Cisco UCS C シリーズ サーバ Integrated Management Controller CLI コンフィギュレーション ガイド リリース 1.1(1)

Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 1.1(1)

初版: 2010 年 03 月 30 日

Text Part Number: OL-22347-01-J

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

目 次

はじめに

この前書きの内容は次のとおりです。

対象読者

このガイドは、次の 1 つ以上に責任と専門知識を持つ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。

タイトル	説明
概要	Cisco UCS C シリーズ ラックマウント サーバおよび CIMC CLI について説明します。

タイトル	説明
サーバの管理	CLI コマンドについて説明します。ブートデバイスの順序の設定、サーバへの電力の制御、およびサーバのリセット方法を説明します。
サーバのプロパティの表示	サーバの CPU、メモリ、電源、およびストレージのプロパティの表示方法を説明します。
サーバのセンサーの表示	電源、ファン、温度、電流、および電圧のセンサーの表示方法を説明します。
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。
ユーザ アカウントの管理	ユーザを追加、削除、認証する方法、およびユーザ セッションの管理方法を説明します。
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、およびネットワーク セキュリティの設定方法を説明します。
コミュニケーション サービスの設定	HTTP、SSH、および IPMI 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。
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。
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 フィルタおよび SNMP 設定の設定および管理方法を説明します。
CIMC 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。
ログの表示	ログ メッセージを表示およびクリアする方法を説明します。
サーバ ユーティリティ	サポートデータをエクスポートする方法、サーバの設定を出荷時デフォルトにリセットする方法、および管理インターフェイスを再起動する方法を説明します。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	意味
bold フォント	コマンド、キーワード、GUI 要素、およびユーザが入力したテキストは **bold** フォントで表示されます。
italic フォント	マニュアルのタイトル、新規用語または重要な用語、値を指定すべき引数は *italic* フォントで表示されます。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z}	必須の代替キーワードは、波カッコ内にグループ化され、垂直バーで区切られます。
[x | y | z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。 string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
`courier` フォント	スイッチが表示する端末セッションおよび情報は、`courier` フォントで表示されます。
< >	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。

ヒント 「問題解決に役立つ情報」です。

注意 「要注意」の意味です。 この状況では、機器の損傷やデータの損失につながるような操作をする可能性があります。

ワンポイント アドバイス　ここで説明されている操作により時間を短縮できることを意味します。 この段落で説明する操作を実行すると、時間を節約することができます。

警告　読者に対する警告を意味します。 この状況では、身体に対する傷害につながるような操作をする可能性があります。

関連資料

Cisco UCS C シリーズ ラックマウント サーバに関するマニュアルは、次の URL から入手できます。

http://www.cisco.com/go/unifiedcomputing/c-series-doc

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、次の URL で、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。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*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。

第 1 章

概要

この章の構成は、次のとおりです。

Cisco UCS C シリーズ ラックマウント サーバの概要

Cisco UCS C シリーズ ラックマウント サーバを次に示します。

- Cisco UCS C200 M1 ラックマウント サーバ
- Cisco UCS C210 M1 ラックマウント サーバ
- Cisco UCS C250 M1 ラックマウント サーバ

UCS C200 M1 ラックマウント サーバ

Cisco UCS C200 M1 サーバは、高密度の 2 ソケット、1 RU ラックマウント サーバです。 このサーバは、実稼動レベルのネットワーク インフラストラクチャ、Web サービス、メインストリーム データセンター、およびブランチオフィスとリモートオフィス用のアプリケーションに対応できるように構築されています。

UCS C210 M1 ラックマウント サーバ

Cisco UCS C210 M1 サーバは、汎用の 2 ソケット、2 RU ラックマウント サーバです。 ストレージ集約型の負荷に対応するため、パフォーマンス、密度、効率をバランスよく実現するように設計されています。 このサーバは、ネットワーク ファイルおよびアプライアンス、ストレージ、データベース、コンテンツ配信など、さまざまな用途に対応できるように構築されています。

UCS C250 M1 ラックマウント サーバ

Cisco UCS C250 M1 サーバは、高性能かつメモリ集約的な 2 ソケット、2 RU ラックマウント サーバです。 パフォーマンスを向上させるように設計されており、要求の厳しいバーチャライゼーションや大量のデータセットの負荷に対応する容量を備えています。 また、C250 M1 サーバでは、メモリ占有スペースが小さいため、コストを削減することができます。

Cisco Integrated Management Controller

Cisco Integrated Management Controller（CIMC）は、C シリーズ サーバ用の管理サービスです。CIMC はサーバ内で動作します。

管理インターフェイス

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。 ほとんどすべてのタスクは、これらの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、次の操作はできません。

- CIMC GUI を使用して CIMC CLI を呼び出す
- CIMC CLI で呼び出したコマンドを CIMC GUI に表示する
- CIMC GUI から CIMC CLI の出力を生成する

CIMC で実行可能なタスク

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
- ロケータ LED を切り替える
- サーバのブート順を設定する
- 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、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 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
- 障害、アラーム、およびサーバのステータスをモニタする

オペレーティング システムやアプリケーションのプロビジョニングや管理はできない

CIMC はサーバのプロビジョニングを行うため、サーバのオペレーティング システムの下に存在します。 したがって、サーバでオペレーティング システムやアプリケーションのプロビジョニングや管理を行うためにこれを使用することはできません。 たとえば、次の操作を実行することはできません。

- Windows や Linux などの OS の展開
- OS やアプリケーションなどのソフトウェアに対するパッチの展開
- アンチウイルス ソフトウェア、モニタリング エージェント、バックアップ クライアントなどのベース ソフトウェア コンポーネントのインストール
- データベース、アプリケーション サーバ ソフトウェア、Web サーバなどのソフトウェア アプリケーションのインストール
- Oracle データベースの再起動、プリンタ キューの再起動、または CIMC 以外のユーザ アカウントの処理を含むオペレータ処理の実行
- SAN や NAS ストレージ上の外部ストレージの設定または管理

CIMC CLI

CIMC CLI は、Cisco UCS C シリーズ サーバのコマンドライン管理インターフェイスです。 CIMC CLI を起動し、シリアル ポートまたは SSH や Telnet によるネットワーク上でサーバを管理できます。 デフォルトでは、Telnet アクセスはディセーブルになります。

CLI のユーザ ロールは、admin、user（制御は可能、設定は不可）、および read-only のいずれかになります。

（注） admin パスワードが失われたために回復する必要がある場合には、ご使用のプラットフォームの Cisco UCS C シリーズ サーバ インストールおよびサービス ガイドを参照してください。

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、主要なコマンド 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。

表 *1*：主要なコマンド モードとプロンプト

モード名	アクセスに使用するコマンド	モード プロンプト
EXEC	任意のモードの **top** コマンド	#
bios	EXEC モードの **scope bios** コマンド	/bios #
certificate	EXEC モードの **scope certificate** コマンド	/certificate #
chassis	EXEC モードの **scope chassis** コマンド	/chassis #
cimc	EXEC モードの **scope cimc** コマンド	/cimc #
firmware	cimc モードの **scope firmware** コマンド	/cimc/firmware #
log	cimc モードの **scope log** コマンド	/cimc/ log #
network	cimc モードの **scope network** コマンド	/cimc/network #
ip-blocking	network モードの **scope ip-blocking** コマンド	/cimc/network/ip-blocking #
tech-support	cimc モードの **scope tech-support** コマンド	/cimc/tech-support #
fault	EXEC モードの **scope fault** コマンド	/fault #
pef	障害モードの **scope pef** コマンド	/fault/pef #
trap-destination	障害モードの **scope trap-destination** コマンド	/fault/trap-destination #
http	EXEC モードの **scope http** コマンド	/http #
ipmi	EXEC モードの **scope ipmi** コマンド	/ipmi #

モード名		アクセスに使用するコマンド	モード プロンプト
	kvm	EXEC モードの **scope kvm** コマンド	/kvm #
	ldap	EXEC モードの **scope ldap** コマンド	/ldap #
	sel	EXEC モードの **scope sel** コマンド	/sel #
	sensor	EXEC モードの **scope sensor** コマンド	/sensor #
	sol	EXEC モードの **scope sol** コマンド	/sol #
	ssh	EXEC モードの **scope ssh** コマンド	/ssh #
	user	EXEC モードの**scope user** *user-number* コマンド	/user #
	user-session	EXEC モードの**scope user-session** *session-number* コマンド	/user-session #
	vmedia	EXEC モードの **scope vmedia** コマンド	/vmedia #

コマンドの実行

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。

コマンド履歴

CLI では、現行のセッションでそれまでに使用したすべてのコマンドを保存しています。 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 chassis
Server /chassis # set locator-led off
Server /chassis *# commit
Server /chassis #
```

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。

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。 **detail** キーワードを使用すると、出力形式を表示するための 2 つの表示形式のいずれかを設定できます。 次の形式を選択できます。

- デフォルト：簡単に確認できるよう、コマンド出力はコンパクト 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
Name HDD_04_STATUS:
    Status : present

Server /chassis #
```

- YAML：スクリプトによる解析を簡単に行うため、コマンド出力は、定義された文字列で区切られた YAML™（YAML Ain't Markup Language）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

---
    name: HDD_04_STATUS
```

```
    hdd-status: present
...
Server /chassis #
```

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

ほとんどの CLI コマンド モードでは、**set cli output default**を入力してデフォルト形式を設定するか、**set cli output yaml**を入力して YAML 形式を設定することができます。

CLI に関するオンラインヘルプ

? 文字を入力すれば、いつでも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できます。 プロンプトに何も入力されていない状態で ? を入力すると、 そのときのモードで使用できるコマンドがすべて表示されます。 コマンドの一部が入力されているときに ? と入力すると、 コマンド構文のそのときの位置で使用できるキーワードと引数がすべて表示されます。

第 2 章

サーバの管理

この章の構成は、次のとおりです。

ロケータ LED の切り替え

操作を行う前に

この操作を含むすべての電力制御操作には、ユーザ権限が必要になります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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 # **set locator-led** {**on** | **off**}	シャーシ ロケータ LED 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 /chassis # **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。

次に、シャーシロケータ LED をディセーブルにして、トランザクションをコミットする例を示します。

```
Server# scope chassis
Server /chassis # set locator-led off
Server /chassis *# commit

Server /chassis #
```

サーバのブート順のリセット

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	bios コマンド モードを開始します。
ステップ 2	Server /bios # **set boot-order** *device1*[,*device2*[,*device3*[,*device4*[,*device5*]]]]	ブート デバイス オプションと順序を指定します。次の 1 つ以上を選択できます。 • cdrom：ブート可能な CD-ROM • fdd：フロッピー ディスク ドライブ • hdd：ハード ディスク ドライブ • pxe：PXE ブート • 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。

新規のブート順は、次の BIOS のブートで使用されます。

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 hdd,cdrom,fdd,pxe,efi
Server /bios *# commit
Server /bios #  show detail
BIOS:
    Boot Order: HDD,CDROM,FDD,PXE,EFI

Server /bios #
```

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。

手順

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

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  UUID
----- ------------- ------------ ------------------------------------
on    Not Specified Not Specified 208F0100020F000000BEA80000DEAD00
```

サーバの電源オフ

手順

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

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  UUID
----- ------------- ------------ ------------------------------------
```

```
off   Not Specified Not Specified 208F0100020F000000BEA80000DEAD00
```

サーバ電源の再投入

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **power cycle**	サーバ電源を再投入します。

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
```

サーバのリセット

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **power hard-reset**	確認プロンプトの後に、サーバがリセットされます。

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

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 モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	Server /chassis # **power shutdown**	サーバをシャットダウンします。

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
```

第 3 章

サーバのプロパティの表示

この章の構成は、次のとおりです。

CPU のプロパティの表示

操作を行う前に

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。

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           E5520  @ 2.27GHz
CPU2         4        Intel(R) Xeon(R) CPU           E5520  @ 2.27GHz

Server /chassis #
```

メモリのプロパティの表示

操作を行う前に

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。

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 (MB)   Speed (MHz)     Type
---------- --------------- --------------- ---------------
DIMM_A1    2048            1067            Other
DIMM_A2    0               1067            Other
DIMM_B1    0               1067            Other
DIMM_B2    0               1067            Other
DIMM_C1    0               1067            Other
DIMM_C2    0               1067            Other
DIMM_D1    2048            1067            Other
DIMM_D2    0               1067            Other
DIMM_E1    0               1067            Other
DIMM_E2    0               1067            Other
DIMM_F1    0               1067            Other
DIMM_F2    0               1067            Other

Server /chassis #
```

電源のプロパティの表示

操作を行う前に

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 psu** [**detail**]	電源のプロパティを表示します。

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 psu
Name       In. Power (Watts)    Out. Power (Watts)   Firmware  Status
---------- -------------------- -------------------- -------- ----------
PSU1       74                   650                  R0E      Present
PSU2       83                   650                  R0E      Present

Server /chassis #
```

ストレージのプロパティの表示

操作を行う前に

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 hdd** [**detail**]	ストレージのプロパティを表示します。

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 hdd
Name                 Status
-------------------- --------------------
HDD_01_STATUS        present
HDD_02_STATUS        present
HDD_03_STATUS        present
HDD_04_STATUS        present

Server /chassis #
```

第 4 章

サーバのセンサーの表示

この章の構成は、次のとおりです。

電流センサーの表示

手順

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

次に、電流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 current
Name                     Sensor Status  Reading    Units      Min. Warning Max. Warning
Min. Failure Max. Failure
------------------------ -------------- ---------- ---------- ------------ ------------
------------ ------------
VR_P2_IMON               Normal         16.00      AMP        N/A          147.20
N/A          164.80
VR_P1_IMON               Normal         27.20      AMP        N/A          147.20
N/A          164.80

Server /sensor #
```

電源センサーの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope sensor**	センサー コマンド モードを開始します。
ステップ 2	Server /sensor # **show psu** [**detail**]	サーバの電源センサーの統計情報を表示します。
ステップ 3	Server /sensor # **show psu-redundancy** [**detail**]	サーバの電源冗長センサーのステータスを表示します。

次に、電源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 psu
Name                 Sensor Status        Reading    Units      Min. Warning    Max. Warning
    Min. Failure    Max. Failure
-------------------- -------------------- ---------- ---------- --------------
-------------- --------------- ---------------
PSU1_STATUS          Normal               present

PSU2_STATUS          Normal               present

Server /sensor # show psu-redundancy
Name                 Reading    Sensor Status
-------------------- ---------- --------------------
PSU_REDUNDANCY       full       Normal

Server /sensor #
```

ファン センサーの表示

手順

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

次に、ファン 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 fan
Name                 Sensor Status  Reading    Units      Min. Warning    Max. Warning
Min. Failure    Max. Failure
-------------------- -------------- ---------- ---------- --------------- ---------------
--------------- ---------------
W793_FAN2_TACH1      Normal         2400       RPM        N/A             N/A
800             N/A
```

```
W793_FAN2_TACH2      Normal          2400       RPM        N/A             N/A
800              N/A
W793_FAN3_TACH1      Normal          2300       RPM        N/A             N/A
800              N/A
W793_FAN3_TACH2      Normal          2300       RPM        N/A             N/A
800              N/A
W793_FAN4_TACH1      Normal          2400       RPM        N/A             N/A
800              N/A
W793_FAN4_TACH2      Normal          1600       RPM        N/A             N/A
800              N/A

Server /sensor #
```

温度センサーの表示

手順

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

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

	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。

	コマンドまたはアクション	目的
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。

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 #
```

第 5 章

リモート プレゼンスの管理

この章の構成は、次のとおりです。

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（KVM）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
- ネットワーク上の CD/DVD またはフロッピー ドライブ
- ネットワーク上のディスク イメージ ファイル

KVM コンソールを使用してサーバに OS をインストールできます。

仮想 KVM のイネーブル化

操作を行う前に

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

	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。

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

操作を行う前に

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

	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。

	コマンドまたはアクション	目的
		（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。

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 #
```

仮想 KVM の設定

操作を行う前に

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

	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。

	コマンドまたはアクション	目的
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。

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 #
```

次の手順

GUI から仮想 KVM を起動します。

仮想メディアの設定

操作を行う前に

仮想メディアを設定するには、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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope vmedia**	仮想メディア コマンド モードを開始します。
ステップ 2	Server /vmedia # **set enabled** {**yes** | **no**}	仮想メディアをイネーブルまたはディセーブルにします。 デフォルトでは、仮想メディアはディセーブルになります。

	コマンドまたはアクション	目的
		（注） 仮想メディアをディセーブルにすると、仮想 CD、仮想フロッピー、および仮想 HDD デバイスがホストから切断されます。
ステップ 3	Server /vmedia # **set encryption {yes | no}**	仮想メディアの暗号化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 /vmedia # **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 /vmedia # **show [detail]**	（任意）仮想メディアの設定を表示します。

次に、仮想メディアの暗号化を設定する例を示します。

```
Server# scope vmedia
Server /vmedia # set enabled yes
Server /vmedia *# set encryption yes
Server /vmedia *# commit
Server /vmedia # show detail
vMedia Settings:
    Encryption Enabled: yes
    Enabled: yes
    Max Sessions: 4
    Active Sessions: 0

Server /vmedia #
```

次の手順

KVM を使用して、仮想メディア デバイスをホストに接続します。

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。

- console redirection to serial port A
- no flow control
- baud rate the same as configured for SoL
- VT-100 terminal type

- legacy OS redirection disabled

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 Operating System（OS; オペレーティング システム）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

操作を行う前に

Serial over LAN（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

	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。 （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。

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

	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 Serial over LAN（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。

次の手順

SoL セッションを終了するには、CLI セッションを終了する必要があります。 たとえば、SSH 接続を介した SoL セッションを終了するには、SSH 接続を切断します。

第 6 章

ユーザ アカウントの管理

この章の構成は、次のとおりです。

ローカル ユーザの設定

操作を行う前に

ローカル ユーザを設定するには、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

	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。

	コマンドまたはアクション	目的
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。 • 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。

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
```

Active Directory の設定

Active Directory

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、Active Directory の Kerberos ベースの認証サービスを利用します。

CIMC で Active Directory をイネーブルにすると、すべてのユーザ認証とロール許可は Active Directory によって実行され、CIMC はローカル データベースを無視します。 CIMC が Active Directory に接続できない場合、CIMC はローカル データベースに戻ります。

サーバでの Active Directory の設定で暗号化をイネーブルにすることで、サーバに Active Directory への送信データを暗号化するよう要求できます。

Active Directory サーバの設定

CIMC を設定して、Active Directory をユーザの認証と認可に使用できます。 Active Directory 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アトリビュート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 アトリビュートを使用できます。または、Active Directory スキーマを変更して、アトリビュート ID 1.3.6.1.4.1.9.287247.1 を持つ CiscoAVPair アトリビュートのような新規のカスタム アトリビュートを追加できます。 Active Directory スキーマの変更の詳細については、http://technet.microsoft.com/en-us/library/bb727064.aspx にある記事を参照してください。

Active Directory サーバで次の手順が実行します。

（注） この例では CiscoAVPair という名前のカスタム アトリビュートを作成しますが、CIMC のユーザ ロールとロケールにマップされた既存の LDAP アトリビュートを使用することもできます。

手順

ステップ 1 Active Directory 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 Active Directory 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アトリビュートを追加します。

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 Active Directory スナップインを使用して、ユーザ クラスに CiscoAVPair アトリビュートを追加します。

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 アトリビュートを選択します。

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 アトリビュートに追加します。

ロール	CiscoAVPair アトリビュート値
admin	shell:roles="admin"
user	shell:roles="user"
read-only	shell:roles="read-only"

（注） アトリビュート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 にある記事を参照してください。

次の手順

CIMC を使用して Active Directory を設定します。

CIMC での Active Directory の設定

ローカル ユーザの認証と許可に Active Directory サーバを使用するには、CIMC で Active Directory を設定します。

操作を行う前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ldap**	Active Directory コマンド モードを開始します。
ステップ 2	Server /ldap # **set enabled** {**yes** | **no**}	Active Directory をイネーブルまたはディセーブルにします。 Active Directory をイネーブルにすると、すべてのユーザ認証とロール許可は Active Directory によって実行され、CIMC はローカル ユーザ データベースを無視します。 （注） CIMC と Active Directory の接続を確立できない場合、CIMC はローカル ユーザ データベースの使用に戻ります。
ステップ 3	Server /ldap # **set server-ip** *ip-address*	Active Directory サーバの IP アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 4	Server /ldap # **set timeout** *seconds*	CIMC が Active Directory への接続を確立できないと判断するまで待機する秒数を指定します。
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 Active Directory に送信す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*	すべてのユーザが属する必要のあるドメインを指定します。
ステップ 7	Server /ldap # **set attribute** *name*	ユーザのロールとロケール情報を保持する LDAP アトリビュートを指定します。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、このアトリビュート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 アトリビュートを使用するか、CiscoAVPair アトリビュートなど、次のアトリビュート ID を持つカスタム アトリビュートを作成できます。 `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 アクセスは read-only に制限されます。
ステップ 8	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 9	Server /ldap # **show** [**detail**]	（任意）Active Directory の設定を表示します。

次に、CiscoAVPair アトリビュートを使用して Active Directory を設定する例を示します。

```
Server# scope ldap
Server /ldap # set enabled yes
Server /ldap *# set server-ip 10.10.10.123
Server /ldap *# set timeout 60
Server /ldap *# set encrypted on
Server /ldap *# set base-dn example.com
Server /ldap *# set attribute CiscoAVPair
Server /ldap *# commit
Server /ldap # show
Server IP       BaseDN       Encrypted Timeout  Enabled Attribute
--------------- ------------ --------- -------- ------- ------------
10.10.10.123    example.com  yes       60       yes     CiscoAvPair

Server /ldap #
```

ユーザ セッションの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **show user-session**	現在のユーザ 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
ID	セッションの固有識別情報。
Name	ユーザのユーザ名。
IP Address	ユーザがサーバにアクセスした IP アドレス。
Type	ユーザがサーバにアクセスした方法。
Killable	ユーザ アカウントに admin 権限があり、関連付けられているユーザセッションを強制的に終了できる場合は、このカラムに yes 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） 現在のセッションを終了することはできません。

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

操作を行う前に

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

	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** *session-number*	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。

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 7 章

ネットワーク関連の設定

この章の構成は、次のとおりです。

サーバの NIC の設定

サーバの NIC

CIMC への接続には、2 種類の NIC モードを使用できます。 一方のモードでは、プラットフォームに応じて、active-active または active-standby の冗長化モードを選択することもできます。

NIC モード

CIMC ネットワークの設定により、CIMC に到達できるポートが決定します。 プラットフォームに応じて、次のネットワーク モード オプションを使用できます。

- 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、LAN On Motherboard（LOM; マザーボードのオンボード LAN）イーサネット ホスト ポートを経由した場合だけ使用できます。

（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。

- Shipping（サポートされている場合）：CIMC への接続は、制限された出荷時デフォルト設定を使用して、管理イーサネット ポートを経由して使用できます。

（注） shipping モードは、CIMC への初期接続の目的だけに用意されています。 運用時には別のモードを設定します。

NIC 冗長化

CIMC ネットワーク冗長化の設定により、NIC 冗長化の処理方法が決定します。

- None：冗長化は使用できません。
- Active-Active：すべてのイーサネット ポートが同時に動作します。 このモードは、CIMC への複数のパスを提供します。
- Active-Standby：1 つのポートから別のポートにフェールオーバーします。

使用できる冗長化モードは、選択されているネットワーク モードとプラットフォームによって異なります。 使用できるモードについては、プラットフォームのインストレーションおよびサービス ガイドを参照してください。

サーバ NIC の設定

NIC モードと NIC 冗長化を設定する場合は、サーバの NIC を設定します。

操作を行う前に

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

	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** | **shipping**}	NIC モードを次のいずれかに設定します。 • Dedicated：CIMC へのアクセスに管理イーサネット ポートを使用します。 • Shared LOM：CIMC へのアクセスに LAN On Motherboard（LOM; マザーボードのオンボード LAN）イーサネット ホスト ポートを使用します。

	コマンドまたはアクション	目的
		（注） Shared LOM を選択した場合は、すべてのホスト ポートが同じサブネットに属することを確認してください。 • Shipping：初期接続用の制限付き設定。 通常の操作には、別のモードを選択します。
ステップ 4	Server /cimc/network # **set redundancy** {**none** | **active-active** | **active-standby**}	NIC モードが Shared LOM である場合に、NIC 冗長モードを設定します。 冗長モードは、次のいずれかになります。 • none：LOM イーサネット ポートは単独で動作し、問題が生じた場合もフェールオーバーしません。 • active-active：サポートされている場合は、すべての LOM イーサネット ポートが利用されます。 • active-standby：1 つの LOM イーサネット ポートに障害が発生すると、トラフィックは別の LOM ポートにフェールオーバーします。
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。

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 dedicated
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。

操作を行う前に

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

	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。

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

操作を行う前に

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

	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。

	コマンドまたはアクション	目的
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。
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。

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 yes
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: yes
    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 #
```

サーバ VLAN の設定

操作を行う前に

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

	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。

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、Denial of Service（DoS; サービス拒絶）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。

操作を行う前に

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

	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**	IP ブロッキング コマンド モードを開始します。
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。

	コマンドまたはアクション	目的
		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。

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 #
```

第 8 章

コミュニケーション サービスの設定

この章の構成は、次のとおりです。

HTTP の設定

操作を行う前に

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

	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。
ステップ 3	Server /http # **set http-port** *number*	HTTP 通信に使用するポートを設定します。 デフォルトは 80 です。
ステップ 4	Server /http # **set https-port** *number*	HTTPS 通信に使用するポートを設定します。 デフォルトは 443 です。
ステップ 5	Server /http # **set timeout** *seconds*	HTTP 要求の間、CIMC がタイム アウトしてセッションを終了するまで待機する秒数を設定します。

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

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

操作を行う前に

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

	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。

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 #
```

IPMI Over LAN の設定

IPMI Over LAN

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 Baseboard Management Controller（BMC; ベースボード管理コントローラ）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。

操作を行う前に

IPMI over LAN 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

	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。

	コマンドまたはアクション	目的
ステップ 3	Server /ipmi # **set privilege-level** {**readonly** | **user** | **admin**}	IPMI を使用してシステムにアクセスするユーザに割り当てる必要のあるユーザ ロールを指定します。ユーザ 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。 • 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。 （注） このフィールドの値は、ログインを試みるユーザに割り当てられているロールと正確に一致する必要があります。 たとえば、このフィールドを readonly に設定した場合に、admin ロールを持つユーザが IPMI を使用してログインを試みると、ログインできません。
ステップ 4	Server /ipmi # **set encryption-key** *key*	IPMI 通信に使用する IMPI 暗号キーを設定します。 キーの値は、40 個の 16 進数であることが必要です。
ステップ 5	Server /ipmi # **commit**	トランザクションをシステムの設定にコミットします。

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 #
```

第 9 章

証明書の管理

この章の構成は、次のとおりです。

サーバ証明書の管理

Certificate Signing Request（CSR; 証明書署名要求）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 Certificate Authority（CA; 認証局）、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。

手順

	コマンドまたはアクション	目的
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。	

	コマンドまたはアクション	目的
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

操作を行う前に

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

	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**	Certificate Signing Request（CSR; 証明書署名要求）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。

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
```

次の手順

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 Certificate Authority（CA; 認証局）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、次を参照してください。 http://www.openssl.org

（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。

操作を行う前に

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 コンフィギュレーション 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 コンフィギュレーション ファイル openssl.conf には、"nsCertType = server" という文が含まれています。

	コマンドまたはアクション	目的
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。

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 #
```

次の手順

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

操作を行う前に

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

	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。

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 10 章

プラットフォームイベントフィルタの設定

この章の構成は、次のとおりです。

プラットフォーム イベント フィルタ

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

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

プラットフォーム イベント アラートのイネーブル化

手順

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

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
SNMP Community String Platform Event Enabled
--------------------- ----------------------
public                yes

Server /fault #
```

プラットフォーム イベント アラートのディセーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope fault**	障害コマンド モードを開始します。
ステップ 2	Server /fault # **set platform-event-enabled 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。
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。

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
```

プラットフォーム イベント フィルタの設定

```
Server /fault *# commit
Server /fault # show
SNMP Community String Platform Event Enabled
--------------------- ------------------------
public                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	電圧警告アサート フィルタ
5	電流アサート フィルタ
6	ファン緊急アサート フィルタ
7	ファン警告アサート フィルタ
8	プロセッサ アサート フィルタ
9	電源緊急アサート フィルタ
10	電源警告アサート フィルタ
11	電源冗長性損失フィルタ
12	ディスクリート電源アサート フィルタ
13	メモリ アサート フィルタ
14	ドライブ スロット アサート フィルタ

プラットフォーム イベント フィルタの設定

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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：アラートは送信されますが、他の処理は実行されません。 • reboot：アラートが送信され、サーバが再起動されます。 • power-cycle：アラートが送信され、サーバの電源が再投入されます。 • power-off：アラートが送信され、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。
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。

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 13
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
--------------------- ---------------------------- ----------- ------------------
13                    Memory Assert Filter         reboot      yes

Server /fault/pef #
```

次の手順

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

SNMP トラップ設定の指定

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope fault**	障害コマンド モードを開始します。
ステップ 2	Server /fault # **set community-str** *string*	トラップ情報の送信先となる SNMP コミュニティの名前を入力します。
ステップ 3	Server /fault # **scope trap-destination** *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 ～ 4 の範囲の整数です。
ステップ 4	Server /fault/trap-destination # **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 5	Server /fault/trap-destination # **set 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 6	Server /fault/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。

次に、SNMP トラップ宛先を設定する例を示します。

```
Server# scope fault
Server /fault # set community-str public
Server /fault *# scope trap-destination 1
Server /fault/trap-destination # set enabled yes
Server /fault/trap-destination *# set addr 10.20.30.41
Server /fault/trap-destination *# commit
Server /fault/trap-destination # show
Trap Destination IP Address       Enabled
---------------- ---------------- --------
1                10.20.30.41      yes

Server /fault/trap-destination #
```

第 11 章

CIMC ファームウェア管理

この章の構成は、次のとおりです。

ファームウェアの概要

C シリーズサーバは、cisco.com からダウンロードされたファームウェアを使用します。このファームウェアでは、C シリーズ サーバのファームウェアをアップグレードすることがシスコによって認可されています。

ダウンロードするファームウェアは、.zip ファイルにパッケージ化されています。 シスコからファームウェアの .zip ファイルをダウンロードした後、これを使用してサーバのファームウェアを更新することができます。また、シスコでは各イメージのリリース ノートも提供しており、イメージを取得したのと同じ Web サイトから入手できます。

警告 .zip ファイルを使用してサーバの再イメージ化を行わないでください。

再イメージ化には .bin ファイルを使用します。 この .zip ファイルから適切な .bin アップグレード ファイルを展開する必要があります。 この .bin ファイルは、TFTP サーバまたはローカル マシンに展開できます。

（注） ファームウェアを更新するときは、古いバージョンのファームウェアを新しいバージョンのファームウェアにアップグレードすることも、新しいバージョンのファームウェアを古いバージョンのファームウェアにダウングレードすることもできます。

CIMC は、サーバの実行中にアップタイムに影響を与えることなくファームウェアをコンポーネントにインストールできるように、ファームウェアの更新プロセスを段階的に分けています。 アクティブにするまでサーバを再起動する必要がないため、夜間やその他のメンテナンス期間にこのタスクを実行することができます。 ファームウェアの更新は、次の段階で行われます。

インストール

この段階では、CIMC は選択されたファームウェア バージョンをサーバに転送します。 インストールプロセスでは、サーバ上の非アクティブ スロット内のファームウェアが常に上書きされます。 ファームウェアは次のいずれかの方法でインストールできます。

- ブラウザ クライアント経由：コンピュータ上でファームウェア イメージを参照し、サーバにインストールすることができます。
- TFTP サーバから：TFTP サーバにあるファームウェア イメージをインストールできます。

アクティブ化

この段階では、CIMC は非アクティブのファームウェア バージョンをアクティブとして設定し、サーバを再起動します。 サーバを再起動すると、非アクティブ スロットはアクティブ スロットになり、アクティブ スロットは非アクティブ スロットになります。 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となります。

シスコからの CIMC ファームウェアの取得

手順

ステップ 1 cisco.com に移動します。

ステップ 2 最上部のツールバーで、[Support] をクリックし、ドロップダウン メニューから [Software Download] を選択します。

ステップ 3 左下隅にある [Unified Computing] リンクをクリックしてからログインします。

ステップ 4 [Cisco C-Series Rack-Mount Servers] ノードを展開します。
次のリンクが表示されます。

- Cisco UCS C250 M1 Extended-Memory Rack-Mount Server
- Cisco UCS C210 M1 General-Purpose Rack-Mount Server
- Cisco UCS C200 M1 High-Density Rack-Mount Server

ステップ 5 適切なリンクをクリックします。

ステップ 6 [Unified Computing System (UCS) Integrated Management Controller Firmware] リンクをクリックしてから、適切なリリース バージョンのリンクをクリックします。

ステップ 7 [Download Now] をクリックします。

[Download Cart] ダイアログボックスが表示されます。

ステップ 8 [Download Cart] ダイアログボックスの情報を確認してから、[Proceed with Download] をクリックします。
[Software Download Rules] ページが表示されます。

ステップ 9 ダウンロード ルールを確認してから、[Agree] をクリックします。
ダウンロード内容を示すダイアログボックスが表示されます。 [Select Location] ダイアログボックスも表示されます。 このダイアログボックスにフォーカスが置かれます。

ステップ 10 [Select Location] ダイアログボックスで場所を選択し、[Open] をクリックします。
ダウンロードが開始します。

ステップ 11 ダウンロードが終了したら、[Close] をクリックします。
ダウンロードしたファイルは、.zip ファイルです。

警告 .zip ファイルを使用してサーバの再イメージ化を行わないでください。

再イメージ化には .bin ファイルを使用します。 この .zip ファイルから適切な .bin アップグレード ファイルを展開する必要があります。 この .bin ファイルは、TFTP サーバまたはローカル マシンに展開できます。

展開した適切な .bin ファイルの名前は、再イメージ化しているモデル サーバによって異なります。 1.0.2 ファームウェアの更新ファイルの例を次のとおりです。

- C200 および C210：upd-pkg-c200-m1-cimc.full.1.0.2.bin
- C250：upd-pkg-c250-m1-cimc.full.1.0.2.bin

次の手順

CIMC ファームウェアをサーバにインストールします。

TFTP サーバからの CIMC ファームウェアのインストール

操作を行う前に

シスコから CIMC ファームウェアを取得し、そのファイルをローカル TFTP サーバに保存します。

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope firmware**	CIMC ファームウェア コマンド モードを開始します。
ステップ 3	Server /cimc/firmware # **update** *tftp-ip-address path-and-filename*	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。
ステップ 4	（任意）Server /cimc/firmware # **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。

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 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/firmware #
```

次の手順

新しいファームウェアをアクティブにします。

インストールされているファームウェアのアクティブ化

操作を行う前に

CIMC ファームウェアをサーバにインストールします。

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope firmware**	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 # **show** [**detail**]	使用可能なファームウェア イメージおよびステータスを表示します。
ステップ 4	Server /cimc/firmware # **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。

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 # scope firmware
Server /cimc/firmware # 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/firmware # activate 1
```

第 12 章

ログの表示

この章の構成は、次のとおりです。

CIMC ログ

CIMC ログの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope log**	CIMC ログ コマンド モードを開始します。
ステップ 3	Server /cimc/log # **show entries** [**detail**]	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。

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

	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。

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
```

システム イベント ログ

システム イベント ログの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope sel**	System Event Log（SEL; システム イベント ログ）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 /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。

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

	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。

	コマンドまたはアクション	目的
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。

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
```

第 13 章

サーバ ユーティリティ

この章の構成は、次のとおりです。

テクニカル サポート データのエクスポート

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope tech-support**	テクニカル サポート コマンド モードを開始します。
ステップ 3	Server /cimc/tech-support # **set tftp-ip** *ip-address*	サポート データ ファイルを保存する必要のある TFTP 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 path** *path/filename*	サーバでサポート データを保存する必要のある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、TFTP ツ

	コマンドまたはアクション	目的
		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 # **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 /cimc/tech-support # **start**	TFTP 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 7	Server /cimc/tech-support # **cancel**	（任意）TFTP 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。

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 tftp-ip 10.20.30.41
Server /cimc/tech-support *# set path /user/user1/supportfile
Server /cimc/tech-support *# commit
Server /cimc/tech-support # start
```

次の手順

生成されたレポート ファイルを Cisco TAC に提供します。

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

	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。 Telnet はディセーブルになります。
- CIMC GUI へのアクセス用に、HTTPS がイネーブルになっている。
- 単一のユーザ 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。

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 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 Power-On Self Test（POST; 電源投入時自己診断テスト）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

	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**	CIMC を再起動します。

次に、CIMC を再起動する例を示します。

```
Server# scope cimc
Server /cimc # reboot
```

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

	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。

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

Server /bios #
```

破損した BIOS のリカバリ

操作を行う前に

- 破損した BIOS を回復するには、admin としてログインしている必要があります。
- BIOS リカバリ ISO イメージを準備します。 BIOS リカバリ ISO イメージは、ファームウェア配布パッケージの Recovery フォルダ内にあります。
- リカバリ手順の最後にサーバの電源が再投入されるため、サーバのダウンタイムをスケジュール設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	bios コマンド モードを開始します。
ステップ 2	Server# **recover**	BIOS リカバリ イメージのロードに関するダイアログを起動します。

次に、破損した BIOS を回復する例を示します。

```
Server# scope bios
Server /bios # recover
This operation will automatically power on the server to perform BIOS FW recovery.
Continue?[y|N]y
```

次の手順

電源を再投入するか、サーバをリセットします。

索 引

い

お

か

き

こ

さ

し

す

せ

て

ね

ふ

め

ゆ

り

ろ