	Server /chassis/storageadapter # **show physical-drive-count** [**detail**]	ストレージ カードの物理ドライブの数を表示します。
ステップ 5	Server /chassis/storageadapter # **scope physical-drive** *slot-number*	指定された物理ドライブのコマンド モードを開始します。
ステップ 6	Server /chassis/storageadapter/physical-drive # **show general** [**detail**]	指定された物理ドライブに関する一般情報を表示します。
ステップ 7	Server /chassis/storageadapter/physical-drive # **show status** [**detail**]	指定された物理ドライブのステータス情報を表示します。

例

次に、SLOT-5 という名前のストレージ カードの物理ドライブ番号 1 に関する一般情報を表示する例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-5
Server /chassis/storageadapter # scope physical-drive 1
Server /chassis/storageadapter/physical-drive # show general
Slot Number 1:
    Controller: SLOT-5
    Enclosure Device ID: 64
    Device ID: 3
    Sequence Number: 2
    Media Error Count: 0
    Other Error Count: 12
    Predictive Failure Count: 0
    Link Speed: 6.0 Gb/s
    Interface Type: SATA
    Media Type: HDD
```

```
    Block Size: 512
    Block Count: 1953525168
    Raw Size: 953869 MB
    Non Coerced Size: 953357 MB
    Coerced Size: 952720 MB
    SAS Address 0: 4433221100000000
    SAS Address 1:
    Connected Port 0:
    Connected Port 1:
    Connected Port 2:
    Connected Port 3:
    Connected Port 4:
```

次に、SLOT-5 という名前のストレージ カードの物理ドライブ番号 1 に関するステータス情報を表示する例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-5
Server /chassis/storageadapter # scope physical-drive 1
Server /chassis/storageadapter/physical-drive # show status
Slot Number 1:
   Controller: SLOT-5
   State: system
   Online: true
   Fault: false
```

仮想ドライブのプロパティの表示

（注） この手順はE シリーズ サーバおよび SM E シリーズ NCE に適用されます。この手順は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

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 # **scope storageadapter SLOT-5**	装着されているストレージカードに対してコマンドモードを開始します。
ステップ 3	Server /chassis/storageadapter # **show virtual-drive** [ドライブ番号] [**detail**]	ストレージカードの仮想ドライブの情報を表示します。
ステップ 4	Server /chassis/storageadapter # **show virtual-drive-count** [**detail**]	ストレージカードに設定された仮想ドライブの数を表示します。
ステップ 5	Server /chassis/storageadapter # **scope virtual-drive** ドライブ番号	指定された仮想ドライブの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 6	Server /chassis/storageadapter/virtual-drive # **show physical-drive** [**detail**]	指定した仮想ドライブに関する物理ドライブ情報を表示します。

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 # scope storageadapter SLOT-5
Server /chassis/storageadapter # show virtual-drive
Virtual Drive  Status               Name                    Size       RAID Level
-------------- -------------------- ----------------------- ---------- ----------
0              Optimal                                      571250 MB  RAID 1

Server /chassis/storageadapter # show virtual-drive-count
PCI Slot SLOT-5:
    Virtual Drive Count: 1
    Degraded Virtual Drive Count: 0
    Offline Virtual Drive Count: 0
Server /chassis/storageadapter # scope virtual-drive 0
Server /chassis/storageadapter/virtual-drive # show physical-drive
Span  Physical Drive Status     Starting Block Number Of Blocks
----- -------------- ---------- -------------- ----------------
0     2              online     0              1169920000
0     1              online     0              1169920000
```

PCI アダプタのプロパティの表示

（注） この手順はE シリーズ サーバおよび SM E シリーズ NCE に適用されます。この手順は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

始める前に

サーバ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。

手順の概要

1. Server# **scope chassis**
2. Server /chassis # **show pci-adapter** [**detail**]

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 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 pci-adapter** [**detail**]	PCI アダプタのプロパティを表示します。

例

次に、PCI アダプタのプロパティを表示する例を示します。

```
Server# scope chassis
Server /chassis # show pci-adapter
Name             Slot  Vendor ID    Device ID    Product Name
---------------- ----- ------------ ------------ -------------------------
PCIe Adapter1    1     0x1137       0x0042       Cisco UCS P81E Virtual...
PCIe Adapter2    5     0x1077       0x2432       Qlogic QLE2462 4Gb dua...

Server /chassis #
```

電源ポリシーの統計情報の表示

始める前に

（注） これは、ISR-G2 プラットフォームでのみ適用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **show power-cap [detail]**	サーバの電力消費量の統計情報および電力制限ポリシーを表示します。

表示されるフィールドについては、次の表で説明します。

名前	説明
[Current Consumption]	現在サーバによって使用されている電源（ワット単位）。
[Maximum Consumption]	最後にリブートされてからサーバが使用した最大ワット数。
[Minimum Consumption]	最後にリブートされてからサーバが使用した最小ワット数。

例

この例では、シングル幅の E シリーズ サーバの詳細な電力統計情報を表示します。

```
Server# scope power-cap
Server /power-cap # show detail
 Cur Consumption (W): 36.10 W
 Max Consumption (W): 075
 Min Consumption (W): 36.10 W
Server /power-cap #
```

この例では、倍幅の E シリーズ サーバの詳細な電力統計情報を表示します。

```
Server# scope power-cap
Server /power-cap # show detail
 Cur Consumption (W): 43.1 W
 Max Consumption (W): 160
 Min Consumption (W): 43.1 W
Server /power-cap #
```

ハード ドライブのプレゼンスの表示

始める前に

サーバ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。

手順の概要

1. Server# **scope chassis**
2. Server /chassis # **show hdd**

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 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_PRS             inserted
```

```
HDD2_PRS              inserted
HDD3_PRS              inserted
```

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。

手順の概要

1. Server# **scope cimc**
2. Server /cimc # **scope network**
3. Server /cimc/network # **show lom-mac-list** [**detail**]

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 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                       00:24:c4:f4:89:ee
GE1                           00:24:c4:f4:89:ef
GE2                           00:24:c4:f4:89:f0
GE3                           00:24:c4:f4:89:f1
```

M3 サーバの場合、インターフェイス GE は TE によって置き換えられます。次の例は、M3 サーバの場合の出力を示しています。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # show lom-mac-list
Interface                     MAC Address
------------------------------ --------------------
```

```
Console                       28:6f:7f:ee:ac:0a
GE1                           28:6f:7f:ee:ac:0b
TE2                           28:6f:7f:ee:ac:0c
TE3                           28:6f:7f:ee:ac:0d
```

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状態を表示するには、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（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）。

手順の概要

1. Server# **scope cimc**
2. Server /cimc # **scope network**
3. Server /cimc/network # **show link state [detail]**

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 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

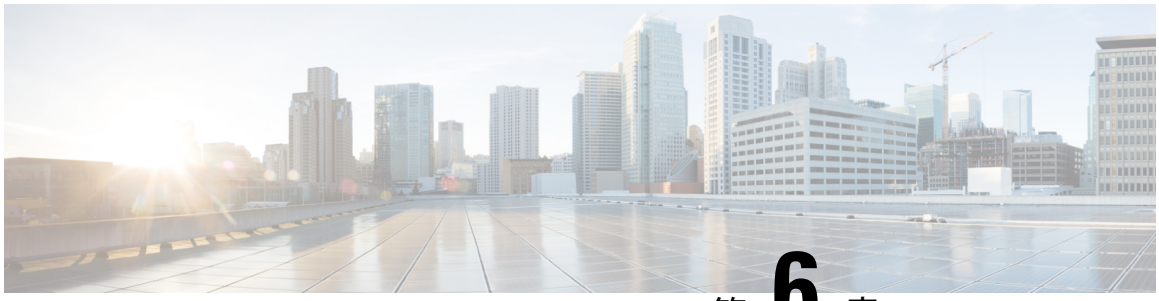
次に、CIMC ネットワーク接続の状態を表示する例を示します。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # show link state
Interface                     State
----------------------------- --------------------
Console                       Link Detected
GE1                           No Link Detected
GE2                           No Link Detected
GE3                           No Link Detected
Dedicated                     Link Detected

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

```
Link State:
    Interface: GE1
    State: No Link Detected
Link State:
    Interface: GE2
    State: No Link Detected
Link State:
    Interface: GE3
    State: No Link Detected
Link State:
    Interface: Dedicated
    State: Link Detected
```

M3 サーバの場合、インターフェイス GE は TE によって置き換えられます。次の例は、M3 サーバの場合の出力を示しています。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # show link state
Interface                     State
----------------------------- --------------------
Console                       Link Detected
GE1                           Link Detected
TE2                           No Link Detected
TE3                           No Link Detected
Dedicated                     No Link Detected
```



第 6 章

サーバのセンサーの表示

この章は、次の項で構成されています。

温度センサーの表示

手順の概要

1. Server# **scope sensor**
2. Server /sensor # **show temperature** [**detail**]

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 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      Min. Warning Max. Warning
 Min. Failure Max. Failure
------------------------ -------------- ---------- ---------- ------------ ------------
 ------------ ------------
IOH_TEMP_SENS            Normal         32.0       C          N/A          80.0
  N/A          85.0
P2_TEMP_SENS             Normal         31.0       C          N/A          80.0
  N/A          81.0
```

```
P1_TEMP_SENS              Normal          34.0       C          N/A           80.0
  N/A           81.0
DDR3_P2_D1_TMP            Normal          20.0       C          N/A           90.0
  N/A           95.0
DDR3_P1_A1_TMP            Normal          21.0       C          N/A           90.0
  N/A           95.0
FP_AMBIENT_TEMP           Normal          28.0       C          N/A           40.0
  N/A           45.0

Server /sensor #
```

電圧センサーの表示

手順の概要

1. Server# **scope sensor**
2. Server /sensor # **show voltage** [**detail**]

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 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      Min. Warning Max. Warning
 Min. Failure Max. Failure
------------------------- -------------- ---------- ---------- ------------ ------------
 ------------ ------------
P3V_BAT_SCALED            Normal         3.022      V          N/A          N/A
  2.798        3.088
P12V_SCALED               Normal         12.154     V          N/A          N/A
  11.623       12.331
P5V_SCALED                Normal         5.036      V          N/A          N/A
  4.844        5.157
P3V3_SCALED               Normal         3.318      V          N/A          N/A
  3.191        3.381
P5V_STBY_SCALED           Normal         5.109      V          N/A          N/A
  4.844        5.157
PV_VCCP_CPU1              Normal         0.950      V          N/A          N/A
  0.725        1.391
PV_VCCP_CPU2              Normal         0.891      V          N/A          N/A
  0.725        1.391
P1V5_DDR3_CPU1            Normal         1.499      V          N/A          N/A
  1.450        1.548
P1V5_DDR3_CPU2            Normal         1.499      V          N/A          N/A
  1.450        1.548
P1V1_IOH                  Normal         1.087      V          N/A          N/A
```

```
  1.068         1.136
P1V8_AUX                  Normal          1.773       V           N/A           N/A
  1.744         1.852

Server /sensor #
```

LED センサーの表示

始める前に

サーバ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_SYS_ACT               OFF        GREEN
LED_HLTH_STATUS           ON         GREEN

Server /chassis #  show led detail
LEDs:
    LED Name: LED_SYS_ACT
    LED State: OFF
    LED Color: GREEN
LEDs:
    LED Name: LED_HLTH_STATUS
    LED State: ON
    LED Color: GREEN
ucs-e160dp-m1 /chassis #
```

ストレージ センサーの表示

手順の概要

1. Server# **scope chassis**
2. Server /chassis # **show hdd** [**detail**]

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 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** [**detail**]	ストレージ センサー情報を表示します。

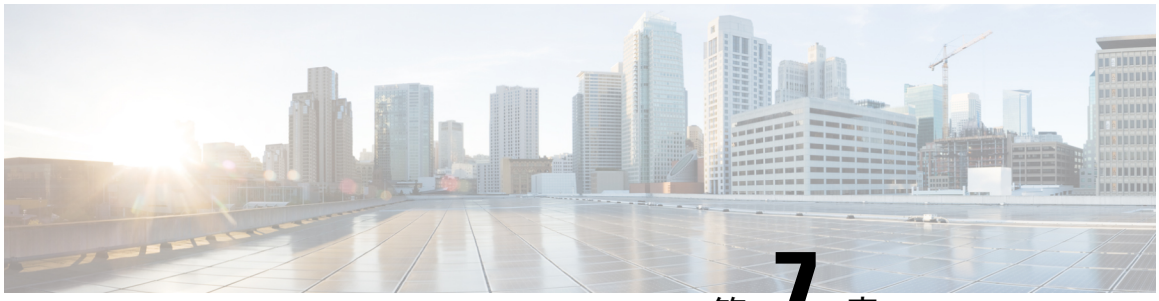
表示されるフィールドについては、次の表で説明します。

名前	説明
[Name] カラム	ストレージ デバイスの名前。ここに表示される値は次のとおりです。 [HDD*X*_PRS]：各ハード ドライブの有無を示します。
[Status] カラム	ストレージ デバイスのステータスの簡単な説明。
[LED Status] カラム	現在の LED の色（ある場合）。 ストレージデバイスの物理LEDを点滅させるには、ドロップダウン リストから [Turn On] を選択します。LED の点滅をストレージ デバイスに制御させるには、[Turn Off] を選択します。

例

次に、ストレージ センサーの情報を表示する例を示します。

```
Server# scope chassis
Server /chassis # show hdd
Name                 Status
-------------------- --------------------
HDD1_PRS             inserted
HDD2_PRS             inserted
HDD3_PRS             inserted

Server /chassis #
```



第 7 章

リモート プレゼンスの管理

この章は、次の項で構成されています。

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に接続できます。サーバに物理的に接続された CD/DVD ドライブまたはフロッピー 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 ドライブまたはフロッピー 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。

- コンピュータ上の CD/DVD またはフロッピー ドライブ
- 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。

（注） CIMC Configuration Utility は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

- Cisco UCS M1 および M2 サーバの場合は、ブートアップ中に **Ctrl+H** を押し、WebBIOS にアクセスして RAID を設定します。

  Cisco UCS M3 サーバの場合は、ブートアップ中に **Ctrl+R** を押し、MegaRAID コントローラにアクセスして RAID を設定します。

（注） RAID は EHWIC E シリーズ NCE および NIM E シリーズ NCE ではサポートされていません。これらの SKU では、**Ctrl+H** および **Ctrl+R** は機能しません。

KVM コンソールを起動するための Java 要件

KVM コンソールを起動するためには、システムにリリース 1.6 以降の Java をインストールしておく必要があります。

証明書が Java で取り消されたために KVM コンソールが起動しない場合は、Java の設定を変更する必要があります。次の手順を実行します。

1. Java コントロール パネルにアクセスします。
2. [Advanced] タブをクリックします。
3. [Perform certificate revocation on] で、[Do not check (not recommended)] ラジオ ボタンを選択します。詳細については、http://www.java.com/en/download/help/revocation_options.xmlを参照してください。

仮想 KVM の設定

始める前に

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

手順の概要

1. Server# **scope kvm**
2. Server /kvm # **set enabled** {**yes** | **no**}
3. Server /kvm # **set encrypted** {**yes** | **no**}
4. Server /kvm # **set kvm-port** *port*
5. Server /kvm # **set local-video** {**yes** | **no**}
6. Server /kvm # **set max-sessions** *sessions*
7. Server /kvm # **commit**
8. Server /kvm # **show** [**detail**]

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 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 encrypted** {**yes** | **no**}	暗号化をイネーブルにすると、サーバは KVM で送信されるすべてのビデオ情報を暗号化します。
ステップ 4	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 5	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に接続されているすべてのモニタにも表示されます。
ステップ 6	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* 引数は、1 ～ 4 の範囲の整数になります。
ステップ 7	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 8	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 encrypted no
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:
    Encryption Enabled: no
    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 権限を持つユーザとしてログインする必要があります。

手順の概要

1. Server# **scope kvm**
2. Server /kvm # **set enabled yes**
3. Server /kvm # **commit**
4. Server /kvm # **show** [**detail**]

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 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
Encryption Enabled Local Video      Active Sessions Enabled KVM Port
------------------ ---------------- --------------- ------- --------
no                 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 権限を持つユーザとしてログインする必要があります。

手順の概要

1. Server# **scope kvm**
2. Server /kvm # **set enabled no**
3. Server /kvm # **commit**
4. Server /kvm # **show** [**detail**]

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 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
Encryption Enabled Local Video      Active Sessions Enabled KVM Port
------------------ ---------------- --------------- ------- --------
no                 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 権限を持つユーザとしてログインする必要があります。

手順の概要

1. Server# **scope sol**
2. Server /sol # **set enabled** {**yes** | **no**}
3. Server /sol # **set baud-rate** {**9600** | **19200** | **38400** | **57600** | **115200**}
4. Server /sol # **commit**
5. Server /sol # **show** [**detail**]

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 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**}	このサーバで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。

	コマンドまたはアクション	目的
		（注） このボー レートは、サーバのシリアル 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)
------- ---------------
yes     115200

Server /sol #
```

Serial Over LAN の起動

手順の概要

1. Server# **connect host**

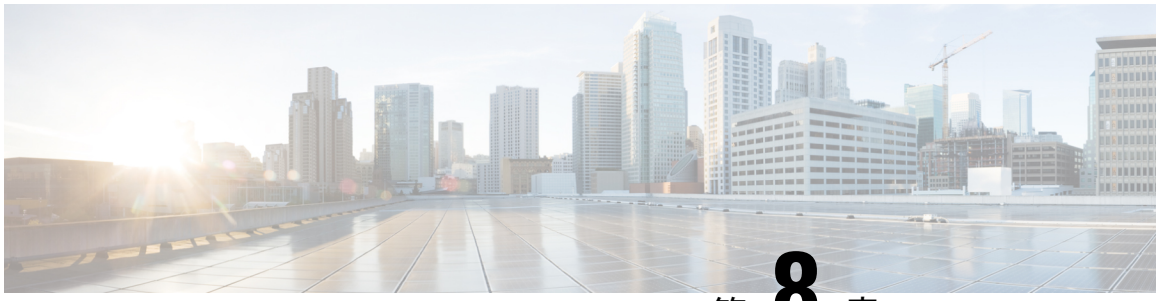
手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Server# **connect host**	リダイレクトされたサーバ 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 8 章

ユーザ アカウントの管理

この章は、次の項で構成されています。

ローカル ユーザの設定

始める前に

ローカル ユーザ 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*	ユーザ番号 *usernumber* に対するユーザ コマンド モードを開始します。
ステップ 2	Server /user # **set enabled** {**yes** |**no**\\	CIMC でユーザ 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*	ユーザのユーザ名を指定します。
ステップ 4	Server /user # **set password**	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**\\	ユーザに割り当てるロールを指定します。ロールには、次のものがあります。 • readonly：このユーザは情報を表示できますが、変更することはできません。 • user：このユーザは、次の操作を実行できます。

	コマンドまたはアクション	目的
		• 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 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
------ ---------------- -------- --------
5      john             readonly yes
```

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 データベース内に見つからないユーザ アカウントに関するユーザ認証とロール許可は、LDAP サーバによって実行されます。LDAP ユーザ認証の形式は 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 サーバへの送信データを暗号化するようサーバに要求できます。

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 ロールとロケールを保持する属性を使用してユーザを設定します。CIMC のユーザ 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 CiscoAVPair 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 CiscoAVPair という名前のカスタム属性を作成しますが、CIMC のユーザ 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**
Description	**CiscoAVPair**
Syntax	**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。

a) 左ペインで [Classes] ノードを展開し、**u** を入力してユーザ クラスを選択します。
b) [Attributes] タブをクリックして、[Add] をクリックします。
c) **c** を入力して CiscoAVPair 属性を選択します。
d) [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に対し、次のユーザ ロール値をCiscoAVPair属性に追加します。

ロール	CiscoAVPair 属性値
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 サーバを設定します。

CIMC での LDAP の設定

ローカル ユーザの認証と許可に LDAP サーバを使用するには、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 権限を持つユーザとしてログインする必要があります。

手順の概要

1. Server# **scope ldap**
2. Server /ldap # **set enabled** {**yes** |**no**\\
3. Server /ldap # **set domain***LDAP* ドメイン名
4. Server /ldap # **set timeout** *seconds*
5. Server /ldap # **set encrypted** {**yes** |**no**\\
6. Server /ldap # **set base-dn** *domain-name*
7. Server /ldap # **set attribute** 名
8. Server /ldap # **set filter-attribute**
9. Server /ldap # **commit**
10. Server /ldap # **show** [**detail**]

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 ldap**	LDAP コマンド モードを開始します。
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

	コマンドまたはアクション	目的
		合、ローカル ユーザ データベースにないユーザ アカウントに対し、ユーザ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* ドメイン名	LDAP ドメイン名を指定します。
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 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 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 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 encrypted yes
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
    Encrypted: yes
    Domain: sample-domain
    BaseDN: example.com
    Timeout: 60
    Filter-Attribute: sAMAccountName
    Attribute: CiscoAvPair
Server /ldap #
```

次のタスク

グループ許可用に 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 データベースにないユーザや、Active Directory で CIMC の使用を許可されていないユーザに対するグループ レベルでのユーザ認証も行われます。

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。

手順の概要

1. Server# **scope ldap**
2. Server /ldap# **scope ldap-group-rule**
3. Server /ldap/ldap-group-rule # **set group-auth** {**yes** |**no**}
4. Server /ldap # **scope role-group** *index*
5. Server /ldap/role-group # **set name** *group-name*
6. Server /ldap/role-group # **set domain** *domain-name*
7. Server /ldap/role-group # **set role** {**admin** | **user** | **readonly**}
8. Server /ldap/role-group # **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 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。

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 #
```

ユーザ セッションの表示

手順の概要

1. Server# **show user-session**

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# **show user-session**	現在のユーザ 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 セッションに関する次の情報が表示されます。

名前	説明
[Session ID] カラム	セッションの固有識別情報。
[Username] カラム	ユーザのユーザ名。
[IP Address] カラム	ユーザがサーバにアクセスした IP アドレス。
[Type] カラム	ユーザがサーバ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	ユーザアカウントに**admin**ユーザ 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 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 セッションの終了

始める前に

ユーザセッションを終了するには、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。

手順の概要

1. Server# **show user-session**
2. Server /user-session # **scope user-session** セッション番号
3. Server /user-session # **terminate**

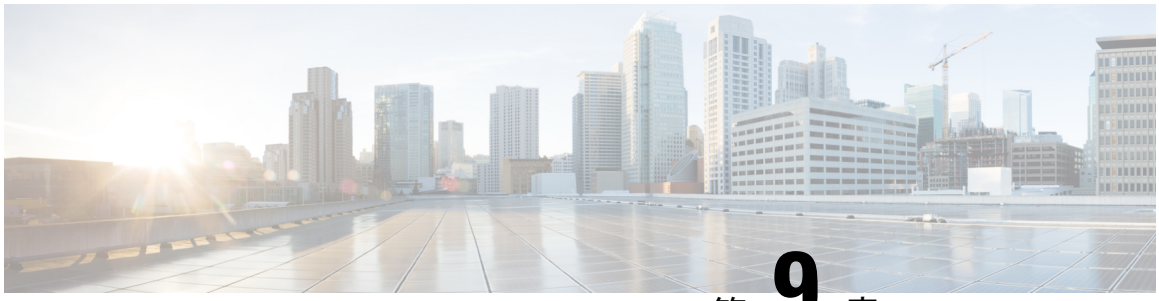
手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Server# **show user-session**	現在のユーザセッションの情報を表示します。終了するユーザセッションは、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** セッション番号	終了する番号付きのユーザセッションに対してユーザ 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 セッションを終了します。

例

次に、ユーザ セッション 10 の admin がユーザ 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 9 章

ネットワーク関連の設定

この章は、次の項で構成されています。

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。

（注） M3 モジュールの場合、GE2 と GE3 は TE2 と TE3 に置き換えられます。

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。

（注） 専用モードはEHWIC E シリーズ NCEには適用されません。

次の例は、リンク状態を示しています。

```
E160S /cimc/network # show link-state
Interface                      State
------------------------------ --------------------
Console                        Link Detected
GE1                            Link Detected
TE2                            Link Detected
TE3                            Link Detected
Dedicated                      No Link Detected

E1120D /cimc/network # show link-state
Interface                      State
------------------------------ --------------------
Console                        Link Detected
GE1                            Link Detected
TE2                            No Link Detected
TE3                            No Link Detected
```

次の例は、LOM MAC リストを示しています。

```
E160S /cimc/network # show lom-mac-list
Interface                      MAC Address
------------------------------ --------------------
Console                        00:f6:63:b9:65:d4
GE1                            00:f6:63:b9:65:d5
TE2                            00:f6:63:b9:65:d6
TE3                            00:f6:63:b9:65:d7

E1120D /cimc/network # show lom-mac-list
Interface                      MAC Address
------------------------------ --------------------
Console                        28:6f:7f:ee:ac:0a
GE1                            28:6f:7f:ee:ac:0b
TE2                            28:6f:7f:ee:ac:0c
TE3                            28:6f:7f:ee:ac:0d
```

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 権限を持つユーザとしてログインする必要があります。

手順の概要

1. Server# **scope cimc**
2. Server /cimc # **scope network**
3. Server /cimc/network # **set mode** {**dedicated** |**shared_lom**}
4. Server /cimc/network # **set interface** {**console** |**ge1**}
5. Server /cimc/network # **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 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。 （注） 専用モードはEHWIC E シリーズ NCE には適用されません。 • **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** |**ge1**}	NIC インターフェイスを次のいずれかに設定します。 • **console**：ルータの PCIe インタ フェースを E シリーズ サーバ に接続するか、またはルータの EHWIC インターフェイスを NCE に接続するために使用される内部インターフェイス。 • **ge1**：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。 • **ge3**：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。 （注） GE3 インターフェイスに関連するすべてのインターフェイス オプションは、ダブル幅の E シリーズ サーバにのみ適用できます。

	コマンドまたはアクション	目的
		（注） M3 サーバの場合、インターフェイス GE は TE によって置き換えられます。 （注） EHWIC E シリーズ NCE または NIM E シリーズ NCE 上で外部 GE2 インターフェイスを使用して CIMC アクセスを設定している場合、サーバのリブート中に CIMC との接続が失われることがあります。これは想定されている動作です。リブート中に CIMC との接続を維持する必要がある場合は、他のネットワーク インターフェイスを使用して CIMC アクセスを設定することをお勧めします。『*Cisco UCS E* シリーズ サーバおよび *Cisco UCS E* シリーズ ネットワーク コンピュート エンジン スタートアップ ガイド』の「CIMC Access Configuration Options—EHWIC E-Series NCE」および「CIMC Access Configuration Options—NIM E-Series NCE」の項を参照してください。
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
Server /cimc/network *# commit
Server /cimc/network #
```

共通プロパティの設定

サーバを説明するには、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権限を持つユーザとしてログインする必要があります。

手順の概要

1. Server# **scope cimc**
2. Server /cimc # **scope network**
3. Server /cimc/network # **set hostname** *host-name*
4. Server /cimc/network # **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 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
Server /cimc/network *# commit
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 権限を持つユーザとしてログインする必要があります。

手順の概要

1. Server# **scope cimc**
2. Server /cimc # **scope network**
3. Server /cimc/network # **set dhcp-enabled** {**yes** |**no**}
4. Server /cimc/network # **set v4-addr** *ipv4-address*
5. Server /cimc/network # **set v4-netmask** *ipv4-netmask*
6. Server /cimc/network # **set v4-gateway** *gateway-ipv4-address*
7. Server /cimc/network # **set dns-use-dhcp** {**yes** |**no**}
8. Server /cimc/network # **set preferred-dns-server** *dns1-ipv4-address*
9. Server /cimc/network # **set alternate-dns-server** *dns2-ipv4-address*
10. Server /cimc/network # **commit**
11. Server /cimc/network # **show** [**detail**]

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 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 サーバを設定することを推奨します。サーバ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 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。

	コマンドまたはアクション	目的
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 dhcp-enabled no
Server /cimc/network *# set v4-addr 10.20.30.11
Server /cimc/network *# set v4-netmask 255.255.248.0
Server /cimc/network *# set v4-gateway 10.20.30.1
Server /cimc/network *# set dns-use-dhcp-enabled no
Server /cimc/network *# set preferred-dns-server 192.168.30.31
Server /cimc/network *# set alternate-dns-server 192.168.30.32
Server /cimc/network *# commit
Server /cimc/network # show detail
Network Setting:
    IPv4 Address: 10.20.30.11
    IPv4 Netmask: 255.255.248.0
    IPv4 Gateway: 10.20.30.1
    DHCP Enabled: no
    Obtain DNS Server by DHCP: no
    Preferred DNS: 192.168.30.31
    Alternate DNS: 192.168.30.32
    VLAN Enabled: no
    VLAN ID: 1
    VLAN Priority: 0
    Hostname: Server
    MAC Address: 01:23:45:67:89:AB
    NIC Mode: dedicated
    NIC Redundancy: none

Server /cimc/network #
```

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 権限を持つユーザとしてログインする必要があります。

手順の概要

1. Server# **scope cimc**
2. Server /cimc # **scope network**
3. Server /cimc/network # **set v6-dhcp no**
4. Server /cimc/network # **set v6-enabled yes**
5. Server /cimc/network # **set v6-addr** *ipv6-address*
6. Server /cimc/network # **set v6-gateway** *gateway-ipv6address*

7. Server /cimc/network # **commit**
8. Server /cimc/network # **show** [**detail**]

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 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-no
Server /cimc/network # set v6-enabled yes
Server /cimc/network *# set v6-addr 2001:db8:101:f101:f2f7::14
Server /cimc/network *# set v6-gateway 2001:db8:101:f101:f2f7::1
Server /cimc/network *# commit
Server /cimc/network # show detail
Network Setting:
    Network Setting:
    IPv4 Address: 10.197.82.23
    IPv4 Netmask: 255.255.255.192
    IPv4 Gateway: 10.197.82.1
    DHCP Enabled: no
    DDNS Enabled: yes
    DDNS Update Domain:
    Obtain DNS Server by DHCP: no
    Preferred DNS: 0.0.0.0
    Alternate DNS: 0.0.0.0
    VLAN Enabled: no
    VLAN ID: 1
    VLAN Priority: 0
    Hostname: E160S
    MAC Address: 00:F6:63:B9:65:DB
    NIC Mode: shared_lom
    NIC Redundancy: none
```

```
    NIC Interface: te3
    IPv6 Enabled: yes
    IPv6 Address: 2600:0:c:87ee::12
    IPv6 Prefix: 64
    IPv6 Gateway: 2600:0:c:87ee::1
    IPv6 Link Local: fe80::2f6:63ff:feb9:65db
    IPv6 SLAAC Address: 2600:0:c:bfe7:2f6:63ff:feb9:65db
    IPV6 DHCP Enabled: no
    IPV6 Obtain DNS Server by DHCP: no
    IPV6 Preferred DNS: ::
    IPV6 Alternate DNS: ::
E160S /cimc/network #
```

サーバ VLAN の設定

始める前に

サーバ 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。

手順の概要

1. Server# **scope cimc**
2. Server /cimc # **scope network**
3. Server /cimc/network # **set vlan-enabled** {**yes** |**no**}
4. Server /cimc/network # **set vlan-id** *id*
5. Server /cimc/network # **set vlan-priority** *priority*
6. Server /cimc/network # **commit**
7. Server /cimc/network # **show** [**detail**]

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 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 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 Address: 10.20.30.11
    IPv4 Netmask: 255.255.248.0
    IPv4 Gateway: 10.20.30.1
    DHCP Enabled: yes
    Obtain DNS Server by DHCP: no
    Preferred DNS: 192.168.30.31
    Alternate DNS: 192.168.30.32
    VLAN Enabled: yes
    VLAN ID: 10
    VLAN Priority: 32
    Hostname: Server
    MAC Address: 01:23:45:67:89:AB
    NIC Mode: dedicated
    NIC Redundancy: none

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、またはその他のインターネット サーバ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 権限を持つユーザとしてログインする必要があります。

手順の概要

1. Server# **scope cimc**
2. Server /cimc # **scope network**
3. Server /cimc/network # **scope ipblocking**
4. Server /cimc/network/ipblocking # **set enabled** {**yes** | **no**}
5. Server /cimc/network/ipblocking # **set fail-count** *fail-count*
6. Server /cimc/network/ipblocking # **set fail-window** *fail-seconds*
7. Server /cimc/network/ipblocking # **set penalty-time** *penalty-seconds*
8. Server /cimc/network/ipblocking # **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 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。
ステップ 5	Server /cimc/network/ipblocking # **set fail-count** *fail-count*	指定された時間ユーザがロックアウトされる前に、ユーザ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 #
```

ネットワーク解析モジュール機能の設定

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。

手順の概要

1. Server# **scope cimc**
2. Server /cimc # **scope network**
3. Server /cimc/network # **scope nam**
4. Server /cimc/network/nam # **set enabled yes**
5. Server /cimc/network/nam # **show detail**

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 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 nam**	ネットワーク解析モジュール（NAM）コマンドモードを開始します。
ステップ 4	Server /cimc/network/nam # **set enabled yes**	NAM 機能をイネーブルにします。 NAM 機能をディセーブルにするには、**set enabled no** コマンドを使用します。
ステップ 5	Server /cimc/network/nam # **show detail**	NAM 機能がイネーブルかディセーブルかを確認します。

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 # scope nam
Server /cimc/network/nam # set enabled yes
Server /cimc/network/nam # show detail
Network Analysis Module:
    Enabled: yes
```

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 サーバと時刻を同期できます。デフォルトでは、NTP サーバは CIMC で動作しません。NTP サーバまたは時刻源サーバとして機能するサーバ（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 サービスをイネーブルにするには、DNS アドレスよりも、サーバの IP アドレスを指定することを推奨します。

NTP 設定の構成

始める前に

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

手順の概要

1. Server# **scope cimc**
2. Server /cimc # **scope network**
3. Server /cimc/network # **scope ntp**
4. Server /cimc/network/ntp # **set enabled yes**
5. Server /cimc/network/ntp # **set** [**server-1** | **server-2** | **server-3** | **server-4**] *ip-address or domain-name*
6. Server /cimc/network/ntp # **show detail**

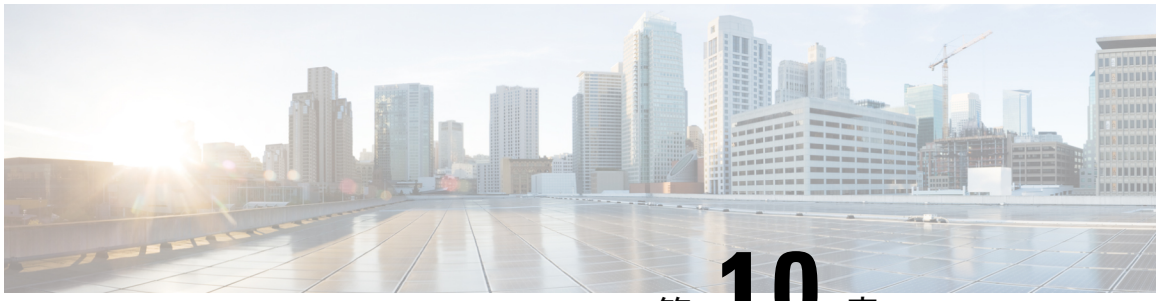
手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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。
ステップ 4	Server /cimc/network/ntp # **set enabled yes**	NTP サービスをイネーブルにします。 NTP サービスをディセーブルにするには、**set enabled no** コマンドを使用します。
ステップ 5	Server /cimc/network/ntp # **set** [**server-1** | **server-2** | **server-3** | **server-4**] *ip-address or domain-name*	NTP サーバまたはタイムソース サーバとして動作する特定のサーバの IP アドレスまたはドメイン名を設定します。 最大 4 つのサーバを設定できます。
ステップ 6	Server /cimc/network/ntp # **show detail**	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
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 # show detail
NTP Service Settings:
    Enabled: yes
    Server 1: 10.50.171.9
    Server 2: time.cisco.com
    Server 3:
    Server 4:
```



第 10 章

コミュニケーション サービスの設定

この章は、次の項で構成されています。

HTTP の設定

始める前に

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

手順の概要

1. Server# **scope http**
2. Server /http # **set enabled** {**yes** | **no**}
3. Server /http # **set http-port** *number*
4. Server /http # **set https-port** *number*
5. Server /http # **set timeout** *seconds*
6. Server /http # **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 http**	HTTP コマンド モードを開始します。
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。

	コマンドまたはアクション	目的
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。 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# scope http
Server /http # set enabled yes
Server /http *# set http-port 80
Server /http *# set https-port 443
Server /http *# set timeout 1800
Server /http *# commit
Server /http # show
HTTP Port  HTTPS Port Timeout  Active Sessions Enabled
---------- ---------- -------- --------------- -------
80         443        1800     0               yes

Server /http #
```

SSH の設定

始める前に

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

手順の概要

1. Server# **scope ssh**
2. Server /ssh # **set enabled** {**yes** | **no**}
3. Server /ssh # **set ssh-port** *number*
4. Server /ssh # **set timeout** *seconds*
5. Server /ssh # **commit**
6. Server /ssh # **show** [**detail**]

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 ssh**	SSH コマンド モードを開始します。
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。 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
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 シリーズ サーバ 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 に関する詳細については、『*CIMC XML API Programmer's Guide for Cisco UCS E-Series Servers*』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 権限を持つユーザとしてログインする必要があります。

手順の概要

1. Server# **scope xmlapi**
2. Server /xmlapi # **set enabled** {**yes** | **no**}
3. Server /xmlapi *# **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 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して、問題を事前に検出できます。サーバ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。
ステップ 3	Server /ipmi # **set privilege-level** {**readonly** | **user** | **admin**}	このサーバで 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 ロールを持つ IPMI ユーザが作成できるのは、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 ロールを持つ IPMI ユーザがこのサーバで作成できるのは、ユーザ 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 ロールを持つ IPMI ユーザは、管理者、ユーザ、および読み取り専用セッションをこのサーバで作成できます。
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。

	コマンドまたはアクション	目的
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-Series Servers は、サーバの設定およびステータスを表示したり、SNMP トラップによって障害とアラートを送信したりするために、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、次の URL にある『*MIB Quick Reference for Cisco UCS*』を参照してください。http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/reference/UCS_MIBRef.html

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。

	コマンドまたはアクション	目的
		（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**	[Disabled]、[Limited]、または [Full] のいずれかになります。
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）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:
    SNMP Port: 161
    System Contact: User Name <username@example.com> +1-408-555-1212
    System Location: San Jose, California
    SNMP Community: cimcpublic
    SNMP Trap community: public
    SNMP Community access: Full
    Enabled: yes

Server /snmp #
```

次のタスク

「SNMP トラップ設定の指定 （131 ページ）」の説明に従って 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。

	コマンドまたはアクション	目的
		（注） 通知オプションは V2 ユーザ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 v4-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: user1
    IPv4 Address: 192.2.3.4
    Delete Trap: no
Server /snmp/trap-destination #
```

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。

	コマンドまたはアクション	目的
		（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。
- 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。

手順の概要

1. Server# **scope snmp**
2. Server /snmp # **scope v3users** *number*
3. サーバ/snmp/v3users # **set v3add** {**yes** |**no**}
4. Server /snmp/v3users # **set v3security-name** *security-name*
5. Server /snmp/v3users # **set v3security-level** {**noauthnopriv** |**authnopriv** |**authpriv**}
6. Server /snmp/v3users # **set v3proto** {**MD5** |**SHA**}
7. Server /snmp/v3users # **set v3auth-key** *auth-key*
8. Server /snmp/v3users # **set v3priv-proto** {**DES** |**AES**}
9. Server /snmp/v3users # **set v3priv-auth-key** *priv-auth-key*
10. Server /snmp/v3users # **commit**

手順の詳細

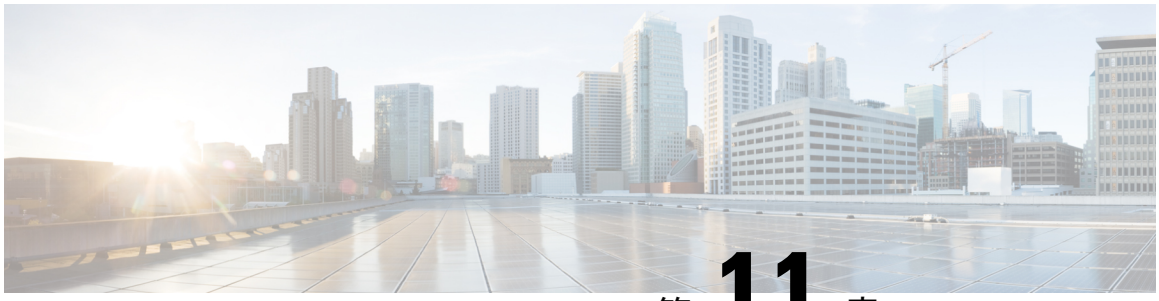
	コマンドまたはアクション	目的
ステップ 1	Server# **scope snmp**	SNMP コマンド モードを開始します。
ステップ 2	Server /snmp # **scope v3users** *number*	指定したユーザ番号の SNMPv3 ユーザのコマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	サーバ/snmp/v3users # **set v3add** {**yes** |**no**}	SNMPv3 ユーザを追加または削除します。次のいずれかになります。 • **yes**：このユーザは SNMPv3 ユーザ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、ユーザの追加に失敗します。 • **no**：このユーザ設定は削除されます。
ステップ 4	Server /snmp/v3users # **set v3security-name** *security-name*	このユーザの SNMP ユーザ名を入力します。
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。
ステップ 6	Server /snmp/v3users # **set v3proto** {**MD5** |**SHA**}	このユーザ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 11 章

証明書の管理

この章は、次の項で構成されています。

サーバ証明書の管理

証明書署名要求（CSR）を生成して新しい証明書を取得し、新しい証明書を CIMC にアップロードして現在のサーバ証明書と交換することができます。サーバ証明書は、Verisign のようなパブリック認証局（CA）、または独自に使用している認証局のいずれかによって署名されます。

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 権限を持つユーザとしてログインする必要があります。

手順の概要

1. Server# **scope certificate**
2. Server /certificate # **generate-csr**

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 certificate**	証明書コマンド モードを開始します。
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# scope certificate
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
Continue to generate CSR?[y|N]y


-----BEGIN CERTIFICATE REQUEST-----
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 REQUEST-----

Copy everything from "-----BEGIN ..."  to "END CERTIFICATE REQUEST-----",
paste to a file, send to your chosen CA for signing,
and finally upload the signed certificate via upload command.
              ---OR---
Continue to self sign CSR and overwrite the current certificate?
All HTTPS and SSH sessions will be disconnected. [y|N]N
```

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 CLI ではなく、OpenSSL パッケージを使用している Linux サーバで入力します。

始める前に

組織内のサーバで、証明書サーバのソフトウェア 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_keyfilename keysize* 例： `# openssl genrsa -out ca.key 1024`	このコマンドは、CA で使用される 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 -req -days** *numdays* **-in** *CSR_filename* **-CA** *CA_certfilename* **-set_serial 04 -CAkey** *CA_keyfilename* **-out** *server_certfilename* **-extfile openssl.conf** 例： `# openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 04 -CAkey ca.key -out myserver05.crt -extfile openssl.conf`	このコマンドは、CA が CSR ファイルを使用してサーバ証明書を生成するように指示します。 サーバ証明書は、出力ファイルに含まれています。

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 サーバで入力します。

```
# /usr/bin/openssl genrsa -out ca.key 1024 Generating RSA private key, 1024
bit long modulus ..............++++++ .....++++++ e is 65537 (0x10001) #
/usr/bin/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) [GB]:US State or Province Name (full
 name) [Berkshire]:California Locality Name (eg, city) [Newbury]:San Jose
Organization Name (eg, company) [My Company Ltd]:Example Incorporated
Organizational Unit Name (eg, section) []:Unit A Common Name (eg, your name or
 your server's hostname) []:example.com Email Address []:admin@example.com #
echo "nsCertType = server" > openssl.conf # /usr/bin/openssl x509 -req -days
365 -in csr.txt -CA ca.crt -set_serial 01 -CAkey ca.key -out server.crt -extfile
 openssl.conf Signature ok subject=/C=US/ST=California/L=San Jose/O=Example
Inc./OU=Unit A/CN=example.com/emailAddress=john@example.com Getting CA Private
 Key #
```

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。

手順の概要

1. Server# **scope certificate**
2. Server /certificate # **upload**

手順の詳細

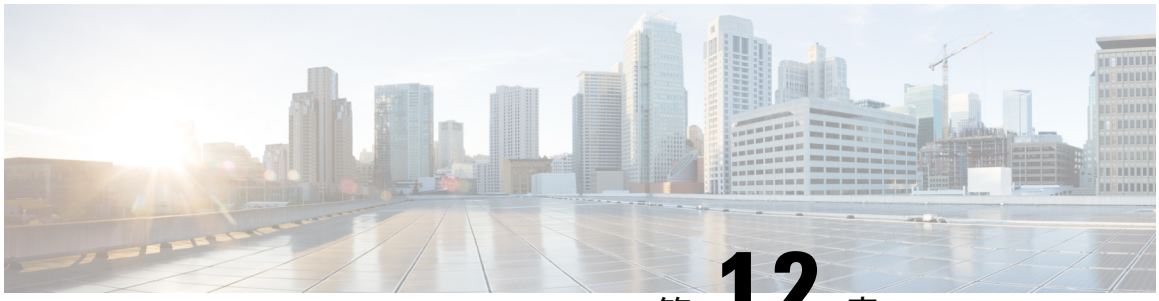
	コマンドまたはアクション	目的
ステップ 1	Server# **scope certificate**	証明書コマンド モードを開始します。
ステップ 2	Server /certificate # **upload**	新しいサーバ証明書を入力してアップロードするためのダイアログが起動します。

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 12 章

プラットフォーム イベント フィルタの設定

この章は、次の項で構成されています。

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

手順の概要

1. Server# **scope fault**
2. Server /fault # **set platform-event-enabled yes**
3. Server /fault # **commit**
4. Server /fault # **show** [**detail**]

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 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**	プラットフォーム イベント アラートをイネーブルにします。
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

手順の概要

1. Server# **scope fault**
2. Server /fault # **set platform-event-enabled no**
3. Server /fault # **commit**
4. Server /fault # **show** [**detail**]

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 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 no**	プラットフォーム イベント アラートをディセーブルにします。
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。

プラットフォーム イベント フィルタの設定

	コマンドまたはアクション	目的
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

手順の概要

1. Server# **scope fault**
2. Server /fault # **scope pef** *id*
3. Server /fault/pef # **set action** {**none** | **reboot** | **power-cycle** | **power-off**}
4. Server /fault/pef # **set send-alert** {**yes** | **no**}
5. Server /fault/pef # **commit**

プラットフォーム イベント フィルタの設定

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 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。 • **none**：システム アクションは実行されません。 • **reboot** ：サーバがリブートされます。 • **power-cycle** ：サーバに電源が再投入されます。 • **power-off** ：サーバの電源がオフになります。
ステップ 4	Server /fault/pef # **set send-alert** {**yes** | **no**}	このイベントに対するプラットフォーム イベント アラートの送信をイネーブルまたはディセーブルにします。 （注） 送信するアラートについて、フィルタ トラップを正しく設定し、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必要があります。 （注） **set send-alert** コマンドは、リリース 3.1.1 以降で廃止されました。このコマンドの代わりに、SNMP を使用してアラートをトリガーできます。
ステップ 5	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 # set send-alert yes
Server /fault/pef *# commit
Server /fault/pef # show
```

```
Platform Event Filter Event                                Action      Send Alert

-------------------- ------------------------------------ ----------- -----------
1                    Temperature Critical Assert Filter  reboot      yes

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

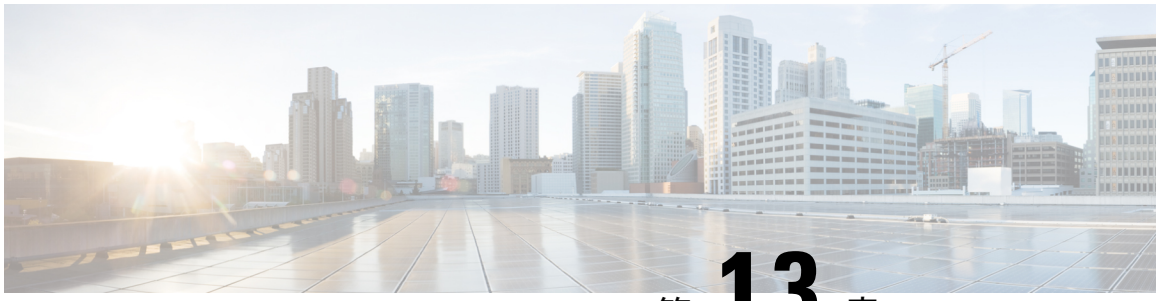
次の表に、プラットフォーム イベント トラップ メッセージで通知されるイベントの説明を示します。これらは、トラップ OID のイベント番号に基づいています。

イベント番号 [注記 1]		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

イベント番号 [注記 1]		プラットフォーム イベントの説明
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
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 [注記 4]
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 [注記 2、3] （注） E シリーズ サーバおよびSM E シリーズ NCE に表示されます。EHWIC E シリーズ NCE および NIM E シリーズ NCE には表示されません。
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 [注記 3] （注） E シリーズ サーバおよびSM E シリーズ NCE に表示されます。EHWIC E シリーズ NCE および NIM E シリーズ NCE には表示されません。
851968	0D0000h	HDD センサーで障害が示されない、汎用センサー [注記 2]
851972	0D0004h	HDD センサーで障害が示される、汎用センサー [注記 2]
854016	0D0800h	HDD が存在しない、汎用センサー [注記 2]
854017	0D0801h	HDD が存在する、汎用センサー [注記 2]

イベント番号 [注記 1]		プラットフォーム イベントの説明
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
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 13 章

ファームウェア管理

この章は、次の項で構成されています。

ファームウェアの概要

Eシリーズサーバは、使用しているEシリーズサーバモデルに特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。このユーティリティの詳細については、*Cisco UCS E シリーズ サーバおよび Cisco UCS E シリーズ ネットワーク コンピュート エンジン スタートアップ ガイド*の「Upgrading Firmware」の章を参照してください。この章には、互換性のある HUU、CIMC、および BIOS ソフトウェア リリースに関する情報も含まれています。

（注） HUU は、CIMC のリリース 2.1.0 以降のリリースでサポートされます。

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

ファームウェア コンポーネントは、Cisco Host Upgrade Utility（HUU）を使用してアップグレードすることも手動でアップグレードすることもできます。

- **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 および BIOS 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。
- **手動によるアップグレード**：BIOS および CIMC のファームウェアを手動でアップグレードするには、シスコからファームウェアを取得し、CIMC GUI または CIMC CLI を使ってアップグレードする必要があります。 ファームウェアのアップグレード後、システムを再起動します。

シスコからのソフトウェアの取得

ドライバ、BIOS と CIMC のファームウェア、および診断イメージをダウンロードするには、次の手順を実行します。

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 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 Drivers]：ドライバが含まれます。
- [Unified Computing System (UCSE) Server Firmware]：Host Upgrade Utility と BIOS、CIMC、および PLD ファームウェア イメージが含まれます。
- [Unified Computing System (UCSE) Utilites]：次の診断イメージが含まれています。

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 サーバからインストールする場合は、使用する TFTP サーバにファイルをコピーします。

サーバは、TFTP サーバ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。

リモートサーバからのCIMCファームウェアのインストール

（注） 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。このユーティリティの詳細については、*Cisco UCS E* シリーズ サーバおよび *Cisco UCS E* シリーズ ネットワーク コンピュート エンジン スタートアップ ガイドの「Upgrading Firmware」の章を参照してください。この章には、互換性のあるHUU、CIMC、および BIOS ソフトウェア リリースに関する情報も含まれています。

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。シスコからのソフトウェアの取得 （152 ページ）を参照してください。

（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。

手順の概要

1. Server# **scope cimc**
2. Server /cimc # **scope firmware**
3. Server /cimc/firmware # **update** *protocol ip-address path*
4. （任意）Server /cimc # **show detail**

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 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。

	コマンドまたはアクション	目的
ステップ 3	Server /cimc/firmware # **update** *protocol ip-address path*	プロトコル、リモート サーバの IP アドレス、サーバ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	（任意）Server /cimc # **show detail**	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。

手順の概要

1. Server# **scope cimc**
2. Server /cimc # **show** [**detail**]
3. Server /cimc # **activate** [**1** | **2**]

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 cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **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 3	Server /cimc # **activate** [**1** | **2**]	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

次に、ファームウェア イメージ 1 をアクティブにする例を示します。

```
Server# scope cimc
Server /cimc # show detail
Firmware Image Information:
    Update Stage: NONE
    Update Progress: 100
    Current FW Version: 1.0(0.74)
    FW Image 1 Version: 1.0(0.66a)
    FW Image 1 State: BACKUP INACTIVATED
    FW Image 2 Version: 1.0(0.74)
    FW Image 2 State: RUNNING ACTIVATED

Server /cimc # activate 1
```

TFTP サーバからの BIOS ファームウェアのインストール

（注） 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。このユーティリティの詳細については、*Cisco UCS E* シリーズ サーバおよび *Cisco UCS E* シリーズ ネットワーク コンピュート エンジン スタートアップ ガイドの「Upgrading Firmware」の章を参照してください。この章には、互換性のある HUU、CIMC、および BIOS ソフトウェア リリースに関する情報も含まれています。

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、サーバがブートしなくなります。

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。シスコからのソフトウェアの取得（152 ページ）を参照してください。

（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、サーバの電源をオフにします。

手順の概要

1. Server# **scope bios**
2. Server /bios # **update** *tftp-ip-address path-and-filename*
3. （任意）Server /bios # **show detail**

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 bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **update** *tftp-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。サーバは、指定の IP アドレスにある TFTP サーバから、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。

	コマンドまたはアクション	目的
ステップ 3	（任意）Server /bios # **show detail**	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、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 #
```

E シリーズ EHWIC NCE での Programmable Logic Device ファームウェアのアップグレード

EHWIC E シリーズ NCE で Programmable Logic Device（PLD）ファームウェア イメージをアップグレードするには、この手順を使用します。

始める前に

シスコから PLD ファームウェア イメージを取得します。シスコからのソフトウェアの取得（152 ページ）を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	Router # **copy tftp flash**	指定された TFTP サーバから PLD イメージ ファイルを取得し、ルータ フラッシュにコピーします。
ステップ 2	Router # **ucse subslot** *slot/port-adapter* **fpga-upgrade flash:***filename*	PLD ファームウェアをアップグレードします。アップグレードを続行するには、確認のプロンプトで **Enter** キーを押します。
ステップ 3	ルータの電源を一度オフにして、すぐにオンにします。	PLD ファームウェアは、ルータの電源を入れ直した後で有効になります。
ステップ 4	（任意）EN120E-FOC181290L1 /cimc/firmware # **show detail**	EHWIC E シリーズ NCE から、CIMC ファームウェア コマンド モードで CPLD バージョン番号を確認して、PLD ファームウェアがアップグレードされていることを確認します。

例

この例は、PLD ファームウェア イメージを更新します。

```
Router# copy tftp flash
Address or name of remote host []? 10.20.34.56
Source filename []? test/pld/alpha_v3p0e_c.rbf
Destination filename [alpha_v3p0e_c.rbf]?
Accessing tftp://10.20.34.56/test/pld/alpha_v3p0e_c.rbf...
Loading test/pld/alpha_v3p0e_c.rbf from 10.20.34.56 (via GigabitEthernet0/0): !!
[OK - 442475 bytes]

442475 bytes copied in 1.824 secs (242585 bytes/sec)


Router# ucse subslot 1/0 fpga-upgrade flash:alpha_v3p0e_c.rbf
Start fpga upgrade? [confirm]
FPGA Upgrade process started...
Step 1: Reading file flash:alpha_v3p0e_c.rbf from flash.!!.. done reading 442475 bytes
Step 2: Erasing the module flash.eeeeeeeeeeeeeee... Done
Step 3: Downloading contents to module
flash.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!...
 Done
Step 4: Validating the flash
data.vvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvvv...
 Done
Total time: 906 seconds
Fpga Upgraded successfully...!

EN120E-FOC181290L1 /cimc/firmware # show detail
  Firmware Image Information:
    Update Stage: NONE
    Update Progress: 0%
    Current FW Version: 2.3(1.20140808133703)
    FW Image 1 Version: 2.3(1.20140808133703)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 2.3(2.20140916114316)
    FW Image 2 State: BACKUP INACTIVATED
    Boot-loader Version: 2.3(1.20140808133703).33
    CPLD Version: 3.14
    Hardware Version: 2
```

E シリーズ サーバまたは NCE のアクセス問題のトラブルシューティング

E シリーズ サーバまたはNCE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、SD カードに問題がある、ファイル システムが破損している、または 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ことが原因として考えられます。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 （160 ページ）を参照してください。

- SD カードに問題がある場合は、「障害がある SD カードからの復旧 （163 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 （167 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。サーバのタイプに応じて、次のいずれかを実行します。
  - ダブル幅 E シリーズ サーバ：シリアル ケーブルの一端を E シリーズ サーバのシリアル ポートに接続し、もう一端を PC に接続します。
  - シングル幅 E シリーズ サーバおよび SM E シリーズ NCE：KVM コネクタを E シリーズ サーバまたは SM E シリーズ NCEの KVM ポートに接続してから、シリアル ケーブルの一端を KVM コネクタの DB9 ポートに接続し、もう一端を PC に接続します。
  - EHWIC E シリーズ NCE：ケーブルの mini USB の終端を EHWIC E シリーズ NCEの mini USB ポートへ接続し、USB ケーブルの他端を PC の USB ポートに接続します。

（注）　mini USB ケーブルは EHWIC E シリーズ NCEには付随しません。自分の mini USB ケーブルを購入する必要があります。

- 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 サーバ の管理（専用）ポートに接続します。

（注）　専用モードはEHWIC E シリーズ NCEには適用されません。

  - 共有 Lom GE2：イーサネット ケーブルを E シリーズ サーバ または NCE の外部 GE2 インターフェイスに接続します。
  - 共有 Lom コンソール：Cisco IOS CLI を使用して E シリーズ サーバまたは NCE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、必要に応じて HyperTerminal または Minicom を開始します。次のいずれかを実行します。
  - Microsoft Windows：Hyper Terminal を起動します。
  - Linux：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 sm** *slot* **oir-stop**	指定したEシリーズサーバの電源をシャットダウンします。 （注） Cisco 2900 シリーズ ISR G2 では E シリーズ サーバの OIR はサポートされません。ルータの損傷を防ぐために、E シリーズ サーバの Cisco 2900 ISR G2 への挿入または取り外しを行う前にルータの電源をオフにして、ネットワーク ケーブルを外します。 （注） ISR G2 は EHWIC E シリーズ NCE の OIR をサポートしていません。ルータの損傷を防ぐために、ルータに対して EHWIC E シリーズ NCE を挿入または取り外しする前にルータの電源をオフにして、ネットワーク ケーブルを外します。
ステップ 2	Router# **hw-module sm** *slot* **oir-start**	指定した E シリーズ サーバを再起動します。 （注） Cisco 2900 シリーズ ISR G2 では E シリーズ サーバの OIR はサポートされません。ルータの損傷を防ぐために、E シリーズ サーバの Cisco 2900 ISR G2 への挿入または取り外しを行う前にルータの電源をオフにして、ネットワーク ケーブルを外します。 （注） ISR G2 は EHWIC E シリーズ NCE の OIR をサポートしていません。ルータの損傷を防ぐために、ルータに対して EHWIC E シリーズ NCE を挿入または取り外しする前にルータの電源をオフにして、ネットワーク ケーブルを外します。

	コマンドまたはアクション	目的
ステップ 3	***	Hyper Terminal または Minicom から、*** コマンドを入力してブートローダプロンプトを開始します。
ステップ 4	ucse-cimc > **boot current recovery**	現在のイメージからEシリーズサーバをブートします。
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。 （注） 専用モードはEHWIC E シリーズ NCEには適用されません。 GE3 はEHWIC E シリーズNCE およびNIM E シリーズ NCE には適用されません。
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

この例は、E シリーズ サーバの 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
```

この例は、EHWIC E シリーズ NCEの CIMC ファームウェア イメージを回復します。

```
***

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
```

障害がある SD カードからの復旧

E シリーズ サーバまたは NCE のブートに問題がある場合、SD カードに障害が発生している可能性があります。新しい SD カードに CIMC ファームウェア イメージを復旧するには、次の手順を実行します。

⚠

注意 UCS E シリーズ サーバ間で SD カードを交換しないでください。

始める前に

- サーバを PC に接続します。サーバのタイプに応じて、次のいずれかを実行します。
  - ダブル幅 E シリーズ サーバ：シリアル ケーブルの一端を E シリーズ サーバのシリアル ポートに接続し、もう一端を PC に接続します。
  - シングル幅 E シリーズ サーバおよび SM E シリーズ NCE：KVM コネクタを E シリーズ サーバまたは SM E シリーズ NCEの KVM ポートに接続してから、シリアル ケーブルの一端を KVM コネクタの DB9 ポートに接続し、もう一端を PC に接続します。
  - EHWIC E シリーズ NCE：ケーブルの mini USB の終端を EHWIC E シリーズ NCEの mini USB ポートへ接続し、USB ケーブルの他端を PC の USB ポートに接続します。

（注） mini USB ケーブルは EHWIC E シリーズ NCEには付随しません。自分の mini USB ケーブルを購入する必要があります。

- 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 サーバ の管理（専用）ポートに接続します。

（注） 専用モードはEHWIC E シリーズ NCEには適用されません。

  - 共有 Lom GE2：イーサネット ケーブルを E シリーズ サーバ または NCE の外部 GE2 インターフェイスに接続します。
  - 共有 Lom コンソール：Cisco IOS CLI を使用して E シリーズ サーバまたは NCE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、必要に応じて HyperTerminal または Minicom を開始します。次のいずれかを実行します。
  - Microsoft Windows：Hyper Terminal を起動します。
  - Linux：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 sm** *slot* **oir-stop**	指定したEシリーズサーバの電源をシャットダウンします。 （注） Cisco 2900 シリーズ ISR G2 では E シリーズ サーバの OIR はサポートされません。ルータの損傷を防ぐために、E シリーズ サーバの Cisco 2900 ISR G2 への挿入または取り外しを行う前にルータの電源をオフにして、ネットワーク ケーブルを外します。

	コマンドまたはアクション	目的
		（注） ISR G2 は EHWIC E シリーズ NCE の OIR をサポートしていません。ルータの損傷を防ぐために、ルータに対して EHWIC E シリーズ NCE を挿入または取り外しする前にルータの電源をオフにして、ネットワーク ケーブルを外します。
ステップ 2	障害のある SD カードを取り外し、新しい SD カードを挿入します。	障害のある SD カードを交換します。
ステップ 3	Router# **hw-module sm** *slot* **oir-start**	指定した E シリーズ サーバを再起動します。 （注） Cisco 2900 シリーズ ISR G2 では E シリーズ サーバの OIR はサポートされません。ルータの損傷を防ぐために、E シリーズ サーバの Cisco 2900 ISR G2 への挿入または取り外しを行う前にルータの電源をオフにして、ネットワーク ケーブルを外します。 （注） ISR G2 は EHWIC E シリーズ NCE の OIR をサポートしていません。ルータの損傷を防ぐために、ルータに対して EHWIC E シリーズ NCE を挿入または取り外しする前にルータの電源をオフにして、ネットワーク ケーブルを外します。
ステップ 4	***	Hyper Terminal または Minicom から、*** コマンドを入力してブートローダ プロンプトを開始します。
ステップ 5	ucse-cimc > **boot current recovery**	現在のイメージから E シリーズ サーバまたは NCE をブートします。
ステップ 6	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。 （注） 専用モードはEHWIC E シリーズ NCEには適用されません。 GE3 は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。
ステップ 7	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 8	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 サーバに保存されています。
ステップ 9	Recovery-shell # **reboot**	CIMC をリブートします。

例

次の例は、E シリーズ サーバ の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 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
```

次の例は、EHWIC E シリーズ NCE の現在のイメージから CIMC ファームウェアを回復します。

```
***

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。サーバのタイプに応じて、次のいずれかを実行します。
  - ダブル幅 E シリーズ サーバ：シリアル ケーブルの一端を E シリーズ サーバのシリアル ポートに接続し、もう一端を PC に接続します。
  - シングル幅 E シリーズ サーバおよび SM E シリーズ NCE：KVM コネクタを E シリーズ サーバまたは SM E シリーズ NCEの KVM ポートに接続してから、シリアル ケーブルの一端を KVM コネクタの DB9 ポートに接続し、もう一端を PC に接続します。
  - EHWIC E シリーズ NCE：ケーブルの mini USB の終端を EHWIC E シリーズ NCEの mini USB ポートへ接続し、USB ケーブルの他端を PC の USB ポートに接続します。

  （注） mini USB ケーブルは EHWIC E シリーズ NCEには付随しません。自分の mini USB ケーブルを購入する必要があります。

- 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 サーバ の管理（専用）ポートに接続します。

    （注） 専用モードはEHWIC E シリーズ NCEには適用されません。

  - 共有 Lom GE2：イーサネット ケーブルを E シリーズ サーバ または NCE の外部 GE2 インターフェイスに接続します。
  - 共有 Lom コンソール：Cisco IOS CLI を使用して E シリーズ サーバまたは NCE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、必要に応じて HyperTerminal または Minicom を開始します。次のいずれかを実行します。
  - Microsoft Windows：Hyper Terminal を起動します。
  - Linux：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 sm** *slot* **oir-stop**	指定した E シリーズ サーバの電源をシャットダウンします。 （注） Cisco 2900 シリーズ ISR G2 では E シリーズ サーバの OIR はサポートされません。ルータの損傷を防ぐために、E シリーズ サーバの Cisco 2900 ISR G2 への挿入または取り外しを行う前にルータの電源をオフにして、ネットワーク ケーブルを外します。 （注） ISR G2 は EHWIC E シリーズ NCE の OIR をサポートしていません。ルータの損傷を防ぐために、ルータに対して EHWIC E シリーズ NCE を挿入または取り外しする前にルータの電源をオフにして、ネットワーク ケーブルを外します。
ステップ 2	Router# **hw-module sm** *slot* **oir-start**	指定した E シリーズ サーバを再起動します。 （注） Cisco 2900 シリーズ ISR G2 では E シリーズ サーバの OIR はサポートされません。ルータの損傷を防ぐために、E シリーズ サーバの Cisco 2900 ISR G2 への挿入または取り外しを行う前にルータの電源をオフにして、ネットワーク ケーブルを外します。 （注） ISR G2 は EHWIC E シリーズ NCE の OIR をサポートしていません。ルータの損傷を防ぐために、ルータに対して EHWIC E シリーズ NCE を挿入または取り外しする前にルータの電源をオフにして、ネットワーク ケーブルを外します。

	コマンドまたはアクション	目的
ステップ 3	***	Hyper Terminal または Minicom から、*** コマンドを入力してブートローダ プロンプトを開始します。
ステップ 4	ucse-cimc > **boot current recovery**	現在のイメージから E シリーズ サーバまたは NCE をブートします。
ステップ 5	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 システムを回復するには、次のコマンドを入力します。	**1.** Recovery-shell # **fs-check [p3 | p4]** （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。 **2.** 次の手順を実行します。 • 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。 （注） 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	（任意） **fs-check [p3 | p4]** コマンドによって破損したファイル システムが回復せず、出力に **clean** が表示されない場合は、次の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。	**1.** Recovery-shell # **sd-card format [p3 | p4]** SD カードの特定の破損したパーティションをフォーマットします。 （注） 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。 **2.** Recovery-shell # **reboot** CIMC をリブートします。 （注） 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。

	コマンドまたはアクション	目的
ステップ 7	（任意）**sd-card format [p3 | p4]** コマンドによって破損したファイル システムが回復しない場合は、次のコマンドを入力して、SDカードの分割とフォーマットを実行します。	**1.** Recovery-shell # **sd-card partition** SD カードにパーティションを作成します。 **2.** Recovery-shell # **sd-card format p3** SD カードの p3 パーティションをフォーマットします。 **3.** Recovery-shell # **sd-card format p4** SD カードの p4 パーティションをフォーマットします。 **4.** Recovery-shell # **reboot** CIMC をリブートします。 **5.** （任意）Recovery-shell # **sd-partition show** SD カードの現在のパーティションを表示します。 （注） SD カードを分割すると、SD カードの内容（設定や ISO ファイルなど）は失われます。
ステップ 8	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。 （注） 専用モードはEHWIC E シリーズ NCEには適用されません。 GE3 は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。
ステップ 9	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 サーバに ping を送信し、ネットワーク接続を確認します。
ステップ 10	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 サーバに保存されています。
ステップ 11	Recovery-shell # **reboot**	CIMC をリブートします。

例

この例は、E シリーズ サーバで **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 sm 2 oir-stop
Router# hw-module sm 2 oir-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
```

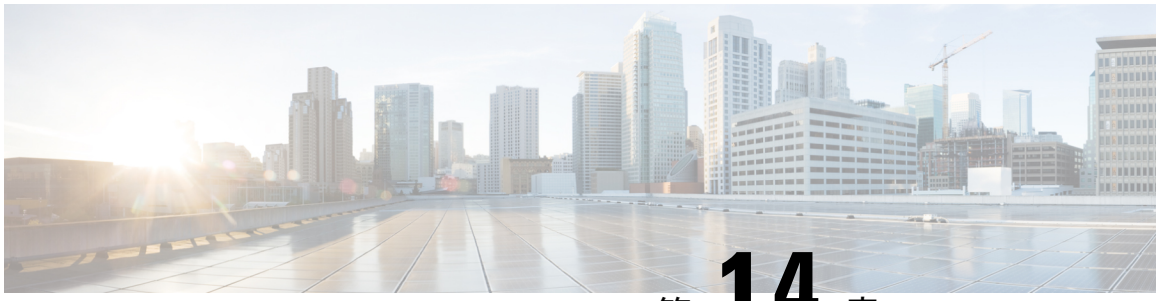
この例は、EHWIC E シリーズ NCEで **fs-check p3** コマンドを使用して、現在のイメージから CIMC ファームウェアを回復します。

```
***

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 # **sd-card format [p3 | p4]**	SD カードの特定の破損したパーティションをフォーマットします。
Recovery-shell # **sd-card partition**	SD カードにパーティションを作成します。
Recovery-shell # **sd-partition show**	SD カードの現在のパーティションを表示します。
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。



第 14 章

障害およびログの表示

この章は、次の項で構成されています。

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]**	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

手順の概要

1. Server# **scope sel**
2. Server /sel # **show entries [detail]**

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 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 [detail]**	システムイベントについて、タイムスタンプ、イベントの重大度、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
-------------------- ------------- ----------------------------------------
[System Boot]        Informational " LED_PSU_STATUS: Platform sensor, OFF event was
asserted"
[System Boot]       Informational " LED_HLTH_STATUS: Platform sensor, GREEN was asserted"

[System Boot]       Normal        " PSU_REDUNDANCY: PS Redundancy sensor, Fully Redundant
 was asserted"
[System Boot]       Normal        " PSU2 PSU2_STATUS: Power Supply sensor for PSU2, Power
 Supply input lost (AC/DC) was deasserted"
[System Boot]       Informational " LED_PSU_STATUS: Platform sensor, ON event was asserted"

[System Boot]       Informational " LED_HLTH_STATUS: Platform sensor, AMBER was asserted"

[System Boot]        Critical      " PSU_REDUNDANCY: PS Redundancy sensor, Redundancy
Lost was asserted"
[System Boot]       Critical      " PSU2 PSU2_STATUS: Power Supply sensor for PSU2, Power
 Supply input lost (AC/DC) was asserted"
[System Boot]        Normal        " HDD_01_STATUS: Drive Slot sensor, Drive Presence was
 asserted"
[System Boot]        Critical      " HDD_01_STATUS: Drive Slot sensor, Drive Presence was
 deasserted"
[System Boot]       Informational " DDR3_P2_D1_INFO: Memory sensor, OFF event was asserted"

2001-01-01 08:30:16 Warning       " PSU2 PSU2_VOUT: Voltage sensor for PSU2, failure
```

```
event was deasserted"
2001-01-01 08:30:16 Critical      " PSU2 PSU2_VOUT: Voltage sensor for PSU2,
non-recoverable event was deasserted"
2001-01-01 08:30:15 Informational " LED_PSU_STATUS: Platform sensor, ON event was asserted"

2001-01-01 08:30:15 Informational " LED_HLTH_STATUS: Platform sensor, AMBER was asserted"

2001-01-01 08:30:15 Informational " LED_HLTH_STATUS: Platform sensor, FAST BLINK event
was asserted"
2001-01-01 08:30:14 Non-Recoverable " PSU2 PSU2_VOUT: Voltage sensor for PSU2,
non-recoverable event was asserted"
2001-01-01 08:30:14 Critical      " PSU2 PSU2_VOUT: Voltage sensor for PSU2, failure
event was asserted"
--More--
```

システム イベント ログのクリア

手順の概要

1. Server# **scope sel**
2. Server /sel # **clear**

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 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

手順の概要

1. Server# **scope cimc**
2. Server /cimc # **scope log**
3. Server /cimc/log # **show entries** [**detail**]

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 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**]	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。

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # show entries
Time                 Source           Description
-------------------- ---------------- ----------------------------------------
1970 Jan 4 18:55:36 BMC:kernel:-
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:306:I2c Controller-4 DAT is stuck-low,
 issuing One Clock Pulse.
1970 Jan 4 18:55:36 BMC:kernel:-
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:301:I2c Controller-4 Loop:[0].
1970 Jan 4 18:55:36 BMC:kernel:-     "
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:422: Controller-4 has a stuck bus,
attempting to clear it now... "
1970 Jan 4 18:55:36 BMC:kernel:-     "
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:402: Controller-4 Initiating I2c
recovery sequence. "
1970 Jan 4 18:55:36 BMC:IPMI:480     last message repeated 22 times
1970 Jan 4 18:55:28 BMC:IPMI:480     "  mcddI2CDrv.c:850:PI2CWriteRead: ioctl to driver
 failed to read Bus[f4].Dev[5e]! ErrorStatus[77] "
1970 Jan 4 18:55:33 BMC:IPMI:486     last message repeated 17 times
1970 Jan 4 18:55:28 BMC:IPMI:486     "  mcddI2CDrv.c:850:PI2CWriteRead: ioctl to driver
 failed to read Bus[f4].Dev[b0]! ErrorStatus[77] "
1970 Jan 4 18:55:31 BMC:IPMI:486     last message repeated 17 times
1970 Jan 4 18:55:26 BMC:IPMI:486     "  mcddI2CDrv.c:850:PI2CWriteRead: ioctl to driver
 failed to read Bus[f4].Dev[b2]! ErrorStatus[77] "
1970 Jan 4 18:55:26 BMC:kernel:-
```

```
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:306:I2c Controller-4 DAT is stuck-low,
 issuing One Clock Pulse.
1970 Jan 4 18:55:26 BMC:kernel:-
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:301:I2c Controller-4 Loop:[8].
--More--
```

CIMC ログのクリア

手順の概要

1. Server# **scope cimc**
2. Server /cimc # **scope log**
3. Server /cimc/log # **clear**

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 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 # **clear**	CIMC ログをクリアします。

例

次に、CIMC イベントのログをクリアする例を示します。

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # clear
```

CIMC ログしきい値の設定

CIMC ログに含まれるメッセージの最低レベルを指定できます。

手順の概要

1. Server# **scope cimc**
2. Server /cimc # **scope log**
3. Server /cimc/log # **set local-syslog-severity** *level*
4. Server /cimc/log # **commit**
5. （任意） Server /cimc/log # **show local-syslog-severity**

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 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 # **set local-syslog-severity** *level*	重大度の *level* には、次のいずれかを指定できます。順に重大度が下がります。 • emergency • alert • critical • error • warning • notice • informational • debug （注） CIMC では、選択した重大度よりも低い重大度のメッセージはログに記録されません。たとえば、**error** を選択した場合、CIMC ログには重大度が Emergency、Alert、Critical、または Error のすべてのメッセージが含まれます。Warning、Notice、Informational、または Debug のメッセージは表示されません。
ステップ 4	Server /cimc/log # **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	（任意） Server /cimc/log # **show local-syslog-severity**	設定された重大度レベルを表示します。

例

次に、最小重大度を警告として、メッセージのロギングを設定する例を示します。

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # set local-syslog-severity warning
Server /cimc/log *# commit
Server /cimc/log # show local-syslog-severity
    Local Syslog Severity: warning

Server /cimc/log #
```

リモート サーバへの CIMC ログの送信

1 台または 2 台のリモート syslog サーバが CIMC ログ エントリを受信するように、プロファイルを設定できます。

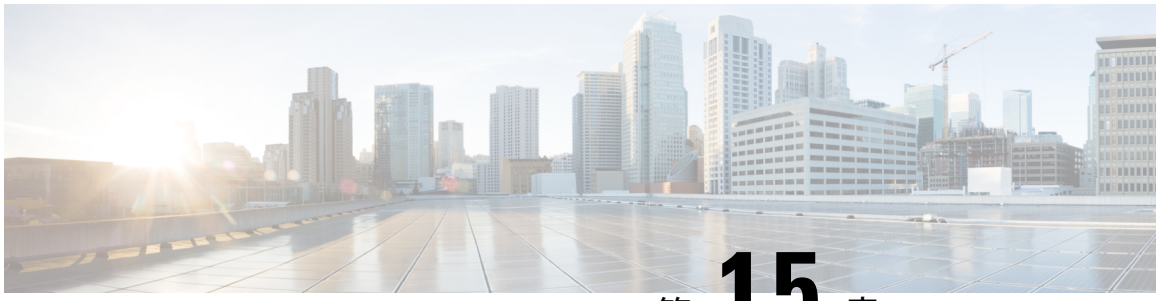
手順

	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 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 # **scope server** {**1** | **2**}	2 つのリモート syslog サーバ プロファイルのうち 1 つを選択し、プロファイルを設定するコマンドモードを開始します。
ステップ 4	Server /cimc/log/server # **set server-ip** *ip-address*	リモート syslog サーバの IP アドレスを指定します。
ステップ 5	Server /cimc/log/server # **set enabled** {**yes** | **no**}	この syslog サーバへの CIMC ログ エントリの送信をイネーブルにします。
ステップ 6	Server /cimc/log/server # **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、リモート syslog サーバ プロファイルを設定し、CIMC ログ エントリの送信をイネーブルにする例を示します。

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # scope server 2
Server /cimc/log/server # set server-ip 192.0.2.34
Server /cimc/log/server *# set enabled yes
Server /cimc/log/server *# commit
Server /cimc/log/server #
```



第 15 章

サーバ ユーティリティ

この章は、次の項で構成されています。

リモート サーバへのテクニカル 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。

手順の概要

1. Server# **scope cimc**
2. Server /cimc # **scope tech-support**
3. Server /cimc/tech-support # **set remote-ip** *ip-address*
4. Server /cimc/tech-support # **set remote-path** *path/filename*
5. Server /cimc/tech-support # **set remote-protocol** *protocol-type*
6. Server /cimc/tech-support # **set remote-username** *username*
7. Server /cimc/tech-support # **set remote-password** *password*
8. Server /cimc/tech-support # **commit**
9. Server /cimc/tech-support # **start**
10. Server /cimc/tech-support # **show detail**
11. Server /cimc/tech-support # **cancel**

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 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 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 サーバのプロトコルを指定します。リモート サーバの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 6	Server /cimc/tech-support # **set remote-username** *username*	（任意）システムがリモート サーバへのログインに使用する必要のあるユーザ名。 （注） ユーザ名は、リモート サーバが 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 ユーザ名のパスワード。 （注） パスワードは、リモート サーバが 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 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。

手順の概要

1. Server# **scope cimc**
2. Server /cimc # **reboot**

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 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。

手順の概要

1. Server# **scope cimc**
2. Server /cimc # **factory-default**

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 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 アカウントが存在している（ユーザ名は **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 EFI、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します。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。サーバ上のデータはバックアップされません。ユーザ アカウントやサーバ証明書など、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、この操作でユーザアカウントやサーバ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

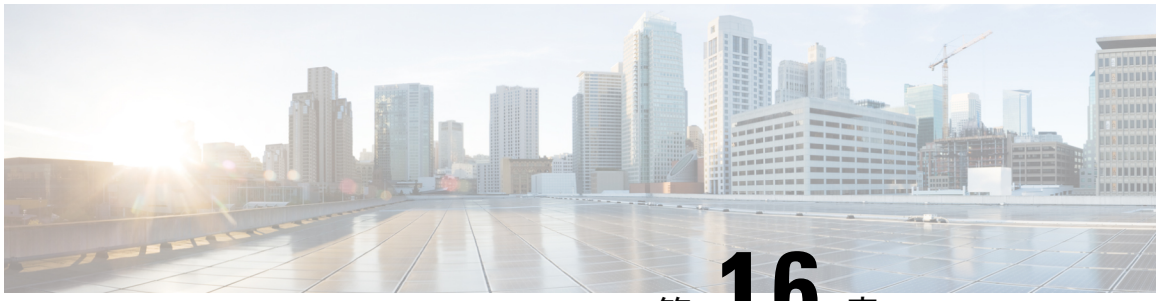
	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope import-export**	import-export コマンド モードを開始します。
ステップ 3	Server /cimc/import-export # **import-config** *tftp-ip-address path-and-filename*	インポート操作を開始します。指定した IP アドレスの TFTP サーバで指定されたパスとファイル名で、コンフィギュレーション ファイ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# scope cimc
Server /cimc # scope import-export
Server /cimc/import-export # import-config 192.0.2.34 /ucs/backups/cimc5.xml
Import config started. Please check the status using "show detail".
Server /cimc/import-export #
```



第 16 章

診断テスト

この章は、次の項で構成されています。

診断テストの概要

診断はEシリーズサーバまたはNCE上で実行されるスタンドアロンユーティリティで、同サーバで動作するオペレーティングシステムやアプリケーションからは独立しています。Eシリーズサーバまたは NCEで問題が発生した場合、診断テストを使用して事前チェックを実行し、問題点を特定することができます。診断テストはサーバの CPU、メモリ、およびブロック デバイスで実行できます。ブロックデバイスにはハードドライブ、USB ドライブ、SD カードなどがあります。

診断テストに合格した場合、サーバのCPU、メモリ、ブロックデバイスに問題はありません。他のハードウェア コンポーネントまたはソフトウェア設定に問題がある可能性があります。http://www.cisco.com/cisco/web/support/index.html の Cisco Technical Assistance Center（TAC）でサービス要求を開始し、問題点を特定してください。

診断テストが失敗した場合は、Cisco TAC でサービス要求を開いて支援を求めます。

⚠

注意 診断テストは非破壊テストですが、テストの実行中に停電または機器の故障が発生した場合、ディスクデータが破損することがあります。診断テストを実行する前に、データをバックアップしておくことを強く推奨します。

診断テストを実行するための基本的なワークフロー

1. データをバックアップします。

2. 診断イメージは購入時にE シリーズ サーバまたはNCEに事前にインストールされています。最新の診断イメージを、指定した FTP または HTTP サーバから CIMC 内部リポジトリにダウンロードすることもできます。
3. 診断イメージを USB コントローラの HDD 仮想ドライブにマウントします。
4. 内部 EFI シェルが最初のブート デバイスになるようにブート順を設定します。
5. サーバをリブートします。

（注）
- E シリーズ サーバおよびSM E シリーズ NCEの場合：サーバのリブート時に EFI シェルが表示されます。
- EHWIC E シリーズ NCE および NIM E シリーズ NCE の場合：サーバのリブート時に AMIDiag EFI シェルが表示されます。

6. 必要に応じて EFI シェルまたは AMIDiag EFI シェルから診断テストを実行します。
7. 仮想メディアのブート順を元の設定にリセットします。

ホストへの診断イメージのマッピング

始める前に

- データをバックアップします。
- admin 権限を持つユーザとして CIMC にログインします。
- E シリーズ サーバには、購入時に診断イメージが事前にインストールされています。最新の診断イメージを、指定した FTP、FTPS、HTTP、または HTTPS サーバから CIMC 内部リポジトリにダウンロードすることもできます。「シスコからのソフトウェアの取得」を参照してください。

（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 remote-install**	remote install 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 /remote-install # **download-image** {**ftp** | **ftps** | **http** | **https**} *server-ip-address path / filename* [**username** *username* **password** *password*]	指定したリモート サーバから CIMC 内部リポジトリにイメージをダウンロードします。診断イメージのファイル拡張子は必ず .diag になります。リモート サーバには、FTP、FTPS、HTTP、または HTTPS サーバを指定できます。リモート サーバでユーザ認証が必要な場合は、リモート サーバのユーザ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。
ステップ 3	（任意）Server /remote-install # **show detail**	診断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 /remote-install # **map-diagnostics**	USB コントローラの HDD 仮想ドライブにイメージをマウントします。
ステップ 5	（任意）Server /remote-install # **show detail**	診断イメージ マッピングのステータスを表示します。

例

次に、診断イメージをマッピングする例を示します。

```
Server# scope remote-install
Server /remote-install # download-image ftp 10.20.34.56 pub/diagnostics-image.diag
---
Server /remote-install # show detail
Host Image Info:
  Name: DiagnosticsImage.diag
  Size: 6626848
  Last Modified Time: Fri, 12 Aug 2011 21:13:27 GMT
  Host Image Status: Download Successful!!
Server /remote-install # map-diagnostics
---
status: ok
---
Server /remote-install # show detail
Host Image Info:
  Name: DiagnosticsImage.diag
  Size: 6626848
  Last Modified Time: Fri, 12 Aug 2011 21:13:27 GMT
  Host Image Status: Image mapped successfully!!
```

次のタスク

1. EFI シェルが最初のブート デバイスになるように、ブート順を設定します。
2. サーバをリブートします。EFI シェルが表示されます。
3. 診断テストを実行します。

診断テストの実行：E シリーズ サーバおよび SM E シリーズ NCE

EFI シェルから、次の手順を使用してE シリーズ サーバおよびSM E シリーズ NCE で診断テストを実行します。

始める前に

- バックアップデータ。テストはすべて非破壊的ですが、テストの実行中に停電や装置の障害が発生すると、ディスクデータが破損する可能性があります。これらのテストを実行する前に、データをバックアップすることを強く推奨します。
- CIMC CLI または CIMC GUI を使用して、診断イメージをダウンロードし、USB コントローラの HDD 仮想ドライブ上にマップします。
- サーバをリブートします。EFI シェルが表示されます。

手順

	コマンドまたはアクション	目的
ステップ 1	Shell > **dir** *virtual-media-drive-name***:**	指定した仮想メディア ドライブ内に存在するすべてのファイルパッケージを表示します。ドライブ名は fs0 から始まり、fs0、fs1、fs2 などがあります。 （注） 仮想メディア ドライブ名の末尾に必ずコロンを追加してください。例：**dir fs1:**
ステップ 2	Shell > *virtual-media-drive-name***:**	診断ファイルが保存されている仮想メディア ドライブに移動します。
ステップ 3	Virtual Media Drive :\> **cp** *package-file-name* **dsh.pkg**	診断を実行するパッケージ ファイルを診断シェル パッケージ ファイルにコピーします。
ステップ 4	Virtual Media Drive :\> **dsh**	診断シェルを開始します。確認プロンプトで、**y** と答えます。
ステップ 5	Server: SRV > **run all**	使用可能なすべての診断テストを実行し、テストの進行状況とステータスを表示します。診断テストは、サーバの CPU、メモリ、およびブロック デバイス上で実行されます。ブロック デバイスにはハードドライブ、USB ドライブ、SD カードなどがあります。

	コマンドまたはアクション	目的
		サーバ上で特定の診断テストを実行するには、**run** *test-name* コマンドを使用します。*test-name* には次のいずれかを指定できます。 • **cpux64**：CPU の診断テスト。 • **diskx64**：ブロック デバイスの診断テスト。ブロック デバイスにはハード ドライブ、USB ドライブ、SD カードなどがあります。 • **memoryx64**：メモリの診断テスト。 （注） 診断テストの実行には、約 10 分の時間がかかる可能性があります。
ステップ 6	（任意）Server: SRV > **results**	テスト ステータスが **Passed** または **Failed** の診断テストのサマリーを表示します。 （注） このサマリー レポートは、失敗および合格したテストの数を示します。どのテストが失敗または合格したかについての情報は提供しません。失敗および合格したテストを判別するには、**run all** コマンドの出力を確認してください。
ステップ 7	（任意）Server: SRV > **show**	サーバ上で管理されていたグローバル パラメータと診断テスト モジュールの一覧を表示します。
ステップ 8	Server: SRV > **exit**	診断シェルを終了します。
ステップ 9	Cisco TAC でサービス要求を開きます。	診断テストに合格した場合、サーバの CPU、メモリ、ブロック デバイスに問題はありません。他のハードウェア コンポーネントまたはソフトウェア設定に問題がある可能性があります。Cisco TAC でサービス要求を開いて、問題を特定します。 診断テストが失敗した場合は、Cisco TAC でサービス要求を開いて支援を求めます。

例

次の例では、すべての診断テストを実行しています。

```
Shell > dir fs1:
  06/27/12  07:48p            1,435,424  Dsh.efi
  06/27/12  08:03p               10,036  dsh-e140d.pkg
  06/25/12  06:00p               10,140  dsh-e140s.pkg
  06/27/12  08:04p               10,042  dsh-e160d.pkg
```

```
          4 File(s)   1,465,642 bytes
Shell > fs1:
fs1:\> cp dsh-e140d.pkg dsh.pkg
copying fs0:\OBD\dsh-e140d.pkg -> fs0:\OBD\dsh.pkg
- [ok]
fs1:\> dsh
Diagnostics is a standalone utility that runs on the server module independent
of the operating system or applications running on the module.All tests are
non-destructive, but there is a possibility of disk datacorruption during
power or equipment failure when the tests are in progress. Therefore, before
executing these tests, we highly recommend that you backup the data.


For questions or concerns with this utility, please open a Service Request
with Cisco TAC at http://www.cisco.com/cisco/web/support/index.html

(Y)es to continue test. (N)o to exit(y/n): Y
Cisco Diagnostics  Shell 1.03(0.3) Thu 06/28/-16:35:08.95-canis-diag@cisco.com
UCS-E140D-M1/K9:SRV>

Server: SRV > run all
Server: SRV > results
Test Name          : all
Test Status        : Passed
Failed/Run History : 0/17
Start Time         : 06/27/12 14:38:19
End Time           : 06/27/12 14:43:36
Diag Version       : 1.03(0.3) Mon 04/02/-17:07:57.19-canis-diag@cisco.com
Board S/N          : FOC160724BY

Server: SRV > show
Server: SRV > exit
```

次のタスク

仮想メディアのブート順を元の設定にリセットします。

診断テストの実行：EHWIC E シリーズ NCE および NIM E シリーズ NCE

診断テストは、サーバの CPU、メモリ、およびブロック デバイス上で実行されます。ブロック デバイスには SSD ドライブおよび USB ドライブが含まれます。

始める前に

- バックアップデータ。テストはすべて非破壊的ですが、テストの実行中に停電や装置の障害が発生すると、ディスクデータが破損する可能性があります。これらのテストを実行する前に、データをバックアップすることを強く推奨します。
- AMIDIAG_OBD.log ファイルの以前のバージョンがある場合は、それを削除します。
- CIMC CLI または CIMC GUI を使用して、診断イメージをダウンロードし、USB コントローラの HDD 仮想ドライブ上にマップします。

- KVM コンソールを起動します。
- サーバをリブートします。KVM コンソールに AMIDiag EFI シェルが表示されます。

```
Found AMI DIAG on fs0:
Diagnostics is a standalone utility that runs on the server module independent
of the operating system or applications running on the module.All tests are
non-destructive, but there is a possibility of disk datacorruption during
power or equipment failure when the tests are in progress. Therefore, before
executing these tests, we highly recommend that you backup the data.

For questions or concerns with this utility, please open a Service Request
with Cisco TAC at http://www.cisco.com/cisco/web/support/index.html

Enter 'q' to quit, any other key to continue:

fs0:\>
```

手順

	コマンドまたはアクション	目的
ステップ 1	AMIDiag EFI シェルから、（q 以外の）任意のキーを押して診断テストを実行します。	有効なすべての診断テストが実行され、進捗が表示されます。テストが完了すると、テスト ステータスとして **Pass** または **Fail** が表示されます。 （注） 診断テストの実行には、約 10 分の時間がかかる可能性があります。
ステップ 2	（任意）fs0:\> **type AMIDIAG_OBD.log**	詳細な Onboard Diag ログ ファイルが表示されます。
ステップ 3	Server: fs0:\> **exit**	AMIDiag EFI シェルを終了します。
ステップ 4	Cisco TAC でサービス要求を開きます。	診断テストに合格した場合、サーバの CPU、メモリ、ブロック デバイスに問題はありません。他のハードウェア コンポーネントまたはソフトウェア設定に問題がある可能性があります。Cisco TAC でサービス要求を開いて、問題を特定します。 診断テストが失敗した場合は、Cisco TAC でサービス要求を開いて支援を求めます。

次のタスク

仮想メディアのブート順を元の設定にリセットします。