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 2.0

初版：2014 年 05 月 19 日

最終更新：2016 年 03 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/

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

目 次

はじめに

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

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、フィールドのラベルのようなGUI要素は、[GUI 要素] のように示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトルのようなメイン タイトルは、[メイン タイトル] のように示しています。
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。
TUI 要素	テキストベースのユーザ インターフェイスでは、システムによって表示されるテキストは、`courier` フォントで示しています。

テキストのタイプ	説明
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、ボールド体（**bold**）で示しています。 CLI コマンド内の変数は、イタリック体（*italic*）で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。stringの前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

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

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

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

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

警告 IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger.You are in a situation that could cause bodily injury.Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Cisco UCS の関連ドキュメント

ドキュメント ロードマップ

すべての B シリーズ マニュアルの完全なリストについては、http://www.cisco.com/go/unifiedcomputing/b-series-doc で入手可能な『*Cisco UCS B-Series Servers Documentation Roadmap*』を参照してください。

すべての C シリーズ マニュアルの一覧については、http://www.cisco.com/go/unifiedcomputing/c-series-doc で入手できる『*Cisco UCS C-Series Servers Documentation Roadmap*』を参照してください。

管理用の UCS Manager と統合されたラック サーバでサポートされるファームウェア バージョンとサポートされる UCS Manager バージョンについては、『Release Bundle Contents for Cisco UCS Software』を参照してください。

その他のマニュアル リソース

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 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 サーバには、次のモデルがあります。

- Cisco UCS C200 ラックマウント サーバ
- Cisco UCS C210 ラックマウント サーバ
- Cisco UCS C220 ラックマウント サーバ
- Cisco UCS C240 ラックマウント サーバ
- Cisco UCS C250 ラックマウント サーバ
- Cisco UCS C260 ラックマウント サーバ
- Cisco UCS C460 ラックマウント サーバ
- Cisco UCS C420 ラックマウント サーバ
- Cisco UCS C3160 ラックマウント サーバ
- Cisco UCS C220 M4 ラックマウント サーバ
- Cisco UCS C240 M4 ラックマウント サーバ

（注） どの Cisco UCS C シリーズ ラックマウント サーバがこのファームウェア リリースでサポートされているかを判断するには、関連するリリース ノートを参照してください。C シリーズのリリース ノートは、次の URL にあります。http://www.cisco.com/en/US/products/ps10739/prod_release_notes_list.html

サーバ ソフトウェアの概要

Cisco UCS C シリーズ ラックマウント サーバには Cisco IMC ファームウェアが付属しています。

Cisco IMC ファームウェア

Cisco IMC は、マザーボードに組み込まれている独立した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 とは別に、Cisco IMC ファームウェアを実行します。システムには Cisco IMC ファームウェアの実行バージョンが付属しています。Cisco IMC ファームウェアは更新できますが、初期インストールは必要ではありません。

サーバ OS

Cisco UCS C シリーズ ラック サーバは、Windows、Linux、Oracle などのオペレーティング システムをサポートします。サポートされているオペレーティング システムの詳細については、スタンドアロン *C* シリーズ サーバのハードウェアおよびソフトウェア相互運用性（http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html）を参照してください。KVM コンソールおよび vMedia を使ってサーバに OS をインストールするために、Cisco IMC を使用できます。

（注） 使用可能な OS のインストール マニュアルには、http://www.cisco.com/go/unifiedcomputing/c-series-doc で『*Cisco UCS C-Series Servers Documentation Roadmap*』からアクセスできます。

Cisco Integrated Management Controller

Cisco IMC は、C シリーズ サーバ用の管理サービスです。Cisco IMC はサーバ内で動作します。

（注） Cisco IMC 管理サービスは、サーバがスタンドアロン モードで動作している場合にだけ使用されます。C シリーズ サーバが UCS システムに統合されている場合は、UCS Manager を使用してそのサーバを管理する必要があります。UCS Manager の使用方法については、http://www.cisco.com/go/unifiedcomputing/b-series-doc の『*Cisco UCS B-Series Servers Documentation Roadmap*』にリストされた設定ガイドを参照してください。

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 または XML ベースの API 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。

- Cisco IMC CLI を呼び出すために Cisco IMC GUI を使用する
- Cisco IMC CLI で呼び出したコマンドを Cisco IMC GUI に表示する
- Cisco IMC GUI から Cisco IMC CLI 出力を生成する

Cisco IMC で実行可能なタスク

Cisco IMC 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、SNMP 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
- Cisco IMC 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
- タイム ゾーンを設定し、ローカル タイムを表示する
- Cisco IMC ファームウェアをインストールしてアクティブにする
- BIOS ファームウェアをインストールしてアクティブにする
- CMC ファームウェアをインストールしてアクティブにする

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

Cisco IMC 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 Cisco IMC 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

Cisco IMC CLI

Cisco IMC 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。SSH または Telnet を使用し、ネットワークを介して Cisco IMC CLI を起動し、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、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 #
boot-device	BIOS モードから **scope boot-device** コマンド	/bios/boot-device #
certificate	EXEC モードから **scope certificate** コマンド	/certificate #
chassis	EXEC モードから **scope chassis** コマンド	/chassis #
adapter	シャーシ モードから **scope adapter***index* コマンド	/chassis/adapter #
host-eth-if	アダプタ モードから **scope host-eth-if** コマンド	/chassis/adapter/host-eth-if #
host-fc-if	アダプタ モードから **scope host-fc-if** コマンド	/chassis/adapter/host-fc-if #
port-profiles	アダプタ モードから **scope port-profiles** コマンド	/chassis/adapter/port-profiles #
vmfex	アダプタ モードから **scope vmfex***index* コマンド	/chassis/adapter/vmfex #
dimm-summary		/chassis/dimm-summary #

モード名	アクセスするコマンド	モード プロンプト
	シャーシ モードから **scope dimm-summary***index* コマンド	
flexflash	シャーシ モードから **scope flexflash***index* コマンド	/chassis/flexflash #
operational-profiles	flexflash モードから **scope operational-profile** コマンド	/chassis/flexflash/operational-profile #
storageadapter	シャーシ モードから **scope storageadapter***slot* コマンド	/chassis/storageadapter #
physical-drive	storageadapter モードから **scope physical-drive** コマンド	/chassis/storageadapter/physical-drive #
virtual-drive	storageadapter モードから **scope virtual-drive** コマンド	/chassis/storageadapter/virtual-drive #
cimc	EXEC モードから **scope cimc** コマンド	/cimc #
firmware	cimc モードから **scope firmware** コマンド	/cimc/firmware #
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 #
fault	EXEC モードから **scope fault** コマンド	/fault #

モード名	アクセスするコマンド	モード プロンプト
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 #
role-group	ldap モードから **scope role-group** コマンド	/ldap/role-group #
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-destinations	snmp モードから **scope trap-destinations** コマンド	/snmp/trap-destinations #
v3users	snmp モードから **scope v3users** コマンド	/snmp/v3users #
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 #

モード名	アクセスするコマンド	モード プロンプト
`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 #
`xmlapi`	EXEC モードから **scope xmlapi** コマンド	/xmlapi #
`dimm-blacklisting`	EXEC モードから **scope dimm-blacklisting** コマンド	/dimm-blacklisting #
`reset-ecc`	EXEC モードから **scope reset-ecc** コマンド	/ reset-ecc #

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 つずつ表示して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、Enter を押す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、出力情報を表示するための 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。

- Default：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、http://www.yaml.org/about.html を参照してください。

ほとんどの CLI コマンド モードで、**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。

スマート アクセス（シリアル）

スマート アクセス（シリアル）では、コマンド ライン インターフェイス（CLI）を使用し、シリアル接続を通じて C シリーズ サーバをオフラインで設定できます。このセットアップでは、コマンド ライン インターフェイスにアクセスするために Cisco IMC をネットワークに接続する必要はありません。

KVM ドングル（DB9）を使用するか、またはシャーシの背面にあるシリアル ポート（RJ-45）を使用してシリアル接続にアクセスできます。

このセットアップを完了し、BIOS と OS メッセージがコンソールに表示されたら、Esc+9 を押すことで Cisco IMC CLI を表示できます。Cisco IMC ユーザ クレデンシャルを使用して接続を認証する必要があります。デフォルトのユーザ名は admin、デフォルトのパスワードは password です。同じコンソールで BIOS または OS に戻すには、Esc+8 を押します。

セッションが作成されると、そのセッションが [Web UI Sessions] タブにシリアル接続として表示されます。

（注） シリアル接続で CLI を使用している間は、次の制限に注意してください。

- 矢印キーを使用して、以前に実行したコマンドに戻すことはできません。
- 端末タイプが [VT100+] または [VTUFT8] のいずれかに設定されている場合、CLI は表示されません。

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しなかった場合、? と入力すると、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た後に ? と入力すると、コマンド構文の現在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。

Cisco IMC へのログイン

手順

ステップ 1 コンソール ポートに接続します。

ステップ 2 未設定のシステムに対する初めてログインする場合は、ユーザ名に **admin**、パスワードに **password** を使用します。
CLI に初めてログインする場合は、次のようになります。

- Cisco IMC Web UI または CLI でデフォルトの管理者クレデンシャルを変更するまでは、操作を実行できません。

（注） Cisco IMC のバージョン 1.5(x) または 2.0(1) から最新のバージョンにアップグレードするか、または初期設定へのリセットを行った場合、最初のログイン時に Cisco IMC はパスワードの変更を求めます。新しいパスワードとして単語「password」を選択することはできません。実行するスクリプトでこの制限が問題になる場合は、ユーザ管理オプションに再びログインしてパスワードを password に変更できますが、これに伴うリスクは完全に自分の責任となります。シスコでは推奨していません。

次に、Cisco IMC に初めてログインする例を示します。

```
Login as # admin
admin10.101.255.255's password # password

**********************WARNING******************
Default credentials were used for login.
Administration passwords needs to be changed for security purpose.
*****************************************************************

Enter current password # abcxyz
Re-enter new password # abcxyz
Updating password...
Password updated successfully.
Server #
```

第 2 章

サーバ OS のインストール

この章は、次の項で構成されています。

OS のインストール方法

C シリーズ サーバは、複数のオペレーティング システムをサポートしています。インストールされている OS 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

KVM コンソール

KVM コンソールは Cisco IMC 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（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
- 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（ISO または IMG ファイル）
- ネットワーク上の 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 OS をインストールできます。

（注） Cisco UCS C3260 サーバに KVM コンソールを正常に設定するには、Cisco IMC、CMC および BMC コンポーネントの IP アドレスを設定する必要があります。CLI インターフェイスまたは Web UI を使用してこれらのコンポーネントの IP アドレスを設定できます。CLI の場合は、コマンド **scope network** を使用するか、または **scope <chassis/server1/2><cmc/bmc><network>** を使用して設定を表示します。

Web インターフェイスでネットワーク コンポーネントの IP アドレスを設定するには、「ネットワーク関連の設定」の項に記載する手順を参照してください。

（注） KVM コンソールの操作には、GUI 以外は使用できません。KVM コンソールの起動手順については、『*Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*』を参照してください。

KVM コンソールを使用した OS のインストール

KVM コンソールは GUI によってのみ操作されるため、CLI を使用してサーバ OS 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 OS をインストールするには、『*Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*』の「Installing an OS Using the KVM Console」の項の手順に従います。

（注） Linux、VMware、および Windows のインストールの詳細なガイドについては、次の URL を参照してください。http://www.cisco.com/en/US/products/ps10493/products_installation_and_configuration_guides_list.html

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 OS 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 OS 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、OS 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、OS、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OS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 OS のインストール

はじめる前に

- VLAN 経由でサーバに到達できることを確認します。
- OSをインストールするには、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

ステップ 1 PXE のブート順を最初に設定します。

ステップ 2 サーバをリブートします。
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 OS のインストレーション ガイドを参照してください。

次の作業

OS の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。

USB ポートからのオペレーティング システムの起動

すべての Cisco UCS C シリーズ サーバでは、サーバ上の任意の USB ポートからオペレーティング システムを起動できます。ただし、USB ポートから OS を起動する前に、いくつかのガイドラインを考慮する必要があります。

- ブート順序の設定を保持するために、内部 USB ポートを使って OS を起動することをお勧めします。

- USB ポートから OS を起動する前に、そのポートを有効にしておく必要があります。

  デフォルトでは、USB ポートは無効になっています。USB ポートを無効化している場合、そこから OS を起動する前に有効にする必要があります。無効化された USB ポートを有効にする方法については、サーバ固有のインストールおよびサービス ガイドにある『内部 *USB* ポートの有効化または無効化』のトピックを参照してください。次のリンクを利用できます。

  http://www.cisco.com/en/US/products/ps10493/prod_installation_guides_list.html。

- USB ポートから OS を起動した後、その USB ソースからサーバが毎回ブートするよう、下位レベルのブート順序を設定する必要があります。

  ブート順序の設定については、レガシー ブート順の設定 を参照してください。

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。

ロケータ LED の切り替え

はじめる前に

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 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 #
```

シャーシの前面ロケータ LED の切り替え

このオプションを使用できるのは一部の UCS C シリーズ サーバだけです。

はじめる前に

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 # **scopechassis**	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 front-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 front-locator-led off
Server /chassis *# commit
```

```
Server /chassis #
```

ハード ドライブのロケータ LED の切り替え

このアクションを使用できるのは一部の UCS C シリーズ サーバだけです。

はじめる前に

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 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 hdd**	ハード ディスク ドライブ（HDD）コマンド モードを開始します。
ステップ 3	Server /chassis/hdd # **setlocateHDD***drivenum* {**1** | **2**}	ここで、*drivenum* は、ロケータ LED を設定するハード ドライブの番号です。値 1 は LED が点灯し、値 2 は LED が消灯します。

次に、HDD 2 のロケータ LED を点灯する例を示します。

```
Server# scope chassis
Server /chassis # scope hdd
Server /chassis/hdd # locateHDD 2 1
HDD Locate LED Status changed to 1
Server /chassis/hdd # show
Name                 Status               LocateLEDStatus
-------------------- -------------------- --------------------
HDD1_STATUS          present              TurnOFF
HDD2_STATUS          present              TurnON
HDD3_STATUS          absent               TurnOFF
HDD4_STATUS          absent               TurnOFF

Server /chassis/hdd #
```

時間帯の選択

タイム ゾーンの選択

タイム ゾーンを選択すると、ローカル タイム ゾーンを選択できるため、デフォルトのマシンの時刻ではなく、ローカル タイムを表示できます。Cisco IMC Web UI および CLI では、希望するタイム ゾーンを選択して設定するオプションが提供されます。

タイムゾーンをローカルタイムに設定すると、システムのタイミングを使用するすべてのサービスにタイム ゾーンの変数が適用されます。これは、ロギング情報に影響し、Cisco IMC の次のアプリケーションで利用されます。

- 障害サマリーと障害履歴のログ
- Cisco IMC のログ
- rsyslog

ローカル タイムを設定すると、表示できるアプリケーションのタイムスタンプが、選択したローカル タイムで更新されます。

タイム ゾーンの選択

はじめる前に

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 # **scopeCIMC**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /CIMC # **timezone-select**	大陸および海洋のリストが表示されます。
ステップ 3	大陸または海洋に対応する番号を入力します。	選択した大陸または海洋のすべての国または地域のリストが表示されます。
ステップ 4	タイム ゾーンとして設定する国または地域に対応する番号を入力します。	国または地域に複数のタイム ゾーンがある場合は、その国または地域のタイム ゾーンのリストが表示されます。
ステップ 5	タイム ゾーンに対応する番号を入力します。	「Is the above information OK?」というメッセージが表示されます。
ステップ 6	1 と入力します。	「Continue?[y|N]:」プロンプトが表示されます。
ステップ 7	選択したタイム ゾーンを設定するには、y を入力します。	選択したタイム ゾーンが Cisco IMC サーバのタイム ゾーンとして設定されます。

次に、タイム ゾーンを設定する例を示します。

```
Server# scope CIMC
Server /CIMC # timezone-select

Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa
```

```
2) Americas
3) Antarctica
4) Arctic Ocean
5) Asia
6) Atlantic Ocean
7) Australia
8) Europe
9) Indian Ocean
10) Pacific Ocean
#? 2
Please select a country whose clocks agree with yours.
1) Anguilla
2) Antigua & Barbuda
3) Argentina
4) Aruba
5) Bahamas
6) Barbados
7) Belize
8) Bolivia
9) Brazil
10) Canada
11) Caribbean Netherlands
12) Cayman Islands
13) Chile
14) Colombia
15) Costa Rica
16) Cuba
17) Curacao
18) Dominica
19) Dominican Republic
20) Ecuador
21) El Salvador
22) French Guiana
23) Greenland
24) Grenada
25) Guadeloupe
26) Guatemala
27) Guyana
28) Haiti
29) Honduras
30) Jamaica
31) Martinique
32) Mexico
33) Montserrat
34) Nicaragua
35) Panama
36) Paraguay
37) Peru
38) Puerto Rico
39) St Barthelemy
40) St Kitts & Nevis
41) St Lucia
42) St Maarten (Dutch part)
43) St Martin (French part)
44) St Pierre & Miquelon
45) St Vincent
46) Suriname
47) Trinidad & Tobago
48) Turks & Caicos Is
49) United States
50) Uruguay
51) Venezuela
52) Virgin Islands (UK)
53) Virgin Islands (US)
#? 49
Please select one of the following time zone regions.
1) Eastern Time
2) Eastern Time - Michigan - most locations
3) Eastern Time - Kentucky - Louisville area
4) Eastern Time - Kentucky - Wayne County
5) Eastern Time - Indiana - most locations
6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
7) Eastern Time - Indiana - Pulaski County
```

```
8) Eastern Time - Indiana - Crawford County
9) Eastern Time - Indiana - Pike County
10) Eastern Time - Indiana - Switzerland County
11) Central Time
12) Central Time - Indiana - Perry County
13) Central Time - Indiana - Starke County
14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
15) Central Time - North Dakota - Oliver County
16) Central Time - North Dakota - Morton County (except Mandan area)
17) Central Time - North Dakota - Mercer County
18) Mountain Time
19) Mountain Time - south Idaho & east Oregon
20) Mountain Standard Time - Arizona (except Navajo)
21) Pacific Time
22) Alaska Time
23) Alaska Time - Alaska panhandle
24) Alaska Time - southeast Alaska panhandle
25) Alaska Time - Alaska panhandle neck
26) Alaska Time - west Alaska
27) Aleutian Islands
28) Metlakatla Time - Annette Island
29) Hawaii
#? 8

The following information has been given:

        United States
        Eastern Time - Indiana - Crawford County

Is the above information OK?
1) Yes
2) No
#? 1

You have chosen to set timezone settings to:

        America/Indiana/Marengo

Continue?[y|N]: y
Timezone has been updated.
The local time now is: Sun Jun 1 02:21:15 2014 EST

Server /CIMC #
```

サーバのブート順の管理

サーバのブート順

Cisco IMC を使用して、使用可能なブート デバイス タイプからサーバがブートを試行する順序を設定できます。レガシー ブート順の設定では、Cisco IMC によりデバイス タイプの並び替えが許可されますが、デバイス タイプ内のデバイスの並べ替えはできません。高精度ブート順の設定により、デバイスの線形順序付けができます。Web UI または CLI では、ブート順およびブート モードの変更、各デバイスタイプ下への複数のデバイスの追加、ブート順の並び替え、各デバイスタイプのパラメータの設定ができます。

ブート順の設定を変更すると、Cisco IMC は、サーバが次にリブートされるときに、設定されたブート順を BIOS に送信します。新しいブート順を実装するには、設定の変更後にサーバをリブートします。新しいブート順は以降のリブートで反映されます。設定されたブート順は、設定が Cisco IMC または BIOS 設定で再度変更されるまで保持されます。

（注） 次のいずれかの条件が発生すると、実際のブート順は設定されたブート順と異なります。

- 設定されたブート順を使用してブートしようとしたときに BIOS で問題が発生した。
- ユーザが BIOS で直接、ブート順を変更した。
- BIOS が、ホストによって認識されているがユーザから設定されていないデバイスを追加した。

（注） ブート順の設定機能を使用して新しいポリシーを作成する場合、BIOS はこの新しいポリシーをシステムのデバイスにマッピングしようとします。実際にマッピングされたデバイス名とポリシー名が [Actual Boot Order] 領域に表示されます。BIOS が Cisco IMC の特定のポリシーにデバイスをマッピングできない場合は、実際のデバイス名が [Actual Boot Order] 領域に [NonPolicyTarget]として示されます。

（注） Cisco IMC を最新のバージョン 2.0(x) に初めてアップグレードすると、レガシー ブート順は高精度ブート順に移行されます。このプロセス中に、前のブート順の設定が削除され、バージョン 2.0 にアップグレードする前に設定されたすべてのデバイス タイプが対応する高精度ブートデバイス タイプに変換され、ダミーのデバイスが同じデバイス タイプ用に作成されます。Web UI の [Configured Boot Order] 領域でこれらのデバイスを確認できます。CLI でこれらのデバイスを表示するには、show boot-device コマンドを入力します。この間に、サーバの実際のブート順が保持され、Web UI と CLI の実際のブート順オプション下で確認できます。

Cisco IMC を 2.0(x) よりも前のバージョンにダウングレードすると、サーバの最後のブート順が保持され、それを [Actual Boot Order] 領域で確認できます。次に例を示します。

- 2.0(x) バージョンでレガシー ブート順でサーバを設定した場合、ダウングレードすると、レガシー ブート順の設定が保持されます。
- 2.0(x) で高精度ブート順でサーバを設定した場合、ダウングレードすると、最後に設定したレガシー ブート順が保持されます。

重要

- 2.0(x) より前のブート順の設定がレガシー ブート順と見なされます。実行中のバージョンが 2.0(x) の場合、Web UI でレガシー ブート順を設定できませんが、CLI および XML API を介して設定できます。CLI では、**set boot-orderHDD,PXE** コマンドを使用して設定できます。CLI または XML API を介してレガシー ブート順を設定できますが、Web UI では設定されたこのブート順は表示されません。
- レガシー ブート順の機能と高精度ブート順の機能は相互に排他的です。レガシー ブート順または高精度ブート順のどちらかを設定できます。レガシー ブート順を設定すると、設定されたすべての高精度ブート デバイスがディセーブルになります。高精度ブート順を設定すると、レガシー ブート順の設定が消去されます。

ブート デバイスの詳細の表示

（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。

はじめる前に

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 # **showboot-device[detail]**.	ブート デバイスの詳細情報を表示します。

次に、作成したブート可能デバイスの詳細情報を表示する例を示します。

```
Server# scope bios
Server /bios # show boot-device
Boot Device          Device Type  Device State       Device Order
-------------------- ------------ ------------------ ----------------
TestUSB              USB          Enabled            1
TestPXE              PXE          Enabled            2
Server /bios # show boot-device detail
Boot Device TestSAN:
    Device Type: SAN
    Device State: Enabled
    Device Order: 1
    Slot Id:
    Lun Id:
Boot Device TestUSB:
```

```
    Device Type: USB
    Device State: Enabled
    Device Order: 2
    Sub Type: HDD
Boot Device TestPXE:
    Device Type: PXE
    Device State: Enabled
    Device Order: 3
    Slot Id: L
    Port Number: 1
```

高精度ブート順の設定

（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。

はじめる前に

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 # **create-boot-device**[*device name*] [*device type*].	BIOS がブートするブート可能デバイスを作成します。次のいずれかになります。 • [HDD]：ハード ディスク ドライブ • [PXE]：PXE ブート • SAN ブート • iSCSI ブート • SD カード （注） SD カード オプションを使用できるのは一部の UCS C シリーズ サーバだけです。 • USB • 仮想メディア • PCHStorage • UEFISHELL

	コマンドまたはアクション	目的
ステップ 3	Server /bios # **scope boot-device***created boot device name*.	作成したブート可能デバイスの管理を入力します。
ステップ 4	Server /bios /boot-device # **set***values*	特定のブート可能なデバイスにプロパティ値を指定します。次のいずれか、または複数を設定できます。 • cli：CLI オプション • state：BIOS がデバイスを認識するかどうか。デフォルトでは、デバイスはディセーブルにされています。 （注） イネーブルである場合、デバイスはレガシーのブート順序の設定を上書きします。 • slot：デバイスが差し込まれるスロットの ID。 • port：デバイスが装着されているスロットのポート。 • LUN：デバイスが装着されているスロットの論理ユニット。 • sub-type：特定のデバイス タイプの下位のサブデバイス タイプ。 • order：デバイスの使用可能なリストにおけるそのデバイスの順序。
ステップ 5	Server /bios /boot-device # **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、ブート順序を設定し、ブート デバイスを作成し、新しいデバイスの属性を設定し、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 #  create boot-device TestPXE PXE
Server /bios #  scope boot-device TestPXE
Server /bios /boot-device #  set state Enabled
Server /bios /boot-device #  set slot L
Server /bios /boot-device #  set port 1
Server /bios /boot-device #  set order 1
Server /bios /boot-device #  commit
Enabling boot device will overwrite Legacy Boot Order configuration
Continue?[y|N]y
Server /bios /boot-device #  y
Commiting device configuration
Server /bios/boot-device # show detail
BIOS:
    BIOS Version: "C240M3.2.0.0.15 (Build Date: 03/16/2014)"
    Boot Order: (none)
    Boot Override Priority:
    FW Update/Recovery Status: None, OK
    UEFI Secure Boot: disabled
    Configured Boot Mode: None
```

```
    Actual Boot Mode: Legacy
    Last Configured Boot Order Source: CIMC

Server /bios/boot-device # show boot-device detail
Boot Device TestPXE:
    Device Type: PXE
    Device State: Enabled
    Device Order: 1
    Slot Id: L
    Port Number: 1
```

次の作業

サーバを再起動して、新しいブート順でブートします。

ブート デバイスの属性の変更

（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。

はじめる前に

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 # **scope boot-device***created boot device name*.	作成したブート可能デバイスの管理を入力します。
ステップ 3	Server /bios /boot-device # **set state** {*Enabled*|*Disabled*}.	デバイスをイネーブルまたはディセーブルにします デフォルトのステートはディセーブルです。 （注） イネーブルである場合、デバイスはレガシーのブート順序の設定を上書きします。
ステップ 4	Server /bios /boot-device* # **set order** {*Index* | *1-50*}.	デバイス リストの特定のデバイスのブート順序を指定します。作成したデバイスの総数に基づいて、1 ～ 50 の範囲の数字を入力します。 （注） ブートデバイス順序を個別に設定すると、設定したとおりに順序が表示されるかの保証はありません。そのため、1 回の実行で複数のデバイスの順序を設定する場合は、**re-arrange-boot-device** コマンドを使用することを推奨します。

	コマンドまたはアクション	目的
ステップ 5	Server /bios /boot-device* # **set port** {*value* | *1-255*}.	デバイスが装着されているスロットのポートを指定します。1～255 の範囲内の数を入力してください。
ステップ 6	Server /bios /boot-device* # **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、既存のデバイスの属性を変更する例を示します。

```
Server# scope bios
Server /bios *# scope boot-device scu-device-hdd
Server /bios/boot-device # set status enabled
Server /bios/boot-device *# set order 2
Server /bios/boot-device *# set port 1
Server /bios/boot-device *# commit
Enabling boot device will overwrite boot order Level 1 configuration
Continue?[y|N]y
Server /bios/boot-device #
```

デバイスのブート順序の並べ替え

（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。

はじめる前に

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 # **rearrangeboot-device**[*device name*]:[*position*].	選択したブート デバイスの順序を 1 回の実行で変更します。

次に、選択したブート デバイスの順序を変更する例を示します。

```
Server# scope bios
Server /bios # rearrange-boot-device  TestPXE:1,TestUSB:2
 Server /bios # show boot-device
Boot Device          Device Type  Device State       Device Order
-------------------- ------------ ------------------ ----------------
TestPXE              PXE          Disabled           1
```

```
TestUSB              USB          Disabled           2

Server /bios #
```

次の作業

ブート順序の設定の再適用

（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。

はじめる前に

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 # **re-apply**.	最後に設定されたブート順の送信元が BIOS の場合は、ブート順序を BIOS に再適用します。

次に、BIOS にブート順序を再適用する例を示します。

```
Server# scope bios
Server /bios # re-apply
Server /bios #
```

次の作業

BIOS にブート順序を再適用した後に、ホストをリブートします。

既存のブート デバイスの削除

（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。

はじめる前に

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 # **remove-boot-device***device name*	特定のデバイスをブート順序から削除します。

次に、選択したデバイスをデバイス リストから削除する例を示します。

```
Server# scope bios
Server /bios # remove-boot-device scu-device-hdd
Server /bios #
```

UEFI セキュア ブートの概要

オペレーティング システムをロードし実行する前に、ロードおよび実行前のすべての EFI ドライバ、EFI アプリケーション、オプション ROM またはオペレーティング システムが確実に署名され信頼性と整合性が確認されるために、Unified Extensible Firmware Interface（UEFI）のセキュア ブートを使用できます。Web UI または CLI を使用して、このオプションをイネーブルにできます。UEFI のセキュア ブート モードをイネーブルにすると、ブート モードは UEFI モードに設定され、UEFI のブート モードがディセーブルになるまで、設定されているブート モードを変更できません。

（注） サポートされていない OS で UEFI セキュア ブートをイネーブルにすると、次の再起動時に、その特定の OS から起動することはできません。前の OS から起動しようとすると、Web UI のシステム ソフトウェア イベントの下にエラーが報告され記録されます。前の OS から起動するには、Cisco IMC を使用して UEFI セキュア ブート オプションをディセーブルにする必要があります。

重要 また、サポートされていないアダプタを使用すると、Cisco IMC SEL のエラー ログ イベントが記録されます。エラー メッセージが次のように表示されます。

System Software event: Post sensor, System Firmware error.EFI Load Image Security Violation.[0x5302] was asserted .

UEFI のセキュア ブートは次のコンポーネントでサポートされます。

コンポーネント	種類
サポートされている OS	• Windows Server 2012 • Windows Server 2012 R2
Broadcom PCI アダプタ	• 5709 デュアルおよびクアッド ポート アダプタ • 57712 10GBASE-T アダプタ • 57810 CNA • 57712 SFP ポート
Intel PCI アダプタ	• i350 クアッド ポート アダプタ • X520 アダプタ • X540 アダプタ • LOM
QLogic PCI アダプタ	• 8362 デュアル ポート アダプタ • 2672 デュアル ポート アダプタ
Fusion-io	
LSI	• LSI MegaRAID SAS 9240-8i • LSI MegaRAID SAS 9220-8i • LSI MegaRAID SAS 9265CV-8i • LSI MegaRAID SAS 9285CV-8e • LSI MegaRAID SAS 9285CV-8e • LSI MegaRAID SAS 9266-8i • LSI SAS2008-8i mezz • LSI Nytro カード

UEFI セキュア ブート モードのイネーブル化

はじめる前に

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 secure-boot enable | disable**	UEFI セキュア ブートを有効または無効にします。 （注） イネーブルにすると、ブート モードが UEFI セキュア モードに設定されます。UEFI セキュア ブート モードがディセーブルになるまでブート モードの設定は変更できません。

次に、UEFI セキュア ブート モードをイネーブルにして、トランザクションをコミットする例を示します。

```
Server# scope bios
Server /bios # set secure-boot enable
Setting Value : enable
Commit Pending.
Server /bios *# commit
UEFI Secure boot state changed successfully. Execute 'show detail' command to check the
current status
Server /bios #
```

次の作業

サーバを再起動してコンフィギュレーション ブート モード設定を有効にします。

UEFI セキュア ブ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 bios**	BIOS コマンド モードを開始します。
ステップ 2	Server/ BIOS # **set secure-boot enable | disable**	UEFI セキュア ブートを有効または無効にします。

次に、UEFI セキュア ブート モードを無効にして、トランザクションをコミットする例を示します。

```
Server# scope bios
Server /bios # set secure-boot disable
Setting Value : enable
Commit Pending.
Server /bios *# commit
UEFI Secure boot state changed successfully. Execute 'show detail' command to check the
current status
Server /bios #
```

次の作業

サーバを再起動してコンフィギュレーション ブート モード設定を有効にします。

サーバの実際のブート順の表示

サーバの実際のブート順とは、サーバが最後にブートされたときに BIOS によって実際に使用されたブート順です。実際のブート順は、Cisco IMC で設定されたブート順とは異なる場合があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scopebios**	bios コマンド モードを開始します。
ステップ 2	Server /bios # **showactual-boot-order[detail]**	サーバが最後に起動したときに実際に BIOS で使用されたブート順序を表示します。

次に、最後のブート以降のレガシー ブート順序の実際のブート順序を表示する例を示します。

```
Server# scope bios
Server /bios #  show actual-boot-order

Boot Order   Type                       Boot Device
------------ ------------------------- -----------------------------------
1            CD/DVD                    CD-ROM
2            CD/DVD                    Cisco   Virtual CD/DVD  1.18
3            Network Device (PXE)      Cisco NIC 23:0.0
4            Network Device (PXE)      MBA v5.0.5  Slot 0100
5            Network Device (PXE)      MBA v5.0.5  Slot 0101
6            Network Device (PXE)      MBA v5.0.5  Slot 0200
7            Network Device (PXE)      MBA v5.0.5  Slot 0201
8            Network Device (PXE)      Cisco NIC 22:0.0
9            Internal EFI Shell        Internal EFI Shell
10           FDD                       Cisco   Virtual HDD     1.18
11           FDD                       Cisco   Virtual Floppy  1.18

Server /bios #
```

次に、最後のブート以降の高精度ブート順序の実際のブート順序を表示する例を示します。

```
Server /bios # show actual-boot-order
Boot Order   Boot Device                          Device Type     Boot Policy
------------ ---------------------------------- --------------- --------------------
1            IBA GE Slot 0201 v1398              PXE             TestPXE
2            IBA GE Slot 0200 v1398              PXE             NonPolicyTarget
3            IBA GE Slot 0202 v1398              PXE             NonPolicyTarget
```

```
4            IBA GE Slot 0203 v1398              PXE              NonPolicyTarget
5            "UEFI: Built-in EFI Shell "         EFI              NonPolicyTarget
Server  /bios #
```

サーバのリセット

重要 ファームウェアまたは BIOS の更新が進行中の場合は、そのタスクが完了するまでサーバをリセットしないでください。

はじめる前に

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 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

重要 ファームウェアまたは BIOS の更新が進行中の場合は、そのタスクが完了するまでサーバをシャットダウンしないでください。

はじめる前に

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 chassis**	シャーシ モードを開始します。
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
```

サーバの電源管理

サーバの電源投入

（注） サーバの電源が Cisco IMC 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、Cisco IMC 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。

重要 ファームウェアまたは BIOS の更新が進行中の場合は、そのタスクが完了するまでサーバの電源を変更しないでください。

はじめる前に

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 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。
ステップ 3	プロンプトで、y を入力して確認します。	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
Warning: System is already powered ON, this action is ineffective.
Do you want to continue?[y|N]y
```

サーバの電源オフ

重要 ファームウェアまたは BIOS の更新が進行中の場合は、そのタスクが完了するまでサーバの電源をオフにしないでください。

はじめる前に

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 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

重要 ファームウェアまたは BIOS の更新が進行中の場合は、そのタスクが完了するまでサーバの電源を再投入しないでください。

はじめる前に

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** 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
```

電力ポリシーの設定

電力の制限

重要 この項が適用されるのは、一部の UCS C シリーズ サーバだけです。

電力制限によって、サーバの電力消費をアクティブに管理する方法が決定されます。電力制限オプションを有効にすると、システムは電力消費をモニタし、割り当てられた電力制限未満の値に電力を維持します。サーバが電力制限を維持できない場合や、プラットフォームの電力を修正用の時間内に指定された電力制限に戻すことができない場合は、電力制限によって、[Power Profile] 領域の [Action] フィールドでユーザが指定したアクションが実行されます。

電力制限が有効になると、定義された属性を使用して、標準または高度な電力プロファイルを持つ複数の電力プロファイルを設定できます。標準の電力プロファイルを選択した場合は、電力制限、修正用時間、是正措置、一時停止期間、ハード キャッピング、およびポリシー状態（有効な場合）を設定できます。高度な電力プロファイルを選択した場合は、標準の電力プロファイルの属性に加えて、ドメイン固有の電力制限、安全なスロットル レベル、周囲温度ベースの電力制限属性も設定できます。

電力特性評価の有効化

このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバだけです。

はじめる前に

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# **scopechassis**	シャーシコマンドモードを開始します。
ステップ 2	Server /chassis # **scopepower-cap-config**	電力制限コマンドモードを開始します。
ステップ 3	Server /chassis # **setrun-pow-char-at-boot**	ブート時に電力特性評価を実行します。
ステップ 4	Server /chassis # **commit**	トランザクションをシステムにコミットします。

次に、ホスト リブート時に電力特性評価を自動的に呼び出す例を示します。

```
Server# scope chassis
Server /chassis# scope power-cap-config
Server /chassis /power-cap-config # set run-pow-char-at-boot
Server /chassis /power-cap-config* # commit
Server /chassis/power-cap-config #
```

電力制限ポリシーの設定

このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバだけです。

はじめる前に

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# **scopechassis**	シャーシコマンドモードを開始します。
ステップ 2	Server /chassis # **scopepower-cap-config**	電力制限コマンドモードを開始します。
ステップ 3	Server /chassis /power-cap-config# **setpow-cap-enable** {**yes** | **no**}	サーバへの電力制限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 /chassis /power-cap-config# **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、電力制限ポリシーをイネーブルにする例を示します。

```
Server# scope chassis
Server /chassis# scope power-cap-config
Server /chassis /power-cap-config # set pow-cap-enable yes
Server /chassis /power-cap-config* # commit
Server /chassis/power-cap-config #
```

標準の電力プロファイルの設定

このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバだけです。

はじめる前に

- 電力制限が有効にされている必要があります。
- 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# **scopechassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scopepower-cap-config**	電力制限コマンド モードを開始します。
ステップ 3	Server /chassis /power-cap-config# **setpow-cap-enable** {**yes** | **no**}	システムの電力制限機能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 /chassis /power-cap-config# **scopepower-profilestandard**	電力プロファイルの標準のコマンドモードを開始します。
ステップ 5	Server /chassis /power-cap-config# **setallow-throttleyes** | **no**	スロットリング状態（T状態）とメモリ スロットルをプロセッサで強制的に使用させるために電力制限を維持するようにシステムを有効または無効にします。
ステップ 6	Server /chassis /power-cap-config# **setcorr-time***value*	**Action** モードで指定したアクションが実行される前に、プラットフォームの電力が指定された電力制限に戻る必要のある時間を設定します。 有効な範囲は 3 ～ 600 秒です。デフォルトは 3 秒です。
ステップ 7	Server /chassis /power-cap-config# **setexcept-actionalert** | **shutdown**	指定した電力制限が修正用の時間内に維持されない場合に実行されるアクションを指定します。次のいずれかになります。 • **Alert**：Cisco IMC SEL にイベントを記録します。

	コマンドまたはアクション	目的
		• **Shutdown**：ホストをグレースフル シャット ダウンします。 • **None**：アクションは実行されません。
ステップ 8	Server /chassis /power-cap-config# **sethard-capyes** | **no**	電力消費を指定した電力制限未満の値に維持するようにシステムを有効または無効にします。
ステップ 9	Server /chassis /power-cap-config# **setpow-limit***value*	電力制限を指定します。 指定した範囲内の値を入力します。
ステップ 10	Server /chassis /power-cap-config# **setsusp-pd** {*h:m-h:m* | |*ll,Mo,Tu,We,Th,Fr,Sa,Su.*}	電力制限プロファイルがアクティブにならない時間を指定します。
ステップ 11	Server /chassis /power-cap-config# **commit**	トランザクションをシステムにコミットします。

次に、標準の電力プロファイルを設定する例を示します。

```
Server# scope chassis
Server /chassis# scope power-cap-config
Server /chassis /power-cap-config # set pow-cap-enable yes
Server /chassis /power-cap-config* # commit
Server /chassis/power-cap-config # scope power-profile advance
Server /chassis/power-cap-config # set allow-throttle yes
Server /chassis/power-cap-config* # set corr-time 6
Server /chassis/power-cap-config* # set except-action alert
Server /chassis/power-cap-config* # set hard-cap yes
Server /chassis/power-cap-config* # set pow-limit 360
Server /chassis/power-cap-config* # set susp-pd 1:30-2:30|All
Server /chassis/power-cap-config* # commit
Server /chassis/power-cap-config #
```

高度な電力プロファイルの設定

これらの設定は、一部の UCS C シリーズ サーバでのみ行うことができます。

はじめる前に

- パワー キャッピングをイネーブルにする必要があります。
- 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# **scopechassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scopepower-cap-config**	電力制限コマンド モードを開始します。
ステップ 3	Server /chassis /power-cap-config# **setpow-cap-enable** {**yes** | **no**}	サーバの電力制限機能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 /chassis /power-cap-config# **commit**	トランザクションをシステムにコミットします。
ステップ 5	Server /chassis /power-cap-config# **scopepower-profileadvance**	電力プロファイルの高度なコマンドモードを開始します。
ステップ 6	Server /chassis /power-cap-config# **setallow-throttle** {**yes** | **no**}	スロットリング状態（T状態）とメモリ スロットルをプロセッサで強制的に使用させるために電力制限を維持するようにシステムを有効または無効にします。
ステップ 7	Server /chassis /power-cap-config# **setcorr-time***value*	**Action** モードで指定したアクションをとる前に、プラットフォームを指定した電力制限に戻すための是正処置を実行する際の最大時間を設定します。 有効な範囲は 3 ～ 600 秒です。デフォルトは 3 秒です。
ステップ 8	Server /chassis /power-cap-config# **setcpu-power-limit***value*	CPU の電力制限を指定します。 指定された範囲内の電力（ワット単位）を入力します。
ステップ 9	Server /chassis /power-cap-config# **setcpu-safe-throttle***value*	CPU のスロットリング レベルを指定します。 有効な範囲は 0 ～ 100 パーセントです。
ステップ 10	Server /chassis /power-cap-config# **setexcept-action** {**alert** | **shutdown**}	指定した電力制限が修正用の時間内に維持されない場合に実行されるアクションを指定します。次のいずれかになります。 • **Alert**：Cisco IMC SEL にイベントを報告します。 • **Shutdown**：ホストをグレースフル シャット ダウンします。 • **None**：アクションは実行されません。

	コマンドまたはアクション	目的
ステップ 11	Server /chassis /power-cap-config# **sethard-cap** {**yes** | **no**}	電力消費を指定した電力制限未満の値に維持するようにシステムを有効または無効にします。
ステップ 12	Server /chassis /power-cap-config# **setmem-pow-limit***value*	メモリの電力制限を指定します。 指定された範囲内の電力（ワット単位）を入力します。
ステップ 13	Server /chassis /power-cap-config# **setmem-safe-Tlvl***value*	メモリのスロットリング レベルを指定します。 有効な範囲は 0 ～ 100 パーセントです。
ステップ 14	Server /chassis /power-cap-config# **setfail-safe-timeout***value*	プラットフォームや CPU の電力読み取りの消失などの内部的な障害で電力制限機能が影響を受けた場合の安全なスロットルポリシーを指定します。 有効な範囲は 1 ～ 10 秒です。
ステップ 15	Server /chassis /power-cap-config# **setplat-safe-Tlvl***value*	プラットフォームのスロットリング レベルをパーセンテージで指定します。 範囲は、0 ～ 100 です。
ステップ 16	Server /chassis /power-cap-config# **setplat-temp***value*	差し込み口の温度センサーを指定します。 摂氏（C°）で値を入力します
ステップ 17	Server /chassis /power-cap-config# **setpow-limit***value*	電力制限を指定します。 指定された範囲内の電力（ワット単位）を入力します。
ステップ 18	Server /chassis /power-cap-config# **setsusp-pd** {*h:m-h:m* | |*ll,Mo,Tu,We,Th,Fr,Sa,Su.*}	電力制限プロファイルがアクティブにならない時間を指定します。
ステップ 19	Server /chassis /power-cap-config# **setthermal-power-limit***value*	維持する電力制限を指定します。 指定された範囲内の電力（ワット単位）を入力します。
ステップ 20	Server /power-cap # **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、高度な電力プロファイル設定を行う例を示します。

```
Server# scope chassis
Server /chassis# scope power-cap-config
Server /chassis /power-cap-config # set pow-cap-enable yes
Server /chassis /power-cap-config* # commit
```

```
Server /chassis/power-cap-config # scope power-profile advance
Server /chassis/power-cap-config # set allow-throttle yes
Server /chassis/power-cap-config* # set corr-time 6
Server /chassis/power-cap-config*# set cpu-power-limit 259
Server /chassis/power-cap-config* # set cpu-safe-Tlvl 50
Server /chassis/power-cap-config* # set except-action alert
Server /chassis/power-cap-config* # set hard-cap yes
Server /chassis/power-cap-config* # set mem-pow-limit 259
Server /chassis/power-cap-config* # set mem-safe-Tlvl 50
Server /chassis/power-cap-config* # set fail-safe-timeout 10
Server /chassis/power-cap-config* # set plat-safe-Tlvl 50
Server /chassis/power-cap-config* # set plat-temp 35
Server /chassis/power-cap-config* # set pow-limit 360
Server /chassis/power-cap-config* # set susp-pd 1:30-2:30|All
Server /chassis/power-cap-config* # set thermal-power-limit 354
Server /chassis/power-cap-config* # commit
Server /chassis/power-cap-config #
```

電力プロファイルのデフォルトへのリセット

このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバだけです。

はじめる前に

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# **scopechassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scopepower-cap-config**	電力制限コマンド モードを開始します。
ステップ 3	Server /chassis # **setreset-power-profile-to-defaults**	電力プロファイルの設定を工場出荷時のデフォルト値にリセットし、電力制限を無効にします。
ステップ 4	Server /chassis # **commit**	トランザクションをシステムにコミットします。

次に、電力プロファイルをデフォルトの設定値にリセットする例を示します。

```
Server# scope chassis
Server /chassis# scope power-cap-config
Server /chassis /power-cap-config # reset-power-profile-to-defaults
Server /chassis /power-cap-config* # commit
Server /chassis/power-cap-config #
```

電力制限設定の表示

このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバだけです。

はじめる前に

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 # **scopechassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **showpower-cap-config**	電力特性評価に関する情報を表示します。

次に、電力制限設定に関する情報を表示する例を示します。

```
Server #scope chassis
Server /chassis # show power-cap-config
Power Capping    Power Characterization at Boot  Power Characterization Status  Min (W) Max
 (W)
---------------- ------------------------------- ------------------------------ ------
------
yes              no                              Completed                      259    580

Server /chassis #
```

電力統計情報の表示

このオプションを使用できるのは一部の UCS C シリーズ サーバだけです。

はじめる前に

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 # **scopechassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **showpower-monitoring**	最後にリブートされてから、サーバ、CPU、およびメモリが使用した電力が表示されます。

次に、個々のドメインの電力統計情報を表示する例を示します。

```
Server #scope chassis
Server /chassis # show power-monitoring
Domain     Current (W)  Minimum (W)  Maximum (W)  Average (W)
```

```
---------- ------------ ------------ ------------ ------------
Platform   180          160          504          180
CPU        53           33           275          53
Memory     2            2            6            2
Server /chassis #
```

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。

はじめる前に

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 # **ScopeCIMC**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /CIMC # **Scopepower-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 # **setpolicy** {**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。これがデフォルトのアクションになります。 • **power-on**：シャーシの電源が回復したときにサーバの電源がオンになります。 • **restore-last-state**：サーバの電源は、シャーシの電源が切断される前の状態に戻ります。 選択したアクションが **power-on** の場合は、サーバに対して電源を回復するまでの遅延を選択できます。
ステップ 4	Server /CIMC/power-restore-policy # **setdelay** {**fixed** | **random**}	（任意） サーバの電源復元までの時間を固定するか、ランダムにするかを指定します。デフォルトは **fixed** です。このコマンドは、電力復元アクションが **power-on** の場合のみ使用可能です。
ステップ 5	Server /CIMC/power-restore-policy # **setdelay-value***delay*	（任意） 遅延時間を秒単位で指定します。指定できる値の範囲は 0 ～ 240 です。デフォルトは 0 です。

	コマンドまたはアクション	目的
ステップ 6	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。

次に、180秒（3分）の固定遅延で電源をオンにする電力復元ポリシーを設定し、トランザクションをコミットする例を示します。

```
Server# scope 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 # set delay fixed
Server /CIMC/power-restore-policy *# set delay-value 180
Server /CIMC/power-restore-policy *# commit
Server /CIMC/power-restore-policy #  show detail
Power Restore Policy:
    Power Restore Policy: power-on
    Power Delay Type: fixed
    Power Delay Value(sec): 180

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

ファン ポリシーの設定

ファン制御ポリシー

ファン制御ポリシーを使ってファンの速度を制御することにより、サーバの消費電力を削減し、ノイズレベルを下げることができます。これらのファンポリシーが導入される前は、いずれかのサーバ コンポーネントの温度が設定済みしきい値を超過した場合に、ファン速度が自動的に増加しました。ファン速度を低く抑えるために、通常、コンポーネントのしきい値温度を高い値に設定しました。この動作はほとんどのサーバ構成に最適でしたが、次のような状況に対処できませんでした。

- 最大の CPU パフォーマンス

  高パフォーマンスを得るには、いくつかのCPUを設定済みしきい値よりもかなり低い温度に冷却する必要があります。これは非常に高速なファン速度を必要とし、結果として電力消費とノイズ レベルが増大しました。

- 低電力消費

  電力消費を最も低く抑えるにはファンを非常に遅くする必要があり、場合によっては、ファン停止をサポートするサーバで完全に停止する必要があります。ただし、ファンの速度を遅くすると、結果としてサーバが過熱します。この状況を回避するには、可能な最低速度よりもやや速くファンを作動させる必要があります。

ファン ポリシーを導入すると、サーバ内のコンポーネントに基づき、そのサーバに適したファン速度を決定できます。さらに、最大のCPUパフォーマンスと低消費電力に関連する問題に対処するために、ファン速度を設定することができます。

次のファン ポリシーの中から選択できます。

- Balanced

  これがデフォルトのポリシーです。この設定でほとんどのサーバ構成を冷却できますが、容易に加熱する PCIe カードを含むサーバには適さない可能性があります。

- パフォーマンス

  この設定は、高パフォーマンスを得るために最高速度でファンを作動させる必要のあるサーバ構成に使用できます。この設定では、Balanced ファン ポリシーと同じ速度またはそれより高速でファンが作動します。

- Low Power

  この設定は、PCIe カードが含まれない最小構成のサーバに最適です。

- High Power

  この設定は、60 ～ 85% の範囲のファン速度を必要とするサーバ構成に使用できます。このポリシーは、容易に過熱して高温になるPCIeカードを含むサーバに最適です。このポリシーで設定される最小ファン速度はサーバ プラットフォームごとに異なりますが、およそ 60 ～ 85% の範囲内です。

- 最大電力

  この設定は、70 ～ 100% の範囲の非常に高いファン速度を必要とするサーバ構成に使用できます。このポリシーは、容易に過熱して非常に高温になる PCIe カードを含むサーバに最適です。このポリシーで設定される最小ファン速度はサーバプラットフォームごとに異なりますが、およそ 70 ~ 100% の範囲内です。

（注） Cisco IMC でファン ポリシーを設定することはできますが、実際のファン作動速度はサーバの構成要件により決定されます。たとえば、ファン ポリシーを [Balanced] に設定しても、容易に加熱する PCIe カードがサーバに含まれる場合は、過熱を防ぐためにサーバのファン速度が必要な最小のファン速度に自動的に調整されます。ファン速度の設定を必要以上に強く設定している場合、システムは選択されたファン速度を保持します。[Applied Fan Policy] には、サーバで実行されている実際のファン速度が表示されます。

[Configuration Status] には、設定されたファン ポリシーのステータスが表示されます。次のいずれかになります。

- [SUCCESS]：選択されたファン ポリシーはサーバで実行されている実際のファン速度に一致します。
- [PENDING]：設定されたファン ポリシーはまだ有効になっていません。これは次のいずれかが原因の可能性があります。
  - サーバの電源がオフになっている

- BIOS POST が完了していない

- [FAN POLICY OVERRIDE]：指定されたファン速度を、サーバの設定要件によって決定された実際の速度で上書きします。

ファン ポリシーの設定

ファンポリシーは、サーバの冷却要件を決定します。ファンポリシーを設定する前に、容易に加熱する PCIe カードがサーバ内にあるかどうかを確認します。

はじめる前に

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 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 fan-policy**	ファン ポリシー コマンド モードを開始します。
ステップ 3	Server /chassis/fan-policy # **set fan-policy**	サーバのファン ポリシーを設定します。次のいずれかを指定できます。 • balanced これがデフォルトのポリシーです。この設定でほとんどのサーバ構成を冷却できますが、容易に加熱する PCIe カードを含むサーバには適さない可能性があります。 • パフォーマンス この設定は、高パフォーマンスを得るために最高速度でファンを作動させる必要のあるサーバ構成に使用できます。この設定では、Balanced ファン ポリシーと同じ速度またはそれより高速でファンが作動します。 • low-power この設定は、PCIe カードが含まれない最小構成のサーバに最適です。 • high-power この設定は、60 ～ 85% の範囲のファン速度を必要とするサーバ構成に使用できます。このポリシーは、容易に過熱して高温になる PCIe カードを含むサーバに最適です。このポリシーで設定される最小ファン速度はサーバ プラット

	コマンドまたはアクション	目的
		フォームごとに異なりますが、およそ 60 ～ 85% の範囲内です。 • maximum-power この設定は、70 ～ 100% の範囲の非常に高いファン速度を必要とするサーバ構成に使用できます。このポリシーは、容易に過熱して非常に高温になる PCIe カードを含むサーバに最適です。このポリシーで設定される最小ファン速度はサーバ プラットフォームごとに異なりますが、およそ 70 ～ 100% の範囲内です。
ステップ 4	Server /chassis/fan-policy # **commit**	サーバへの変更をコミットします。

次に、サーバのファン ポリシーを最大電力に設定する例を示します。

```
server # scope chassis
server /chassis # scope fan-policy
server /chassis/fan-policy # set fan-policy maximum-power
server /chassis/fan-policy* # commit
server /chassis/fan-policy # show detail
  Fan Policy: maximum-power
  Applied Fan Policy: Max Power
  Configuration Status: SUCCESS
server /chassis/fan-policy #
```

Flexible Flash コントローラの管理

Cisco Flexible Flash

C シリーズ ラックマウント サーバ の中には、サーバ ソフトウェア ツールおよびユーティリティのストレージとして、内蔵 Secure Digital（SD）メモリ カードをサポートしているものがあります。この SD カードは Cisco Flexible Flash ストレージ アダプタでホストされます。

Cisco IMC では、単一ハイパーバイザ（HV）パーティション構成として SD ストレージが使用可能です。以前のバージョンでは 4 つの仮想 USB ドライブがありました。3 つには Cisco UCS Server Configuration Utility、Cisco ドライバ、および Cisco Host Upgrade Utility が事前ロードされ、4 番目はユーザ インストールによるハイパーバイザでした。また、Cisco IMC の最新バージョンにアップグレードするか、旧バージョンにダウングレードした後、設定をリセットした場合にも、単一 HV パーティション構成が作成されます。

シスコ ソフトウェア ユーティリティおよびパッケージの詳細については、次の URL の『*Cisco UCS C-Series Servers Documentation Roadmap*』を参照してください。

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

Cisco Flexible Flash コントローラのカード管理機能

Cisco Flexible Flash コントローラでは、単一のカードに加えて 2 つの SD カードを RAID-1 ペアとして管理できます。カード管理機能の導入により、次の作業を実行できます。

（注）

- バージョン 1.4(5e) から 1.5(4) 以降のバージョンにアップグレードする場合は、まずバージョン 1.5(2) にアップグレードしてから、Cisco IMC の高位バージョンにアップグレードする必要があります。
- すべての Cisco IMC のファームウェア アップグレード後に、最新の Flex Flash ファームウェアをロードするには、Cisco Flexible Flash コントローラをリセットします。

Action	説明
Reset Cisco Flex Flash	コントローラをリセットできます。
Reset Partition Defaults	選択したスロットの設定をデフォルト設定にリセットできます。
Synchronize Card Configuration	ファームウェア バージョン 253 以降をサポートする SD カードの設定を保持できます。
Configure Operational Profile	選択した Cisco Flexible Flash コントローラの SD カードを設定できます。

RAID パーティションの列挙

非 RAID パーティションは常にプライマリ カードから列挙されます。列挙はプライマリ カードのステータスに依存しません。

次に、Cisco Flexible Flash コントローラに 2 枚のカードがあるときの RAID パーティションの列挙の動作を示します。

シナリオ	動作
シングル カード	RAID パーティションは、カードが正常に動作している場合、およびモードが Primary または Secondary-active の場合に列挙されます。

シナリオ	動作
デュアル ペア カード	RAID パーティションは、カードの 1 つが正常に動作していれば列挙されます。 1 枚のカードだけが正常に動作している場合、すべての読み取り/書き込み操作は、この正常に動作しているカードで行われます。2 つの RAID パーティションを同期するには UCS SCU を使用する必要があります。
デュアル非ペア カード	サーバを再起動するときにこのシナリオが検出された場合、RAID パーティションはいずれも列挙されません。 サーバが稼働しているときにこのシナリオが検出された場合、ユーザが新しい SD カードを取り付けても、そのカードは Cisco Flexible Flash コントローラによって管理されません。これはホストの列挙には影響しません。これらを管理するためにカードをペアにする必要があります。カードをペアにするには、[Reset Partition Defaults] または [Synchronize Card Configuration] オプションを使用できます。

FlexFlash でのシングル カード ミラーリングからデュアル カード ミラーリングへのアップグレード

次のいずれかの方法で、FlexFlash を使用したシングル カード ミラーリングからデュアル カード ミラーリングにアップグレードできます。

- 空の FlexFlash をサーバに追加し、SD ファームウェアを旧バージョンから最新バージョンにアップグレードします。

  この作業を完了する方法については、を参照してください。

- FlexFlash ファームウェアを最新バージョンにアップグレードした後、空のカードをサーバに追加します。

このいずれかの方法を使用する前に、次のガイドラインに注意してください。

- RAID1 ミラーリングを作成するには、サーバに追加される空のカードのサイズが、サーバ上の既存のカードと正確に同じである必要があります。RAID1 ミラーリングをセットアップするうえで、同じカード サイズは必須事項です。

- ハイパーバイザ パーティション内の有効なデータを持つカードが、プライマリ正常カードとしてマークされていることを確認してください。Cisco IMC GUI または Cisco IMC CLI でこの状態を判別できます。カードの状態をプライマリ正常としてマークするには、Cisco IMC GUI の [Reset Configuration] オプションを使用するか、Cisco IMC CLI で **reset-config** コマンドを実行することができます。特定のカードの設定をリセットすると、セカンダリ カードはセカンダリ アクティブ非正常としてマークされます。
- RAID 正常性「Degraded」状態である場合、すべての読み取りおよび書き込みトランザクションは正常なカードで実行されます。このシナリオでは、データのミラーリングは行われません。データのミラーリングは、正常な RAID 状態の場合にのみ行われます。
- データのミラーリングは RAID パーティションにのみ適用されます。C シリーズ サーバでは、RAID モードでハイパーバイザ パーティションだけが動作します。
- 旧バージョンで使用するよう SD カードを設定していない場合、最新バージョンにアップグレードすると最新の 253 ファームウェアがロードされ、4 個のパーティションすべてがホストに列挙されます。

FlexFlash バージョンのアップグレード中に次のエラー メッセージが表示される場合があります。

```
Unable to communicate with Flexible Flash controller: operation ffCardsGet, status
CY_AS_ERROR_INVALID_RESPONSE”
```

さらに、カード ステータスが [missing] と示されることもあります。このエラーが発生する原因は、1.4(x) などの代替リリースまたは旧バージョンに意図せず切替えたためです。このシナリオでは、最新バージョンに戻すか、元の FlexFlash 1.4(x) 設定に切り替えることができます。最新の Cisco IMC バージョンに戻すことを選択した場合、Cisco FlexFlash 設定はそのまま残ります。旧バージョンの設定に切り替えることを選択した場合は、Flexflash 設定をリセットする必要があります。その場合、次の点に注意する必要があります。

- 複数のカードが存在する状態で旧バージョンに戻すと、2 番目のカードを検出したり管理したりすることはできません。
- カード タイプが SD253 である場合、Cisco IMC CLI から **reset-config** コマンドを 2 回実行する必要があります。1 回目は古いファームウェアをコントローラに再ロードして SD253 から SD247 タイプに移行し、2 回目の実行では列挙を開始します。

C220 M3 サーバ、C240 M3 サーバ、および C460 M4 サーバの Flexible Flash コントローラ プロパティの設定

はじめる前に

- 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。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされ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 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 # **scopeflexflash***index*	指定コントローラに対して Cisco Flexible Flash コントローラ コマンド モードを開始します。この時点では、許容される *index* 値は **FlexFlash-0** だけです。
ステップ 3	Server /chassis/flexflash # **scopeoperational-profile**	Operational Profile コマンド モードを開始します。
ステップ 4	Server /chassis/flexflash/operational-profile # **setraid-primary-member** {**slot1** | **slot2**}	データのプライマリ コピーが存在するスロットを指定します。 **重要** 現在、Cisco Flexible Flash カードは、スロット 1 とスロット 2 でサポートされています。したがって、**slot1** または **slot2** を指定できます。
ステップ 5	Server /chassis/flexflash/operational-profile # **setraid-secondary-role** {**active** | **initializing**}	セカンダリ RAID の役割です。現在サポートされている値は **active** です。
ステップ 6	Server /chassis/flexflash/operational-profile # **setread-error-count-threshold**	Cisco Flexible Flash カードへのアクセス中に許可される読み取りエラーの数を指定します。エラー数がこのしきい値を超えると、Cisco Flexible Flash カードがディセーブルになります。Cisco IMC が再アクセスを試みる前に、カードをリセットする必要があります。 読み取りエラーのしきい値を指定するには、1 ～ 255 の整数を入力します。検出されたエラー数に関係なく、カードがディセーブルにならないように指定するには、0（ゼロ）を入力します。
ステップ 7	Server /chassis/flexflash/operational-profile # **setwrite-error-count-threshold**	Cisco Flexible Flash カードへのアクセス中に許可される書き込みエラーの数を指定します。エラー数がこのしきい値を超えると、Cisco Flexible Flash カードがディセーブルになります。Cisco IMC が再アクセスを試みる前に、カードをリセットする必要があります。 書き込みエラーのしきい値を指定するには、1 ～ 255 の整数を入力します。検出されたエラー数に関係なく、カードがディセーブルにならないように指定するには、0（ゼロ）を入力します。

	コマンドまたはアクション	目的
ステップ 8	Server /chassis/flexflash/operational-profile # **setvirtual-drives-enabled***list*	サーバから USB 形式のドライブとして使用できるようにする仮想ドライブのリストを指定します。オプションは次のとおりです。 • [SCU]：サーバは Cisco UCS Server Configuration Utility にアクセスできます。 • DRIVERS：サーバはシスコ ドライバ ボリュームにアクセスできます。 • [HV]：サーバはユーザがインストールしたハイパーバイザにアクセスできます。 • [HUU]：サーバは Cisco Host Upgrade Utility にアクセスできます。 複数のオプションを指定する場合は、リストを引用符（"）で囲む必要があります。
ステップ 9	Server /chassis/adapter # **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、Flash コントローラのプロパティを設定する例を示します。

```
Server# scope chassis
Server /chassis # scope flexflash FlexFlash-0
Server /chassis/flexflash # scope operational-profile
Server /chassis/flexflash/operational-profile # set read-error-count-threshold 100
Server /chassis/flexflash/operational-profile # set write-error-count-threshold 100
Server /chassis/flexflash/operational-profile *# set raid-primary-member slot1
Server /chassis/flexflash/operational-profile # set raid-secondary-role active
Server /chassis/flexflash/operational-profile *# set virtual-drives-enabled "SCU HUU"
Server /chassis/flexflash/operational-profile *# commit
Server /chassis/flexflash/operational-profile #
```

C220 M4 サーバおよび C240 M4 サーバの Flexible Flash コントローラ プロパティの設定

（注）

- [Mirror] モードでは、[Slot1 Read/Write Error Threshold] が両方の SD カード（2 枚のカードがある場合）に適用されます。
- [Util] モードでは、[Slot1 Read/Write Error Threshold] がスロット 1 のカードに適用され、[Slot2 Read/Write Error Threshold] がスロット 2 のカードに適用されます。

はじめる前に

- 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。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされ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 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 # **scopeflexflash***index*	指定コントローラに対して Cisco Flexible Flash コントローラ コマンド モードを開始します。この時点では、許容される *index* 値は **FlexFlash-0** だけです。
ステップ 3	Server /chassis/flexflash # **scopeoperational-profile**	Operational Profile コマンド モードを開始します。
ステップ 4	Server /chassis/flexflash/operational-profile # **setread-error-count- slot1-threshold***threshold*	スロット 1 の Cisco Flexible Flash カードへのアクセス中に許可される読み取りエラーの数を指定します。エラー数がこのしきい値を超えると、Cisco Flexible Flash カードがディセーブルになります。Cisco IMC が再アクセスを試みる前に、カードをリセットする必要があります。 読み取りエラーのしきい値を指定するには、1 ～ 255 の整数を入力します。検出されたエラー数に関係なく、カードがディセーブルにならないように指定するには、0（ゼロ）を入力します。
ステップ 5	Server /chassis/flexflash/operational-profile # **setread-error-count- slot2-threshold***threshold*	スロット 2 の Cisco Flexible Flash カードへのアクセス中に許可される読み取りエラーの数を指定します。エラー数がこのしきい値を超えると、Cisco Flexible Flash カードがディセーブルになります。Cisco IMC が再アクセスを試みる前に、カードをリセットする必要があります。 読み取りエラーのしきい値を指定するには、1 ～ 255 の整数を入力します。検出されたエラー数に関係なく、カードがディセーブルにならないように指定するには、0（ゼロ）を入力します。

	コマンドまたはアクション	目的
ステップ 6	Server /chassis/flexflash/operational-profile # **setwrite-error-count-slot1-threshold***threshold*	スロット 1 の Cisco Flexible Flash カードへのアクセス中に許可される書き込みエラーの数を指定します。エラー数がこのしきい値を超えると、Cisco Flexible Flash カードがディセーブルになります。Cisco IMC が再アクセスを試みる前に、カードをリセットする必要があります。 書き込みエラーのしきい値を指定するには、1 ～ 255 の整数を入力します。検出されたエラー数に関係なく、カードがディセーブルにならないように指定するには、0（ゼロ）を入力します。
ステップ 7	Server /chassis/flexflash/operational-profile # **setwrite-error-count-slot2-threshold***threshold*	スロット 2 の Cisco Flexible Flash カードへのアクセス中に許可される書き込みエラーの数を指定します。エラー数がこのしきい値を超えると、Cisco Flexible Flash カードがディセーブルになります。Cisco IMC が再アクセスを試みる前に、カードをリセットする必要があります。 書き込みエラーのしきい値を指定するには、1 ～ 255 の整数を入力します。検出されたエラー数に関係なく、カードがディセーブルにならないように指定するには、0（ゼロ）を入力します。
ステップ 8	Server /chassis/flexflash/operational-profile # **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、Flash コントローラのプロパティを設定する例を示します。

```
Server# scope chassis
Server /chassis # scope flexflash FlexFlash-0
Server /chassis/flexflash # scope operational-profile
Server /chassis/flexflash/operational-profile # set read-err-count-slot1-threshold 9
Server /chassis/flexflash/operational-profile *# set read-err-count-slot2-threshold 10
Server /chassis/flexflash/operational-profile *# set write-err-count-slot1-threshold 11
Server /chassis/flexflash/operational-profile *# set write-err-count-slot2-threshold 12
Server /chassis/flexflash/operational-profile *# commit
Server /chassis/flexflash/operational-profile # show detail
FlexFlash Operational Profile:
    Firmware Operating Mode: util
    SLOT1 Read Error Threshold: 9
    SLOT1 Write Error Threshold: 11
    SLOT2 Read Error Threshold: 10
    SLOT2 Write Error Threshold: 12
```

Flexible Flash からのブート

Cisco Flexible Flash カード上のブート可能な仮想ドライブを指定して、サーバが次に再起動されたときにそのドライブをデフォルトのブートプライオリティよりも優先させることができます（サーバに定義されているデフォルトブート順は無視されます）。指定したブートデバイスは一度だけ使用されます。サーバがリブートした後、この設定は無効になります。

（注） サーバをリブートする前に、選択する仮想ドライブが Cisco Flexible Flash カード上でイネーブルになっていることを確認してください。

Cisco IMC の最新バージョンにアップグレードするか、以前のバージョンにダウングレードしてから設定をリセットすると、サーバはHVパーティションだけを介してブートします。以前のバージョンに有効な SCU のデータがあった場合、サーバは単一 HV パーティションにもかかわらず SCU を介してブートします。

はじめる前に

- 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。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされ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 bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **setboot-override** {**None** | **HV**}	次回サーバが再起動されるときにブートを試行する仮想ドライブ。次のいずれかになります。 • None：サーバはデフォルトのブート オーダーを使用します • HV：サーバはハイパーバイザ仮想ドライブから起動します
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。

この例では、サーバが次の再起動時に Cisco UCS Server Configuration Utility からブートするよう指定します。

```
Server# scope bios
Server /bios # set boot-override HV
Committing the boot override BIOS will try boot to
the specified boot device first. Failure to detect
the boot device BIOS will boot from the list
```

```
configured in the BIOS boot order.
Server /bios *# commit
Server /bios #
```

Flexible Flash コントローラのリセット

通常の操作では、Cisco Flexible Flash のリセットが必要になることはありません。テクニカル サポートの担当者から明確に指示された場合にだけ、この手順を実行することを推奨します。

（注） この操作は、Cisco Flexible Flash コントローラ上の仮想ドライブへのトラフィックを中断させます。

はじめる前に

- 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。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされ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 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 flexflash***index*	指定コントローラに対して Cisco Flexible Flash コントローラ コマンド モードを開始します。この時点では、許容される *index* 値は **FlexFlash-0** だけです。
ステップ 3	Server /chassis/flexflash # **reset**	Cisco Flexible Flash コントローラをリセットします。

この例では、フラッシュ コントローラをリセットします。

```
Server# scope chassis
Server /chassis # scope flexflash FlexFlash-0
Server /chassis/flexflash # reset
This operation will reset Cisco Flexible Flash controller.
Host traffic to VDs on this device will be disrupted.
Continue?[y|N] y

Server /chassis/flexflash #
```

ミラー モードでの Flexible Flash コントローラ カードの設定

ミラー モードでコントローラ カードを設定します。

はじめる前に

- 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。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされ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 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 # **scopeflexflash**	指定コントローラに対して Cisco Flexible Flash コントローラ コマンド モードを開始します。
ステップ 3	Server /chassis/flexflash # **configure-cards-mirrorSLOT-1**.	正常なプライマリとして SLOT-1 を設定します。
ステップ 4	「**Enable auto sync(by default auto sync is disabled)?[y|N]**」プロンプトで y を入力します。	スロット 1 のカードとスロット 2 のカードを同期します。
ステップ 5	「**Set Mirror PartitionName(Default name is Hypervisor)?[y|N]**」プロンプトで y を入力します。	ミラー パーティションの名前を設定できるようにします。
ステップ 6	「**Enter Partition Name MirrorPartition Name:***Hypervisor*」プロンプトで、ミラー パーティションの名前を入力します。	ミラー パーティションの名前を設定します。 次のメッセージが表示されます。 このアクションは、SLOT-1 を正常なプライマリ スロットしてマークし、SLOT-2 を非正常なセカンダリとしてマークします。 この操作は、ホスト接続を妨げる場合もあります。
ステップ 7	「**Continue?[y|N]y**」プロンプトで y を入力します。	ミラー モードでカードを設定し、SLOT-1 のカードをプライマリで正常なカード、SLOT-2 （カードが存在する場合）を非正常なセカンダリのカードとして設定します。

	コマンドまたはアクション	目的
ステップ 8	Server /chassis/flexflash # **show physical-drive**	（任意） 設定したカードのステータスを表示します。 （注） • カードが自動同期モードで設定されており、それらのカードが同期してい場合は、良好なカードと不良なカードとの同期が自動的に開始されます。 • カードが自動同期モードで設定されており、1 つのカードが同期していない場合は、良好なカードからの同期が自動的に開始されます。 • サーバが 1 枚の自動ミラーの正常なカードを使用して実行している場合に新しいカードが挿入されると、新しいカード上にメタデータが自動的に作成され、自動ミラーが設定されたカードから新しいペアのカードへのデータ同期が開始されます。

次に、ミラー モードでコントローラ カードを設定する例を示します。

```
Server# scope chassis
Server /chassis # scope flexflash
Server /chassis/flexflash #  configure-cards-mirror SLOT-1
Enable auto sync(by default auto sync is disabled)?[y|N]y
Set Mirror Partition Name(Default name is Hypervisor)?[y|N]y
Enter Partition Name Mirror Partition Name :hfldjslkjdfs
This action will mark the SLOT-1 as healthy primary slot and SLOT-2 (if card existing) as
unhealthy secondary.
This operation may disturb the host connectivity as well.
Continue?[y|N]y
Server /chassis/flexflash # show detail
Controller FlexFlash-0:
    Product Name: Cisco FlexFlash
    Controller HW: FX3S
    Vendor: Cypress
    Firmware Version: 1.3.2 build 159
    Firmware Operating Mode: mirror
    Firmware Configured Mode: mirror
    Has Error: No
    Error Description:
    Internal State: Disconnected
    Controller Status: OK
    Cards Manageable: Yes
    Startup Firmware Version: 1.3.2 build 159

Server /chassis/flexflash # show physical-drive
Physical Drive  Status    Controller   Card Type         Card mode         Health     Sync
 Mode
--------------- --------- ------------ ----------------- ----------------- ----------
----------
SLOT-1          present   FlexFlash-0  FX3S configured   mirror-primary    healthy    auto
SLOT-2          present   FlexFlash-0  FX3S configured   mirror-secondary  unhealthy  auto
```

```
Server /chassis/flexflash #
```

Util モードでのコントローラ カードの設定

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **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 # **scopeflexflash**	指定コントローラに対して Cisco Flexible Flash コントローラ コマンド モードを開始します。
ステップ 3	Server /chassis/flexflash # **configure-cards-utilSLOT-1**	Slot-1 のカードを 4 つのパーティション（SCU、HUU、ドライバ、およびユーザ パーティション）を持つ Util カードとして設定します。
ステップ 4	「**Set User Partition Name on Util Card(Default name is UserPartition)?[y|N]**」プロンプトで y を入力します。	ユーザ パーティションの名前を設定できるようにします。
ステップ 5	「**Enter UserPartiton Name:***UserPartition*」プロンプトでユーザ パーティションの名前を入力します。	ユーザ パーティションの名前を設定します。
ステップ 6	「Set Partition Name on Non Util Card(Default name is Hypervisor)?[y|N」で y を入力します。	Util 以外のカード上の単一のパーティションの名前を設定できるようにします。
ステップ 7	「**Enter Partition Name of Non UtilCard:***Hypervisor*」プロンプトで、ミラー パーティションの名前を入力します。	Util以外のパーティションの名前を設定します。 次のメッセージが表示されます。 このアクションによって SLOT-1 上で Util 設定（4 パーティション）が、SLOT-2（カードが存在する場合）上で Util 以外の設定（1 パーティション）が作成されます。 この操作は、ホスト接続を妨げる場合もあります。
ステップ 8	「**Continue?[y|N]y**」プロンプトで y を入力します。	Util モードでカードを設定します。SLOT-1 のカードに 4 つのパーティションを作成し、そのカードを正常なプライマリとして設定し、SLOT-2 のカード（カードが存在する場合）は正常なセカンダリとして設定します。

	コマンドまたはアクション	目的
ステップ 9	Server /chassis/flexflash # **show physical-drive**	（任意） 設定したカードのステータスを表示します。 （注） 4 つのパーティションがある Util カード上には、1 つのパーティションが余分に作成され、SCU、HUU、およびドライバの OOB 更新時に使用されます。

次に、Util モードでコントローラ カードを設定する例を示します。

```
Server# scope chassis
Server /chassis # scope flexflash
Server /chassis/flexflash #  configure-cards-mirror SLOT-1
Set User Partiton Name on Util Card (Default name is UserPartition)?[y|N]y
Enter User Partiton Name :UserPartition
Set Partition Name on Non Util Card(Default name is Hypervisor)?[y|N]y
Enter Partition Name of Non Util Card :Hypervisor
This action will create util configuration (4 partitons) on SLOT-1 card and
non-util configuration(1 partition) on SLOT-2 (if card existing)
This operation may disturb the host connectivity as well.
Continue?[y|N]y

Server /chassis/flexflash # show detail
Controller FlexFlash-0:
    Product Name: Cisco FlexFlash
    Controller HW: FX3S
    Vendor: Cypress
    Firmware Version: 1.3.2 build 159
    Firmware Operating Mode: util
    Firmware Configured Mode: util
    Has Error: No
    Error Description:
    Internal State: Disconnected
    Controller Status: OK
    Cards Manageable: Yes
    Startup Firmware Version: 1.3.2 build 159

Server /chassis/flexflash # show physical-drive
Physical Drive  Status    Controller   Card Type         Card mode         Health     Sync
 Mode
--------------- --------- ------------ ----------------- ----------------- ----------
----------
SLOT-1          present   FlexFlash-0  FX3S configured   util              healthy    NA
SLOT-2          present   FlexFlash-0  FX3S configured   util              healthy    NA

Server /chassis/flexflash #
```

Flexible Flash コントローラ ファームウェア モードの設定

はじめる前に

- 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。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされ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 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 # **scopeflexflash**	指定コントローラに対して Cisco Flexible Flash コントローラ コマンド モードを開始します。
ステップ 3	Server /chassis/flexflash # **configure-firmware-mode**.	ファームウェア モードを現在のモードから他のモードに切り替えます。 次のメッセージが表示されます。 This action will switch firmware mode from util to mirror この操作は、ホスト接続を妨げる場合もあります。
ステップ 4	「**Continue?[y|N]y**」プロンプトで y を入力します。	ファームウェア モードをミラーから Util、または Util からミラーに切り替えます。

次に、コントローラのファームウェア モードを設定する例を示します。

```
Server# scope chassis
Server /chassis # scope flexflash
Server /chassis/flexflash #  configure-firmware-mode
This action will switch fimrware mode from util to mirror
This operation may disturb the host connectivity as well.
Continue?[y|N]y
Server /chassis/flexflash # show detail
Controller FlexFlash-0:
    Product Name: Cisco FlexFlash
    Controller HW: FX3S
    Vendor: Cypress
    Firmware Version: 1.3.2 build 159
    Firmware Operating Mode: mirror
    Firmware Configured Mode: mirror
    Has Error: Yes
    Error Description:
    Internal State: Failed
    Controller Status: Mode Mismatch SDcard(s)
    Cards Manageable: NO
    Startup Firmware Version: 1.3.2 build 159

*+-------------------------------------------------------------------------------+
+ Based on type and number of cards please execute mirror/util Configuration +
+ (configure-mirror/configure-util) commands to start monitoring/managing SD cards +
+                              OR                                               +
+                        Switch Firmware Operating Mode                         +
+-------------------------------------------------------------------------------+

Server /chassis/flexflash #
```

Cisco Flexible Flash コントローラでのカードの設定のリセット

Cisco Flexible Flash コントローラで、選択したスロットの設定をデフォルト設定にリセットできます。

Cisco Flexible Flash カードのスロットの設定をリセットすると、次の状況が発生します。

- 選択されたスロットのカードは、プライマリ - 正常としてマークされます。
- もう一方のスロットのカードは、セカンダリ アクティブ- 非正常としてマークされます。
- 1 つの RAID パーティションが作成されます。
- カードの読み取り/書き込みエラー数および読み取り/書き込みしきい値は0に設定されます。
- ホストの接続が停止される可能性があります。

最新バージョンにアップグレードして、設定のリセット オプションを選択した場合、単一のハイパーバイザ（HV）パーティションが作成され、既存の4パーティション構成は消去されます。これにより、データ損失が生じることもあります。失われたデータを取り出すことができるのは、HVパーティションにまだデータを書き込んでおらず、以前のバージョンにダウングレードする場合だけです。

はじめる前に

- 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。
- Cisco Flexible Flash は、サーバでサポートされ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 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 # **scopeflexflash***index*	指定コントローラに対して Cisco Flexible Flash コントローラ コマンド モードを開始します。この時点では、許容される *index* 値は **FlexFlash-0** だけです。
ステップ 3	Server /chassis/flexflash # **reset-partition-defaults***primary slot ID*	選択したスロットの設定をデフォルト設定にリセットします。

次に、スロットから設定をデフォルト設定にリセットする例を示します。

```
Server# scope chassis
Server /chassis # scope flexflash FlexFlash-0
Server /chassis/flexflash # reset-partition-defaults slot1

This action will mark the slot1 as the healthy primary slot, and slot2 (if card exists)
```

```
as unhealthy secondary active.
This operation may disturb the host connectivity as well.
Continue? [y|N] y

Server /chassis/flexflash/operational-profile #
```

Flexible Flash コントローラの設定の保持

Cisco Flexible Flash カードの特定のスロットの設定を他のスロットにコピーできます。ただし、設定のコピー元スロットはSDK523タイプである必要があります。設定は次の場合に保持できます。

- 2 つの非ペアの FlexFlash があります
- 単一 FlexFlash からサーバが稼働していて、非ペアの FlexFlash が他のスロットにあります。
- 1 つの FlexFlash がファームウェア バージョン 253 をサポートし、もう 1 つの FlexFlash はパーティション化されていません。

はじめる前に

- 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。
- Cisco Flexible Flash は、サーバでサポートされ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 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 # **scopeflexflash***index*	指定コントローラに対して Cisco Flexible Flash コントローラ コマンド モードを開始します。この時点では、許容される *index* 値は **FlexFlash-0** だけです。
ステップ 3	Server /chassis/flexflash # **synchronize-card-configuration***primary slot ID*	プライマリ スロットからセカンダリ スロットに設定をコピーします。

次に、あるスロットから他のスロットに設定をコピーする例を示します。

```
Server# scope chassis
Server /chassis # scope flexflash FlexFlash-0
Server /chassis/flexflash # synchronize-card-configuration slot1

This action will copy the config of slot1 to both the slots, mark slot1 as healthy,
primary slot and slot2 (card must be present) as unhealthy secondary active.
This operation may disturb the host connectivity as well.
Continue? [y|N] y

Server /chassis/flexflash/operational-profile #
```

ISO イメージ設定の追加

はじめる前に

- 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。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされている必要があります。
- カードは Util モードにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server/chassis # **scope flexflash**	指定コントローラに対して Cisco Flexible Flash コントローラ コマンド モードを開始します。
ステップ 3	Server/chassis/flexflash/ # **scope vd-image-configs**	仮想ドライブ コンフィギュレーション コマンド モードを開始します。
ステップ 4	Server/chassis/flexflash/vd-image-configs # **vd-image-cifs***virtual_drive//serverip/remote_share<remote_file>*	「Server username:」プロンプトが表示されます。 **1** Server username: *server username* サーバのユーザ名を入力します。 **2** Server password: *server password* サーバのパスワードを入力します。 **3** Confirm password: *server password* サーバのパスワードを再度入力します。
ステップ 5	Server/chassis/flexflash/vd-image-configs # **vd-image-nfs***virtual_driveserverip:/remote_share<remote_file>*	「Server username:」プロンプトが表示されます。

	コマンドまたはアクション	目的
ステップ 6	Server/chassis/flexflash/vd-image-configs # **show detail**	（任意） 仮想デバイスの詳細を表示します。

```
Server # scope chassis
Server/chassis # scope flexflash
Server/chassis/flexflash # scope vd-image-configs
Server/chassis/flexflash/vd-image-configs # vd-image-cifs SCU //10.106.146.69/pdagguma
/softwares/ucs-cxx-scu-3.1.9.iso
Server/chassis/flexflash/vd-image-configs # show detail
Vritual Drive SCU:
    Mount Type: cifs
    Remote Share: //10.106.146.69/pdagguma
    Remote File: /softwares/ucs-cxx-scu-3.1.9.iso
    Mount Options:
"username=pdagguma,password*********,soft,nounix,noserverino,rsize=3072,wsize=3072"
Vritual Drive HUU:
    Mount Type: cifs
    Remote Share: //10.101
    Remote File: DFLJD_huu.iso
    Mount Options:
"username=pdagguma,password*********,soft,nounix,noserverino,rsize=3072,wsize=3072"
Vritual Drive Drivers:
    Mount Type: None
    Remote Share: None
    Remote File: None
    Mount Options: None
Server/chassis/flexflash/vd-image-configs #
```

仮想ドライブの有効化

はじめる前に

- 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。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされ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 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 # **scopeflexflash**	指定コントローラに対して Cisco Flexible Flash コントローラ コマンド モードを開始します。
ステップ 3	Server /chassis/ flexflash # **scopevirtual-drive**	指定したコントローラに対して仮想デバイス 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/flexflash/virtual-drive # **enable-vds** *"SCU HUU dlfd"*	ホストに対して仮想ドライブをイネーブルにします。

次に、仮想デバイスをホストに対してイネーブルにする例を示します。

```
Server# scope chassis
Server /chassis # scope flexflash
Server /chassis/flexflash #  scope virtual-drive
Server /chassis/flexflash/virtual-drive # enable-vds "SCU HUU dlfd"
Server /chassis/flexflash/virtual-drive # show detail

Virtual Drive SCU:
    VD ID: 1
    Size: 2560 MB
    VD Scope: Non-Raid
    VD Status: Healthy
    VD Type: Removable
    Read/Write: R/W
    Host Accessible: Connected
    Operation in progress: NA
    Last Operation completion status: none
Virtual Drive HUU:
    VD ID: 2
    Size: 1536 MB
    VD Scope: Non-Raid
    VD Status: Healthy
    VD Type: Removable
    Read/Write: R/W
    Host Accessible: Connected
    Operation in progress: NA
    Last Operation completion status: none
Virtual Drive Drivers:
    VD ID: 3
    Size: 8192 MB
    VD Scope: Non-Raid
    VD Status: Healthy
    VD Type: Removable
    Read/Write: R/W
    Host Accessible: Not-Connected
    Operation in progress: NA
    Last Operation completion status: none
Virtual Drive dlfd:
    VD ID: 4
    Size: 9952 MB
    VD Scope: Non-Raid
    VD Status: Healthy
    VD Type: Removable
    Read/Write: R/W
    Host Accessible: Connected
    Operation in progress: NA
    Last Operation completion status: none
Virtual Drive dfdff:
    VD ID: 5
    Size: 30432 MB
    VD Scope: Non-Raid
    VD Status: Healthy
    VD Type: Removable
    Read/Write: R/W
    Host Accessible: Not-Connected
    Operation in progress: NA
    Last Operation completion status: none

Server /chassis/flexflash/virtual-drive #
```

仮想ドライブの消去

はじめる前に

- 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。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされ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 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 # **scopeflexflash**	指定コントローラに対して Cisco Flexible Flash コントローラ コマンド モードを開始します。
ステップ 3	Server /chassis/ flexflash # **scopevirtual-drive**	指定したコントローラに対して仮想デバイス コマンド モードを開始します。
ステップ 4	Server /chassis/flexflash/virtual-drive # **erase-vds "SCU HUU"**	FAT 32 の消去を開始します。

次に、仮想デバイスでデータを消去する例を示します。

```
Server# scope chassis
Server /chassis # scope flexflash
Server /chassis/flexflash #  scope virtual-drive
Server /chassis/flexflash/virtual-drive #  erase-vds "SCU HUU"
Server /chassis/flexflash/virtual-drive # show detail

Virtual Drive SCU:
    VD ID: 1
    Size: 2560 MB
    VD Scope: Non-Raid
    VD Status: Healthy
    VD Type: Removable
    Read/Write: R/W
    Host Accessible: Not-Connected
    Operation in progress: Erasing
    Last Operation completion status: none
Virtual Drive HUU:
    VD ID: 2
    Size: 1536 MB
    VD Scope: Non-Raid
    VD Status: Healthy
    VD Type: Removable
    Read/Write: R/W
    Host Accessible: Connected
    Operation in progress: Erase-Pending
    Last Operation completion status: none
Virtual Drive Drivers:
    VD ID: 3
    Size: 8192 MB
    VD Scope: Non-Raid
    VD Status: Healthy
```

```
    VD Type: Removable
    Read/Write: R/W
    Host Accessible: Not-Connected
    Operation in progress: NA
    Last Operation completion status: none
Virtual Drive dlfd:

Server /chassis/flexflash/virtual-drive #
```

仮想ドライブの同期

はじめる前に

- 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。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされている必要があります。
- カードは手動ミラー モードで設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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 # **scopeflexflash**	指定コントローラに対して Cisco Flexible Flash コントローラ コマンド モードを開始します。
ステップ 3	Server /chassis/ flexflash # **scopevirtual-drive**	指定したコントローラに対して仮想デバイス コマンド モードを開始します。
ステップ 4	Server /chassis/flexflash/virtual-drive # **sync-vds***Hypervisor*	仮想ドライブを同期します。 （注） • カードが自動同期モードで設定されており、1 つのカードが同期していない場合は、良好なカードからの同期が自動的に開始されます。 • サーバが 1 枚の自動ミラーの正常なカードを使用して実行している場合に新しいカードが挿入されると、新しいカード上にメタデータが自動的に作成され、自動ミラーが設定されたカードから新しいペアのカードへのデータ同期が開始されます。

次に、仮想ドライブを同期する例を示します。

```
Server# scope chassis
Server /chassis # scope flexflash
Server /chassis/flexflash #  scope virtual-drive
```

```
Server /chassis/flexflash/virtual-drive # sync-vds Hypervisor
Server /chassis/flexflash/virtual-drive # show detail

Virtual Drive Hypervisor:
    VD ID: 1
    Size: 30432 MB
    VD Scope: Raid
    VD Status: Degraded
    VD Type: Removable
    Read/Write: R/W
    Host Accessible: Not-Connected
    Operation in progress: Syncing(Manual)
    Last Operation completion status: none

Server /chassis/flexflash/virtual-drive #
```

DIMM のブラックリストの設定

DIMM のブラックリスト化

Cisco IMC で、デュアル インライン メモリ モジュール（DIMM）の状態は、SEL イベント レコードに基づいています。BIOS が BIOS ポスト中のメモリ テスト実行時に 16000 のエラー件数を伴う修正不可能なメモリ エラーまたは修正可能なメモリ エラーに遭遇した場合、DIMM は不良と判断されます。不良と判別された DIMM は機能しないデバイスと見なされます。

DIMM のブラックリスト化を有効にすると、Cisco IMC はメモリ テスト実行メッセージをモニタし、あらゆる時点でDIMM SPD データ内でメモリ エラーに遭遇した DIMM をブラックリストに載せます。これにより、ホストはこれらの DIMM をマップから外すことができます。

DIMM は、修正不可能なエラーが発生した場合にのみマッピング解除またはブラックリスト化されます。DIMM がブラックリスト化されると、同じチャネル上にある他の DIMM が無視されるかディセーブルとなり、その DIMM は不良として見なされなくなります。

（注） DIMM は、修正可能なエラー 16000 の場合はマッピング解除またはブラックリスト化されません。

DIMM のブラックリストのイネーブル化

はじめる前に

管理者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 dimm-blacklisting**/	DIMM ブラックリスト モードを開始します。
ステップ 2	Server /dimm-blacklisting # **set enabled** {**yes** | **no**}	DIMM ブラックリス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 /dimm-blacklisting* # **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、DIMM のブラックリストをイネーブルにする例を示します。

```
Server# scope dimm-blacklisting
Server /dimm-blacklisting # set enabled yes
Server /dimm-blacklisting* # commit
Server /dimm-blacklisting #
Server /dimm-blacklisting # show detail

DIMM Blacklisting:
      Enabled: yes
```

BIOS の設定

BIOS ステータスの表示

手順

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

BIOS ステータス情報には、次のフィールドが含まれます。

名前	説明
BIOS Version	実行中の BIOS のバージョン文字列。
Boot Order	サーバが使用を試行する、ブート可能なターゲット タイプのレガシー ブート順序。
Boot Override Priority	None または HV のいずれかを選択できます。

名前	説明
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。
UEFI セキュア ブート	UEFI セキュア ブートを有効または無効にします。
Configured Boot Mode	BIOS がデバイスのブートを試行するブートモード。
Actual Boot Mode	BIOS がデバイスを起動した実際のブート モード。
Last Configured Boot Order Source	BIOS が最後に設定したブート順序送信元。

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
Server /bios # show detail
BIOS Version: "C460M1.1.2.2a.0 (Build Date: 01/12/2011)"
Boot Order: EFI,CDROM,HDD
Boot Override Priority:
FW Update/Recovery Status: NONE
FW Update/Recovery Progress: 100
Server /bios #

 Server# scope bios
Server /bios # show detail
BIOS:
    BIOS Version: "C240M3.2.0.0.15 (Build Date: 03/16/2014)"
    Boot Order: (none)
    Boot Override Priority:
    FW Update/Recovery Status: None, OK
    UEFI Secure Boot: disabled
    Configured Boot Mode: Legacy
    Actual Boot Mode: Legacy
    Last Configured Boot Order Source: CIMC
Server /bios #
```

主要な BIOS の設定

はじめる前に

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 # **scopemain**	主要な 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。	使用可能な BIOS パラメータは、使用しているサーバのモデルによって異なります。各 BIOS 設定のオプションの詳細については、次の項のいずれかを参照してください。 • C22 および C24 サーバの主要な BIOS パラメータ，（307 ページ） • C220 および C240 サーバの主要な BIOS パラメータ，（331 ページ） • C460 サーバの主要な BIOS パラメータ，（356 ページ） • C220M4 および C240M4 サーバの [Main] タブ，（372 ページ） • C3160 サーバの主要な BIOS パラメータ，（398 ページ）
ステップ 4	Server /bios/main # **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。

この例では、重大な POST エラーの発生時にブートを一時停止するよう BIOS を設定し、トランザクションをコミットします。

```
Server# scope bios
Server /bios # scope main
Server /bios/main # set POSTErrorPause Enabled
Server /bios/main *# 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/main #
```

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。

はじめる前に

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 # **scopeadvanced**	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。	使用可能な BIOS パラメータは、使用しているサーバのモデルによって異なります。各 BIOS 設定のオプションの詳細については、次の項のいずれかを参照してください。 • C22 および C24 サーバの高度な BIOS パラメータ，（308 ページ） • C220 および C240 サーバの高度な BIOS パラメータ，（332 ページ） • C460 サーバの高度な BIOS パラメータ，（357 ページ） • C220M4 および C240M4 サーバの [Advanced] タブ，（374 ページ） • C3160 サーバの高度な BIOS パラメータ，（399 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。

この例では、低電圧 DDR メモリ モードを有効にし、トランザクションをコミットします。

```
Server# scope bios
Server /bios # scope advanced
Server /bios/advanced # set LvDDRMode 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

はじめる前に

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 # **scopeserver-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。	使用可能なBIOSパラメータは、使用しているサーバのモデルによって異なります。各BIOS設定のオプションの詳細については、次の項のいずれかを参照してください。 • C22 および C24 サーバのサーバ管理 BIOS パラメータ，（329 ページ） • C220 および C240 サーバのサーバ管理 BIOS パラメータ，（354 ページ） • C460 サーバのサーバ管理 BIOS パラメータ，（369 ページ） • C220M4 および C240M4 サーバの [Server Management] タブ，（396 ページ） • C3160 サーバの [Server Management] タブ，（419 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。 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。

次に、BMC の自動検出をイネーブルにし、トランザクションをコミットする例を示します。

```
Server# scope bios
Server /bios # scope server-management
```

```
Server /bios/server-management # set BMCPnP Enabled
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 デフォルトの復元

はじめる前に

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 # **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。

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
```

BIOS セットアップの開始

はじめる前に

- サーバの電源が投入されている。
- 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 # **enter-bios-setup**	リブート時に BIOS セットアップを開始します。

次に、BIOS セットアップを開始できるようにする例を示します。

```
Server# scope bios
Server /bios # enter-bios-setup
This operation will enable Enter BIOS Setup option.
Host must be rebooted for this option to be enabled.
Continue?[y|N]y
```

BIOS の工場出荷時のデフォルト設定への復元

BIOS のコンポーネントが正常に動作しない場合、BIOS セットアップ トークンを工場出荷時のデフォルト値に復元できます。

（注） このアクションは、一部の C シリーズ サーバのみで使用できます。

はじめる前に

- 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。
- サーバの電源をオフに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 # **restore-mfg-defaults**	セットアップ トークンを工場出荷時のデフォルト値に復元します。

次に、BIOS セットアップ トークンを工場出荷時のデフォルト値に復元する例を示します。

```
Server # scope bios
Server /bios # restore-mfg-defaults
This operation will reset the BIOS set-up tokens to manufacturing defaults.
The system will be powered on.
Continue? [y|n] N
Server /bios #
```

サーバ コンポーネントのファームウェアの更新

重要 ファームウェアまたは BIOS の更新が進行中の場合は、そのタスクが完了するまでサーバをリセットしないでください。

はじめる前に

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。

サーバの電源をオフに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# **scopechassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scopefirmware**	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 /chassis/firmware # **show detail**	一部のコンポーネント メッセージで必要なファームウェアの更新を表示します。
ステップ 4	Server /chassis/firmware # **update-all**	サーバ コンポーネントのファームウェアを更新します。

次に、サーバをリセットする例を示します。

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

Firmware update required on some components,
please run update-all (under chassis/firmware scope).

Server /chassis / firmware # update-all
```

第 4 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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **showchassis** [**detail**]	サーバのプロパティを表示します。

次に、サーバのプロパティを表示する例を示します。

```
Server# show chassis detail
Chassis:
    Power: on
    Serial Number: QCI140205ZG
```

```
    Product Name: UCS C210 M2
    PID : R210-2121605W
    UUID: FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF
    Locator LED: off
    Description: This shows the chassis details.

Server#
```

次に、C3160 サーバのサーバ プロパティを表示する例を示します。

```
Server# show chassis detail
Chassis:
    Power: on
    Serial Number: FCH1821JAVL
    Product Name: UCS C3160
    PID : UCSC-C3X60-SVRNB
    UUID: 84312F76-75F0-4BD1-9167-28B74EBB444C
    Locator LED: off
    Front Panel Locator LED: off
    Description: This shows the chassis details
Server#
```

サーバ使用率の表示

一部の UCS C シリーズ サーバでのみサーバ使用率を確認できます。

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 cups-utilization**	使用可能なすべてのCPUのサーバ使用率値を表示します。 （注） これらの使用率の値は、ハードウェアの合計帯域幅のパーセンテージとして報告されます。これらの値は、ホスト ベースのリソース モニタリング ソフトウェアで表示される値と一致しないことがあります。

次に、サーバ使用率値を表示する例を示します。

```
Server# scope chassis
Server /chassis # show cups-utilization

CPU Utilization (%)  Memory Utilization (%)  I/O Utilization (%)  Overall Utilization (%)
-------------------- ------------------------ -------------------- -------------------------
100                  69                       0                    86

Server /chassis #
```

Cisco IMC プロパティの表示

（注） Cisco IMC は、サーバ BIOS から現在の日時を取得します。この情報を変更するには、サーバをリブートし、BIOS設定メニューへのアクセスに関するメッセージが表示されたらF2キーを押します。メインの BIOS 設定タブでオプションを使用して日付または時刻を変更します。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **showcimc** [**detail**]	Cisco IMC プロパティを表示します。

次に、Cisco IMC のプロパティを表示する例を示します。

```
Server# show cimc detail
Cisco IMC:
    Firmware Version: 2.0(8.122)
    Current Time: Wed Dec  9 23:14:28 2015
    Boot-loader Version: 2.0(8.122).36
    Local Time: Wed Dec  9 23:14:28 2015 UTC +0000
    Timezone: UTC
    Reset Reason: graceful-reboot (This provides the last Cisco IMC reboot reason.)

Server#
```

CPU のプロパティの表示

はじめる前に

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。

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

はじめる前に

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。
ステップ 3	Server /chassis # **show dimm-summary**	DIMM サマリー情報を表示します。

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        Channel Speed (MHz) Channel Type
-------------------- --------------- ------------------- ---------------
DIMM_A1              2048 MB         1067                Other
DIMM_A2              2048 MB         1067                Other
DIMM_B1              2048 MB         1067                Other
DIMM_B2              2048 MB         1067                Other
DIMM_C1              Not Installed   Unknown             Other
DIMM_C2              Not Installed   Unknown             Other
DIMM_D1              2048 MB         1067                Other
DIMM_D2              2048 MB         1067                Other
DIMM_E1              2048 MB         1067                Other
DIMM_E2              2048 MB         1067                Other
DIMM_F1              Not Installed   Unknown             Other
DIMM_F2              Not Installed   Unknown             Other

Server /chassis #
```

次に、メモリのプロパティに関する詳細情報を表示する例を示します。

```
Server# scope chassis
Server /chassis # show dimm detail
Name DIMM_A1:
    Capacity: 2048 MB
    Channel Speed (MHz): 1067
    Channel Type: Other
    Memory Type Detail: Synchronous
    Bank Locator: NODE 0 CHANNEL 0 DIMM 0
    Visibility: Yes
    Operability: Operable
    Manufacturer: 0x802C
    Part Number: 18JSF25672PY-1G1D1
    Serial Number: 0xDA415F3F
    Asset Tag: Unknown
    Data Width: 64 bits
Name DIMM_A2:
```

```
    Capacity: 2048 MB
--More--

Server /chassis #
```

次の例では、DIMM サマリー情報を表示します。

```
Server# scope chassis
Server /chassis # show dimm-summary
DIMM Summary:
    Memory Speed: 1067 MHz
    Total Memory: 16384 MB
    Effective Memory: 16384 MB
    Redundant Memory: 0 MB
    Failed Memory: 0 MB
    Ignored Memory: 0 MB
    Number of Ignored Dimms: 0
    Number of Failed Dimms: 0
    Memory RAS possible: Memory configuration can support mirroring
    Memory Configuration: Maximum Performance

Server /chassis #
```

電源のプロパティの表示

はじめる前に

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# **scopechassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **showpsu** [**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 #
```

（注） Input Power オプションと Maximum Output Power オプションを使用できるのは一部の C シリーズ サーバだけです。

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

はじめる前に

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 # **showstorageadapter** [*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。 （注） このコマンドは、Cisco IMC 経由で管理できるサーバ上にあるすべての MegaRAID 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、Cisco IMC 経由で管理できません。
ステップ 3	Server /chassis # **scope storageadapter***slot*	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 # **showbbu** [**detail**]	ストレージ カードのバッテリ バックアップ ユニットの情報を表示します。
ステップ 5	Server /chassis/storageadapter # **showcapabilites** [**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 6	Server /chassis/storageadapter # **showerror-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 7	Server /chassis/storageadapter # **showfirmware-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 8	Server /chassis/storageadapter # **showhw-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 9	Server /chassis/storageadapter # **showmfg-data** [**detail**]	ストレージカードの製造元のデータを表示します。

	コマンドまたはアクション	目的
ステップ 10	Server /chassis/storageadapter # **showpci-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 11	Server /chassis/storageadapter # **showrunning-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 12	Server /chassis/storageadapter # **showsettings** [**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。
ステップ 13	Server /chassis/storageadapter # **showstartup-firmware-images** [**detail**]	ストレージカードの起動時にアクティブにするファームウェア イメージを表示します。

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 storageadapter
PCI Slot Product Name                        Serial Number  Firmware Package Build
-------- ---------------------------------- -------------- --------------------------
SAS      LSI MegaRAID SAS 9260-8i            SV93404392     12.12.0-0038


          Product ID     Battery Status Cache Memory Size
     ---- -------------- -------------- --------------
          LSI Logic      fully charged  0 MB

Server /chassis #
```

次に、SAS という名前のストレージ カードのバッテリ バックアップ ユニットの情報を表示する例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SAS
Server /chassis/storageadapter # show bbu
Controller Battery Type Battery Present Voltage    Current    Charge Charging State
---------- ------------ --------------- ---------- ---------- ------ --------------
SAS        iBBU         true            4.051 V    0.000 A    100%   fully charged

Server /chassis/storageadapter #
```

Flexible Flash コントローラ プロパティの表示

はじめる前に

- お使いのプラットフォームで Cisco Flexible Flash がサポートされ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 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 flexflash [detail]**	（任意）使用可能な Cisco Flexible Flash コントローラを表示します。
ステップ 3	Server /chassis # **scope flexflash***index*	指定コントローラに対して Cisco Flexible Flash コントローラ コマンド モードを開始します。この時点では、許容される *index* 値は **FlexFlash-0** だけです。
ステップ 4	Server /chassis/flexflash # **show operational-profile [detail]**	Operational Profile のプロパティを表示します。

この例では、フラッシュ コントローラのプロパティを表示します。

```
Server# scope chassis
Server /chassis # show flexflash
Controller   Product Name     Has Error  Firmware Version  Vendor   Internal State
------------ ---------------- ---------- ----------------- -------- ---------------
FlexFlash-0  Cisco FlexFlash  No         1.2 build 247     Cypress  Connected

Server /chassis # scope flexflash FlexFlash-0
Server /chassis # show operational-profile
Primary Member Slot  I/O Error Threshold  Host Accessible VDs
-------------------- -------------------- --------------------
slot1                100                   SCU Drivers

Server /chassis/flexflash #
```

物理ドライブのプロパティの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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*	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** [*drive-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。

	コマンドまたはアクション	目的
ステップ 5	Server /chassis/storageadapter # **scope physical-drive** *drive-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 inquiry-data** [**detail**]	指定された物理ドライブに関する問い合わせのデータを表示します。
ステップ 8	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。

次に、SAS 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 SAS
Server /chassis/storageadapter # scope physical-drive 1
Server /chassis/storageadapter/physical-drive # show general
Slot Number 1:
    Controller: SAS
    Enclosure Device ID: 27
    Device ID: 34
    Sequence Number: 2
    Media Error Count: 0
    Other Error Count: 0
    Predictive Failure Count: 0
    Link Speed: 6.0 Gb/s
    Interface Type: SAS
    Media Type: HDD
    Block Size: 512
    Block Count: 585937500
    Raw Size: 286102 MB
    Non Coerced Size: 285590 MB
    Coerced Size: 285568 MB
    SAS Address 0: 500000e112693fa2
    SAS Address 1:
    Connected Port 0:
    Connected Port 1:
    Connected Port 2:
    Connected Port 3:
    Connected Port 4:
    Connected Port 5:
    Connected Port 6:
    Connected Port 7:
    Power State: powersave

Server /chassis/storageadapter/physical-drive #
```

次に、SAS という名前のストレージ カードの物理ドライブ番号 1 に関する問い合わせデータを表示する例を表示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SAS
Server /chassis/storageadapter # scope physical-drive 1
Server /chassis/storageadapter/physical-drive # show inquiry-data
Slot Number 1:
    Controller: SAS
```

```
    Product ID: MBD2300RC
    Drive Firmware: 5701
    Drive Serial Number: D010P9A0016D

Server /chassis/storageadapter/physical-drive #
```

次に、SAS という名前のストレージ カードの物理ドライブ番号 1 の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 SAS
Server /chassis/storageadapter # scope physical-drive 1
Server /chassis/storageadapter/physical-drive # show inquiry-data
Slot Number 1:
    Controller: SAS
    State: online
    Online: true
    Fault: false

Server /chassis/storageadapter/physical-drive #
```

仮想ドライブのプロパティの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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*	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** [*drive-number*] [**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** *drive-number*	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 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。

次に、SAS という名前のストレージ カードの仮想ドライブに関する情報を表示する例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SAS
Server /chassis/storageadapter # show virtual-drive
Virtual Drive  Status          Name                      Size       RAID Level
-------------- --------------- ------------------------- ---------- ----------
0              Optimal         SLES1SP1beta5             30720 MB   RAID 0
1              Optimal         RHEL5.5                   30720 MB   RAID 0
2              Optimal         W2K8R2_DC                 30720 MB   RAID 0
3              Optimal         VD_3                      30720 MB   RAID 0
```

```
4              Optimal         ESX4.0u2                 30720 MB   RAID 0
5              Optimal         VMs                      285568 MB  RAID 0
6              Optimal         RHEL6-35GB               35840 MB   RAID 0
7              Optimal         OS_Ins_Test_DR           158720 MB  RAID 0
8              Optimal                                  285568 MB  RAID 1

Server /chassis/storageadapter #
```

次に、SAS という名前のストレージ カードの仮想ドライブ番号 1 に関する物理ドライブ情報を表示する例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SAS
Server /chassis/storageadapter # scope virtual-drive 1
Server /chassis/storageadapter/virtual-drive # show physical-drive
Span  Physical Drive Status     Starting Block Number Of Blocks
----- -------------- ---------- -------------- ----------------
0     12             online     62914560       62914560

Server /chassis/storageadapter/virtual-drive #
```

Nvidia GPU カード情報の表示

これらのコマンドは、すべての UCS C シリーズ サーバで使用できるわけではありません。

はじめる前に

Nvidia GPU カードの情報を表示するには、サーバの電源をオンにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **show gpu**	システム上の使用可能な Nvidia GPU カードを表示します。
ステップ 3	Server /chassis # **scope gpu** *slot-number*	GPU カード コマンド モードを開始します。GPU カードのスロット番号を指定します。
ステップ 4	Server /chassis/gpu # **show gpu-list**	GPU カードの温度情報を表示します。

次に、システム上の使用可能な GPU カードの温度情報を表示する例を示します。

```
Server # scope chassis
Server /chassis # show gpu

Slot       Product Name         Num of GPUs
----       ------------         -----------
5          Nvidia GRID K2 @ BD     2

Server /chassis # scope gpu 5
Server /chassis/gpu # show gpu-list

GPU ID       Temperature
------       -----------
0             32
1             33
```

```
Server /chassis/gpu #
```

PCI アダプタのプロパティの表示

はじめる前に

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

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
Slot Vendor ID Device ID  SubVendor ID SubDevice ID  Firmware Version Product Name
---- --------- ---------- ------------ ------------- ---------------- -------------------
L    0x8086    0x1521     0x1137        0x008b        0x80000AA5... Intel(R) I350 1 Gbps N...
1    0x19a2    0x0710     0x10df        0xe702        4.6.142.10    Emulex OCe11102-FX 2 p...
3    0x10de    0x118f     0x10de        0x097f        N/A           Nvidia TESLA K10 P2055...
4    0x14e4    0x1639     0x14e4        0x1639        N/A           Broadcom 5709 1 Gbps 2...
5    0x10de    0x0ff2     0x10de        0x1012        N/A           Nvidia GRID K1 P2401-502
M    0x1000    0x0073     0x1137        0x00b1        N/A           Cisco UCSC RAID SAS 20…

Server /chassis #
```

ネットワーク関連のプロパティの表示

LOM のプロパティの表示

LAN On Motherboard（LOM）イーサネット ポートの MAC アドレスを表示できます。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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 network-adapter** *slot ID*	特定のネットワーク アダプタのコマンド 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	Server /chassis/network-adapter # **show mac-list** [**detail**]	LOM ポートの MAC アドレスを表示します。

次に、LOM ポートの MAC アドレスを表示する例を示します。

```
Server# scope chassis
Server /chassis # scope network-adapter L
Server /chassis/network-adapter # show mac-list
Interface ID       MAC Address
-------------  --------------------
eth0            010000002000
eth1            010000002000

Server /chassis/network-adapter #
```

TPM のプロパティの表示

はじめる前に

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 # **showtpm-inventory**	TPM プロパティを表示します。

次に、TPM のプロパティを表示する例を示します。

```
Server# scope chassis
Server /chassis # show tpm-inventory

Version Presence  Enabled-Status  Active-Status  Ownership  Revision     Model
Vendor      Serial
------- --------  --------------  -------------- ---------- ---------  -------------
--------   -----------
 A      equipped    disabled       deactivated    unowned      1       UCSX-TPMX-00X   ABC
 Inc    FCHXXXXXXXX

Server /chassis #
```

第 5 章

センサーの表示

この章は、次の項で構成されています。

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# **scopesensor**	センサー コマンド モードを開始します。
ステップ 2	Server /sensor # **showpsu**	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 # **showpsu-redundancy**	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
------------  -------------- -------- ------ ------------ ------------  -------------
```

```
-------------
SU1_PIN       Normal        102      Watts      N/A        882             N/A
 1098
PSU2_PIN       Normal        96       Watts      N/A       882             N/A
 1098
PSU3_PIN       Normal        102      Watts      N/A       882             N/A
 1098
PSU4_PIN       Normal        96       Watts      N/A       882             N/A
 1098
PSU1_POUT      Normal        78       Watts      N/A       798             N/A
 996
PSU2_POUT      Normal        78       Watts      N/A       798             N/A
 996
PSU3_POUT      Normal        84       Watts      N/A       798             N/A
 996
PSU4_POUT      Normal        84       Watts      N/A       798             N/A
 996
POWER_USAGE    Normal        406      Watts      N/A       N/A             N/A
 2674
PSU1_DC_OK     Normal        good

PSU2_DC_OK     Normal        good

PSU3_DC_OK     Normal        good

PSU4_DC_OK     Normal        good

PSU1_AC_OK     Normal        good

PSU2_AC_OK     Normal        good

PSU3_AC_OK     Normal        good

PSU4_AC_OK     Normal        good

PSU1_STATUS    Normal        present

PSU2_STATUS    Normal        present

PSU3_STATUS    Normal        present

PSU4_STATUS    Normal        present

Server /sensor # show psu-redundancy
Name                 Reading         Sensor Status
-------------------- --------------- --------------------
PS_RDNDNT_MODE       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# **scopesensor**	センサー コマンド モードを開始します。
ステップ 2	Server /sensor # **showfan** [**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
--------------- -------------  ---------- ------ ------------- ------------ -------------
------------
PSU1_FAN_SPEED   Normal         5160       RPM    1118            N/A             946
  N/A
PSU2_FAN_SPEED   Normal         6106       RPM    1118            N/A             946
  N/A
PSU3_FAN_SPEED   Normal         5762       RPM    1118            N/A             946
  N/A
PSU4_FAN_SPEED   Normal         4988       RPM    1118            N/A             946
  N/A
FAN1_SPEED       Normal         6600       RPM    2040            N/A             1800
  N/A
FAN2_SPEED       Normal         6660       RPM    2040            N/A             1800
  N/A
FAN3_SPEED       Normal         6600       RPM    2040            N/A             1800
  N/A
FAN4_SPEED       Normal         6660       RPM    2040            N/A             1800
  N/A
FAN5_SPEED       Normal         6660       RPM    2040            N/A             1800
  N/A
FAN6_SPEED       Normal         6660       RPM    2040            N/A             1800
  N/A
FAN7_SPEED       Normal         6660       RPM    2040            N/A             1800
  N/A
FAN8_SPEED       Normal         6660       RPM    2040            N/A             1800
  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。
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 #
```

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 #
```

ストレージ 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 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。
[Status] カラム	ストレージ デバイスのステータスに関する簡単な説明。

名前	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。 （注） この情報は、一部の C シリーズ サーバのみで使用できます。

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
-------------------- --------------------
HDD_01_STATUS        present
HDD_02_STATUS        present
HDD_03_STATUS        present
HDD_04_STATUS        present

Server /chassis #
```

第 6 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 Cisco IMC 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（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
- 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（ISO または IMG ファイル）
- ネットワーク上の 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 OS をインストールできます。

（注） Cisco UCS C3260 サーバに KVM コンソールを正常に設定するには、Cisco IMC、CMC および BMC コンポーネントの IP アドレスを設定する必要があります。CLI インターフェイスまたは Web UI を使用してこれらのコンポーネントの IP アドレスを設定できます。CLI の場合は、コマンド **scope network** を使用するか、または **scope <chassis/server1/2><cmc/bmc><network>** を使用して設定を表示します。

Web インターフェイスでネットワーク コンポーネントの IP アドレスを設定するには、「ネットワーク関連の設定」の項に記載する手順を参照してください。

（注） KVM コンソールの操作には、GUI 以外は使用できません。KVM コンソールの起動手順については、『*Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*』を参照してください。

仮想 KVM のイネーブル化

はじめる前に

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

	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

はじめる前に

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

	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。

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

はじめる前に

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

	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。

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 #
```

次の作業

GUI から仮想 KVM を起動します。

仮想メディアの設定

はじめる前に

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# **scopevmedia**	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 # **setenabled** {**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。 （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 # **setencryption** {**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 # **setlow-power-usb-enabled** {**yes** | **no**}	低電力USBをイネーブルまたはディセーブルにします。 （注） UCS VIC P81E カードを持つサーバに ISO をマッピングしているときに NIC が Cisco Card モードである場合： • 低電力 USB をイネーブルにすると、ISO をマッピングしてホストを再起動した後にカードがリセットされ、ISOマッピングは失われます。仮想ドライブはブートの選択メニューに表示されません。 • 低電力USBをディセーブルにすると、ISO をマッピングしてホストと Cisco IMC を再起動した後、ブートの選択メニューに仮想ドライバが正しく表示されます。
ステップ 5	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 6	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 *# set low-power-use-enabled no
Server /vmedia *# commit
Server /vmedia # show detail
vMedia Settings:
    Encryption Enabled: yes
    Enabled: yes
    Max Sessions: 1
    Active Sessions: 0
    Low Power USB Enabled: no

Server /vmedia #
```

次の作業

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。

Cisco IMC マップされた vMedia ボリュームの設定

はじめる前に

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 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 # **map-cifs** {**volume-name** | **remote-share** | **remote-file-path** [*mount options*]	vMedia の CIFS ファイルをマッピングします。次を指定する必要があります。 • 作成するボリュームの名前 • IP アドレスおよびエクスポートされるディレクトリを含むリモート共有 • エクスポートされるディレクトリに対応するリモート ファイルのパス。 • （任意）マッピング オプション • サーバに接続するためのユーザ名とパスワード
ステップ 3	Server /vmedia # **map-nfs** {**volume-name** | **remote-share** | **remote-file-path**} [*mount options*]	vMedia の NFS ファイルをマッピングします。次を指定する必要があります。 • 作成するボリュームの名前 • IP アドレスおよびエクスポートされるディレクトリを含むリモート共有

	コマンドまたはアクション	目的
		• エクスポートされるディレクトリに対応するリモート ファイルのパス。 • （任意）マッピング オプション
ステップ 4	Server /vmedia # **map-www** {**volume-name** | **remote-share** | **remote-file-path** [*mount options*]	vMedia の HTTPS ファイルをマッピングします。次を指定する必要があります。 • 作成するボリュームの名前 • IP アドレスおよびエクスポートされるディレクトリを含むリモート共有 • エクスポートされるディレクトリに対応するリモート ファイルのパス。 • （任意）マッピング オプション • サーバに接続するためのユーザ名とパスワード

次に、CIFS Cisco IMC マップされた vmedia 設定を作成する例を示します。

```
Server # scope vmedia
Server /vmedia # map-cifs sample-volume //10.10.10.10/project /test/sample
Server username:
Server password: ****
Confirm password: ****

Server /vmedia #
```

Cisco IMC マップされた vMedia ボリュームのプロパティの表示

はじめる前に

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 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 # **show mappings***detail*	設定されたすべての vMedia マッピングの情報を表示します。

次に、設定されたすべての vMedia マッピングのプロパティを表示する例を示します。

```
Server # scope vmedia
Server /vmedia # show mappings

Volume  Map-status   Drive-type     remote-share        remote-file               mount-type
------  ----------  ------------  --------------------- --------------------       -----------

Huu     OK           removable    http://10.104.236.99/ rhel-server-6.1-x86_6.iso      www
Rhel    OK           CD           http://10.104.236.99/ rhel-server-6.1-x86_6.iso      www
```

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、Cisco IMC 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
- フロー制御なし
- 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

はじめる前に

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 # **set comport** {**com0** | **com1**	（任意） システムが SoL 通信をルーティングするシリアル ポートを設定します。 （注） このフィールドは一部のCシリーズサーバだけで使用できます。使用できない場合、サーバは、SoL 通信に COM ポート 0 を使用します。 次を指定することができます。 • [com0]：SoL 通信は、外部デバイスへの物理 RJ45 接続またはネットワーク デバイスへの仮想 SoL 接続をサポートする、外部からアクセス可能なシリアル ポートであるCOMポート0を介してルーティングされます。 このオプションを選択すると、システムは、SoL をイネーブルにし、RJ45 接続をディセーブルにします。これは、サーバが外部シリアル デバイスをサポートできなくなることを意味します。 • [com1]：SoL 通信は、SoL だけを介してアクセス可能な内部ポートである、COM ポート 1 経由でルーティングされます。 このオプションを選択した場合、COM ポート 1 上の SoL および COM ポート 0 上の物理 RJ45 接続を使用できます。 （注） comport 設定を変更すると、既存のすべての SoL セッションは切断されます。
ステップ 5	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 6	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)  Com Port
------- --------------- --------
yes     115200          com2
Server /sol # show detail
Serial Over LAN:
    Enabled: yes
    Baud Rate(bps): 115200
    Com Port: com2
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。

次の作業

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 7 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

はじめる前に

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# **scopeuser***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。

	コマンドまたはアクション	目的
ステップ 2	Server /user # **setenabled** {**yes** | **no**}	Cisco IMC 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 # **setname***username*	ユーザのユーザ名を指定します。
ステップ 4	Server /user # **setpassword**	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 # **setrole** {**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
		  • タイム ゾーンを設定する
		  • IP アドレスを ping する
		• 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
```

強力なパスワードの無効化

Cisco IMC では、強力なパスワード ポリシーが実装されるようになったため、サーバに最初にログインした際に、ガイドラインに従って強力なパスワードを設定するよう要求されます。Cisco IMC の CLI では、強力なパスワード ポリシーを無効にし、ガイドラインを無視して希望するパスワードを設定することができます。強力なパスワードを無効にすると、[Enable Strong Password] ボタンが表示されます。デフォルトでは、強力なパスワード ポリシーが有効になっています。

はじめる前に

このアクションを実行するには、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# **scopeuser-policy**	ユーザ ポリシー コマンド モードを開始します。
ステップ 2	Server /user-policy # **setpassword-policy** {**enabled** | **disabled**}	確認プロンプトで、y を入力してアクションを完了するか、または n を入力してアクションをキャンセルします。強力なパスワードを有効または無効にします。
ステップ 3	Server /user-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。

次に、強力なパスワードを無効にする例を示します。

```
Server# scope user-policy
Server /user-policy # set password-policy disabled
Warning: Strong password policy is being disabled.
Do you wish to continue? [y/N] y
Server /user-policy *# commit
Server /user-policy #
```

LDAP サーバ

Cisco IMC 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。Cisco IMC は、ネットワークでディレクトリ情報を保管および保守する Lightweight Directory Access Protocol（LDAP）をサポートします。さらに、Cisco IMC 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。Cisco IMC は LDAP での Kerberos ベースの認証サービスを利用します。

Cisco IMC で LDAP が有効になっている場合、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。

サーバの Active Directory 設定で暗号化をイネーブルにすることで、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

ユーザ認証および権限付与のために LDAP を使用するよう、Cisco IMC を設定できます。LDAP を使用するには、Cisco IMC に関するユーザ ロール情報とロケール情報を保持する属性を使ってユーザを設定します。Cisco IMC 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、Cisco IMC 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。

手順

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。

Properties	値
Common Name	CiscoAVPair
LDAP Display Name	CiscoAVPair
Unique X500 Object ID	1.3.6.1.4.1.9.287247.1
説明	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 Cisco IMC 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。

次の作業

Cisco IMC を使用して LDAP サーバを設定します。

Cisco IMC 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、Cisco IMC で LDAP を設定します。

はじめる前に

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# **scopeldap**	LDAP コマンド モードを開始します。
ステップ 2	Server /ldap # **setenabled** {**yes** | **no**}	LDAP セキュリティをイネーブルまたはディセーブルにします。LDAP セキュリティがイネーブルの場合、ローカル ユーザ 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 # **setdomain***LDAP domain name*	LDAP ドメイン名を指定します。

	コマンドまたはアクション	目的
ステップ 4	Server /ldap # **settimeout***seconds*	LDAP 検索操作がタイムアウトするまで Cisco IMC 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 # **setencrypted** {**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 # **setbase-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 # **setattribute***name*	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。 Cisco IMC 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 # **setfilter-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。

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 #
```

次の作業

グループ許可用に LDAP グループを使用する場合は、「*Cisco IMC での LDAP グループの設定*」を参照してください。

Cisco IMC 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 Cisco IMC 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。

はじめる前に

- 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

	コマンドまたはアクション	目的
ステップ 1	Server# **scopeldap**	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# **scopeldap-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 # **setgroup-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 # **scoperole-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 # **setname***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 # **setdomain***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 # **setrole** {**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。

	コマンドまたはアクション	目的
		• **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。

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 #
```

LDAPグループでのネストされたグループの検索深度の設定

LDAP グループ マップで別の定義済みグループ内にネストされた LDAP グループを検索することができます。

- 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

	コマンドまたはアクション	目的
ステップ 1	Server# **scopeldap**	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# **scopeldap-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 # **setgroup-search-depth***value*	ネストされた LDAP グループの検索を有効にします。
ステップ 4	Server /ldap/role-group-rule # **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、別の定義済みのグループ内にネストされた LDAP グループの検索を実行するために検索する例を示します。

```
Server# scope ldap
Server /ldap # scope ldap-group-rule
Server /ldap/ldap-group-rule # set group-search-depth 10
Server /ldap/role-group-rule* # commit
Server /ldap/role-group-rule # show detail
Group rules for LDAP:
    Group search attribute: memberOf
    Enable Group Authorization: yes
    Nested group search depth: 10
Server/ldap/ldap-group-rule #
```

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# **showuser-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。
[User name] 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。シリアル接続の場合は、[N/A] と表示されます。
[Type] カラム	ユーザがサーバにアクセスするために選択したセッションタイプ。次のいずれかになります。 • [webgui]：ユーザが Web UI を使用してサーバに接続されていることを示します。 • [CLI]：ユーザが CLI を使用してサーバに接続されていることを示します。 • [serial]：ユーザがシリアル ポートを使用してサーバに接続されていることを示します。
[Action] カラム	このカラムには、SOL が有効の場合は [N/A] と表示され、SOL が無効の場合は [Terminate] と表示されます。Web UI で [Terminate] をクリックすることでセッションを終了できます。

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

はじめる前に

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

	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。

	コマンドまたはアクション	目的
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 8 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。

サーバ NIC の設定

サーバの NIC

NIC モード

NIC モード設定は、Cisco IMC に到達できるポートを決定します。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]：Cisco IMC へのアクセスに使用される管理ポート。
- [Shared LOM]：Cisco IMC へのアクセスに使用できる任意の LOM（LAN on Motherboard）ポート。

- [Shared LOM 10G]：どの 10G LOM ポートも、Cisco IMC にアクセスするために使用できます。
- [Cisco Card]：Cisco IMC へのアクセスに使用できるアダプタ カード上の任意のポート。Cisco アダプタ カードは、ネットワーク通信サービス インターフェイス プロトコル サポート（NCSI）のあるスロットに取り付ける必要があります。
- [Shared LOM Extended]：Cisco IMC へのアクセスに使用できる任意の LOM ポートまたはアダプタ カードのポート。Cisco アダプタ カードは NCSI サポートのあるスロットに取り付ける必要があります。

（注） [Shared LOM Extended] および [Shared LOM 10G] は、一部の UCS C シリーズ サーバでのみ使用できます。

NIC 冗長化

選択した NIC モードとプラットフォームに応じて、次の NIC 冗長化オプションを使用できます。

- [none]：設定されている NIC モードに関連付けられた各ポートは個別に動作します。問題が発生した場合、ポートは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、設定されている NIC モードに関連付けられたすべてのポートは同時に動作します。この機能により、スループットが増加し、Cisco IMC への複数のパスが提供されます。
- [active-standby]：設定されている NIC モードに関連付けられたポートで障害が発生した場合、トラフィックは、その NIC モードに関連付けられている他のポートの 1 つにフェールオーバーします。

（注） このオプションを選択する場合は、設定されている NIC モードに関連付けられたすべてのポートが同じサブネットに接続され、どのポートが使用されてもトラフィックの安全が保証されるようにする必要があります。

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。使用可能なモードについては、使用するサーバの『*Hardware Installation Guide*』（HIG）を参照してください。C シリーズの HIG は、次の URL にあります。http://www.cisco.com/en/US/products/ps10493/prod_installation_guides_list.html

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。

はじめる前に

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scopecimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scopenetwork**	Cisco IMC 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 # **setmode** {**dedicated** | **shared_lom** | **shared_lom_10g** | **shipping** | **cisco_card**}	NIC モードを次のいずれかに設定します。 • Dedicated：Cisco IMC 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：Cisco IMC 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 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。 • Shared LOM 10G：Cisco IMC へのアクセスに 10 G LOM イーサネット ホスト ポートを使用します。 • 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。 • Cisco Card：Cisco IMC へのアクセスにアダプタ カードのポートを使用します。
ステップ 4	Server /cimc/network # **set vic-slot** {**none** | **riser1** | **riser2** | **flex-lom**}	VIC スロットは、FLEX LOM、あるいはライザー 1 スロットまたはライザー 2 スロットで使用可能なシスコのカードに設定できます。 C220 M4 サーバでは、VIC スロット オプションは次のとおりです。 • Riser 1：スロット 1 が選択されます。 • Riser 2：スロット 2 が選択されます。 • FLEX LOM：スロット 3（MLOM）が選択されます。 C240 M4 サーバでは、VIC スロット オプションは次のとおりです。

	コマンドまたはアクション	目的
		• Riser 1：スロット 2 がプライマリ スロットですが、スロット 1 も使用できます。 • Riser 2：スロット 5 がプライマリ スロットですが、スロット 4 も使用できます。 • FLEX LOM：スロット 7（MLOM）が選択されます。 **重要** VIC スロットが適用されるのは、シスコのカードおよび一部の UCS C シリーズ サーバのみです。
ステップ 5	Server /cimc/network # **setredundancy** {**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 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。 （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。
ステップ 7	プロンプトで、y を入力して確認します。	サーバ NIC の設定

次に、Cisco IMC 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。

```
scope cimc
Server /cimc # scope network
Server /cimc/network # set mode cisco_card
Server /cimc/network # set vic-slot <flex-lom>
Server /cimc/network *# set redundancy <active-active>
Server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network #
```

共通プロパティの設定

共通プロパティの設定の概要

Hostname

ダイナミックホストコンフィギュレーションプロトコル（DHCP）拡張機能は、ホスト名をDHCPパケットに追加することで利用でき、DHCPサーバ側でこれを解釈または表示できます。ホスト名はDHCPパケットのオプションフィールドに追加され、最初にDHCPサーバに送信されるDHCP DISCOVERパケットで送信されます。

サーバのデフォルトのホスト名はucs-c2XXからCXXX-YYYYYYに変更されます（XXXはサーバのモデル番号で、YYYYYYはシリアル番号です）。この一意のストリングはクライアントIDとして機能し、DHCPサーバからCisco IMCにリースされるIPアドレスを追跡してマッピングするのに役立ちます。サーバのステッカーまたはラベルとしてデフォルトシリアル番号が製造者から提供され、サーバを識別するのに役立ちます。

ダイナミック DNS

ダイナミックDNS（DDNS）は、Cisco IMCからDNSサーバのリソースレコードを追加または更新するために使用されます。Web UIまたはCLIを使用してダイナミックDNSをイネーブルにできます。[DDNS]オプションをイネーブルにすると、DDNSサービスは現在のホスト名、ドメイン名、および管理IPアドレスを記録し、Cisco IMCからDNSサーバのリソースレコードを更新します。

（注） DDNSサーバは、次のDNS設定のいずれかが変更された場合に、DNSサーバの以前のリソースレコード（もしあれば）を削除し、新しいリソースレコードを追加します。

- Hostname
- LDAP設定のドメイン名
- DDNSとDHCPがイネーブルの場合に、ネットワークまたはサブネットの変更による新しいIPアドレスまたはDNS IPまたはドメイン名をDHCPが取得する場合。
- DHCPがディセーブルの場合に、CLIまたはWeb UIを使用してスタティックIPアドレスを設定する場合。
- **dns-use-dhcp** コマンドを入力したとき。

[Dynamic DNS Update Domain]：ドメインを指定できます。ドメインは、メインドメインまたはサブドメインのどちらでも可です。このドメイン名は、DDNS更新のためCisco IMCのホスト名に付加されます。

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。

はじめる前に

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scopecimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scopenetwork**	Cisco IMC 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 # **sethostname***host-name*	ホストの名前を指定します。 ホスト名の変更時に、コモン ネーム（CN）を使用した新しい自己署名証明書を新しいホスト名として作成するかどうかを確認するプロンプトが表示されます。 プロンプトに **y** と入力した場合、CN を使用した新しい自己署名証明書が新しいホスト名として作成されます。 プロンプトに **n** と入力すると、ホスト名だけが変更され、証明書は生成されません。
ステップ 4	Server /cimc/network # **setddns-enabled**	（任意） Cisco IMC に対して DDNS サービスを有効にします。
ステップ 5	Server /cimc/network # **setddns-update-domain***value*	（任意） 選択したドメインまたはそのサブドメインを更新します。
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	プロンプトで、y を入力して確認します。	共通プロパティを設定します。

次に、共通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
Create new certificate with CN as new hostname? [y|N]
```

```
y
New certificate will be generated on committing changes.
All HTTPS and SSH sessions will be disconnected.
Server /cimc/network # set ddns-enabled
Server /cimc/network # set ddns-update-domain 1.2.3.4
Server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network #
```

次の作業

ネットワークへの変更がすぐに適用されます。Cisco IMC への接続が切断され、再度ログインが必要な場合があります。新しいSSHセッションが作成されたため、ホストキーを確認するプロンプトが表示される場合があります。

IPv4 の設定

はじめる前に

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scopecimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scopenetwork**	Cisco IMC 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 # **setdhcp-enabled** {**yes** | **no**}	Cisco IMC 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、Cisco IMC 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 Cisco IMC 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 # **setv4-addr***ipv4-address*	Cisco IMC 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 5	Server /cimc/network # **setv4-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 # **setv4-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 # **setdns-use-dhcp** {**yes** | **no**}	Cisco IMC 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 # **setpreferred-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 # **setalternate-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	プロンプトで、y を入力して確認します。	IPv4 を設定します。
ステップ 12	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
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network # 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
    IPv6 Enabled: no
    IPv6 Address: ::
    IPv6 Prefix: 64
    IPv6 Gateway: ::
    IPv6 Link Local: ::
    IPv6 SLAAC Address: ::
```

```
    IPV6 DHCP Enabled: no
    IPV6 Obtain DNS Server by DHCP: no
    IPV6 Preferred DNS: ::
    IPV6 Alternate DNS: ::
    VLAN Enabled: no
    VLAN ID: 1
    VLAN Priority: 0
    Port Profile:
    Hostname: C240-FCH1938V17L
    MAC Address: E4:AA:5D:AD:19:81
    NIC Mode: shared_lom_ext
    NIC Redundancy: active-active
    VIC Slot: riser1
    Auto Negotiate: no
    Admin Network Speed: NA
    Admin Duplex: NA
    Operational Network Speed: NA
    Operational Duplex: NA

Server /cimc/network #
```

IPv6 の設定

はじめる前に

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scopecimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scopenetwork**	Cisco IMC 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 # **setv6-enabled** {**yes** | **no**}	IPv6 を有効にします。

	コマンドまたはアクション	目的
ステップ 4	Server /cimc/network # **setv6-dhcp-enabled** {**yes** | **no**}	Cisco IMC 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、Cisco IMC 用に 1 つの IPv6 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 Cisco IMC 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 Ipv6 アドレスを予約する必要があります。
ステップ 5	Server /cimc/network # **setv6-addr***ipv6-address*	Cisco IMC の IP アドレスを指定します。
ステップ 6	Server /cimc/network # **setv6-prefix***ipv6-prefix-length*	IP アドレスのプレフィックス長を指定します。
ステップ 7	Server /cimc/network # **setv6-gateway***gateway-ipv6-address*	IP アドレスのゲートウェイを指定します。
ステップ 8	Server /cimc/network # **setv6-dns-use-dhcp** {**yes** | **no**}	Cisco IMC 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。 （注） DHCP がイネーブルである場合にのみ、このオプションを使用できます。
ステップ 9	Server /cimc/network # **setv6-preferred-dns-server***dns1-ipv6-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 10	Server /cimc/network # **setv6-alternate-dns-server***dns2-ipv6-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 11	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 12	プロンプトで、y を入力して確認します。	IPv6 を設定します。
ステップ 13	Server /cimc/network # **show** [**detail**]	（任意）IPv6 ネットワークの設定を表示します。

次に、スタティック IPv6 をイネーブルにし、IPv6 ネットワークの設定を表示する例を示します。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set v6-enabled yes
Server /cimc/network *# set v6-addr 2010:201::279
Server /cimc/network *# set v6-gateway 2010:201::1
Server /cimc/network *# set v6-prefix 64
Server /cimc/network *# set v6-dns-use-dhcp no
Server  /cimc/network *# set v6-preferred-dns-server 2010:201::100
Server  /cimc/network *# set v6-alternate-dns-server 2010:201::101
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network # show detail
Network Setting:
    IPv4 Enabled: yes
    IPv4 Address: 10.106.145.76
    IPv4 Netmask: 255.255.255.0
    IPv4 Gateway: 10.106.145.1
    DHCP Enabled: yes
    DDNS Enabled: yes
    DDNS Update Domain: example.com
    Obtain DNS Server by DHCP: no
    Preferred DNS: 171.70.168.183
    Alternate DNS: 0.0.0.0
    IPv6 Enabled: yes
    IPv6 Address: 2010:201::279
    IPv6 Prefix: 64
    IPv6 Gateway: 2010:201::1
    IPv6 Link Local: fe80::523d:e5ff:fe9d:395d
    IPv6 SLAAC Address: 2010:201::523d:e5ff:fe9d:395d
    IPV6 DHCP Enabled: no
    IPV6 Obtain DNS Server by DHCP: no
    IPV6 Preferred DNS: 2010:201::100
    IPV6 Alternate DNS: 2010:201::101
    VLAN Enabled: no
    VLAN ID: 1
    VLAN Priority: 0
    Port Profile:
    Hostname: CIMC_C220
    MAC Address: 50:3D:E5:9D:39:5C
    NIC Mode: dedicated
    NIC Redundancy: none
    Network Speed: 100Mbps
    Duplex: full
    Auto Negotiate: no
   Admin Network Speed: NA
    Admin Duplex: NA
    Operational Network Speed: NA
    Operational Duplex: NA

Server /cimc/network #
```

次に、DHCP for IPv6 をイネーブルにし、IPv6 ネットワークの設定を

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set v6-enabled yes
Server /cimc/network *# set v6-dhcp-enabled yes
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network # show detail
Network Setting:
    IPv4 Enabled: yes
```

```
    IPv4 Address: 10.106.145.76
    IPv4 Netmask: 255.255.255.0
    IPv4 Gateway: 10.106.145.1
    DHCP Enabled: yes
    DDNS Enabled: yes
    DDNS Update Domain: example.com
    Obtain DNS Server by DHCP: no
    Preferred DNS: 171.70.168.183
    Alternate DNS: 0.0.0.0
    IPv6 Enabled: yes
    IPv6 Address: 2010:201::253
    IPv6 Prefix: 64
    IPv6 Gateway: fe80::222:dff:fec2:8000
    IPv6 Link Local: fe80::523d:e5ff:fe9d:395d
    IPv6 SLAAC Address: 2010:201::523d:e5ff:fe9d:395d
    IPV6 DHCP Enabled: yes
    IPV6 Obtain DNS Server by DHCP: no
    IPV6 Preferred DNS: ::
    IPV6 Alternate DNS: ::
    VLAN Enabled: no
    VLAN ID: 1
    VLAN Priority: 0
    Port Profile:
    Hostname: CIMC_C220
    MAC Address: 50:3D:E5:9D:39:5C
    NIC Mode: dedicated
    NIC Redundancy: none
    Network Speed: 100Mbps
    Duplex: full
    Auto Negotiate: no
    Admin Network Speed: NA
    Admin Duplex: NA
    Operational Network Speed: NA
    Operational Duplex: NA

Server /cimc/network #
```

サーバ VLAN の設定

はじめる前に

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scopecimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scopenetwork**	Cisco IMC 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 # **setvlan-enabled** {**yes** | **no**}	Cisco IMC 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 # **setvlan-id***id*	VLAN 番号を指定します。

	コマンドまたはアクション	目的
ステップ 5	Server /cimc/network # **setvlan-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	プロンプトで、y を入力して確認します。	サーバ LAN を設定します。
ステップ 8	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
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network # 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
    IPv6 Enabled: no
    IPv6 Address: ::
    IPv6 Prefix: 64
    IPv6 Gateway: ::
    IPv6 Link Local: ::
    IPv6 SLAAC Address: ::
    IPV6 DHCP Enabled: no
    IPV6 Obtain DNS Server by DHCP: no
    IPV6 Preferred DNS: ::
    IPV6 Alternate DNS: ::
    VLAN Enabled: yes
    VLAN ID: 10
    VLAN Priority: 32
    Port Profile:
    Hostname: C240-FCH1938V17L
    MAC Address: E4:AA:5D:AD:19:81
    NIC Mode: shared_lom_ext
    NIC Redundancy: active-active
    VIC Slot: riser1
    Auto Negotiate: no
    Admin Network Speed: NA
    Admin Duplex: NA
    Operational Network Speed: NA
    Operational Duplex: NA

Server /cimc/network #
```

ポート プロファイルへの接続

（注） ポートプロファイルまたはVLANを設定できますが、両方を使用することはできません。ポート プロファイルを使用する場合は、**set vlan-enabled** コマンドが **no** に設定されていることを確認します。

はじめる前に

ポート プロファイルに接続するには、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# **scopecimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scopenetwork**	Cisco IMC 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 # **setport-profile***port_profile_name*	Cisco UCS VIC 1225 仮想インターフェイス カードなど、サポートされているアダプタ カード上の管理インターフェイス、仮想イーサネット、VIF を設定するためにポート プロファイル Cisco IMC を使用するように指定します。 最大 80 文字の英数字を入力します。-（ハイフン）と _（アンダースコア）を除き、スペースなどの特殊文字は使用できません。ポート プロファイル名をハイフンで始めることもできません。 （注） ポート プロファイルは、このサーバが接続されているスイッチに定義されている必要があります。
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。
ステップ 5	プロンプトで、y を入力して確認します。	ポート プロファイルに接続します。
ステップ 6	Server /cimc/network # **show** [**detail**]	（任意） ネットワーク設定を表示します。

次に、ポート プロファイル abcde12345 に接続する例を示します。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set port-profile abcde12345
Server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network # show detail
Network Setting:
    IPv4 Address: 10.193.66.174
    IPv4 Netmask: 255.255.248.0
    IPv4 Gateway: 10.193.64.1
    DHCP Enabled: no
    Obtain DNS Server by DHCP: no
    Preferred DNS: 0.0.0.0
    Alternate DNS: 0.0.0.0
    IPv6 Enabled: no
    IPv6 Address: ::
    IPv6 Prefix: 64
    IPv6 Gateway: ::
    IPv6 Link Local: ::
    IPv6 SLAAC Address: ::
    IPV6 DHCP Enabled: no
    IPV6 Obtain DNS Server by DHCP: no
    IPV6 Preferred DNS: ::
    IPV6 Alternate DNS: ::
    VLAN Enabled: no
    VLAN ID: 1
    VLAN Priority: 0
    Port Profile: abcde12345
    Hostname: C240-FCH1938V17L
    MAC Address: E4:AA:5D:AD:19:81
    NIC Mode: shared_lom_ext
    NIC Redundancy: active-active
    VIC Slot: riser1
    Auto Negotiate: no
    Admin Network Speed: NA
    Admin Duplex: NA
    Operational Network Speed: NA
    Operational Duplex: NA

Server /cimc/network #
```

ネットワーク インターフェイスの設定

ネットワーク インターフェイス設定の概要

Cisco IMC 管理ポートのネットワーク速度とデュプレックス モードを設定するために、このサポートが追加されています。自動ネゴシエート モードは、専用モードでのみ設定できます。自動ネゴシエーションを有効にすると、ネットワーク ポート速度とデュプレックスの設定がシステムによって無視され、Cisco IMC がスイッチに設定された速度を保持します。自動ネゴシエーションを無効にすると、ネットワーク ポート速度（10 Mbps、100 Mbps、または1 Gbps）を設定し、デュプレックス値を [Full] または [Half] で設定できます。

ポート プロパティは次の 2 つのモードで管理できます。

- [Admin Mode]：[Auto Negotiation] オプションを無効にすることで、ネットワーク速度とデュプレックス値を設定できます。admin モードのネットワーク速度のデフォルト値は 100 Mbps

で、デュプレックス モードは [Full] に設定されます。ネットワーク速度を変更する前に、接続したスイッチに同じポート速度があることを確認します。

- [Operation Mode]：運用ネットワークのポート速度とデュプレックス値が表示されます。自動ネゴシエーション モードを有効にした場合は、スイッチのネットワーク ポート速度とデュプレックスの詳細が表示されます。オフにした場合は、[Admin Mode] で設定したネットワーク ポート速度とデュプレックス値が表示されます。

Cisco IMC 1.5(x)、2.0(1)、および 2.0(3) バージョンを工場出荷時の初期状態にリセットすると、[Shared LOM] モードがデフォルトで設定されます。

C3160 サーバの場合、工場出荷時の初期状態にリセットすると、[Dedicated] モードが [Full] デュプレックス モードに設定され、速度はデフォルトで 100 Mbps になります。

インターフェイス プロパティの設定

速度またはデュプレックスの不一致を回避するために、スイッチの設定を Cisco IMC 設定と一致させる必要があります。

重要 このアクションを使用できるのは一部の UCS C シリーズ サーバだけです。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scopecimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server/cimc # **scopenetwork**	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* # **setmodededicated**	dedicated コマンド モードを開始します。
ステップ 4	Server/cimc/network # **setauto-negotiate {yes | no}**	自動ネゴシエーション コマンド モードをイネーブルまたはディセーブルにします。 • **yes** を入力した場合、ネットワーク ポート速度とデュプレックス設定は無視され、Cisco IMC はスイッチに設定された速度を保持します。 • **no** を入力した場合は、ネットワーク ポート速度とディプレックス値を設定できます。

	コマンドまたはアクション	目的
ステップ 5	Server/cimc/network # **setnet-speed** {**10 Mbps** | **100 Mbps** | **1 Gbps**}	指定したネットワーク ポート速度を設定します。 （注） このオプションは、[auto-negotiate] が [no] に設定されている場合にのみ使用できます。ポート速度を変更する前に、接続しているスイッチのポート速度が同じであることを確認してください。[Auto-negotiate] が [yes] に設定されている場合、ネットワーク ポート速度はデフォルトで 100 Mbps に設定されます。
ステップ 6	Server/cimc/network* # **setduplex** {**full** | **half**}	指定されたデュプレックス モードのタイプを設定します。デフォルトでは、デュプレックス モードは [Full] に設定されます。 （注） ネットワーク速度が 1 Gbps の場合、全二重モードのみが許可されます。

次に、インターフェイス 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 cimc
Server/cimc # scope network
Server/cimc/network* # set mode dedicated
Server/cimc/network # set auto-negotiate no
Warning: You have chosen to set auto-negotiate to no
 Please set speed and duplex
 If not set then a default speed of 100Mbps and duplex full will be applied
Server/cimc/network* # commit
Server/cimc/network* # set net-speed 100 Mbps
Server/cimc/network # set duplex full
Server/cimc/network* # commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server/cimc/network #
```

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

Cisco IMC 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、サービス拒否（DoS）攻撃から保護するために使用されます。Cisco IMC 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。

はじめる前に

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scopecimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scopenetwork**	Cisco IMC 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 # **scopeipblocking**	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 # **setenabled** {**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 # **setfail-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 # **setfail-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 # **setpenalty-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 #
```

ネットワーク タイム プロトコルの設定

ネットワーク タイム プロトコル設定の設定

デフォルトでは、Cisco IMC がリセットされると、ホストと時刻が同期されます。NTP サービスを導入すると、Cisco IMC を設定して NTP サーバで時刻を同期することができます。デフォルトでは、NTP サーバは Cisco IMC で動作しません。少なくとも 1 台、最大 4 台の、NTP サーバまたは時刻源サーバとして動作するサーバの IP/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、Cisco IMC 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 Cisco IMC 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。

はじめる前に

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 cimc**	Cisco IMC 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 # **scope ntp**	NTP サービス 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**	サーバの NTP サービスをイネーブルにします。
ステップ 5	Server /cimc/network/ntp* # **commit**	トランザクションをコミットします。

	コマンドまたはアクション	目的
ステップ 6	Server /cimc/network/ntp # **set server-1 10.120.33.44**	NTP サーバまたは時刻源サーバとして機能する 4 台のサーバのうち 1 台のサーバの IP/DNS アドレスを指定します。
ステップ 7	Server /cimc/network/ntp # **set server-2 10.120.34.45**	NTP サーバまたは時刻源サーバとして機能する 4 台のサーバのうち 1 台のサーバの IP/DNS アドレスを指定します。
ステップ 8	Server /cimc/network/ntp # **set server-3 10.120.35.46**	NTP サーバまたは時刻源サーバとして機能する 4 台のサーバのうち 1 台のサーバの IP/DNS アドレスを指定します。
ステップ 9	Server /cimc/network/ntp # **set server-4 10.120.36.48**	NTP サーバまたは時刻源サーバとして機能する 4 台のサーバのうち 1 台のサーバの IP/DNS アドレスを指定します。
ステップ 10	Server /cimc/network/ntp # **commit**	トランザクションをコミットします。

次に、NTP サービスを設定する例を示します。

```
Server # scope cimc
Server /cimc # scope network
Server /cimc/network # scope ntp
Server /cimc/network/ntp # set enabled yes
Warning: IPMI Set SEL Time Command will be
disabled if NTP is enabled.
Do you wish to continue? [y|N]
y
Server /cimc/network/ntp* # commit
Server /cimc/network/ntp # set server-1 10.120.33.44
Server /cimc/network/ntp* # set server-2 10.120.34.45
Server /cimc/network/ntp* # set server-3 10.120.35.46
Server /cimc/network/ntp* # set server-4 10.120.36.48
Server /cimc/network/ntp* # commit
Server /cimc/network/ntp #
```

IP アドレスの ping

Cisco IMC の IP アドレスとのネットワーク接続を検証する場合に IP アドレスを ping します。

はじめる前に

IP アドレスを ping するには、管理者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# **scopecimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scopenetwork**	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# **pingaddress***IP address* | **retries***number* | **timeout***seconds*	IPアドレスまたはホスト名をタイムアウトまでの指定回数 ping します。 • IP address/hostname：サーバの IP アドレスまたはホスト名。 • Number of retries：システムがサーバへの接続を試行する回数。デフォルト値は3です。有効な範囲は 1 ～ 10 です。 • Timeout：システムが ping を中止するまでに待機する秒数。デフォルトの最大値は 20 秒です。有効な範囲は、1 ～ 20 秒です。
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。
ステップ 5	プロンプトで、y を入力して確認します。	IP アドレスを ping します。

次に IP アドレスを ping する例を示します。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # ping 10.10.10.10
Server /cimc/network *# commit
Changes to the network settings will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Server /cimc/network #
```

第 9 章

ネットワーク アダプタの管理

この章は、次の項で構成されています。

Cisco UCS C シリーズ ネットワーク アダプタの概要

（注） この章の手順は、Cisco UCS C シリーズ ネットワーク アダプタがシャーシに設置される場合にのみ使用できます。

Cisco UCS C シリーズ ネットワーク アダプタを設置することで、I/O の統合と仮想化をサポートするためのオプションが提供されます。次のアダプタを使用できます。

- Cisco UCS P81E 仮想インターフェイス カード
- Cisco UCS VIC 1225 仮想インターフェイス カード
- Cisco UCS VIC 1385 仮想インターフェイス カード
- Cisco UCS VIC 1227T 仮想インターフェイス カード

- Cisco UCS VIC 1387 仮想インターフェイス カード

対話型の*UCS* ハードウェアおよびソフトウェア相互運用性ユーティリティを使用すると、選択したサーバモデルとソフトウェアリリース用のサポートされているコンポーネントと構成を表示できます。このユーティリティは次の URL で入手できます。http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html

Cisco UCS P81E 仮想インターフェイス カード

Cisco UCS P81E 仮想インターフェイス カードは、仮想化された環境、物理環境のモビリティ強化を求めている組織、および NIC、HBA、ケーブル配線、スイッチの減少によるコスト削減と管理オーバーヘッドの軽減を目指しているデータセンターに対して最適化されています。Fibre Channel over Ethernet（FCoE）PCIe カードには、次の利点があります。

- ジャストインタイムのプロビジョニングを使用して、最大で 16 個の仮想ファイバ チャネルと 16 個のイーサネット アダプタを仮想化または非仮想化環境でプロビジョニングできます。それにより、システムの柔軟性が大幅に向上するとともに、複数の物理アダプタを統合することが可能になります。
- 仮想化を全面的にサポートしたドライバ（Cisco VN-Link テクノロジーとパススルー スイチングのハードウェアベースの実装を含む）。
- ネットワーク ポリシーとセキュリティの可視性およびポータビリティが、仮想マシンにまでわたる全域で提供されることにより、システムのセキュリティおよび管理性が向上します。

仮想インターフェイス カードは、親ファブリック インターコネクトに対して Cisco VN-Link 接続を確立します。それにより、仮想マシン内の仮想 NIC を仮想リンクでインターコネクトに接続できるようになります。Cisco Unified Computing System 環境では、仮想リンクを管理し、ネットワーク プロファイルを適用することができます。また、仮想マシンがシステム内のサーバ間を移動する際に、インターフェイスを動的に再プロビジョニングできます。

Cisco UCS VIC 1225 仮想インターフェイス カード

Cisco UCS VIC 1225 仮想インターフェイス カードは、サーバ仮想化によって導入される種々の新しい動作モードを高速化する、高性能の統合型ネットワーク アダプタです。優れた柔軟性、パフォーマンス、帯域幅を新世代の Cisco UCS C シリーズ ラックマウント サーバに提供します。

Cisco UCS VIC 1225 は、仮想ネットワーキングと物理ネットワーキングを単一のインフラストラクチャに統合する Cisco 仮想マシン ファブリック エクステンダ（VM-FEX）を実装しています。これにより、物理ネットワークから仮想マシンへのアクセスに対する可視性と、物理サーバと仮想サーバに対する一貫したネットワーク運用モデルの実現が可能になります。仮想化環境では、この高度に設定可能な自己仮想化アダプタにより、Cisco UCS C シリーズ ラックマウント サーバに統合モジュラ LAN インターフェイスを提供します。その他の機能と特長には次のようなものがあります。

- 最大 256 台の PCIe 仮想デバイス、仮想ネットワーク インターフェイス カード（vNIC）または仮想ホストバスアダプタ（vHBA）のサポート、高い I/O 処理/秒（IOPS）、ロスレスイーサネットのサポート、サーバへの 20 Gbps の接続を提供。

- PCIe Gen2 x16 により、ファブリック インターコネクトへの冗長パスを通じてネットワーク集約型アプリケーションのホスト サーバに適切な帯域幅を確実に提供。
- シスコ認定のサードパーティ製アダプタ用にサーバのフルハイト スロットが確保されたハーフハイト設計。
- Cisco UCS Manager による一元管理。Microsoft Windows、Red Hat Enterprise Linux、SUSE Linux、VMware vSphere、および Citrix XenServer をサポート。

Cisco UCS VIC 1385 仮想インターフェイス カード

この Cisco UCS VIC 1385 仮想インターフェイス カード は、デュアルポートの拡張型 Quad Small Form-Factor Pluggable（QSFP）40 ギガビット イーサネットおよび Fibre Channel over Ethernet（FCoE）対応のハーフハイト PCI Express（PCIe）カードで、Cisco UCS C シリーズ ラック サーバ専用に設計されています。シスコの次世代統合型ネットワーク アダプタ（CNA）技術は、包括的にさまざまな機能を提供し、今後のソフトウェア リリースに対応して投資を保護します。このカードでは、ポリシーベースでステートレス、かつ俊敏性の高いサーバ インフラストラクチャを構築できます。このインフラストラクチャは、ネットワーク インターフェイス カード（NIC）またはホスト バス アダプタ（HBA）として動的に設定可能な、256 を超える PCIe 規格準拠インターフェイスをホストに提供します。さらに、Cisco UCS VIC 1385 カードは、Cisco UCS ファブリック インターコネクトのポートを仮想マシンまで拡張する Cisco Data Center Virtual Machine Fabric Extender（VM-FEX）テクノロジーをサポートしているため、サーバ仮想化の展開が容易になります。

カードの特性は、ブート時にサーバに関連付けられたサービス プロファイルを使用して動的に決定されます。サービス プロファイルでは、PCIe インターフェイスの番号、タイプ（NIC または HBA）、ID（MAC アドレスおよび World Wide Name（WWN））、フェールオーバー ポリシー、帯域幅、Quality of Service（QoS）ポリシーを定義できます。インターフェイスをオンデマンドで定義、作成、利用できるため、ステートレスで俊敏性の高いサーバ インフラストラクチャが実現します。その他の機能と特長には次のようなものがあります。

- VIC 上に作成された各 PCIe インターフェイスは、それぞれ Cisco UCS ファブリック インターコネクト上のインターフェイスに関連付けられ、VIC 上の PCIe デバイスとファブリック インターコネクト上のインターフェイスを結ぶ各仮想ケーブルは、それぞれ完全に分離して認識されます。
- Cisco UCS VIC 1385 仮想インターフェイス カード は高いネットワーク パフォーマンスに加え、SMB-Direct、VMQ、DPDK、Cisco NetFlow などの最も要求の厳しいアプリケーションに対する低遅延を実現します。

Cisco UCS VIC 1227T 仮想インターフェイス カード

Cisco UCS VIC 1227T 仮想インターフェイス カード は、Cisco UCS C シリーズ ラック サーバ専用に設計された、デュアルポートの 10GBASE-T（RJ-45）10-Gbps イーサネットおよび Fibre Channel over Ethernet（FCoE）対応の PCI Express（PCIe）モジュラ LAN-on-motherboard（mLOM）アダプタです。Cisco のラック サーバに新たに導入された mLOM スロットを使用すると、PCIe スロットを使用せずに Cisco VIC を装着できます。これにより、I/O 拡張性が向上します。シスコの次世代統合型ネットワーク アダプタ（CNA）技術が取り入れられており、低コストのツイストペア ケーブルで、30 メートルまでのビット エラー レート（BER）が 10 ～ 15 のファイバ チャネル接続を

提供します。また、将来の機能リリースにおける投資保護を実現します。mLOM カードでは、ポリシーベースでステートレス、かつ俊敏性の高いサーバ インフラストラクチャを構築できます。このインフラストラクチャは、ネットワーク インターフェイス カード（NIC）またはホスト バス アダプタ（HBA）として動的に設定可能な、最大 256 の PCIe 規格準拠インターフェイスをホストに提供します。さらに、Cisco UCS VIC 1227T 仮想インターフェイス カード は、Cisco UCS ファブリック インターコネクトのポートを仮想マシンまで拡張する Cisco Data Center Virtual Machine Fabric Extender（VM-FEX）テクノロジーをサポートしているため、サーバ仮想化の展開が容易になります。その他の機能と特長には次のようなものがあります。

- ステートレスで俊敏性の高い設計：このカードの特性は、サーバブート時にサーバに関連付けられたサービス プロファイルを使用して動的に決定されます。サービス プロファイルでは、PCIe インターフェイスの番号、タイプ（NIC または HBA）、ID（MAC アドレスおよび World Wide Name（WWN））、フェールオーバー ポリシー、帯域幅、Quality of Service（QoS）ポリシーを定義できます。インターフェイスをオンデマンドで定義、作成、利用できるため、ステートレスで俊敏性の高いサーバ インフラストラクチャが実現します。
- VIC 上に作成された各 PCIe インターフェイスは、それぞれ Cisco UCS ファブリック インターコネクト上のインターフェイスに関連付けられ、VIC 上の PCIe デバイスとファブリック インターコネクト上のインターフェイスを結ぶ各仮想ケーブルは、それぞれ完全に分離して認識されます。
- Cisco SingleConnect テクノロジーは、データセンターのコンピューティングを接続、管理するためのきわめて簡単、効率的かつインテリジェントな方法を提供します。Cisco SingleConnect テクノロジーによって、データセンターがラック サーバおよびブレード サーバ、物理サーバ、仮想マシン、LAN、SAN、および管理ネットワークに接続する方法が劇的に簡略化されます。

Cisco UCS VIC 1387 仮想インターフェイス カード

Cisco UCS VIC 1387 仮想インターフェイス カードは、デュアルポートの拡張型 Quad Small Form-Factor Pluggable（QSFP）40 ギガビット イーサネットおよび Fibre Channel over Ethernet（FCoE）対応のハーフハイト PCI Express（PCIe）カードで、Cisco UCS C シリーズ ラック サーバ専用に設計されています。シスコの次世代統合型ネットワーク アダプタ（CNA）技術は、包括的にさまざまな機能を提供し、今後のソフトウェア リリースに対応して投資を保護します。このカードでは、ポリシーベースでステートレス、かつ俊敏性の高いサーバ インフラストラクチャを構築できます。このインフラストラクチャは、ネットワーク インターフェイス カード（NIC）またはホスト バス アダプタ（HBA）として動的に設定可能な、256 を超える PCIe 規格準拠インターフェイスをホストに提供します。さらに、Cisco UCS VIC 1387 カードは、Cisco UCS ファブリック インターコネクトのポートを仮想マシンまで拡張する Cisco Data Center Virtual Machine Fabric Extender（VM-FEX）テクノロジーをサポートしているため、サーバ仮想化の展開が容易になります。

カードの特性は、ブート時にサーバに関連付けられたサービス プロファイルを使用して動的に決定されます。サービス プロファイルでは、PCIe インターフェイスの番号、タイプ（NIC または HBA）、ID（MAC アドレスおよび World Wide Name（WWN））、フェールオーバー ポリシー、帯域幅、Quality of Service（QoS）ポリシーを定義できます。インターフェイスをオンデマンドで定義、作成、利用できるため、ステートレスで俊敏性の高いサーバ インフラストラクチャが実現します。その他の機能と特長には次のようなものがあります。

- VIC 上に作成された各 PCIe インターフェイスは、それぞれ Cisco UCS ファブリック インターコネクト上のインターフェイスに関連付けられ、VIC 上の PCIe デバイスとファブリック インターコネクト上のインターフェイスを結ぶ各仮想ケーブルは、それぞれ完全に分離して認識されます。
- Cisco UCS VIC 1387 仮想インターフェイス カードは高いネットワーク パフォーマンスに加え、SMB-Direct、VMQ、DPDK、Cisco NetFlow などの最も要求の厳しいアプリケーションに対する低遅延を実現します。

ネットワーク アダプタのプロパティの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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 adapter** [*index*] [**detail**]	アダプタのプロパティを表示します。1 つのアダプタのプロパティを表示するには、*index* 引数として PCI スロット番号を指定します。

次に、アダプタ 2 のプロパティを表示する例を示します。

```
Server# scope chassis
Server /chassis # show adapter
PCI Slot Product Name   Serial Number  Product ID     Vendor
-------- -------------- -------------- -------------- --------------------
1        UCS VIC 1225   FCH1613796C    UCSC-PCIE-C... Cisco Systems Inc

Server /chassis # show adapter 2 detail
PCI Slot 2:
    Product Name: UCS VIC 1225
    Serial Number: FCH1613796C
    Product ID: UCSC-PCIE-CSC-02
    Adapter Hardware Revision: 4
    Current FW Version: 2.1(0.291)
    NIV: Disabled
    FIP: Enabled
    Configuration Pending: no
    CIMC Management Enabled : no
    VID: V00
    Vendor: Cisco Systems Inc
    Description:
    Bootloader Version: 2.1(0.291)
    FW Image 1 Version: 2.1(0.291)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 1.6(0.547)
    FW Image 2 State: BACKUP INACTIVATED
    FW Update Status: Idle
    FW Update Error: No error
    FW Update Stage: No operation (0%)
    FW Update Overall Progress: 0%

Server /chassis #
```

ネットワーク アダプタのプロパティの設定

はじめる前に

- 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。
- サポートされた仮想インターフェイス カード（VIC）がシャーシに取り付けられ、サーバの電源がオンである必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **showadapter**	（任意）使用可能なアダプタ デバイスを表示します。
ステップ 3	Server /chassis # **scope adapter***index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 4	Server /chassis/adapter # **setfip-mode** {**disable**|**enable**}	アダプタ カードで FCoE Initialization Protocol（FIP）をイネーブルまたはディセーブルにします。FIP はデフォルトで有効になっています。 （注） テクニカル サポートの担当者から明確に指示された場合にだけ、このオプションをディセーブルにすることを推奨します。
ステップ 5	Server /chassis/adapter # **setlldp** {**disable**|**enable**}	アダプタ カードで Link Layer Discovery Protocol（LLDP）をイネーブルまたはディセーブルにします。LLDP はデフォルトでイネーブルです。 （注） LLDP オプションをディセーブルにすると、すべての Data Center Bridging Capability Exchange Protocol（DCBX）機能が無効になるため、このオプションはディセーブルにしないことを推奨します。
ステップ 6	Server /chassis/adapter # **setniv-mode** {**disable**|**enable**}	アダプタ カードで Network Interface Virtualization（NIV）をイネーブルまたはディセーブルにします。NIV はデフォルトで無効になっています。 NIV モードがイネーブルな場合、vNIC は以下の操作を実行できます。

	コマンドまたはアクション	目的
		• 特定のチャネルに割り当てることができます • ポート プロファイルに関連付けることができます • 通信の問題がある場合に別の vNIC にフェールオーバーできます
ステップ 7	Server /chassis/adapter # **configure-vmfex***port-count*	NIV モードがイネーブルの場合、*port-count* には Cisco IMC を使用して作成する VM FEX インターフェイスの数を 0 ～ 112 の範囲で指定します。
ステップ 8	Server /chassis/adapter # **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、アダプタ 1 のプロパティを設定する例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # set fip-mode enable
Server /chassis/adapter *# commit
Server /chassis/adapter #
```

vHBA の管理

vHBA 管理のガイドライン

vHBA を管理する場合は、次のガイドラインと制限事項を考慮してください。

- Cisco UCS P81E 仮想インターフェイス カードおよびCisco UCS VIC 1225 仮想インターフェイス カードには 2 つの vHBA（fc0 と fc1）があります。これらのアダプタ カードに最大 16 個の vHBA を追加作成できます。

  （注） アダプタに対してネットワーク インターフェイスの仮想化（NIV）モードがイネーブルになっている場合は、vHBA を作成するときにチャネル番号を割り当てる必要があります。

- FCoE アプリケーションで Cisco UCS P81E 仮想インターフェイス カードまたはCisco UCS VIC 1225 仮想インターフェイス カードを使用している場合は、vHBA を FCoE VLAN に関連付ける必要があります。vHBA のプロパティの変更, （153 ページ） の説明に従って VLAN を割り当ててください。
- 設定の変更後は、その設定を有効にするためにホストをリブートする必要があります。

vHBA のプロパティの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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 adapter***index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **show host-fc-if** [**fc0** | **fc1** | *name*] [**detail**]	指定した単一の vHBA またはすべての vHBA のプロパティを表示します。

次に、アダプタ カード 1 上のすべての vHBA および fc0 の詳細なプロパティを表示する例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # show host-fc-if
Name     World Wide Port Name     FC SAN Boot Uplink Port
-------- ------------------------ ----------- -----------
fc0      20:00:00:22:BD:D6:5C:35  Disabled    0
fc1      20:00:00:22:BD:D6:5C:36  Disabled    1

Server /chassis/adapter # show host-fc-if fc0 detail
Name fc0:
    World Wide Node Name: 10:00:00:22:BD:D6:5C:35
    World Wide Port Name: 20:00:00:22:BD:D6:5C:35
    FC SAN Boot: Disabled
    Persistent LUN Binding: Disabled
    Uplink Port: 0
    MAC Address: 00:22:BD:D6:5C:35
    CoS: 3
    VLAN: NONE
    Rate Limiting: OFF
    PCIe Device Order: ANY
    EDTOV: 2000
    RATOV: 10000
    Maximum Data Field Size: 2112
    Channel Number: 3
    Port Profile:

Server /chassis/adapter #
```

vHBA のプロパティの変更

はじめる前に

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 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 adapter**	（任意）使用可能なアダプタ デバイスを表示します。
ステップ 3	Server /chassis # **scope adapter***index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンドモードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 4	Server /chassis/adapter # **scope host-fc-if** {**fc0** | *fc1* | name}	指定した vHBA に対してホスト ファイバ チャネル インターフェイス コマンド モードを開始します。
ステップ 5	Server /chassis/adapter/host-fc-if # **set wwnn** *wwnn*	アダプタの一意のワールド ワイド ノード名（WWNN）を hh:hh:hh:hh:hh:hh:hh:hh の形式で指定します。 このコマンドで指定しない場合、WWNN はシステムによって自動的に生成されます。
ステップ 6	Server /chassis/adapter/host-fc-if # **set wwpn** *wwpn*	アダプタの一意のワールド ワイド ポート名（WWPN）を hh:hh:hh:hh:hh:hh:hh:hh の形式で指定します。 このコマンドで指定しない場合、WWPN はシステムによって自動的に生成されます。
ステップ 7	Server /chassis/adapter/host-fc-if # **set boot** {**disable** | **enable**}	FC SAN ブートを有効または無効にします。デフォルトはディセーブルです。
ステップ 8	Server /chassis/adapter/host-fc-if # **set persistent-lun-binding** {**disable** | **enable**}	永続的な LUN バインディングを有効または無効にします。デフォルトはディセーブルです。
ステップ 9	Server /chassis/adapter/host-fc-if # **set mac-addr** *mac-addr*	vHBA の MAC 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 10	Server /chassis/adapter/host-fc-if # **set vlan** {**none** | *vlan-id*}	この vHBA のデフォルトの VLAN を指定します。有効な VLAN 番号は 1 ～ 4094 です。デフォルトは none です。
ステップ 11	Server /chassis/adapter/host-fc-if # **set cos** *cos-value*	受信パケットにマークされるサービスクラス（CoS）値を指定します。この設定は、vHBA がホスト CoS を信頼するように設定されていない場合に限り有効です。有効な CoS 値は 0 ～ 6 です。デフォルトは 0 です。値が大きいほど重要なトラフィックであることを意味します。 この設定は NIV モードでは動作しません。
ステップ 12	Server /chassis/adapter/host-fc-if # **set rate-limit** {**off** | *rate*}	vHBA の最大データ レートを指定します。指定できる範囲は 1 ～ 10000 Mbps です。デフォルトは off です。 この設定は NIV モードでは動作しません。
ステップ 13	Server /chassis/adapter/host-fc-if # **set order** {**any** | *0-99*}	PCIe バスのデバイス番号割り当てについて、このデバイスの相対順序を指定します。デフォルトは any です。
ステップ 14	Server /chassis/adapter/host-fc-if # **set error-detect-timeout** *msec*	Error Detect TimeOut Value（EDTOV）を指定します。エラーが発生したとシステムが見なすまでに待機するミリ秒数です。指定できる値の範囲は、1000 ～ 100000 です。デフォルトは、2000 ミリ秒です。
ステップ 15	Server /chassis/adapter/host-fc-if # **set resource-allocation-timeout** *msec*	Resource Allocation TimeOut Value（RATOV）を指定します。リソースを適切に割り当てることができないとシステムが見なすまでに待機するミリ秒数です。指定できる値の範囲は、5000 ～ 100000 です。デフォルトは、10000 ミリ秒です。
ステップ 16	Server /chassis/adapter/host-fc-if # **set max-field-size** *size*	vHBA がサポートするファイバ チャネル フレーム ペイロードの最大サイズ（バイト数）を指定します。指定できる値の範囲は 1 ～ 2112 です。デフォルトは 2112 バイトです。
ステップ 17	Server /chassis/adapter/host-fc-if # **scope error-recovery**	ファイバ チャネル エラー回復コマンド 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 18	Server /chassis/adapter/host-fc-if/error-recovery # **set fcp-error-recovery** {**disable** | **enable**}	FCP エラー回復を有効または無効にします。デフォルトはディセーブルです。
ステップ 19	Server /chassis/adapter/host-fc-if/error-recovery # **set link-down-timeout** *msec*	リンク ダウン タイムアウト値を指定します。アップリンク ポートがダウンし、ファブリック接続が失われていることをシステムに通知する前に、アップリンク ポートがオフラインになっていなければならないミリ秒数です。指定できる値の範囲は、0 ～ 240000 です。デフォルトは、30000 ミリ秒です。
ステップ 20	Server /chassis/adapter/host-fc-if/error-recovery # **set port-down-io-retry-count** *count*	ポート ダウン I/O 再試行回数値を指定します。ポートが使用不可能であるとシステムが判断する前に、そのポートへの I/O 要求がビジー状態を理由に戻される回数です。指定できる値の範囲は、0 ～ 255 です。デフォルトは、8 回です。
ステップ 21	Server /chassis/adapter/host-fc-if/error-recovery # **set port-down-timeout** *msec*	ポートダウンタイムアウト値を指定します。リモート ファイバ チャネル ポートが使用不可能であることを SCSI 上位層に通知する前に、そのポートがオフラインになっていなければならないミリ秒数です。指定できる値の範囲は、0 ～ 240000 です。デフォルトは、10000 ミリ秒です。
ステップ 22	Server /chassis/adapter/host-fc-if/error-recovery # **exit**	ホスト ファイバ チャネル インターフェイス コマンド モードを終了します。
ステップ 23	Server /chassis/adapter/host-fc-if # **scope interrupt**	割り込みコマンド モードを開始します。
ステップ 24	Server /chassis/adapter/host-fc-if/interrupt # **set interrupt-mode** {**intx** | **msi** | **msix**}	ファイバチャネル割り込みモードを指定します。次のモードがあります。 • **intx**：ラインベースの割り込み（INTx） • **msi**：メッセージ シグナル割り込み（MSI） • **msix**：機能拡張されたメッセージシグナル割り込み（MSIx）。これは推奨オプションであり、デフォルトになっています。

	コマンドまたはアクション	目的
ステップ 25	Server /chassis/adapter/host-fc-if/interrupt # **exit**	ホスト ファイバ チャネル インターフェイス コマンド モードを終了します。
ステップ 26	Server /chassis/adapter/host-fc-if # **scope port**	ファイバ チャネル ポート コマンド モードを開始します。
ステップ 27	Server /chassis/adapter/host-fc-if/port # **set outstanding-io-count** *count*	I/O スロットル数を指定します。vHBA 内に同時に保留可能な I/O 操作の数です。指定できる値の範囲は、1 ～ 1024 です。デフォルトは、512 個の操作です。
ステップ 28	Server /chassis/adapter/host-fc-if/port # **set max-target-luns** *count*	ターゲットあたりの論理ユニット番号（LUN）の最大数を指定します。ドライバで検出される LUN の最大数です。通常は、オペレーティング システム プラットフォームの制限です。指定できる値の範囲は、1 ～ 1024 です。デフォルトは、256 個の LUN です。
ステップ 29	Server /chassis/adapter/host-fc-if/port # **exit**	ホスト ファイバ チャネル インターフェイス コマンド モードを終了します。
ステップ 30	Server /chassis/adapter/host-fc-if # **scope port-f-logi**	ファイバ チャネル ファブリック ログイン コマンド モードを開始します。
ステップ 31	Server /chassis/adapter/host-fc-if/port-f-logi # **set flogi-retries** {**infinite** | *count*}	ファブリック ログイン（FLOGI）の再試行回数値を指定します。システムがファブリックへのログインを最初に失敗してから再試行する回数です。0 ～ 4294967295 の数値を入力するか、**infinite** を入力します。デフォルトは無限（infinite）の再試行です。
ステップ 32	Server /chassis/adapter/host-fc-if/port-f-logi # **set flogi-timeout** *msec*	ファブリック ログイン（FLOGI）タイムアウト値を指定します。システムがログインを再試行する前に待機するミリ秒数です。指定できる値の範囲は、1 ～ 255000 です。デフォルトは、2000 ミリ秒です。
ステップ 33	Server /chassis/adapter/host-fc-if/port-f-logi # **exit**	ホスト ファイバ チャネル インターフェイス コマンド モードを終了します。
ステップ 34	Server /chassis/adapter/host-fc-if # **scope port-p-logi**	ファイバ チャネル ポート ログイン コマンド モードを開始します。
ステップ 35	Server /chassis/adapter/host-fc-if/port-p-logi # **set plogi-retries** *count*	ポート ログイン（PLOGI）の再試行回数値を指定します。システムがファブリックへのログインを最初に失敗してから再試行する回数

	コマンドまたはアクション	目的
		です。指定できる値の範囲は、0～255 です。デフォルトは、8 回です。
ステップ 36	Server /chassis/adapter/host-fc-if/port-p-logi # **set plogi-timeout** *msec*	ポートログイン（PLOGI）タイムアウト値を指定します。システムがログインを再試行する前に待機するミリ秒数です。指定できる値の範囲は、1 ～ 255000 です。デフォルトは、2000 ミリ秒です。
ステップ 37	Server /chassis/adapter/host-fc-if/port-p-logi # **exit**	ホスト ファイバ チャネル インターフェイス コマンド モードを終了します。
ステップ 38	Server /chassis/adapter/host-fc-if # **scope scsi-io**	SCSI I/O コマンド モードを開始します。
ステップ 39	Server /chassis/adapter/host-fc-if/scsi-io # **set cdb-wq-count** *count*	割り当てる Command Descriptor Block（CDB）送信キュー リソースの数です。指定できる値の範囲は 1 ～ 8 です。デフォルトは 1 です。
ステップ 40	Server /chassis/adapter/host-fc-if/scsi-io # **set cdb-wq-ring-size** *size*	Command Descriptor Block（CDB）送信キュー内の記述子の数。指定できる値の範囲は 64 ～ 512 です。デフォルトは 512 です。
ステップ 41	Server /chassis/adapter/host-fc-if/scsi-io # **exit**	ホスト ファイバ チャネル インターフェイス コマンド モードを終了します。
ステップ 42	Server /chassis/adapter/host-fc-if # **scope trans-queue**	ファイバ チャネル送信キュー コマンド モードを開始します。
ステップ 43	Server /chassis/adapter/host-fc-if/trans-queue # **set fc-wq-ring-size** *size*	ファイバ チャネル送信キュー内の記述子の数。指定できる値の範囲は 64 ～ 128 です。デフォルトは 64 です。
ステップ 44	Server /chassis/adapter/host-fc-if/trans-queue # **exit**	ホスト ファイバ チャネル インターフェイス コマンド モードを終了します。
ステップ 45	Server /chassis/adapter/host-fc-if # **scope recv-queue**	ファイバ チャネル受信キュー コマンド モードを開始します。
ステップ 46	Server /chassis/adapter/host-fc-if/recv-queue # **set fc-rq-ring-size** *size*	ファイバ チャネル受信キュー内の記述子の数。指定できる値の範囲は 64 ～ 128 です。デフォルトは 64 です。
ステップ 47	Server /chassis/adapter/host-fc-if/recv-queue # **exit**	ホスト ファイバ チャネル インターフェイス コマンド モードを終了します。

	コマンドまたはアクション	目的
ステップ 48	Server /chassis/adapter/host-fc-if # **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） 変更内容は次のサーバのリブート時に有効になります。

次の例では、vHBA のプロパティを設定しています。

```
Server# scope chassis
Server /chassis # show adapter
PCI Slot Product Name   Serial Number  Product ID     Vendor
-------- -------------- -------------- -------------- --------------------
1        UCS VIC P81E   QCI1417A0QK    N2XX-ACPCI01   Cisco Systems Inc

Server /chassis # scope adapter 1
Server /chassis/adapter # scope host-fc-if fc1
Server /chassis/adapter/host-fc-if # set boot enable
Server /chassis/adapter/host-fc-if *# scope scsi-io
Server /chassis/adapter/host-fc-if/scsi-io *# set cdb-wq-count 2
Server /chassis/adapter/host-fc-if/scsi-io *# exit
Server /chassis/adapter/host-fc-if *# commit
Server /chassis/adapter/host-fc-if #
```

次の作業

サーバをリブートして変更内容を適用します。

vHBA の作成

アダプタには 2 つの永続的 vHBA があります。NIV モードがイネーブルの場合、最大 16 の追加 vHBAs を作成できます。

はじめる前に

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 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 adapter***index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンドモードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。

	コマンドまたはアクション	目的
ステップ 3	Server /chassis/adapter # **create host-fc-if** *name*	vHBA を作成し、ホストのファイバ チャネル インターフェイスのコマンドモードを開始します。*name* 引数には最大 32 文字の ASCII 文字を使用できます。
ステップ 4	Server /chassis/adapter/host-fc-if # **set channel-number** *number*	（任意） アダプタで NIV モードがイネーブルになっている場合、この vHBA にチャネル番号を割り当てる必要があります。指定できる範囲は 1 ～ 1000 です。
ステップ 5	Server /chassis/adapter/host-fc-if # **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） 変更内容は次のサーバのリブート時に有効になります。

次に、アダプタ 1 の vHBA を作成する例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # create host-fc-if Vhba5
Server /chassis/adapter/host-fc-if *# commit
New host-fc-if settings will take effect upon the next server reset
Server /chassis/adapter/host-fc-if #
```

次の作業

- サーバをリブートして vHBA を作成します。
- 設定の変更が必要な場合は、vHBA のプロパティの変更, （153 ページ）の説明に従って、新しい vHBA を設定します。

vHBA の削除

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 adapter***index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。

	コマンドまたはアクション	目的
ステップ 3	Server /chassis/adapter # **delete host-fc-if** *name*	指定された vHBA を削除します。 （注） 2 つのデフォルトの vHBA である [fc0] または [fc1] は削除できません。
ステップ 4	Server /chassis/adapter # **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） 変更内容は次のサーバのリブート時に有効になります。

次に、アダプタ 1 の vHBA を削除する例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # delete host-fc-if Vhba5
Server /chassis/adapter *# commit
Server /chassis/adapter #
```

vHBA ブート テーブル

vHBA ブート テーブルには、サーバがブート可能な LUN を 4 つまで指定できます。

ブート テーブルの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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 adapter***index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **scope host-fc-if** {**fc0** | *fc1* | name}	指定した vHBA に対してホスト ファイバ チャネル インターフェイス コマンド モードを開始します。
ステップ 4	Server /chassis/adapter/host-fc-if # **show boot**	ファイバチャネルインターフェイスのブートテーブルを表示します。

次に、vHBA のブート テーブルを表示する例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # scope host-fc-if fc1
Server /chassis/adapter/host-fc-if # show boot
Boot Table Entry  Boot Target WWPN           Boot LUN ID
----------------- -------------------------- ------------
0                 20:00:00:11:22:33:44:55    3
1                 20:00:00:11:22:33:44:56    5

Server /chassis/adapter/host-fc-if #
```

ブート テーブル エントリの作成

最大 4 個のブート テーブル エントリを作成できます。

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 # **scope adapter***index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **scope host-fc-if** {**fc0** | *fc1* | name}	指定した vHBA に対してホスト ファイバ チャネル インターフェイス コマンド モードを開始します。
ステップ 4	Server /chassis/adapter/host-fc-if # **create-boot-entry** *wwpn lun-id*	ブート テーブル エントリを作成します。 • *wwpn*：ブート ターゲットの hh:hh:hh:hh:hh:hh:hh:hh 形式の World Wide Port Name（WWPN）。 • *lun-id*：ブート LUN の LUN ID。指定できる範囲は 0 ～ 255 です。
ステップ 5	Server /chassis/adapter/host-fc-if # **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） 変更内容は次のサーバのリブート時に有効になります。

次に、vHBA fc1 のブート テーブル エントリを作成する例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # scope host-fc-if fc1
Server /chassis/adapter/host-fc-if # create-boot-entry 20:00:00:11:22:33:44:55 3
Server /chassis/adapter/host-fc-if *# commit
New boot table entry will take effect upon the next server reset
Server /chassis/adapter/host-fc-if #
```

ブート テーブル エントリの削除

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 adapter***index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **scope host-fc-if** {**fc0** | *fc1* | name}	指定した vHBA に対してホスト ファイバ チャネル インターフェイス コマンド モードを開始します。
ステップ 4	Server /chassis/adapter/host-fc-if # **show boot**	ブート テーブルを表示します。ブート テーブル エントリ フィールドから、削除するエントリの番号を探します。
ステップ 5	Server /chassis/adapter/host-fc-if # **delete boot** *entry*	テーブルの指定した位置からブート テーブル エントリを削除します。*entry* の範囲は 0 ～ 3 です。変更は、サーバを次にリセットしたときに有効になります。
ステップ 6	Server /chassis/adapter/host-fc-if # **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） 変更内容は次のサーバのリブート時に有効になります。

次に、vHBA fc1 のブート テーブル エントリ番号 1 を削除する例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # scope host-fc-if fc1
Server /chassis/adapter/host-fc-if # show boot
Boot Table Entry  Boot Target WWPN           Boot LUN ID
----------------- -------------------------- ------------
0                 20:00:00:11:22:33:44:55    3
```

```
1                 20:00:00:11:22:33:44:56    5

Server /chassis/adapter/host-fc-if # delete boot 1
Server /chassis/adapter/host-fc-if *# commit
New host-fc-if settings will take effect upon the next server reset
Server /chassis/adapter/host-fc-if # show boot
Boot Table Entry  Boot Target WWPN           Boot LUN ID
----------------- -------------------------- ------------
0                 20:00:00:11:22:33:44:55    3

Server /chassis/adapter/host-fc-if #
```

次の作業

サーバをリブートして変更内容を適用します。

vHBA の永続的なバインディング

永続的なバインディングは、システムによって割り当てられたファイバ チャネル ターゲットのマッピングがリブート後も維持されることを保証します。

永続的なバインディングのイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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 adapter***index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **scope host-fc-if** {**fc0** | *fc1* | name}	指定した vHBA に対してホスト ファイバ チャネル インターフェイス コマンド モードを開始します。
ステップ 4	Server /chassis/adapter/host-fc-if # **scope perbi**	vHBA の永続的なバインディングのコマンド モードを開始します。
ステップ 5	Server /chassis/adapter/host-fc-if/perbi # **set persistent-lun-binding enable**	vHBA の永続的なバインディングをイネーブルにします。
ステップ 6	Server /chassis/adapter/host-fc-if/perbi # **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、vHBA の永続的なバインディングをイネーブルにする例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 4
Server /chassis/adapter # scope host-fc-if fc1
Server /chassis/adapter/host-fc-if # scope perbi
Server /chassis/adapter/host-fc-if/perbi # set persistent-lun-binding enable
Server /chassis/adapter/host-fc-if/perbi *# commit
Server /chassis/adapter/host-fc-if/perbi #
```

永続的なバインディングのディセーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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 adapter***index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **scope host-fc-if** {**fc0** | *fc1* | name}	指定した vHBA に対してホスト ファイバ チャネル インターフェイス コマンド モードを開始します。
ステップ 4	Server /chassis/adapter/host-fc-if # **scope perbi**	vHBA の永続的なバインディングのコマンド モードを開始します。
ステップ 5	Server /chassis/adapter/host-fc-if/perbi # **set persistent-lun-binding disable**	vHBA の永続的なバインディングをディセーブルにします。
ステップ 6	Server /chassis/adapter/host-fc-if/perbi # **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、vHBA の永続的なバインディングをディセーブルにする例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 4
Server /chassis/adapter # scope host-fc-if fc1
Server /chassis/adapter/host-fc-if # scope perbi
Server /chassis/adapter/host-fc-if/perbi # set persistent-lun-binding disable
Server /chassis/adapter/host-fc-if/perbi *# commit
Server /chassis/adapter/host-fc-if/perbi #
```

永続的なバインディングの再構築

はじめる前に

vHBA のプロパティで永続的なバインディングをイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope adapter***index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **scope host-fc-if** {**fc0** | *fc1* | name}	指定した vHBA に対してホスト ファイバ チャネル インターフェイス コマンド モードを開始します。
ステップ 4	Server /chassis/adapter/host-fc-if # **scope perbi**	vHBA の永続的なバインディングのコマンド モードを開始します。
ステップ 5	Server /chassis/adapter/host-fc-if/perbi # **rebuild**	vHBA の永続的なバインディング テーブルを再構築します。

次に、vHBA の永続的なバインディング テーブルを再構築する例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 4
Server /chassis/adapter # scope host-fc-if fc1
Server /chassis/adapter/host-fc-if # scope perbi
Server /chassis/adapter/host-fc-if/perbi # rebuild

Server /chassis/adapter/host-fc-if/perbi #
```

vNIC の管理

vNIC 管理のガイドライン

vNIC を管理する場合は、次のガイドラインと制限事項を考慮してください。

- Cisco UCS P81E 仮想インターフェイス カードおよびCisco UCS VIC 1225 仮想インターフェイス カードには 2 つのデフォルト vNIC（eth0 と eth1）があります。これらのアダプタ カードに最大 16 個の vNIC を追加作成できます。

（注） アダプタに対してネットワーク インターフェイスの仮想化（NIV）モードがイネーブルになっている場合、vNIC を作成するときにチャネル番号を割り当てる必要があります。

- 設定の変更後は、その設定を有効にするためにホストをリブートする必要があります。

vNIC のプロパティの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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 adapter***index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンドモードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **showhost-eth-if** [**eth0** | **eth1** | *name*] [**detail**]	指定した単一の vNIC またはすべての vNIC のプロパティを表示します。
ステップ 4	Server /chassis/adapter # **showext-eth-if** [**detail**]	外部イン—サネット インターフェイスの詳細を表示します。

次に、すべての vNIC の簡単なプロパティと、eth0 および外部インターフェイスの詳細なプロパティを表示する例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # show host-eth-if
Name   MTU  Uplink Port  MAC Address       CoS VLAN PXE Boot iSCSI Boot usNIC
----- ----- -----------  ------------ ---  ------------ --------------- ------
eth0   1500 0            74:A2:E6:28:C6:AE N/A N/A  disabled disabled   0
eth1   1500 1            74:A2:E6:28:C6:AF N/A N/A  disabled disabled   0
srg    1500 0            74:A2:E6:28:C6:B2 N/A N/A  disabled disabled   64
hhh    1500 0            74:A2:E6:28:C6:B3 N/A N/A  disabled disabled   0

Server /chassis/adapter # show host-eth-if eth0 detail
Name eth0:
    MTU: 1500
```

```
    Uplink Port: 0
    MAC Address: 00:22:BD:D6:5C:33
    CoS: 0
    Trust Host CoS: disabled
    PCI Link: 0
    PCI Order: ANY
    VLAN: NONE
    VLAN Mode: TRUNK
    Rate Limiting: OFF
    PXE Boot: disabled
    iSCSI Boot: disabled
    usNIC: 0
    Channel Number: N/A
    Port Profile: N/A
    Uplink Failover: disabled
    Uplink Failback Timeout: 5
    aRFS: disabled
    VMQ: disabled
    NVGRE: disabled
    VXLAN: disabled
    RDMA Queue Pairs: 1
    RDMA Memory Regions: 4096
    RDMA Resource Groups: 1
    CDN Name: VIC-1-eth0

Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # show ext-eth-if
Port MAC Address       Link State Encap.. Mode Admin Speed Oper..Speed   Link Training
Connector Present Connector Supported
---- ----------------- ---------- ------------ ----------- ------------- -------------
----------------- -------------------
0    74:A2:E6:28:C6:A2 Link       CE           40Gbps      40Gbps          N/A
Yes               Yes
1    74:A2:E6:28:C6:A3 Link       CE           40Gbps      40Gbps          N/A
Yes               Yes

Server /chassis/adapter # show ext-eth-if detail

C220-FCH1834V23X /chassis/adapter # show ext-eth-if detail
Port 0:
    MAC Address: 74:A2:E6:28:C6:A2
    Link State: Link
    Encapsulation Mode: CE
    Admin Speed: 40Gbps
    Operating Speed: 40Gbps
    Link Training: N/A
    Connector Present: Yes
    Connector Supported: Yes
    Connector Type: QSFP_XCVR_CR4
    Connector Vendor: CISCO
    Connector Part Number: 2231254-3
    Connector Part Revision: B
Port 1:
    MAC Address: 74:A2:E6:28:C6:A3
    Link State: Link
    Encapsulation Mode: CE
    Admin Speed: 40Gbps
    Operating Speed: 40Gbps
    Link Training: N/A
    Connector Present: Yes
    Connector Supported: Yes
    Connector Type: QSFP_XCVR_CR4
    Connector Vendor: CISCO
    Connector Part Number: 2231254-3
    Connector Part Revision: B


Server /chassis/adapter #
```

vNIC のプロパティの変更

はじめる前に

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 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 # **showadapter**	（任意）使用可能なアダプタ デバイスを表示します。
ステップ 3	Server /chassis # **scope adapter***index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 4	Server /chassis/adapter # **scope host-eth-if** {**eth0** | **eth1** | *name*}	指定した vNIC に対してホスト イーサネット インターフェイス コマンド モードを開始します。
ステップ 5	Server /chassis/adapter/host-eth-if # **setmtu***mtu-value*	vNIC で受け入れられる Maximum Transmission Unit（MTU）またはパケット サイズを指定します。有効な MTU 値は 1500 ～ 9000 バイトです。デフォルトは 1500 です。
ステップ 6	Server /chassis/adapter/host-eth-if # **setuplink** {**0**|**1**}	この vNIC に関連付けられているアップリンク ポートを指定します。この vNIC に対するすべてのトラフィックは、このアップリンク ポートを通過します。
ステップ 7	Server /chassis/adapter/host-eth-if # **setmac-addr***mac-addr*	hh:hh:hh:hh:hh:hh または hhhh:hhhh:hhhh の形式で vNIC の MAC アドレスを指定します。
ステップ 8	Server /chassis/adapter/host-eth-if # **setcos***cos-value*	受信パケットにマークされるサービス クラス（CoS）値を指定します。この設定は、vNIC がホスト CoS を信頼するように設定されていない場合に限り有効です。有効な CoS 値は 0 ～ 6 です。デフォルトは 0 です。値が大きいほど重要なトラフィックであることを意味します。 （注） NIV がイネーブルの場合、この設定はスイッチによって決定され、コマンドは無視されます。

	コマンドまたはアクション	目的
ステップ 9	Server /chassis/adapter/host-eth-if # **settrust-host-cos** {**disable**|**enable**}	vNIC がホスト CoS を信頼するか、パケットを再マーキングするかを指定します。動作は次のようになります。 • **disable**：受信パケットは設定済み CoS と再マーキングされます。これはデフォルトです。 • **enable**：インバウンド パケット（ホスト CoS）の既存の CoS 値が保持されます。
ステップ 10	Server /chassis/adapter/host-eth-if # **setorder** {**any**|*0-99*}	PCI バスのデバイス番号割り当てについて、このデバイスの相対順序を指定します。デフォルトは any です。
ステップ 11	Server /chassis/adapter/host-eth-if # **setvlan** {**none**|*vlan-id*}	この vNIC のデフォルトの VLAN を指定します。有効な VLAN 番号は 1 ～ 4094 です。デフォルトは none です。 （注） NIV がイネーブルの場合、この設定はスイッチによって決定され、コマンドは無視されます。
ステップ 12	Server /chassis/adapter/host-eth-if # **setvlan-mode** {**access**|**trunk**}	vNIC に VLAN モードを指定します。次のモードがあります。 • **access**：vNIC は 1 つの VLAN だけに属します。VLAN がアクセス モードに設定されている場合、TAG 付きのスイッチから受信された、指定のデフォルトの VLAN（1-4094）から受信されるフレームは、vNIC 経由でホスト OS に送信されるときにその TAG を削除します。 • **trunk**：vNIC は複数の VLAN に属することができます。これはデフォルトです。 （注） NIV がイネーブルの場合、この設定はスイッチによって決定され、コマンドは無視されます。
ステップ 13	Server /chassis/adapter/host-eth-if # **setrate-limit** {**off**|*rate*}	vNIC の最大データ レートを指定します。指定できる範囲は 1 ～ 10000 Mbps です。デフォルトは off です。 （注） NIV がイネーブルの場合、この設定はスイッチによって決定され、コマンドは無視されます。

	コマンドまたはアクション	目的
ステップ 14	Server /chassis/adapter/host-eth-if # **setboot** {**disable**|**enable**}	vNIC を使用して PXE ブートを実行するかどうかを指定します。デフォルトでは、2つのデフォルト vNIC に対してはイネーブル、ユーザ作成の vNIC に対してはディセーブルです。
ステップ 15	Server /chassis/adapter/host-eth-if # **setchannel-number***number*	アダプタに対して NIV モードがイネーブルである場合、この vNIC に割り当てられるチャネル番号を選択します。指定できる範囲は 1 ～ 1000 です。
ステップ 16	Server /chassis/adapter/host-eth-if # **setport-profile***name*	アダプタに対して NIV モードがイネーブルである場合、vNIC に関連付けられるポートプロファイルを選択します。 （注） *name* は、このサーバが接続されているスイッチに定義されているポートプロファイルである必要があります。
ステップ 17	Server /chassis/adapter/host-eth-if # **setuplink-failover** {**disable**|**enable**}	アダプタに対して NIV モードがイネーブルである場合、通信問題が発生したときにこの vNIC 上のトラフィックがセカンダリ インターフェイスにフェールオーバーするようにするには、この設定をイネーブルにします。
ステップ 18	Server /chassis/adapter/host-eth-if # **setuplink-failback-timeout***seconds*	セカンダリ インターフェイスを使用して vNIC が始動した後、その vNIC のプライマリ インターフェイスが再びシステムで使用されるには、プライマリ インターフェイスが一定時間使用可能な状態になっている必要があり、その時間の長さをこの設定で制御します。 *seconds* に 0 ～ 600 の範囲の秒数を入力します。
ステップ 19	Server /chassis/adapter/host-eth-if # **setvmq** {**disable**|**enable**}	このアダプタに対して仮想マシン キュー（VMQ）をイネーブルまたはディセーブルにします。 （注） SR-IOV またはネットフローがアダプタでイネーブルになっている場合は、VMQ をイネーブルにしないでください。
ステップ 20	Server /chassis/adapter/host-eth-if # **setarfs** {**disable**|**enable**}	このアダプタに対して Accelerated Receive Flow ステアリング（aRFS）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 21	Server /chassis/adapter/host-eth-if # **scopeinterrupt**	割り込みコマンド モードを開始します。
ステップ 22	Server /chassis/adapter/host-eth-if/interrupt # **setinterrupt-count***count*	割り込みリソースの数を指定します。指定できる値の範囲は 1 ～ 514 です。デフォルトは 8 です。通常は、完了キューごとに 1 つの割り込みリソースを割り当てる必要があります。
ステップ 23	Server /chassis/adapter/host-eth-if/interrupt # **setcoalescing-time***usec*	割り込み間の待機時間、または割り込みが送信される前に必要な休止期間。 指定できる範囲は 1 ～ 65535 ミリ秒です。デフォルト値は 125 ミリ秒です。調停をオフにするには、0（ゼロ）を入力します。
ステップ 24	Server /chassis/adapter/host-eth-if/interrupt # **setcoalescing-type** {**idle**|**min**}	調停には次のタイプがあります。 • **idle**：アクティビティなしの期間が少なくとも調停時間設定に指定された時間内は、システムから割り込み送信されません。 • **min**：システムは、別の割り込みイベントを送信する前に、調停時間設定に指定された時間だけ待機します。これはデフォルトです。
ステップ 25	Server /chassis/adapter/host-eth-if/interrupt # **setinterrupt-mode** {**intx**|**msi**|**msix**}	イーサネット割り込みモードを指定します。次のモードがあります。 • **intx**：ラインベースの割り込み（PCI INTx） • **msi**：メッセージ シグナル割り込み（MSI） • **msix**：機能拡張されたメッセージ シグナル割り込み（MSI-X）。これは推奨オプションであり、デフォルトになっています。
ステップ 26	Server /chassis/adapter/host-eth-if/interrupt # **exit**	ホスト イーサネット インターフェイス コマンド モードを終了します。
ステップ 27	Server /chassis/adapter/host-eth-if # **scoperecv-queue**	受信キューのコマンド 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 28	Server /chassis/adapter/host-eth-if/recv-queue # **setrq-count***count*	割り当てる受信キューリソースの数。指定できる値の範囲は 1 ～ 256 です。デフォルトは 4 です。
ステップ 29	Server /chassis/adapter/host-eth-if/recv-queue # **setrq-ring-size***size*	受信キュー内の記述子の数。指定できる値の範囲は 64 ～ 4094 です。デフォルトは 512 です。
ステップ 30	Server /chassis/adapter/host-eth-if/recv-queue # **exit**	ホスト イーサネット インターフェイス コマンド モードを終了します。
ステップ 31	Server /chassis/adapter/host-eth-if # **scopetrans-queue**	送信キューのコマンド モードを開始します。
ステップ 32	Server /chassis/adapter/host-eth-if/trans-queue # **setwq-count***count*	割り当てる送信キューリソースの数。指定できる範囲は 1 ～ 256 です。デフォルト値は 1 です。
ステップ 33	Server /chassis/adapter/host-eth-if/trans-queue # **setwq-ring-size***size*	送信キュー内の記述子の数。指定できる値の範囲は 64 ～ 4094 です。デフォルトは 256 です。
ステップ 34	Server /chassis/adapter/host-eth-if/trans-queue # **exit**	ホスト イーサネット インターフェイス コマンド モードを終了します。
ステップ 35	Server /chassis/adapter/host-eth-if # **scopecomp-queue**	完了キューのコマンド モードを開始します。
ステップ 36	Server /chassis/adapter/host-eth-if/comp-queue # **setcq-count***count*	割り当てる完了キューリソースの数。指定できる値の範囲は 1 ～ 512 です。デフォルトは 5 です。 一般に、完了キューの数は、送信キューの数と受信キューの数の合計と等しくなります。
ステップ 37	Server /chassis/adapter/host-eth-if/comp-queue # **exit**	ホスト イーサネット インターフェイス コマンド モードを終了します。
ステップ 38	Server /chassis/adapter/host-eth-if/ # **setrdma_mr***number*	アダプタごとに使用するメモリ領域の数を設定します。値の範囲は 4096 ～ 524288 です。
ステップ 39	Server /chassis/adapter/host-eth-if/ # **setrdma_qp***number*	アダプタごとに使用するキューペアの数を設定します。値の範囲は 1 ～ 8192 のキュー ペアです。
ステップ 40	Server /chassis/adapter/host-eth-if/ # **setrdma_resgrp***number*	使用するリソース グループの数を設定します。値の範囲は 1 ～ 128 のリソース グループです。

	コマンドまたはアクション	目的
		（注） RoCE の詳細をコミットしたら、サーバをリブートして変更を反映させる必要があります。
ステップ 41	Server /chassis/adapter/host-eth-if # **scopeoffload**	TCP オフロードのコマンド モードを開始します。
ステップ 42	Server /chassis/adapter/host-eth-if/offload # **settcp-segment-offload** {**disable**|**enable**}	次のように、TCP セグメンテーション オフロードをイネーブルまたはディセーブルにします。 • **disable**：CPU は大きな TCP パケットをセグメント化します。 • **enable**：CPU はセグメント化する必要がある大きな TCP パケットをハードウェアに送信します。このオプションにより、CPU のオーバーヘッドが削減され、スループット率が向上する可能性があります。これはデフォルトです。 （注） このオプションは、Large Send Offload（LSO）とも呼ばれています。
ステップ 43	Server /chassis/adapter/host-eth-if/offload # **settcp-rx-checksum-offload** {**disable**|**enable**}	次のように、TCP 受信オフロードのチェックサム検証をイネーブルまたはディセーブルにします。 • **disable**：CPU はすべてのパケット チェックサムを検証します。 • **enable**：CPU はすべてのパケット チェックサムを検証のためにハードウェアに送信します。このオプションにより、CPU のオーバーヘッドが削減される可能性があります。これはデフォルトです。
ステップ 44	Server /chassis/adapter/host-eth-if/offload # **settcp-tx-checksum-offload** {**disable**|**enable**}	次のように、TCP 送信オフロードのチェックサム検証をイネーブルまたはディセーブルにします。 • **disable**：CPU はすべてのパケット チェックサムを検証します。 • **enable**：CPU はすべてのパケット チェックサムを検証のためにハードウェアに送信します。このオプションにより、CPU の

	コマンドまたはアクション	目的
		オーバーヘッドが削減される可能性があります。これはデフォルトです。
ステップ 45	Server /chassis/adapter/host-eth-if/offload # **settcp-large-receive-offload** {**disable**|**enable**}	次のように、TCP 大きなパケット受信オフロードをイネーブルまたはディセーブルにします。 • **disable**：CPU はすべての大きなパケットを処理します。 • **enable**：ハードウェアはすべてのセグメント化されたパケットを CPU に送信する前に再構成します。このオプションにより、CPU の使用率が削減され、インバウンドのスループットが増加する可能性があります。これはデフォルトです。
ステップ 46	Server /chassis/adapter/host-eth-if/offload # **exit**	ホスト イーサネット インターフェイス コマンド モードを終了します。
ステップ 47	Server /chassis/adapter/host-eth-if # **scoperss**	Receive Side Scaling（RSS）のコマンド モードを開始します。
ステップ 48	Server /chassis/adapter/host-eth-if/rss # **setrss** {**disable**|**enable**}	マルチプロセッサ システム内でネットワーク受信処理の複数の CPU への効率的な配分を可能にする RSS 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、2 つのデフォルト vNIC に対してはイネーブル、ユーザ作成の vNIC に対してはディセーブルです。
ステップ 49	Server /chassis/adapter/host-eth-if/rss # **setrss-hash-ipv4** {**disable**|**enable**}	IPv4 RSS をイネーブルまたはディセーブルにします。デフォルトはイネーブルです。
ステップ 50	Server /chassis/adapter/host-eth-if/rss # **setrss-hash-tcp-ipv4** {**disable**|**enable**}	TCP/IPv4 RSS をイネーブルまたはディセーブルにします。デフォルトはイネーブルです。
ステップ 51	Server /chassis/adapter/host-eth-if/rss # **setrss-hash-ipv6** {**disable**|**enable**}	IPv6 RSS をイネーブルまたはディセーブルにします。デフォルトはイネーブルです。
ステップ 52	Server /chassis/adapter/host-eth-if/rss # **setrss-hash-tcp-ipv6** {**disable**|**enable**}	TCP/IPv6 RSS をイネーブルまたはディセーブルにします。デフォルトはイネーブルです。
ステップ 53	Server /chassis/adapter/host-eth-if/rss # **setrss-hash-ipv6-ex** {**disable**|**enable**}	IPv6 拡張 RSS をイネーブルまたはディセーブルにします。デフォルトはディセーブルです。

	コマンドまたはアクション	目的
ステップ 54	Server /chassis/adapter/host-eth-if/rss # **setrss-hash-tcp-ipv6-ex** {**disable**|**enable**}	TCP/IPv6 拡張 RSS をイネーブルまたはディセーブルにします。デフォルトはディセーブルです。
ステップ 55	Server /chassis/adapter/host-eth-if/rss # **exit**	ホスト イーサネット インターフェイス コマンド モードを終了します。
ステップ 56	Server /chassis/adapter/host-eth-if # **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） 変更内容は次のサーバのリブート時に有効になります。

次の例では、vNIC のプロパティを設定しています。

```
Server# scope chassis
Server /chassis # show adapter
PCI Slot Product Name   Serial Number  Product ID     Vendor
-------- -------------- -------------- -------------- --------------------
1        UCS VIC P81E   QCI1417A0QK    N2XX-ACPCI01   Cisco Systems Inc

Server /chassis # scope adapter 1
Server /chassis/adapter # scope host-eth-if Test1
Server /chassis/adapter/host-eth-if # set uplink 1
Server /chassis/adapter/host-eth-if # enable vmq
Server /chassis/adapter/host-eth-if # enable arfs
Server /chassis/adapter/host-eth-if *# scope offload
Server /chassis/adapter/host-eth-if/offload *# set tcp-segment-offload enable
Server /chassis/adapter/host-eth-if/offload *# exit
Server /chassis/adapter/host-eth-if *# commit
Server /chassis/adapter/host-eth-if #
```

次の作業

サーバをリブートして変更内容を適用します。

外部イーサネット インターフェイスでのリンク トレーニングの有効化または無効化

指定した vNIC の外部イーサネット インターフェイス上のポート ファイルのリンク トレーニングを有効または無効にすることができます。

はじめる前に

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 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 # **showadapter**	（任意）使用可能なアダプタ デバイスを表示します。
ステップ 3	Server /chassis # **scope adapter***index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 4	Server /chassis / adapter # **scopeext-eth-if0** | **1***name*	指定した vNIC に対して外部イーサネット インターフェイス コマンド モードを開始します。
ステップ 5	Server /chassis / adapter / ext-eth-if # **setlink-trainingon** | **off**	指定した vNIC に対するリンク トレーニングを有効または無効にします。
ステップ 6	Server /chassis / adapter / ext-eth-if * # **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、外部イーサネットインターフェイスでのリンク トレーニングを有効または無効にする例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # scope ext-eth-if 1
Server /chassis/adapter/ext-eth-if* # set link-training on
Server /chassis/adapter/ext-eth-if# commit
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] y
Port 1:
    MAC Address: 74:A2:E6:28:C6:A3
    Link State: Link
    Encapsulation Mode: CE
    Admin Speed: 40Gbps
    Operating Speed: -
    Link Training: N/A
    Connector Present: Yes
    Connector Supported: Yes
    Connector Type: QSFP_XCVR_CR4
    Connector Vendor: CISCO
    Connector Part Number: 2231254-3
    Connector Part Revision: B
```

vNIC の作成

アダプタは、永続的な vNIC を 2 つ提供します。追加の vNIC を 16 個まで作成できます。

はじめる前に

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 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 adapter***index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンドモードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **create host-eth-if** *name*	vNIC を作成し、ホストのイーサネットインターフェイスのコマンド モードを開始します。*name* 引数には最大 32 文字の ASCII 文字を使用できます。
ステップ 4	Server /chassis/adapter/host-eth-if # **set channel-number** *number*	（任意） アダプタで NIV モードがイネーブルになっている場合、この vNIC にチャネル番号を割り当てる必要があります。指定できる範囲は 1 ～ 1000 です。
ステップ 5	Server /chassis/adapter/host-eth-if # **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） 変更内容は次のサーバのリブート時に有効になります。

次に、アダプタ 1 の vNIC を作成する例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # create host-eth-if Vnic5
Server /chassis/adapter/host-eth-if *# commit
New host-eth-if settings will take effect upon the next server reset
Server /chassis/adapter/host-eth-if #
```

vNIC の削除

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 adapter***index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **delete host-eth-if** *name*	指定された vNIC を削除します。 （注） デフォルトの 2 つの vNIC（[eth0] と [eth1]）は、どちらも削除することはできません。
ステップ 4	Server /chassis/adapter # **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） 変更内容は次のサーバのリブート時に有効になります。

次に、アダプタ 1 の vNIC を削除する例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # delete host-eth-if Vnic5
Server /chassis/adapter *# commit
Server /chassis/adapter #
```

Cisco IMC CLI を使用した Cisco usNIC の作成

（注） [vNIC properties] ダイアログボックスに Cisco usNIC に対する複数のプロパティが一覧表示されていますが、その他のプロパティが現在使用されていないため、次のプロパティだけを設定する必要があります。

- **cq-count**
- **rq-count**
- **tq-count**
- **usnic-count**

はじめる前に

このタスクを実行するには、管理者権限で Cisco IMC CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	server/chassis# **scope adapter***index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源がオンであることを確認します。サーバに設定されたアダプタのインデックスを表示するには、**show adapter** コマンドを使用します。
ステップ 3	server/chassis/adapter# **scopehost-eth-if** {**eth0** | **eth1**}	vNIC のコマンド モードを開始します。お客様の環境に設定された vNIC の数に基づいてイーサネット ID を指定します。たとえば、1 つの vNIC だけを設定した場合は、**eth0** を指定します。
ステップ 4	server/chassis/adapter/host-eth-if# **createusnic-config0**	usNIC config を作成します。続いて、コマンド モードを開始します。インデックス値を必ず 0 に設定してください。

	コマンドまたはアクション	目的
		（注） Cisco IMC CLI を使用して特定の vNIC に初めて Cisco usNIC を作成するには、**usnic-config** を最初に作成する必要があります。その後、**usnic-config** にスコープして、Cisco usNIC のプロパティを変更するだけで十分です。Cisco usNIC プロパティの変更の詳細については、Cisco IMC CLI を使用した Cisco usNIC 値の変更，（182 ページ）を参照してください。
ステップ 5	server/chassis/adapter/host-eth-if/usnic-config# **setcq-count***count*	割り当てる完了キュー リソースの数を指定します。この値を 6 に設定することを推奨します。 完了キューの数は、送信キューの数と受信キューの数の合計と等しくなります。
ステップ 6	server/chassis/adapter/host-eth-if/usnic-config# **setrq-count***count*	割り当てる受信キュー リソースの数を指定します。この値を 6 に設定することを推奨します。
ステップ 7	server/chassis/adapter/host-eth-if/usnic-config# **settq-count***count*	割り当てる送信キュー リソースの数を指定します。この値を 6 に設定することを推奨します。
ステップ 8	server/chassis/adapter/host-eth-if/usnic-config# **set usnic-count** *number of usNICs*.	作成する Cisco usNIC の数を指定します。サーバで実行されている各 MPI プロセスには、専用の Cisco usNIC が必要です。したがって、64 の MPI プロセスを同時に実行させるには、最大 64 の Cisco usNIC を作成する必要がある場合があります。Cisco usNIC 対応 vNIC ごとに、サーバの物理コアの数と同数の Cisco usNIC を最低限作成することを推奨します。たとえば、サーバに 8 つの物理コアがある場合は、8 つの Cisco usNIC を作成します。
ステップ 9	server/chassis/adapter/host-eth-if /usnic-config# **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） 変更はサーバのリブート時に有効になります。

	コマンドまたはアクション	目的
ステップ 10	server/chassis/adapter/host-eth-if/usnic-config# **exit**	ホスト イーサネット インターフェイス コマンド モードを終了します。
ステップ 11	server/chassis/adapter/host-eth-if#**exit**	アダプタ インターフェイス コマンドモードを終了します。
ステップ 12	server/chassis/adapter#**exit**	シャーシインターフェイス コマンドモードを終了します。
ステップ 13	server/chassis#**exit**	サーバ インターフェイス コマンド モードを終了します。
ステップ 14	server#**scope bios**	Bios コマンド モードを開始します。
ステップ 15	server/bios#**scope advanced**	BIOS コマンド モードの高度な設定を開始します。
ステップ 16	server/bios/advanced#**set IntelVTD Enabled**	インテル バーチャライゼーション テクノロジーをイネーブルにします。
ステップ 17	server/bios/advanced#**set ATS Enabled**	プロセッサの Intel VT-d Address Translation Services（ATS）のサポートをイネーブルにします。
ステップ 18	server/bios/advanced#**set CoherencySupport Enabled**	プロセッサの Intel VT-d coherency のサポートをイネーブルにします。
ステップ 19	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。 （注） 変更はサーバのリブート時に有効になります。

次の例は、Cisco usNIC プロパティの設定方法を示します。

```
Server # scope chassis
server /chassis # show adapter
server /chassis # scope adapter 2
server /chassis/adapter # scope host-eth-if eth0
server /chassis/adapter/host-eth-if # create usnic-config 0
server /chassis/adapter/host-eth-if/usnic-config *# set usnic-count 64
server /chassis/adapter/host-eth-if/usnic-config *# set cq-count 6
server /chassis/adapter/host-eth-if/usnic-config *# set rq-count 6
server /chassis/adapter/host-eth-if/usnic-config *# set tq-count 6
server /chassis/adapter/host-eth-if/usnic-config *# commit
Committed settings will take effect upon the next server reset
server /chassis/adapter/host-eth-if/usnic-config # exit
server /chassis/adapter/host-eth-if # exit
server /chassis/adapter # exit
server /chassis # exit
server # exit
```

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

Cisco IMC CLI を使用した Cisco usNIC 値の変更

はじめる前に

このタスクを実行するには、管理者権限で Cisco IMC GUI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	server/chassis# **scope adapter** *index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源がオンであることを確認します。サーバに設定されたアダプタのインデックスを表示するには、**show adapter** コマンドを使用します。
ステップ 3	server/chassis/adapter# **scopehost-eth-if** {**eth0** | **eth1**}	vNIC のコマンド モードを開始します。お客様の環境に設定された vNIC の数に基づいてイーサネット ID を指定します。たとえば、1 つの vNIC だけを設定した場合は、**eth0** を指定します。
ステップ 4	server/chassis/adapter/host-eth-if# **scopeusnic-config0**	usNIC のコマンド モードを開始します。Cisco usNIC を設定する場合は、インデックス値を必ず 0 に設定してください。
ステップ 5	server/chassis/adapter/host-eth-if/usnic-config# **set usnic-count** *number of usNICs*.	作成する Cisco usNIC の数を指定します。サーバで実行されている各 MPI プロセスには、専用の Cisco usNIC が必要です。したがって、64 の MPI プロセスを同時に実行させるには、最大 64 の Cisco usNIC を作成する必要がある場合があります。Cisco usNIC 対応 vNIC ごとに、サーバの

	コマンドまたはアクション	目的
		物理コアの数と同数の Cisco usNIC を最低限作成することを推奨します。たとえば、サーバに 8 つの物理コアがある場合は、8 つの usNIC を作成します。
ステップ 6	server /chassis/adapter/host-eth-if /usnic-config# **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） 変更はサーバのリブート時に有効になります。
ステップ 7	server/chassis/adapter/host-eth-if/usnic-config# **exit**	ホストイーサネットインターフェイス コマンド モードを終了します。
ステップ 8	server/chassis/adapter/host-eth-if#**exit**	アダプタインターフェイス コマンドモードを終了します。
ステップ 9	server/chassis/adapter#**exit**	シャーシインターフェイス コマンドモードを終了します。
ステップ 10	server/chassis#**exit**	サーバインターフェイス コマンドモードを終了します。

次の例は、Cisco usNIC プロパティの設定方法を示します。

```
server # scope chassis
server /chassis # show adapter
server /chassis # scope adapter 2
server /chassis/adapter # scope host-eth-if eth0
server /chassis/adapter/host-eth-if # scope usnic-config 0
server /chassis/adapter/host-eth-if/usnic-config # set usnic-count 32
server /chassis/adapter/host-eth-if/usnic-config # commit
Committed settings will take effect upon the next server reset
server /chassis/adapter/host-eth-if/usnic-config # exit
server /chassis/adapter/host-eth-if # exit
server /chassis/adapter # exit
server /chassis # exit
server # exit
```

usNIC プロパティの表示

はじめる前に

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。

usNIC は vNIC 上で構成する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope adapter***index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンドモードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **scope host-eth-if** {**eth0** | **eth1** | *name*}	指定した vNIC に対してホスト イーサネット インターフェイス コマンドモードを開始します。
ステップ 4	Server /chassis/adapter/host-eth-if # **show usnic-config** *index*	vNIC の usNIC プロパティを表示します。

次の例は、vNIC の usNIC プロパティを表示する例を示します。

```
Server # scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # scope host-eth-if eth0
Server /chassis/adapter/host-eth-if # show usnic-config 0
Idx usNIC Count TQ Count RQ Count CQ Count TQ Ring Size RQ Ring Size Interrupt Count
--- ----------- -------- -------- -------- ------------ ------------ ---------------
0   113         2        2        4        256          512          4
Server /chassis/adapter/host-eth-if #
```

vNIC からの Cisco usNIC の削除

はじめる前に

このタスクを実行するには、admin 権限で Cisco IMC CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	server/chassis# **scope adapter** *index*	*index* で指定した PCI スロット番号に装着されているアダプタ 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
		（注） アダプタの設定を表示または変更する前に、サーバの電源がオンであることを確認します。サーバに設定されたアダプタのインデックスを表示するには、**show adapter** コマンドを使用します。
ステップ 3	server/chassis/adapter# **scopehost-eth-if** {**eth0** | **eth1**}	vNIC のコマンド モードを開始します。お客様の環境に設定された vNIC の数に基づいてイーサネット ID を指定します。たとえば、1 つの vNIC だけを設定した場合は、**eth0** を指定します。
ステップ 4	Server/chassis/adapter/host-eth-if# **delete usnic-config 0**	vNIC の Cisco usNIC 設定を削除します。
ステップ 5	Server/chassis/adapter/host-eth-if# **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） 変更はサーバのリブート時に有効になります。

次に、vNIC の Cisco usNIC 設定を削除する例を示します。

```
server # scope chassis
server/chassis # show adapter
server/chassis # scope adapter 1
server/chassis/adapter # scope host-eth-if eth0
server/chassis/adapter/host-eth-if # delete usnic-config 0
server/chassis/host-eth-if/iscsi-boot *# commit
New host-eth-if settings will take effect upon the next adapter reboot

server/chassis/host-eth-if/usnic-config #
```

iSCSI ブート機能の設定

vNIC の iSCSI ブート機能の設定

ラック サーバがスタンドアロン モードに設定されていて、VIC アダプタが Nexus 5000 スイッチ ファミリに直接接続されている場合は、iSCSI ストレージ ターゲットからサーバがリモートでブートされるようにこれらの VIC アダプタを設定できます。ラック サーバがリモート iSCSI ターゲット デバイスからホスト OS イメージをロードできるようにイーサネット vNIC を設定できます。

vNIC で iSCSI ブート機能を設定する方法は、次のとおりです。

- 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。
- iSCSI ストレージ ターゲットからサーバをリモートでブートするように vNIC を設定するには、vNIC の PXE ブート オプションをイネーブルにする必要があります。

（注） ホストごとに最大 2 つの iSCSI vNIC を設定できます。

vNIC 上の iSCSI ブート機能の設定

ホストごとに最大 2 つの iSCSI vNIC を設定できます。

はじめる前に

- iSCSI ストレージ ターゲットからサーバをリモートでブートするように vNIC を設定するには、vNIC の PXE ブート オプションをイネーブルにする必要があります。
- 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 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 adapter***index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **scope host-eth-if** {**eth0** | **eth1** | *name*}	指定した vNIC に対してホスト イーサネット インターフェイス コマンド モードを開始します。
ステップ 4	Server /chassis/adapter/host-eth-if # **create iscsi-boot** *index*	vNIC の iSCSI ブート インデックスを作成します。この時点では、0 だけがインデックスとして許可されます。
ステップ 5	Server /chassis/adapter/host-eth-if/iscsi-boot* # **create iscsi-target** *index*	vNIC の iSCSI ターゲットを作成します。値は 0 または 1 を指定できます。
ステップ 6	Server /chassis/adapter/host-eth-if/iscsi-boot* # **set dhcp-net-settings enabled**	iSCSI ブートの DHCP ネットワーク設定をイネーブルにします。
ステップ 7	Server /chassis/adapter/host-eth-if/iscsi-boot* # **set initiator-name** *string*	発信側名を設定します。これは 223 文字以内である必要があります。

	コマンドまたはアクション	目的
ステップ 8	Server /chassis/adapter/host-eth-if/iscsi-boot* # **set dhcp-iscsi-settings enabled**	DHCP iSCSI 設定をイネーブルにします。
ステップ 9	Server /chassis/adapter/host-eth-if/iscsi-boot* # **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） 変更内容は次のサーバのリブート時に有効になります。

次に、vNIC の iSCSI ブート機能を設定する例を示します。

```
Server # scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # scope host-eth-if eth0
Server /chassis/adapter/host-eth-if # create iscsi-boot 0
Server /adapter/host-eth-if/iscsi-boot *# set dhcp-net-settings enabled
Server /adapter/host-eth-if/iscsi-boot *# set initiator-name iqn.2012-01.com.adser:abcde
Server /adapter/host-eth-if/iscsi-boot *# set dhcp-iscsi-settings enabled
Server /adapter/host-eth-if/iscsi-boot *# commit

New host-eth-if settings will take effect upon the next server reset
Server /adapter/host-eth-if/iscsi-boot #
```

vNIC の iSCSI ブート設定の削除

はじめる前に

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 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 adapter***index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **scope host-eth-if** {**eth0** | **eth1** | *name*}	指定した vNIC に対してホスト イーサネット インターフェイス コマンド モードを開始します。
ステップ 4	Server /chassis/adapter/host-eth-if # **delete iscsi-boot 0**	vNIC の iSCSI ブート機能を削除します。

	コマンドまたはアクション	目的
ステップ 5	Server /chassis/adapter/host-eth-if* # **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） 変更内容は次のサーバのリブート時に有効になります。

次に、vNIC の iSCSI ブート機能を削除する例を示します。

```
Server # scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # scope host-eth-if eth0
Server /chassis/adapter/host-eth-if # delete iscsi-boot 0
Server /adapter/host-eth-if/iscsi-boot *# commit
New host-eth-if settings will take effect upon the next server reset

Server /adapter/host-eth-if/iscsi-boot #
```

VM FEX の管理

仮想マシン ファブリック エクステンダ

Cisco Virtual Machine Fabric Extender（VM FEX）は、（prestandard）IEEE 802.1Qbh ポート エクステンダ アーキテクチャを仮想マシンにまで拡張します。このアーキテクチャでは、各 VM インターフェイスに対してスイッチ上で仮想 Peripheral Component Interconnect Express（PCIe）デバイスと仮想ポートが提供されます。

このリリースでは、VM FEX は、次のカードとオペレーティング システムをサポートします。

カード：Cisco UCS 1225 仮想インターフェイス カード

オペレーティング システム：

- VMware ESXi 5.1 Update 2
- VMware ESXi 5.5

このリリースの VM FEX は、Microsoft Hyper-V および Red Hat KVM でサポートされていません。

VM FEX のプロパティの表示

はじめる前に

- 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。
- サポートされた仮想インターフェイス カード（VIC）がシャーシに取り付けられ、サーバの電源がオンである必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope adapter***index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **show vmfex [detail]**	一般的な VM FEX プロパティを表示します。フィールドの説明については、全般的なプロパティ設定,（190 ページ）を参照してください。
ステップ 4	Server /chassis/adapter # **scope vmfex** *name*	指定された VM FEX インターフェイスのコマンド モードを開始します。
ステップ 5	Server /chassis/adapter/vmfex # **show interrupt [detail]**	イーサネット割り込み設定を表示します。フィールドの説明については、イーサネット割り込みの設定,（192 ページ）を参照してください。
ステップ 6	Server /chassis/adapter/vmfex # **show recv-queue [detail]**	イーサネット受信キューの設定を表示します。フィールドの説明については、イーサネット受信キューの設定,（192ページ）を参照してください。
ステップ 7	Server /chassis/adapter/vmfex # **show trans-queue [detail]**	イーサネット送信キューの設定を表示します。フィールドの説明については、イーサネット送信キューの設定,（192ページ）を参照してください。
ステップ 8	Server /chassis/adapter/vmfex # **show comp-queue [detail]**	完了キューの設定を表示します。フィールドの説明については、完了キューの設定,（193 ページ）を参照してください。
ステップ 9	Server /chassis/adapter/vmfex # **show offload [detail]**	TCP オフロードの設定を表示します。フィールドの説明については、TCP オフロードの設定,（193 ページ）を参照してください。
ステップ 10	Server /chassis/adapter/vmfex # **show rss [detail]**	RSS 設定を表示します。フィールドの説明については、Receive Side Scaling 設定,（194 ページ）を参照してください。

次に、VM FEX のプロパティを表示する例を示します。

```
Server /chassis/adapter # show vmfex detail
```

```
Name pts0:
    MTU: 1500
    Uplink Port: 0
    MAC Address: 00:00:00:00:00:00
    CoS: N/A
    Trust Host CoS:
    PCI Order:
    VLAN: N/A
    VLAN Mode: N/A
    Rate Limiting:
    PXE Boot: disabled
    Channel Number: 0
    Port Profile:
    Uplink Failover: Enabled
    Uplink Failback Timeout: 5

Server /chassis/adapter # scope vmfex pts0

Server /chassis/adapter/vmfex # show interrupt
Interrupt Count Coalescing Time (us) Coalescing Type Interrupt Mode
--------------- -------------------- --------------- ---------------
6               125                  MIN             MSI

Server /chassis/adapter/vmfex # show recv-queue
Receive Queue Count Receive Queue Ring Size
------------------- ------------------------------
4                   512

Server /chassis/adapter/vmfex # show trans-queue
Transmit Queue Count Transmit Queue Ring Size
-------------------- -------------------------------
1                    256

Server /chassis/adapter/vmfex # show comp-queue
Completion Queue Count    Completion Queue Ring Size
------------------------- --------------------------
5                         1

Server /chassis/adapter/vmfex # show offload
TCP Segment Offload  TCP Rx Checksum  TCP Tx Checksum  Large Receive
-------------------- ---------------- ---------------- -------------
enabled              enabled          enabled          enabled

Server /chassis/adapter/vmfex # show rss
TCP Rx Side Scaling
--------------------
enabled

Server /chassis/adapter/vmfex #
```

VM FEX 設定

次の表に、表示できる VM FEX 設定について説明します。

全般的なプロパティ設定

名前	説明
名前	VM FEX のユーザ定義名。
MTU	この VM FEX で受け入れられる最大伝送単位、つまりパケットサイズ。

名前	説明
アップリンク ポート	この VM FEX に関連付けられたアップリンク ポート。この VM FEX へのすべてのトラフィックは、このアップリンク ポートを通過します。
MAC アドレス	VM FEX に関連付けられた MAC アドレス。
Class of Service	この VM FEX からのトラフィックに関連付けられるサービス クラス。
Trust Host CoS	VM FEX がホスト オペレーティング システムが提供するサービス クラスを使用できるかどうか。
PCI Order	この VM FEX が使用される順序。
Default VLAN	この VM FEX のデフォルト VLAN。
VLAN モード	VLAN トランキングまたはアクセスが設定されているかどうか。
Rate Limit	レート制限が設定されている場合、最大レート。
Enable PXE Boot	VM FEX を使用して PXE ブートを実行できるかどうか。
Channel Number	アダプタで NIV モードがイネーブルにされている場合、この VM FEX に割り当てられるチャネル番号。
Port Profile	アダプタで NIV モードがイネーブルにされている場合、VM FEX に関連付けられたポート プロファイル。 （注） このフィールドには、このサーバが接続しているスイッチに定義されたポート プロファイルが表示されます。
Enable Uplink Failover	アダプタで NIV モードがイネーブルにされている場合、通信に問題が発生したときにこの VM FEX のトラフィックがセカンダリ インターフェイスにフェールオーバーするかどうか。
Failback Timeout	セカンダリ インターフェイスを使用して VM FEX が始動した後、その VM FEX のプライマリ インターフェイスが再びシステムで使用されるには、プライマリ インターフェイスが一定時間使用可能な状態になっている必要があり、その時間の長さをこの設定で制御します。

イーサネット割り込みの設定

名前	説明
[Interrupt Count] フィールド	この VM FEX に割り当てられた割り込みリソースの数。
[Coalescing Time] フィールド	割り込み間の Cisco IMC の待機時間、または割り込みが送信される前に必要な休止期間。
[Coalescing Type] フィールド	次のいずれかになります。 • [MIN]：システムは、別の割り込みイベントを送信する前に [Coalescing Time] フィールドに指定された時間だけ待機します。 • [IDLE]：アクティビティなしの期間が少なくとも [Coalescing Time] フィールドに指定された時間続くまで、システムから割り込みは送信されません。
[Interrupt Mode] フィールド	優先ドライバ割り込みモード。次のいずれかになります。 • [MSIx]：機能拡張された Message Signaled Interrupts（MSI）。 • [MSI]：MSI だけ。 • [INTx]：PCI INTx 割り込み。

イーサネット受信キューの設定

名前	説明
[Receive Queue Count] フィールド	この VM FEX に割り当てられた受信キュー リソースの数。
[Receive Queue Ring Size] フィールド	各受信キュー内の記述子の数。

イーサネット送信キューの設定

名前	説明
[Transmit Queue Count] フィールド	この VM FEX に割り当てられた送信キュー リソースの数。

名前	説明
[Transmit Queue Ring Size] フィールド	各送信キュー内の記述子の数。

完了キューの設定

名前	説明
[Completion Queue Count] フィールド	この VM FEX に割り当てられた完了キュー リソースの数。
[Completion Queue Ring Size] フィールド	各完了キュー内の記述子の数。

TCP オフロードの設定

名前	説明
[Enable TCP Segmentation Offload] フィールド	イネーブルの場合、CPU はセグメント化する必要がある大きな TCP パケットをハードウェアに送信します。ディセーブルの場合、CPU は大きいパケットをセグメント化します。 （注） このオプションは、Large Send Offload（LSO）とも呼ばれています。
[Enable TCP Rx Offload Checksum Validation] フィールド	イネーブルの場合、CPU はすべてのパケット チェックサムを検証のためにハードウェアに送信します。ディセーブルの場合、CPU はすべてのパケット チェックサムを検証します。
[Enable TCP Tx Offload Checksum Generation] フィールド	イネーブルの場合、CPU はすべてのパケットをハードウェアに送信し、ハードウェアでチェックサムを計算できるようにします。ディセーブルの場合、CPU はすべてのパケット チェックサムを計算します。
[Enable Large Receive] フィールド	イネーブルの場合、ハードウェアはすべてのセグメント化されたパケットを CPU に送信する前に再構成します。ディセーブルの場合、CPU は大きいパケットをすべて処理します。

Receive Side Scaling 設定

名前	説明
[Enable TCP Receive Side Scaling] フィールド	Receive Side Scaling（RSS）は、ネットワーク受信処理をマルチプロセッサ システム内の複数の CPU に分散させます。 イネーブルの場合、可能であれば、ネットワーク受信処理がプロセッサ間で共有されます。ディセーブルの場合、ネットワーク受信処理は、追加のプロセッサが使用可能であっても、常に 1 つのプロセッサで処理されます。
[Enable IPv4 RSS] フィールド	イネーブルの場合、RSS が IPv4 ネットワークでイネーブルになります。
[Enable TCP-IPv4 RSS] フィールド	イネーブルの場合、IPv4 ネットワーク間での TCP 送信に対して RSS がイネーブルになります。
[Enable IPv6 RSS] フィールド	イネーブルの場合、RSS が IPv6 ネットワークでイネーブルになります。
[Enable TCP-IPv6 RSS] フィールド	イネーブルの場合、IPv6 ネットワーク間での TCP 送信に対して RSS がイネーブルになります。
[Enable IPv6 Extension RSS] フィールド	イネーブルの場合、IPv6 拡張に対して RSS がイネーブルになります。
[Enable TCP-IPv6 Extension RSS] フィールド	イネーブルの場合、IPv6 ネットワーク間での TCP 送信に対して RSS がイネーブルになります。

アダプタ設定のバックアップと復元

アダプタ設定のエクスポート

アダプタ設定は、XML ファイルとして TFTP サーバにエクスポートできます。

重要 ファームウェアまたは BIOS の更新が進行中の場合は、それらのタスクが完了するまで、アダプタ構成をエクスポートしないでください。

はじめる前に

サポートされた仮想インターフェイス カード（VIC）がシャーシに取り付けられ、サーバの電源がオンである必要があります。

TFTP サーバの IP アドレスを取得します。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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 adapter***index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **export-vnic***protocolremote server IP address*	エクスポート操作を開始します。アダプタ コンフィギュレーション ファイルは、指定した IP アドレスにあるリモート サーバ上に指定したパスとファイル名で保存されます。プロトコルは次のいずれかになります。 • TFTP • FTP • SFTP • SCP • HTTP （注） Cisco UCS C シリーズ サーバでは、リモート サーバからファームウェアを更新すると、サーバのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバ タイプとして SCP または SFTP を選択した場合にのみ使用できます。 このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」というメッセージが表示されます。サーバ フィンガープリントの信頼性に応じて、[Y] または [N] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。

次に、アダプタ 1 設定をエクスポートする例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
```

```
Server /chassis/adapter # export-vnic ftp 192.0.20.34 //test/dnld-ucs-k9-bundle.1.0.2h.bin
Server /chassis/adapter #
```

アダプタ設定のインポート

重要 ファームウェアまたはBIOSの更新が進行中の場合は、それらのタスクが完了するまで、アダプタ構成をインポートしないでください。

はじめる前に

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 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 adapter***index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **import-vnic** *tftp-ip-address path-and-filename*	インポート操作を開始します。アダプタは、指定された IP アドレスの TFTP サーバから、指定されたパスの設定ファイルをダウンロードします。この設定は、サーバが次にリブートされたときにインストールされます。

次に、PCI スロット 1 のアダプタの設定をインポートする例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # import-vnic 192.0.2.34 /ucs/backups/adapter4.xml
Import succeeded.
New VNIC adapter settings will take effect upon the next server reset.
Server /chassis/adapter #
```

次の作業

サーバをリブートして、インポートした設定を適用します。

アダプタのデフォルトの復元

はじめる前に

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 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 # **adapter-reset-defaults***index*	*index* 引数で指定された PCI スロット番号のアダプタを出荷時の設定に復元します。 （注） アダプタをデフォルト設定にリセットすると、ポート速度が 4 X 10 Gbps に設定されます。40 Gbps スイッチを使用している場合にのみ、ポート速度として 40 Gbps を選択してください。

次に、PCI スロット 1 のアダプタのデフォルト設定を復元する例を示します。

```
Server# scope chassis
Server /chassis # adapter-reset-defaults 1
This operation will reset the adapter to factory default.
All your configuration will be lost.
Continue?[y|N] y
Server /chassis #
```

アダプタ ファームウェアの管理

アダプタ ファームウェア

Cisco UCS C シリーズ ネットワーク アダプタには、次のファームウェア コンポーネントが含まれています。

- アダプタ ファームウェア：メインのオペレーティング ファームウェア（アクティブ イメージとバックアップ イメージで構成）は、Cisco IMC GUI または CLI インターフェイスから、または Host Upgrade Utility（HUU）からインストールできます。ファームウェア イメージをローカル ファイル システムまたは TFTP サーバからアップロードできます。
- ブートローダ ファームウェア：ブートローダ ファームウェアは、Cisco IMC からインストールできません。このファームウェアは、Host Upgrade Utility を使用してインストールできます。

アダプタ ファームウェアのインストール

重要 ファームウェアまたはBIOSの更新が進行中の場合は、それらのタスクが完了するまで、アダプタ ファームウェアをインストールしないでください。

はじめる前に

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 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 # **update-adapter-fw** *tftp-ip-address path-and-filename* {**activate** | **no-activate**} [*pci-slot*] [*pci-slot*]	指定したアダプタ ファームウェア ファイルを TFTP サーバからダウンロードし、アダプタを指定した場合は1つまたは2つの指定アダプタ上に、指定しなかった場合にはすべてのアダプタ上にこのファームウェアをバックアップイメージとしてインストールします。**activate** キーワードを指定した場合、新しいファームウェアがインストール後にアクティブになります。
ステップ 3	Server /chassis # **recover-adapter-update** [*pci-slot*] [*pci-slot*]	（任意） アダプタを指定した場合には1つまたは2つの指定アダプタについて、指定しない場合にはすべてのアダプタについて、不完全なファームウェア アップデートの状態をクリアします。

次に、PCI スロット 1 のアダプタ上のアダプタ ファームウェア アップグレードを開始する例を示します。

```
Server# scope chassis
Server /chassis # update-adapter-fw 192.0.2.34 /ucs/adapters/adapter4.bin activate 1
Server /chassis #
```

次の作業

新しいファームウェアをアクティブにするには、アダプタ ファームウェアのアクティブ化, （199 ページ）を参照してください。

アダプタ ファームウェアのアクティブ化

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。
- Cisco IMC のリブートまたはリセット。
- 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。

はじめる前に

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 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 # **activate-adapter-fw** *pci-slot* {**1** | **2**}	指定された PCI スロットのアダプタ上のアダプタ ファームウェア イメージ 1 または 2 をアクティブ化します。 （注） 変更内容は次のサーバのリブート時に有効になります。

次に、PCI スロット 1 のアダプタ上のアダプタ ファームウェア イメージ 2 をアクティブにする例を示します。

```
Server# scope chassis
Server /chassis # activate-adapter-fw 1 2
Firmware image activation suceeded
Please reset the server to run the activated image
Server /chassis #
```

次の作業

サーバをリブートして変更内容を適用します。

アダプタのリセット

はじめる前に

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 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 # **adapter-reset** *index*	*Index* 引数で指定された PCI スロット番号のアダプタをリセットします。 （注） アダプタをリセットすると、ホストもリセットされます。

次に、PCI スロット 1 のアダプタをリセットする例を示します。

```
Server# scope chassis
Server /chassis # adapter-reset 1
This operation will reset the adapter and the host if it is on.
You may lose connectivity to the CIMC and may have to log in again.
Continue?[y|N] y
Server /chassis #
```

第 10 章

ストレージ アダプタの管理

この章は、次の項で構成されています。

自己暗号化ドライブ（フル ディスク暗号化）

Cisco IMC は、自己暗号化ドライブ（SED）をサポートしています。ドライブ内の特別なハードウェアがリアルタイムで入力データを暗号化し、出力データを復号します。この機能は、フル ディスク暗号化（FDE）とも呼ばれます。

ドライブ上のデータは、ドライブに入力される際に暗号化され、出力される際に復号されます。ただし、ドライブをロックしている場合は、データを取得するためにセキュリティ キーは必要ありません。

ドライブがロックされると、暗号化キーが内部で作成され保存されます。このドライブに保存されているすべてのデータは、そのキーを使用して暗号化され、暗号化された形式で保存されます。データをこのように保存すると、データを非暗号化してドライブから取得するためにセキュリティ キーが必要になります。ドライブのロックを解除すると、その暗号化キーが削除され、保存されたデータは使用できなくなります。これは、Secure Erase と呼ばれます。FDE は、キー ID とセキュリティ キーで構成されます。

FDE 機能は次の操作をサポートしています。

- コントローラでのセキュリティの有効化および無効化
- セキュアな仮想ドライブの作成
- 非セキュアなドライブ グループの保護

- 外部の設定ドライブのロック解除
- 物理ドライブ（JBOD）でのセキュリティの有効化
- セキュアな SED ドライブのクリア
- セキュアな外部設定のクリア

未使用の物理ドライブからの仮想ドライブの作成

はじめる前に

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 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*	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 # **create virtual-drive**	この時点で、RAID レベル、使用する物理ドライブ、ドライブのフル ディスク暗号化をイネーブルにするサイズ、新しい仮想ドライブのサイズと書き込みポリシーに関する情報の入力を求めるプロンプトが表示されます。プロンプトごとに適切な情報を入力します。 仮想ドライブの情報の指定が完了したら、情報が正しいことの確認を求めるプロンプトが表示されます。確認する場合は **y**（yes）を入力し、操作をキャンセルする場合は **n**（no）を入力します。 （注） フルディスク暗号化をイネーブルにすると、ドライブが保護されます。
ステップ 4	Server /chassis/storageadapter # **show virtual-drive**	既存の仮想ドライブが表示されます。

次に、2 台の未使用の物理ドライブにまたがる新しい仮想ドライブの作成方法を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # create-virtual-drive
Please enter RAID level
0, 1, 5, 10, 50 --> 1

Please choose from the following 10 unused physical drives:
```

```
    ID  Size(MB)       Model        Interface  Type
     1  571776         SEAGATE      SAS        HDD
     2  571776         SEAGATE      SAS        HDD
     4  571776         SEAGATE      SAS        HDD
     5  428672         SEAGATE      SAS        HDD
     6  571776         SEAGATE      SAS        HDD
     7  571776         SEAGATE      SAS        HDD
     8  571776         SEAGATE      SAS        HDD
     9  428672         SEAGATE      SAS        HDD
    10  571776         SEAGATE      SAS        HDD
    11  953344         SEAGATE      SAS        HDD

Specify physical disks for span 0:
  Enter comma-separated PDs from above list--> 1,2
  Please enter Virtual Drive name (15 characters maximum)--> test_v_drive
  Please enter Virtual Drive size in MB, GB, or TB
   Example format: '400 GB' --> 10 GB

Optional attribute:

  stripsize: defaults to 64K Bytes

     0: 8K Bytes
    1: 16K Bytes
    2: 32K Bytes
    3: 64K Bytes
    4: 128K Bytes
    5: 256K Bytes
    6: 512K Bytes
    7: 1024K Bytes
  Choose number from above options or hit return to pick default--> 2
stripsize will be set to 32K Bytes (6 and 'strip-size\:32k')

  Disk Cache Policy: defaults to Unchanged

     0: Unchanged
    1: Enabled
    2: Disabled
  Choose number from above options or hit return to pick default--> 0
Disk Cache Policy will be set to Unchanged (0 and 'disk-cache-policy\:unchanged'

         )

  Read Policy: defaults to No Read Ahead

     0: No Read Ahead
    1: Always
  Choose number from above options or hit return to pick default--> 0
Read Policy will be set to No Read Ahead (0 and 'read-policy\:no-read-ahead')

  Write Policy: defaults to Write Through

     0: Write Through
    1: Write Back Good BBU
    2: Always Write Back
  Choose number from above options or hit return to pick default--> 0
Write Policy will be set to Write Through (0 and 'write-policy\:write-through')

  IO Policy: defaults to Direct I/O

     0: Direct I/O
    1: Cached I/O
  Choose number from above options or hit return to pick default--> 0
IO Policy will be set to Direct I/O (0 and 'io-policy\:direct-io')

  Access Policy: defaults to Read Write

     0: Read Write
    1: Read Only
    2: Blocked
  Choose number from above options or hit return to pick default--> 0
Access Policy will be set to Read Write (0 and 'access-policy\:read-write')
```

```
Enable SED security on virtual drive (and underlying drive group)?
Enter y or n--> y
Virtual drive and drive group will be secured

New virtual drive will have the following characteristics:
  - Spans: '[1.2]'
  - RAID level: '1'
  - Name: 'test_v_drive'
  - Size: 10 GB
  - stripsize: 32K Bytes
  - Disk Cache Policy: Unchanged
  - Read Policy: No Read Ahead
  - Write Policy: Write Through
  - IO Policy: Direct I/O
  - Access Policy: Read Write
  - Encryption: FDE

OK? (y or n)--> y

Server /chassis/storageadapter # show virtual-drive
Virtual Drive Health         Status               Name             Size       RAID Level
Boot Drive
------------- -------------- -------------------- ---------------- ---------- ----------
----------
0             Good           Optimal                               150528 MB  RAID 0
false
1             Good           Optimal                               20480 MB   RAID 0
true
2             Good           Optimal                               114140 MB  RAID 0
false
3             Good           Optimal              test_v_drive     10000 MB   RAID 1
false
4             Good           Optimal              new_from_test    500 MB     RAID 1
false

Server /chassis/storageadapter #
```

既存のドライブ グループからの仮想ドライブの作成

はじめる前に

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 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*	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 # **carve-virtual-drive**	この時点で、使用する仮想ドライブに関する情報、新しい仮想ドライブのサイズと書き込みポリシーに関する情報の入力を求めるプロンプトが表示されます。プロンプトごとに適切な情報を入力します。 仮想ドライブの情報の指定が完了したら、情報が正しいことの確認を求めるプロンプトが表示されます。

	コマンドまたはアクション	目的
		確認する場合は **y**（yes）を入力し、操作をキャンセルする場合は **n**（no）を入力します。
ステップ 4	Server /chassis/storageadapter # **show virtual-drive**	既存の仮想ドライブが表示されます。

次に、既存の RAID 1 ドライブ グループ内の未使用のスペースから新しい仮想ドライブを分割する例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # carve-virtual-drive
  < Fetching virtual drives...>

ID  Name              RL  VDSize        MaxPossibleSize PD(s)
-----------------------------------------------------------------
0  RAID0_12          0   100 MB        Unknown         1,2

Please choose from the above list the virtual drive number
whose space the new virtual drive will share--> 0
New virtual drive will share space with VD 0

Please enter Virtual Drive name (15 characters maximum)--> test_v_drive
Please enter Virtual Drive size in MB, GB, or TB (maximum: Unknown)
  Example format: '400 GB' --> 10 GB

Optional attributes:

  stripsize: defaults to 64K Bytes
     0: 8K Bytes
    1: 16K Bytes
    2: 32K Bytes
    3: 64K Bytes
    4: 128K Bytes
    5: 256K Bytes
    6: 512K Bytes
    7: 1024K Bytes
  Choose number from above options or hit return to pick default--> 0
stripsize will be set to 8K Bytes (4 and 'strip-size\:8k')

  Disk Cache Policy: defaults to Unchanged
     0: Unchanged
    1: Enabled
    2: Disabled
  Choose number from above options or hit return to pick default--> 0
Disk Cache Policy will be set to Unchanged (0 and 'disk-cache-policy\:unchanged')

  Read Policy: defaults to No Read Ahead
     0: No Read Ahead
    1: Always
  Choose number from above options or hit return to pick default--> 0
Read Policy will be set to No Read Ahead (0 and 'read-policy\:no-read-ahead')

  Write Policy: defaults to Write Through
     0: Write Through
    1: Write Back Good BBU
    2: Always Write Back
  Choose number from above options or hit return to pick default--> 0
Write Policy will be set to Write Through (0 and 'write-policy\:write-through')

  IO Policy: defaults to Direct I/O
     0: Direct I/O
    1: Cached I/O
```

```
  Choose number from above options or hit return to pick default--> 0
IO Policy will be set to Direct I/O (0 and 'io-policy\:direct-io')

  Access Policy: defaults to Read Write
     0: Read Write
    1: Read Only
    2: Blocked
  Choose number from above options or hit return to pick default--> 0
Access Policy will be set to Read Write (0 and 'access-policy\:read-write')

New virtual drive will have the following characteristics:
  - It will share space with virtual drive 0
  - Name: 'amit'
  - Size: 10 GB
  - stripsize: 8K Bytes
  - Disk Cache Policy: Unchanged
  - Read Policy: No Read Ahead
  - Write Policy: Write Through
  - IO Policy: Direct I/O
  - Access Policy: Read Write

OK? (y or n)--> y
Server /chassis/storageadapter # show virtual-drive
Virtual Drive Health         Status               Name             Size       RAID Level
Boot Drive
------------- -------------- -------------------- ---------------- ---------- ----------
----------
0             Good           Optimal                               150528 MB  RAID 0
false
1             Good           Optimal                               20480 MB   RAID 0
true
2             Good           Optimal                               114140 MB  RAID 0
false
3             Good           Optimal              test_v_drive     10000 MB   RAID 1
false
4             Good           Optimal              new_from_test    500 MB     RAID 1
false

Server /chassis/storageadapter #
```

外部設定のインポート

別のコントローラで以前に設定されている 1 つ以上の物理ドライブがサーバにインストールされると、それらは外部設定として識別されます。コントローラにこれらの外部設定をインポートできます。

はじめる前に

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 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*	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 # **import-foreign-config**	処理の確認を求めるプロンプトが表示されます。確認のために **yes** を入力します。

	コマンドまたはアクション	目的
		（注） **yes** と入力しなかった場合、アクションは強制終了されます。

次に、スロット 3 にある MegaRAID コントローラのすべての外部設定をインポートする例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # import-foreign-config
Are you sure you want to import all foreign configurations on this controller?
Enter 'yes' to confirm -> yes
Server /chassis/storageadapter #
```

外部設定ドライブのロック解除

セキュアなドライブ グループをホストする物理ドライブのセットが別のサーバまたはコントローラ（または、それらが存在しない間にセキュリティ キーが変更された同じコントローラ）に挿入されると、それらは外部設定になります。これらは保護されているため、外部設定をインポートする前にロックを解除する必要があります。外部設定ドライブのロックを解除する方法を次の手順で説明します。

はじめる前に

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 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*	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 # **unlock-foreign-configuration**	プロンプトで、セキュリティ キーを入力し、確認プロンプトで yes と入力します。
ステップ 4	Server /chassis/storageadapter # **scope physical-drive 2**	（任意） 物理ドライブ コマンド モードを開始します。
ステップ 5	Server /chassis/storageadapter/physicsl-drive # **show detail**	（任意） ロックが解除された外部ドライブのステータスが表示されます。

次に、外部設定ドライブのロックを解除する例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # unlock-foreign-configuration
Please enter the security key to unlock the foreign configuration -> testSecurityKey
Server /chassis/storageadapter # import-foreign-config
Are you sure you want to import all foreign configurations on this controller?
Enter 'yes' to confirm -> yes
Server /chassis/storageadapter # scope physical-drive 2
Server /chassis/storageadapter/physical-drive # show detail
Physical Drive Number 2:
    Controller: SLOT-HBA
    Health: Good
    Status: Online
    .
    .
    FDE Capable: 1
    FDE Enabled: 1
    FDE Secured: 1
    FDE Locked: 0
    FDE locked foreign config: 0

Server /chassis/storageadapter/physical-drive #
```

外部設定のクリア

重要 このタスクでは、コントローラのすべての外部設定をクリアします。また、外部設定をホスティングしているすべての物理ドライブからすべての設定情報が削除されます。このアクションは元に戻せません。

はじめる前に

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 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*	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 # **clear-foreign-config**	処理の確認を求めるプロンプトが表示されます。確認のために **yes** を入力します。 （注） **yes** と入力しなかった場合、アクションは強制終了されます。

次に、スロット 3 にある MegaRAID コントローラのすべての外部設定をクリアする例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # clear-foreign-config
Are you sure you want to clear all foreign configurations on this controller?
All data on the drive(s) will be lost.
Enter 'yes' to confirm -> yes
Server /chassis/storageadapter #
```

JBOD のイネーブル化

（注） 一部の UCS C シリーズ サーバでのみ Just a Bunch of Disks（JBOD）をイネーブルにできます。

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 # **scope storageadapter***slot*	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 # **enable-jbod-mode**	選択したコントローラに対して JBOD モードをイネーブルにします。

次に、選択したコントローラに対して JBOD モードをイネーブルにする例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # enable-jbod-mode
Are you sure you want to enable JBOD mode?
Enter 'yes' to confirm -> yes
Server/chassis/storageadapter # show settings
PCI Slot SLOT-3:
    Info Valid: Yes
    Enable JBOD Mode: true
```

JBOD のディセーブル化

（注） このオプションを使用できるのは一部の UCS C シリーズ サーバだけです。

はじめる前に

選択したコントローラに対して JBOD モードをイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope storageadapter***slot*	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 # **disable-jbod-mode**	選択したコントローラの JBOD モードをディセーブルにします。

次に、選択したコントローラの JBOD モードをディセーブルにする例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # disable-jbod-mode
Are you sure you want to disable JBOD mode?
Enter 'yes' to confirm -> yes
Server/chassis/storageadapter # show settings
PCI Slot SLOT-3:
    Info Valid: Yes
    Enable JBOD Mode: false
```

ブート ドライブのクリア

重要 このタスクでは、コントローラのブート ドライブ設定がクリアされます。このアクションは元に戻せません。

はじめる前に

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 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*	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 # **clear-boot-drive**	処理の確認を求めるプロンプトが表示されます。確認のために **yes** を入力します。 （注） **yes** と入力しなかった場合、アクションは強制終了されます。

次に、スロット 3 にある MegaRAID コントローラ上のブート ドライブ設定をクリアする例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # clear-boot-drive
Are you sure you want to clear the controller's boot drive?
Enter 'yes' to confirm -> yes
Server /chassis/storageadapter #
```

JBOD でのセキュリティのイネーブル化

物理ドライブが BOD である場合にのみ、そのドライブでセキュリティをイネーブルにできます。次に、JBOD でセキュリティをイネーブルにする手順を示します。

はじめる前に

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 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*	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 physical-drive 2**	物理ドライブ コマンド モードを開始します。
ステップ 4	Server /chassis/storageadapter # **enable-security-on-jbod**	確認プロンプトに yes と入力します。 JBOD でセキュリティをイネーブルにします。
ステップ 5	Server /chassis/storageadapter/physicsl-drive # **show detail**	（任意） 物理ドライブの詳細が表示されます。

次に、JBOD でセキュリティをイネーブルにする例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
savbu-stordev-dn1-2-cimc /chassis/storageadapter # scope physical-drive 2
server /chassis/storageadapter/physical-drive # enable-security-on-jbod
Are you sure you want to enable security on this JBOD?
NOTE: this is not reversible!
Enter 'yes' to confirm -> yes
server /chassis/storageadapter/physical-drive # show detail
Physical Drive Number 2:
    .
```

```
    .
    Status: JBOD
    .
    .
    FDE Capable: 1
    FDE Enabled: 1
    FDE Secured: 1
server /chassis/storageadapter/physical-drive #
```

セキュアな物理ドライブのクリア

セキュアなドライブをクリアすると、FDE ドライブはセキュアなドライブから非セキュアなドライブに変換されます。このアクションを実行するには、物理ドライブのステータスを [Unconfigured Good] にする必要があります。これによって、物理ドライブ上のデータが削除されます。セキュアな SED 物理ドライブをクリアする方法を次の手順で説明します。

はじめる前に

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 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*	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 physical-drive 2**	物理ドライブ コマンド モードを開始します。
ステップ 4	Server /chassis/storageadapter/physicsl-drive # **clear-secure-drive**	確認プロンプトに yes と入力します。 これによって、セキュアな SED 物理ドライブがクリアされ、すべてのデータが失われます。
ステップ 5	Server /chassis/storageadapter/physicsl-drive # **show detail**	（任意） 物理ドライブの詳細を表示します。

次に、SED 外部設定物理ドライブをクリアする例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope physical-drive 2
Server /chassis/storageadapter/physical-drive #  clear-secure-drive
Are you sure you want to erase all data from this physical drive?
NOTE: this is not reversible!  ALL DATA WILL BE LOST!!
Enter 'yes' to confirm -> yes
Server /chassis/storageadapter/physical-drive # show detail
Physical Drive Number 2:
    Controller: SLOT-HBA
```

```
    Health: Good
    Status: Unconfigured Good
    .
    .
    FDE Capable: 1
    FDE Enabled: 0
    FDE Secured: 0

Server /chassis/storageadapter/physical-drive #
```

セキュア SED 外部設定物理ドライブのクリア

ロックされている外部設定フルディスク暗号化ドライブを非セキュアなロックされていないドライブに変換します。これによって、物理ドライブ上のデータが削除されます。セキュアな SED 外部設定物理ドライブをクリアする方法を次の手順で説明します。

はじめる前に

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 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*	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 physical-drive 2**	物理ドライブ コマンド モードを開始します。
ステップ 4	Server /chassis/storageadapter/physicsl-drive # **clear-secure-foreign-config-drive**	確認プロンプトに yes と入力します。 これによって、セキュアな SED 外部設定物理ドライブがクリアされ、すべてのデータが失われます。
ステップ 5	Server /chassis/storageadapter/physicsl-drive # **show detail**	（任意） 物理ドライブの詳細を表示します。

次に、SED 外部設定物理ドライブをクリアする例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope physical-drive 2
Server /chassis/storageadapter/physical-drive # clear-secure-foreign-config-drive
Are you sure you want to erase all data from this foreign-configuration physical drive?
NOTE: this is not reversible!  ALL DATA WILL BE LOST!!
Enter 'yes' to confirm -> yes
Server /chassis/storageadapter/physical-drive # show detail
Physical Drive Number 2:
    Controller: SLOT-HBA
```

```
    Health: Good
    Status: Unconfigured Good
    .
    .
    FDE Capable: 1
    FDE Enabled: 0
    FDE Secured: 0
    FDE Locked: 0
    FDE Locked Foreign Config: 0

Server /chassis/storageadapter/physical-drive #
```

コントローラの TTY ログの取得

このタスクは、コントローラの TTY ログを取得し、それを /var/log の場所に配置します。これにより、テクニカル サポート データが要求された場合にこのログ データを確実に使用できるようになります。

はじめる前に

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 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*	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 # **get-tty-log**	
ステップ 4	Server /chassis/storageadapter # **show detail**	取得プロセスのステータスを表示します。 **重要** コントローラの TTY ログを取得するには 2 ～ 4 分かかる場合があります。このプロセスが完了するまで、テクニカル サポート データのエクスポートを開始しないでください。

次に、スロット 3 の MegaRAID コントローラの TTY ログを取得する例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # get-tty-log
Server /chassis/storageadapter # show detail
PCI Slot SLOT-3:
TTY Log Status: In progress (8192 bytes fetched)
Server /chassis/storageadapter # show detail
PCI Slot SLOT-3:
TTY Log Status: In progress (90112 bytes fetched)
Server /chassis/storageadapter # show detail
PCI Slot SLOT-3:
TTY Log Status: Complete (172032 bytes fetched)
```

コントローラでのドライブセキュリティのイネーブル化

はじめる前に

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 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*	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 # **enable-controller-security**	この時点で、セキュリティ キーを入力するように求められますが、希望するセキュリティ キーを入力することも、提案されているセキュリティ キーを使用することもできます。希望するセキュリティ キーを割り当てる場合は、プロンプトでそのセキュリティ キーを入力します。 提案されたセキュリティ キーを使用するか、希望のセキュリティ キーを使用するかによって、該当するプロンプトで **y**（yes）を入力して確認するか、**n**（no）を入力して操作をキャンセルします。
ステップ 4	Server /chassis/storageadapter # **show detail**	ストレージ ドライブの詳細が表示されます。

次に、コントローラでセキュリティをイネーブルにする例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # enable-controller-security
Use generated key-id 'UCSC-MRAID12G_FHH18250010_1d85dcd3'?  (y or n)--> y
Use suggested security-key '6ICsmuX@oVB7e9wXt79qsTgp6ICsmuX@'?  (y or n)--> n
Enter security-key --> testSecurityKey
Will use security-key 'testSecurityKey'
Server /chassis/storageadapter show detail
PCI Slot SLOT-HBA:
    <stuff deleted>
    Controller is Secured: 1

Server /chassis/storageadapter #
```

コントローラでのドライブセキュリティのディセーブル化

はじめる前に

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 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*	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 # **disable-controller-security**	確認のプロンプトが表示されます。 確認プロンプトで、**yes** と入力して確認するか、または **n**（no）を入力して操作をキャンセルします。 セキュリティ キーを入力するための別のプロンプトが表示されます。セキュリティ キーを入力します。 これにより、コントローラのセキュリティがディセーブルになります。
ステップ 4	Server /chassis/storageadapter # **show detail**	ストレージ ドライブの詳細が表示されます。

次に、コントローラでセキュリティをディセーブルにする例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter #  disable-controller-security
Note: this operation will fail if any secured drives are present.
Are you sure you want to disable security on this controller?
Enter 'yes' to confirm -> yes
Please enter the controller's security-key -> testSecurityKey
savbu-stordev-dn1-2-cimc /chassis/storageadapter # show detail
PCI Slot SLOT-HBA:
    <stuff deleted>
    Controller is Secured: 0

Server /chassis/storageadapter #
```

コントローラ セキュリティ設定の変更

はじめる前に

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 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*	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 # **modify-controller-security**	この時点で、現在のセキュリティ キーを入力するように求められます。また、任意で、キー ID をリセットするかどうかを選択したり、新しいセキュリティ キーを選択することもできます。適切な情報を入力します。 確認プロンプトで、**y**（yes）と入力して確認するか、または **n**（no）と入力して操作をキャンセルします。

次に、コントローラのセキュリティ設定を変更する例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # modify-controller-security
Please enter current security-key --> testSecurityKey
Keep current key-id 'UCSC-MRAID12G_FHH18250010_1d85dcd3'? (y or n)--> n
Enter new key-id: NewKeyId
Will change key-id to 'NewKeyId'
Keep current security-key? (y or n)--> y

Server /chassis/storageadapter #
```

セキュリティ キー認証の確認

セキュリティ キーがわからない場合は、次の手順を使用すると、入力したセキュリティ キーがコントローラのセキュリティ キーと一致しているかどうかを確認できます。

はじめる前に

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 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*	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 # **verify-controller-security-key**	プロンプトで、セキュリティ キーを入力して、Enter キーを押します。 コントローラのセキュリティ キーと一致しないセキュリティ キーを入力した場合は、検証失敗メッセージが表示されます。

次に、コントローラのセキュリティ キーを確認する例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter #  verify-controller-security-key
Please enter the security key to verify -> WrongSecurityKey
verify-controller-security-key failed.
Error: "r-type: RAID controller: SLOT-HBA command-status: Lock key from backup failed
verification"
savbu-stordev-dn1-2-cimc /chassis/storageadapter #
savbu-stordev-dn1-2-cimc /chassis/storageadapter # verify-controller-security-key
Please enter the security key to verify -> testSecurityKey

Server /chassis/storageadapter #
```

仮想ドライブの削除

重要 このタスクでは、ブートされたオペレーティング システムを実行するドライブを含む仮想ドライブを削除します。そのため、仮想ドライブを削除する前に、保持するデータをバックアップします。

はじめる前に

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 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 # **scope storageadapter***slot*	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** *drive-number*	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 4	Server /chassis/storageadapter/virtual-drive # **delete-virtual-drive**	処理の確認を求めるプロンプトが表示されます。確認のために **yes** を入力します。 （注） **yes** と入力しなかった場合、アクションは強制終了されます。

次に、仮想ドライブ 3 を削除する例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope virtual-drive 3
Server /chassis/storageadapter/virtual-drive # delete-virtual-drive
Are you sure you want to delete virtual drive 3?
All data on the drive will be lost.  Enter 'yes' to confirm -> yes
Server /chassis/storageadapter/virtual-drive #
```

仮想ドライブの初期化

ドライブを初期化すると、仮想ドライブ上のすべてのデータが失われます。初期化を実行する前に、保存する仮想ドライブのデータをバックアップします。

はじめる前に

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 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*	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** *drive-number*	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 4	Server /chassis/storageadapter/virtual-drive # **start-initialization**	指定した仮想ドライブを初期化します。

	コマンドまたはアクション	目的
ステップ 5	Server /chassis/storageadapter/virtual-drive # **cancel-initialization**	（任意）指定した仮想ドライブの初期化をキャンセルします。
ステップ 6	Server /chassis/storageadapter/physical-drive # **get-operation-status**	ドライブ上で処理中のタスクのステータスを表示します。

次に、高速初期化を使用して仮想ドライブ 3 を初期化する例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope virtual-drive 3
Server /chassis/storageadapter/virtual-drive # start-initialization
Are you sure you want to initialize virtual drive 3?
All data on the drive will be lost.  Enter 'yes' to confirm -> yes
Fast (0) or full (1) initialization?  -> 0
Server /chassis/storageadapter/virtual-drive # get-operation-status

progress-percent: 20%
elapsed -seconds: 30
operation-in-progress: initializing virtual drive

Server /chassis/storageadapter/virtual-drive #
```

ブート ドライブとしての設定

はじめる前に

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 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*	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** *drive-number*	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 4	Server /chassis/storageadapter # **set-boot-drive**	コントローラがこの仮想ドライブからブートするように指定します。

次に、コントローラが仮想ドライブ 3 からブートするように指定する例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope virtual-drive 3
Server /chassis/storageadapter/virtual-drive # set-boot-drive
Are you sure you want to set virtual drive 3 as the boot drive?
Enter 'yes' to confirm -> yes
Server /chassis/storageadapter/virtual-drive #
```

仮想ドライブの編集

はじめる前に

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 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*	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** *drive number*	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 4	Server chassis /storageadapter /virtual-drive # **modify-attributes**	現在のものとは異なるポリシーを選択するように求めるプロンプトが表示されます。
ステップ 5	Server chassis /storageadapter /virtual-drive# **set raid-level** *value*	指定した仮想ドライブの RAID レベルを指定します。
ステップ 6	Server chassis /storageadapter /virtual-drive# **set physical-drive** *value*	指定した仮想ドライブに物理ドライブを指定します。

次に、仮想ドライブを編集する例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter slot-3
Server /chassis/storageadapter # scope virtual-drive 3
Server /chassis/storageadapter/virtual-drive #set raid-level 1
Server /chassis/storageadapter/virtual-drive *# physical-drive 1
Server /chassis/storageadapter/virtual-drive* #commit
Server /chassis/storageadapter /virtual-drive # modify-attribute
Current write policy: Write Back Good BBU

    0: Write Through
    1: Write Back Good BBU
    2: Always Write Back
  Choose number from above options--> 0
The following attribute will be modified:
  - Write Policy: Write Through
```

```
OK? (y or n)--> y
Server /chassis/storageadapter/virtual-drive #
```

仮想ドライブの保護

重要 このタスクでは、仮想ドライブがドライブ グループの仮想ドライブのターゲット ID である場合に、既存のドライブ グループ内のすべての VD を保護します。

はじめる前に

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 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*	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***drive-number*	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 4	Server /chassis/storageadapter/virtual-drive # **secure-drive-group**	処理の確認を求めるプロンプトが表示されます。確認のために **yes** を入力します。 （注） **yes** と入力しなかった場合、アクションは強制終了されます。

次に、仮想ドライブ グループを保護する例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope virtual-drive 3
Server /chassis/storageadapter/virtual-drive # secure-drive-group
This will enable security for virtual drive 16, and all virtual drives sharing this drive
group.
It is not reversible.  Are you quite certain you want to do this?
Enter 'yes' to confirm -> yes
server /chassis/storageadapter/virtual-drive # show detail
Virtual Drive 16:
    .
    .
    FDE Capable: 1
    FDE Enabled: 1
    .
    .
 server /chassis/storageadapter/virtual-drive #
```

仮想ドライブの属性の変更

はじめる前に

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 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*	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** *3*	仮想ドライブのコマンド モードを開始します。
ステップ 4	Server /chassis/storageadapter/virtual-drive # **modify-attributes**	現在のものとは異なるポリシーを選択するように求めるプロンプトが表示されます。

次に、既存の RAID 1 ドライブ グループ内の未使用のスペースから新しい仮想ドライブを分割する例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope virtual-drive
Server /chassis/storageadapter/virtual-drive # modify-attributes

Current write policy: Write Back

  0: Write Through
  1: Write Back
  2: Write Back even if Bad BBU

Choose number from above options --> 0

The following attribute will be modified:

 - Write policy: Write Through

OK? (y or n) --> y

operation in progress.

Server /chassis/storageadapter/virtual-drive #
```

専用ホット スペアの作成

はじめる前に

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 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*	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 physical-drive** *drive-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 4	Server /chassis/storageadapter/physical-drive # **make-dedicated-hot-spare**	専用ホット スペアが作成される仮想ドライブの選択を求めるプロンプトが表示されます。

次に、物理ドライブ 3 を仮想ドライブ 6 の専用ホット スペアにする例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope physical-drive 3
Server /chassis/storageadapter/physical-drive # make-dedicated-hot-spare
  5: VD_OS_1, RAID 0, 102400 MB, physical disks: 1
  6: VD_OS_2, RAID 0, 12288 MB, physical disks: 1
  7: VD_OS_3, RAID 0, 12288 MB, physical disks: 1
  8: VD_DATA_1, RAID 0, 12512 MB, physical disks: 1
  9: RAID1_2358, RAID 1, 40000 MB, physical disks: 2,3,5,8
  11: JFB_RAID1_67, RAID 1, 20000 MB, physical disks: 6,7
  12: JFB_Crv_R1_40, RAID 1, 40000 MB, physical disks: 6,7
  13: JFB_R1_10GB, RAID 1, 10000 MB, physical disks: 6,7

  Please choose from the above 8 virtual drives-->6

Server /chassis/storageadapter/physical-drive #
```

グローバル ホット スペアの作成

はじめる前に

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 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*	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 3	Server /chassis/storageadapter # **scope physical-drive** *drive-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 4	Server /chassis/storageadapter/physical-drive # **make-global-hot-spare**	
ステップ 5	Server /chassis/storageadapter/physical-drive # **get-operation-status**	ドライブ上で処理中のタスクのステータスを表示します。

次に、物理ドライブ 3 をグローバル ホット スペアにする例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope physical-drive 3
Server /chassis/storageadapter/physical-drive # make-global-hot-spare
Server /chassis/storageadapter/physical-drive #
```

削除するドライブの準備

Unconfigured Good ステータスが表示された物理ドライブ上でのみ、このタスクを確認できます。

はじめる前に

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 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*	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 physical-drive** *drive-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 4	Server /chassis/storageadapter/physical-drive # **prepare-for-removal**	

次に、物理ドライブ 3 を削除する準備をする例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope physical-drive 3
Server /chassis/storageadapter/physical-drive # prepare-for-removal
Server /chassis/storageadapter/physical-drive #
```

物理ドライブのステータスの切り替え

はじめる前に

- 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。
- コントローラは、JBOD モードをサポートする必要があり、JBOD モードはイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシコマンドモードを開始します。
ステップ 2	Server /chassis # **scope storageadapter***slot*	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 physical-drive 4**	物理ドライブのコマンドモードを開始します。
ステップ 4	Server /chassis/storageadapter/physical-drive # **make-unconfigured-good**	ドライブのステータスを Unconfigured good に変更します。
ステップ 5	Server /chassis/storageadapter/physical-drive # **make-jbod**	物理ドライブの JBOD モードをイネーブルにします。

次に、物理ドライブのステータスを切り替える例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope physical-drive 4
Server /chassis/storageadapter/physical-drive # show detail
Physical Drive Number 4:
    Controller: SLOT-4
    Health: Good
    Status: JBOD
    Boot Drive: true
    Manufacturer: ATA
    Model: ST500NM0011
    Predictive Failure Count: 0
    Drive Firmware: CC02
    Coerced Size: 476416 MB
    Type: HDD
Server /chassis/storageadapter/physical-drive # make-unconfigured-good
```

```
Server /chassis/storageadapter/physical-drive # show detail
Physical Drive Number 4:
    Controller: SLOT-4
    Health: Good
    Status: Unconfigured Good
    Boot Drive: true
    Manufacturer: ATA
    Model: ST500NM0011
    Predictive Failure Count: 0
    Drive Firmware: CC02
    Coerced Size: 476416 MB
    Type: HDD
Server /chassis/storageadapter/physical-drive # make-jbod
Server /chassis/storageadapter/physical-drive # show detail
Physical Drive Number 4:
    Controller: SLOT-4
    Health: Good
    Status: JBOD
    Boot Drive: true
    Manufacturer: ATA
    Model: ST500NM0011
    Predictive Failure Count: 0
    Drive Firmware: CC02
    Coerced Size: 476416 MB
    Type: HDD
```

コントローラのブートドライブとしての物理ドライブの設定

はじめる前に

- 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。
- コントローラは、JBOD モードをサポートする必要があり、JBOD モードはイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope storageadapter***slot*	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 physical-drive 4**	物理ドライブのコマンド モードを開始します。
ステップ 4	Server /chassis/storageadapter/physical-drive # **set-boot-drive**	処理の確認を求めるプロンプトが表示されます。確認のために **yes** を入力します。 （注） **yes** と入力しなかった場合、アクションは強制終了されます。

次に、物理ドライブをコントローラのブート ドライブとして設定する例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # show detail
PCI Slot SLOT-4:
    Health: Good
    Controller Status: Optimal
    ROC Temperature: Not Supported
    Product Name: MegaRAID 9240-8i (RAID 0,1,10,5)
    Serial Number: SP23807413
    Firmware Package Build: 20.11.1-0159
    Product ID: LSI Logic
    Battery Status: no battery
    Cache Memory Size: 0 MB
    Boot Drive: none
    Boot Drive is PD: false
    TTY Log Status: Not Downloaded
Server /chassis/storageadapter # scope physical-drive 4
Server /chassis/storageadapter/physical-drive # set-boot-drive
Are you sure you want to set physical drive 4 as the boot drive?
Enter 'yes' to confirm -> yes
Server /chassis/storageadapter/physical-drive # exit
Server /chassis/storageadapter # show detail
PCI Slot SLOT-4:
    Health: Good
    Controller Status: Optimal
    ROC Temperature: Not Supported
    Product Name: MegaRAID 9240-8i (RAID 0,1,10,5)
    Serial Number: SP23807413
    Firmware Package Build: 20.11.1-0159
    Product ID: LSI Logic
    Battery Status: no battery
    Cache Memory Size: 0 MB
    Boot Drive: 4
    Boot Drive is PD: true
    TTY Log Status: Not Downloaded
```

ホット スペア プールからのドライブの削除

はじめる前に

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 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*	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 physical-drive** *drive-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 4	Server /chassis/storageadapter/physical-drive # **remove-hot-spare**	ホット スペア プールからドライブを削除します。

次に、ホット スペア プールから物理ドライブ 3 を削除する例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope physical-drive 3
Server /chassis/storageadapter/physical-drive # remove-hot-spare
Server /chassis/storageadapter/physical-drive #
```

削除するドライブの準備の取り消し

はじめる前に

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 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*	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 physical-drive** *drive-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 4	Server /chassis/storageadapter/physical-drive # **undo-prepare-for-removal**	

次に、物理ドライブ 3 の削除を準備した後にドライブをリスピンする例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope physical-drive 3
Server /chassis/storageadapter/physical-drive # undo-prepare-for-removal
Server /chassis/storageadapter/physical-drive #
```

バッテリバックアップユニットの自動学習サイクルのイネーブル化

はじめる前に

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 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*	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 bbu**	バッテリ バックアップ ユニット コマンド モードを開始します。
ステップ 4	Server /chassis/storageadapter # **enable-auto-learn**	バッテリの自動学習サイクルをイネーブルにします。

次に、バッテリの自動学習サイクルをイネーブルにする例を示します。

```
Server # scope chassis
Server /chassis # scope storageadapter SLOT-2
Server /chassis/storageadapter # scope bbu
Server /chassis/storageadapter/bbu # enable-auto-learn
Automatic BBU learn cycles will occur without notice if enabled.
Are you sure? [y/n] --> y
enable-auto-learn initiated
Server /chassis/storageadapter/bbu #
```

バッテリ バックアップ ユニットの自動学習サイクルのディセーブル化

はじめる前に

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 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*	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 bbu**	バッテリ バックアップ ユニット コマンド モードを開始します。
ステップ 4	Server /chassis/storageadapter # **disable-auto-learn**	バッテリの自動学習サイクルをディセーブルにします

次に、バッテリの自動学習サイクルをディセーブルにする例を示します。

```
Server # scope chassis
Server /chassis # scope storageadapter SLOT-2
Server /chassis/storageadapter # scope bbu
Server /chassis/storageadapter/bbu # disable-auto-learn
Automatic BBU learn cycles will no longer occur if disabled.
Are you sure? [y/n] --> y
disable-auto-learn initiated

Server /chassis/storageadapter/bbu #
```

バッテリ バックアップ ユニットの学習サイクルの開始

はじめる前に

このコマンドを使用するには、admin としてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope storageadapter***slot*	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 bbu**	バッテリ バックアップ ユニット コマンド モードを開始します。
ステップ 4	Server /chassis/storageadapter # **start-learn-cycle**	バッテリの学習サイクルを開始します。

次に、バッテリの学習サイクルを開始する例を示します。

```
Server # scope chassis
Server /chassis # scope storageadapter SLOT-2
Server /chassis/storageadapter # scope bbu
Server /chassis/storageadapter/bbu # start-learn-cycle
Server /chassis/storageadapter/bbu #
```

物理ドライブのロケータ LED の切り替え

はじめる前に

このタスクを実行するには、admin としてログオンする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope storageadapter***slot*	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 physical-drive 3**	物理ドライブ コマンド モードを開始します。
ステップ 4	Server /chassis/storageadapter/physical-drive # **locator-led** {**on** | **off**}	物理ドライブのロケータ LED をイネーブルまたはディセーブルにします。

次に、物理ドライブ 3 のロケータ LED をイネーブルにする例を示します。

```
Server # scope chassis
Server /chassis # scope storageadapter SLOT-2
Server /chassis/storageadapter # scope physical-drive 3
Server /chassis/storageadapter/physical-drive # locator-led on
Server /chassis/storageadapter/physical-drive* # commit
Server /chassis/storageadapter/physical-drive #
```

ストレージ コントローラのログの表示

はじめる前に

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 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*	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 log**	ストレージ コントローラのログを表示します。

次に、ストレージ コントローラのログを表示する例を示します。

```
Server # scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # show log
```

```
Time                        Severity         Description
----                        --------        -------------
Fri March 1 09:52:19 2013   Warning      Predictive Failure
Fri March 1 07:50:19 2013   Info         Battery charge complete
Fri March 1 07:50:19 2013   Info         Battery charge started
Fri March 1 07:48:19 2013   Info         Battery relearn complete
Fri March 1 07:47:19 2013   Info         Battery is discharging
Fri March 1 07:45:19 2013   Info         Battery relearn started

Server /chassis/storageadapter #
```

第 11 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

はじめる前に

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

	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**}	Cisco IMC 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。

	コマンドまたはアクション	目的
ステップ 5	Server /http # **set http-redirect** {**yes** | **no**}	HTTPS への HTTP 要求のリダイレクトをイネーブルまたはディセーブルにします。
ステップ 6	Server /http # **set timeout***seconds*	HTTP 要求の間に Cisco IMC 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 7	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、Cisco IMC 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 http-redirect yes
Server /http *# set timeout 1800
Server /http *# commit
Server /http # show
HTTP Port  HTTPS Port Timeout  Active Sessions Enabled HTTP Redirected
---------- ---------- -------- --------------- ------- ----------------
80         443        1800     0               yes     yes

Server /http #
```

SSH の設定

はじめる前に

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scopessh**	SSH コマンド モードを開始します。
ステップ 2	Server /ssh # **setenabled** {**yes** | **no**}	Cisco IMC 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 # **setssh-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 # **settimeout***seconds*	SSH 要求がタイムアウトしたものとシステムが判断するまで待機する秒数を設定します。

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

次に、Cisco IMC 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 #
```

XML API の設定

Cisco IMC 用の XML API

Cisco Cisco IMC XML アプリケーション プログラミング インターフェイス（API）は、C シリーズ ラックマウント サーバ用の Cisco IMC に対するプログラマチック インターフェイスです。この API は、HTTP または HTTPS 経由で XML ドキュメントを受け取ります。

XML API の詳細については、『*Cisco UCS Rack-Mount Servers Cisco IMC XML API Programmer's Guide*』を参照してください。

XML API のイネーブル化

はじめる前に

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# **scopexmlapi**	XML API 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 /xmlapi # **setenabled** {**yes** | **no**}	Cisco IMC 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。

次に、Cisco IMC の XML API 制御をイネーブルにし、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

Server /xmlapi #
```

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、Cisco IMC を IPMI メッセージで管理する場合に設定します。

はじめる前に

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# **scopeipmi**	IPMI コマンド モードを開始します。
ステップ 2	Server /ipmi # **setenabled** {**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 # **setprivilege-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 # **setencryption-key***key*	IPMI 通信に使用する IPMI 暗号キーを設定します。キーの値は、40 個の 16 進数であることが必要です。
ステップ 5	Server /ipmi # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 6	Server /ipmi # **randomise-key**	IPMI 暗号化キーをランダムな値に設定します。 （注） ステップ 4 および 5 ではなく、ステップ 6 のアクションを実行できます。
ステップ 7	プロンプトで、y を入力し、暗号キーをランダムにします。	IPMI 暗号化キーをランダムな値に設定します。

次に、Cisco IMC 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 # randomise-key
This operation will change the IPMI Encryption Key to a random value
Continue?[y|N]y
Setting IPMI Encryption Key to a random value...

Server /ipmi # show
Enabled Encryption Key                           Privilege Level Limit
------- ---------------------------------------- ---------------------
yes     abcdef01234567890abcdef01234567890abcdef admin

Server /ipmi #
```

SNMP の設定

SNMP

Cisco UCS C シリーズ ラックマウント サーバ 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。Cisco IMC でサポートされている管理情報ベース（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/c/en/us/td/docs/unified_computing/ucs/sw/mib/b-series/b_UCS_MIBRef.html

SNMP プロパティの設定

はじめる前に

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# **scopesnmp**	SNMP コマンド モードを開始します。
ステップ 2	Server /snmp # **setenabled** {**yes** | **no**}	SNMP をイネーブルまたはディセーブルにします。 （注） 追加の SNMP コンフィギュレーション コマンドが受け入れられる前には、SNMP をイネーブルにして保存する必要があります。

	コマンドまたはアクション	目的
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 # **setenable-serial-num** {**yes** | **no**}	サーバのリアル番号を使用してトラップにプレフィックスを追加します。
ステップ 5	Server /snmp # **setsnmp-port***port number*	SNMP エージェントを実行するポート番号を設定します。1 ～ 65535 の範囲内の数字を選択できます。デフォルト ポート番号は、161 です。 （注） システム コールに予約済みのポート番号（たとえば 22、23、80、123、443、623、389、636、3268、3269、2068 など）は、SNMP ポートとして使用できません。
ステップ 6	Server /snmp # **setcommunity-str***community*	Cisco IMC 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 7	Server /snmp # **setcommunity-access**	[Disabled]、[Limited]、または [Full] のいずれかになります。
ステップ 8	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 9	Server /snmp # **setsys-contact***contact*	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 10	Server /snmp # **setsys-location***location*	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 11	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。

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 enable-serial-num yes
Server /snmp *# set snmp-port 20000
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: 20000
    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
    Serial Number Enabled: yes

Server /snmp #
```

次の作業

「SNMP トラップ設定の指定, （242 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

はじめる前に

- 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# **scopesnmp**	SNMP コマンド モードを開始します。
ステップ 2	Server /snmp # **scopetrap-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 # **setenabled** {**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 # **setversion** { | **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。

	コマンドまたはアクション	目的
ステップ 5	Server /snmp/trap-destinations # **settype** {**trap** | **inform**}	SNMP 通知メッセージを単純なトラップとして送信するのか、レシーバによる確認応答が必要なインフォーム要求として送信するかを指定します。 （注） 通知オプションはV2ユーザに対してのみ選択できます。
ステップ 6	Server /snmp/trap-destinations # **setuser***user*	
ステップ 7	Server /snmp/trap-destination # **settrap-addr***trap destination address*	トラップ情報を送信するトラップの宛先アドレスを指定します。トラップの宛先としてIPv4またはIPv6アドレスまたはドメイン名を設定できます。 （注） Ipv6をイネーブルにすると、SNMP トラップの宛先発信元アドレスは、SLAAC Ipv6 アドレス（使用可能な場合）かユーザが割り当てた IPv6 アドレスのいずれかにすることができます。これらは両方とも、サーバを一意に識別する有効なSNMP Ipv6 宛先アドレスです。
ステップ 8	Server /snmp/trap-destinations # **settrap-port***trap destination port*	サーバがトラップの宛先との通信に使用するポート番号を設定します。1 ～ 65535 の範囲内の数字を選択できます。
ステップ 9	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。

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

```
Server# scope snmp
Server /snmp # Scope trap-destinations 1
Server /snmp/trap-destination *# set enabled yes
Server /snmp/trap-destination *#  set version 2
Server /snmp/trap-destination *# set type inform
Server /snmp/trap-destination *# set user user1
Server /snmp/trap-destination *# set trap-addr www.cisco.com
Server /snmp/trap-destination *# set trap-port 10000
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
    Trap Address: www.cisco.com
    Trap Port: 10000
    Delete Trap: no
Server /snmp/trap-destination #
```

テスト SNMP トラップ メッセージの送信

はじめる前に

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

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 #  send-test-trap
SNMP Test Trap sent to the destination.
Server /snmp #
```

SNMPv3 ユーザの設定

はじめる前に

- 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

	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	Server /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であり、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 コンフィギュレーションは削除されます。
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**：ユーザは許可またはプライバシー パスワードを必要としません。 • **authnopriv**：ユーザは許可パスワードを必要としますが、プライバシー パスワードは必要としません。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**：ユーザ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。

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 12 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Cisco IMC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。生成される証明書キーの長は 2048 ビットです。

（注） この章に記載されている以下のタスクを実行する前に、Cisco IMC の時刻が現在の時刻に設定されていることを確認します。

手順

ステップ 1 Cisco IMC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Cisco IMCにアップロードします。

（注） アップロードされた証明書は、Cisco IMC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

自己署名証明書は、**generate-csr** コマンドを使用して手動で生成するか、ホスト名の変更時に自動的に生成できます。自己署名証明書のホスト名と自動生成の変更の詳細については、共通プロパティの設定, （128 ページ）を参照してください。

証明書署名要求を手動で生成するには、次の手順を実行します。

はじめる前に

- 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。
- Cisco IMC の時刻が現在の時刻に設定されていることを確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scopecertificate**	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。

名前	説明
[Common Name] フィールド	Cisco IMC の完全修飾名。 デフォルトでは、サーバの CN は CXXX-YYYYYY 形式で表示されます（XXX はサーバのモデル番号で YYYYYY はシリアル番号です）。 最新バージョンにアップグレードするとき、CN はそのまま保持されます。
[Organization Name] フィールド	証明書を要求している組織。
[Organization Unit] フィールド	組織ユニット
[Locality] フィールド	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。
[State Name] フィールド	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] ドロップダウンリスト	会社が存在する国。

名前	説明
[Email] フィールド	会社の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
```

次の作業

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せず、組織も独自の認証局を運用していない場合、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、Cisco IMC 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。

- 証明書のタイプが「**Server**」あることを確認します。

Cisco IMC 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、Cisco IMC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。

はじめる前に

- 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。
- Cisco IMC の時刻が現在の時刻に設定されていることを確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**openssl genrsa -out***CA_keyfilenamekeysize* 例： `# openssl genrsa -out ca.key 2048`	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。

	コマンドまたはアクション	目的
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。
ステップ 5	**openssl x509 -noout -text -purpose -in <cert file>** 例： `openssl x509 -noout -text -purpose -in <cert file>`	生成された証明書のタイプが [Server] であることを確認します。 （注） フィールド [Server SSL] および [Netscape SSL] サーバの値が [Yes] でない場合は、タイプが [Server] の証明書を生成するように openssl.conf が設定されていることを確認します。

	コマンドまたはアクション	目的
ステップ 6	生成された証明書に正しい使用期限が設定されていない場合は、Cisco IMC の時刻が現在の時刻に設定されていることを確認し、手順 1 ～ 5 を繰り返して証明書を再生成します。	（任意） 正しい使用期限が設定された証明書が作成されます。

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 2048
Generating RSA private key, 2048 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
#
```

次の作業

新しい証明書をCisco IMCにアップロードします。

サーバ証明書のアップロード

はじめる前に

- 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。
- 生成された証明書のタイプが **Server** であることを確認します。

（注） 最初に、Cisco IMC 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# **scopecertificate**	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/SINv7wd6Vv2pBt6ZpXgD4VBNKOND1
GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
```

```
mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
-----END CERTIFICATE-----
<CTRL+D>
```

第 13 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、アクションをトリガーできます。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。

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	電圧緊急アサート フィルタ
3	電流アサート フィルタ
4	ファン緊急アサート フィルタ
5	プロセッサ アサート フィルタ
6	電源緊急アサート フィルタ

ID	プラットフォーム イベント フィルタ
7	メモリ緊急アサート フィルタ

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scopefault**	障害コマンド モードを開始します。
ステップ 2	Server /fault # **scopepef***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 # **setaction** {**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**：サーバの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 # **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 11
Server /fault/pef # set action reboot
Server /fault/pef *# commit
Server /fault/pef # show
Platform Event Filter Event                       Action
--------------------- --------------------------- -----------
11                    Memory Assert Filter        reboot

Server /fault/pef #
```

イベント プラットフォーム フィルタのリセット

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scopefault**	障害コマンド モードを開始します。
ステップ 2	Server /fault # **setplatform-event-enabledyes**	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 # **reset-event-filters**	プラットフォーム イベント フィルタをリセットします。
ステップ 5	Server /fault # **showpef**	最新のプラットフォーム イベント フィルタが表示されます。

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
Platform Event Enabled
-----------------------
   yes

Server /fault # reset-event-filters
Server /fault # show pef
Platform Event Filter   Event                                Action
--------------------- ----------------------------------- -----------
1                     Temperature Critical Assert Filter  none
2                     Voltage Critical Assert Filter      none
3                     Current Assert Filter               none
4                     Fan Critical Assert Filter          none
5                     Processor Assert Filter             none
6                     Power Supply Critical Assert Filter none
7                     Memory Critical Assert Filter       none

Server /fault #
```

第 14 章

Cisco IMC 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

C シリーズ サーバは、使用する C 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。

注意 新しい BIOS ファームウェアをインストールするとき、それはサーバで実行されている Cisco IMC ファームウェアと同じソフトウェア リリースに属する必要があります。新しいBIOSファームウェアのインストールは、必ず一致する Cisco IMC ファームウェアをアクティブにした後に行ってください。そうしないと、サーバはブートしません。

起こりうる問題を避けるため、Cisco Host Upgrade Utility（HUU）を使用することを強く推奨します。このユーティリティはBIOS、Cisco IMCおよびその他のファームウェア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、インストールする Cisco IMC ソフトウェア リリースに対応する HUU のバージョンの『*Cisco Host Upgrade Utility Guide*』を参照してください。HUU のガイドは次の URL にあります。http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html。

ファームウェアを手動で更新する場合は、最初に Cisco IMC ファームウェアを更新する必要があります。Cisco IMC 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、Cisco IMC は選択した非アクティブまたはバックアップの Cisco IMC ファームウェアをサーバの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、Cisco IMC 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するため、サービスの中断の原因となります。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。

Cisco IMC 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。BIOS 更新のプロセス全体でサーバの電源をオフにする必要があるため、プロセスは段階に分類されません。その代わり、入力するコマンドは 1 つで済みます。Cisco IMC は BIOS ファームウェアをできる限り迅速にインストールし、更新します。Cisco IMC 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。
- この手順は、スタンドアロン モードで実行している Cisco UCS C シリーズ サーバにのみ適用されます。Cisco UCS Manager の統合モードで実行している UCS C シリーズのファームウェアをアップグレードするには、Cisco Technical Assistance Center にお問い合わせください。

セキュア モードの Cisco IMC では、ロードおよび実行前のすべてのファームウェア イメージがデジタル的に署名され、信頼性と整合性が確認され、改竄されたソフトウェアの実行からデバイスを確実に保護できます。

シスコからのファームウェアの取得

手順

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。

ステップ 4 ロール ダウン メニューの [All Downloads] をクリックします。

ステップ 5 使用しているサーバ モデルが [Recently Used Products] リストに表示される場合は、サーバ名をクリックします。表示されない場合は、次の手順を実行します。

a) 左側のボックスの [Products] をクリックします。

b) 中央のボックスで、[Unified Computing and Servers] をクリックします。

c) 右側のボックスで、[Cisco UCS C-Series Rack-Mount Standalone Server Software] をクリックします。

d) 右側のボックスで、ダウンロードするソフトウェアのサーバ モデルをクリックします。

ステップ 6 [Unified Computing System (UCS) Server Firmware] リンクをクリックします。

ステップ 7 （任意） ページの左側のメニュー バーから以前のリリースを選択します。

ステップ 8 選択したリリースの Cisco Host Upgrade Utility ISO に関連付けられている [Download] ボタンをクリックします。

ステップ 9 [Accept License Agreement] をクリックします。

ステップ 10 ISO ファイルをローカル ドライブに保存します。
この ISO ファイルを使用してサーバの Cisco IMC と BIOS ファームウェアをアップグレードすることをお勧めします。この ISO ファイルには、Cisco Host Upgrade Utility が含まれます。このユーティリティの詳細については、インストールする Cisco IMC ソフトウェア リリースに対応する HUU のバージョンの『*Cisco Host Upgrade Utility Guide*』を参照してください。HUU のガイドは次の URL にあります。http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html。

ステップ 11 （任意） Cisco IMC と BIOS ファームウェアを手動でアップグレードする予定の場合、次の手順を実行します。

a) ISO ファイルから、ファームウェア インストール ファイルが格納されている ZIP ファイルを開きます。
この ZIP ファイルは ISO ファイルの最上位にあり、名前の形式は `ServerModel_ReleaseNumber.ZIP` です。

たとえば、`C240M3_1.4.4A.ZIP` という名前になっています。

この ZIP ファイルに格納されているすべてのファイルを抽出する必要はありません。このファイルを開くだけで、BIOS ファームウェアのインストール用 CAP ファイルと、Cisco IMC ファームウェアのインストール用 BIN ファイルが含まれる ZIP ファイルにアクセスできます。

b) *ServerModel_ReleaseNumber*.ZIP ファイルから、BIOS ファームウェアのインストール用の CAP ファイルを抽出し、ローカル ドライブに保存します。
CAP ファイルは *ReleaseNumber*/bios/cisco imc フォルダにあり、ファイル名は *Server*-BIOS-*Release-Number*.CAP という形式です。

たとえば、1.4.4a/bios/cisco imc/C240-BIOS-1-4-4c-0.CAP などです。

c) *ServerModel_ReleaseNumber*.ZIP ファイルから、Cisco IMC ファームウェアのインストール用ファイルを含む ZIP ファイルを開きます。
ZIP ファイルは *ReleaseNumber*/cisco imc フォルダにあり、ファイル名は *server-model*-cisco imc-*release*.zip という形式です。

たとえば、1.4.4a/cisco imc/c240-m3-cisco imc.1.4.4a.zip などです。

この ZIP ファイルに格納されているすべてのファイルを抽出する必要はありません。このファイルを開くだけで、Cisco IMC ファームウェアのインストール用 BIN ファイルにアクセスできます。

d) *server-model*-cisco imc-*release*.zip ファイルから、完全な Cisco IMC ファームウェアのインストール用 BIN ファイルを抽出し、ローカル ドライブに保存します。
BIN ファイルは *server-model*-cisco imc-*release* フォルダにあり、ファイル名は upd-pkg-*server-model*-cisco imc.full.*release*.bin という形式です。

たとえば、c240-m3-cisco imc.1.4.4a/upd-pkg-c240-m3-cisco imc.full.1.4.4a.bin などです。

ステップ 12 （任意） リモート サーバからファームウェアをインストールする予定の場合、そのリモート サーバに BIOS のインストール用 CAP ファイルと Cisco IMC インストール用 BIN ファイルをコピーします。
リモート サーバは次のいずれかになります。

- TFTP
- FTP
- SFTP
- SCP
- HTTP

サーバにはリモート サーバのコピー先フォルダに対する読み取り権限が必要です。

（注） Cisco UCS C シリーズ サーバでは、リモート サーバからファームウェアを更新すると、サーバのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバ タイプとして SCP または SFTP を選択した場合にのみ使用できます。

このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」というメッセージが表示されます。サーバ フィンガープリントの信頼性に応じて、[Y] または [N] をクリックします。

フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。

次の作業

Cisco Host Upgrade Utility を使用してサーバ上のすべてのファームウェアをアップグレードするか、手動でサーバに Cisco IMC ファームウェアをインストールします。

Cisco IMC セキュア ブートについて

Cisco IMC のセキュア モードについて

（注） Cisco IMC のセキュア ブート モードは、一部の Cisco UCS C シリーズ サーバでのみデフォルトで有効になっています。

Host Upgrade Utility（HUU）、Web UI または CLI を使用して、Cisco IMC を最新バージョンに更新できます。Cisco IMC をアップグレードするために HUU を使用する場合は、セキュア ブート モードをイネーブルにするよう求めるプロンプトが表示されます。[Yes] を選択すると、システムはセキュア モードを開始し、ファームウェアを 2 度インストールします。[No] を選択すると、システムは非セキュア モードを開始します。Cisco IMC をアップグレードするために Web UI または CLI を使用する場合は、バージョン 2.0(x) にアップグレードする必要があります。バージョン 2.0(x) でシステムを起動した後、システムはデフォルトでは非セキュア モードで起動します。セキュア モードを有効にする必要があります。セキュア モードを有効にすると、自動的にファームウェアが再インストールされます。Web UI では、セキュア モード オプションが Cisco IMC ファームウェア更新ページ内のチェックボックスとして利用できます。CLI では、update-secure コマンドを使用してセキュア モードを有効にできます。

Cisco IMC バージョン 2.0 への最初のアップグレード時に、機能およびアプリケーションの一部が正しくインストールされておらず、2回目のアップグレードが必要であることを示す警告メッセージが表示される場合があります。Cisco IMC ファームウェア バージョン 2.0(x) をセキュア モードで正しくインストールするために、セキュア ブート オプションをイネーブルまたは非イネーブルにした状態で2回目のアップグレードを実行することを推奨します。インストールが完了した後、

イメージをアクティブ化する必要があります。セキュアブートオプションをイネーブルにしたままシステムを起動した後は、Cisco IMC はセキュア モードのままとなり、後でディセーブルにできません。このイメージがアクティブになっていない場合や、他のファームウェア イメージを再インストールした場合、Cisco IMC が応答不能になる場合があります。

警告 セキュア ブートの移行でファームウェアをインストールした後は、他の通常のサーバベースのタスクを実行する前にイメージをアクティブにする必要があります。このイメージがアクティブになっていない場合や、他のファームウェアイメージを再インストールした場合、Cisco IMC が応答不能になる場合があります。

セキュア ブートは、ファームウェアのインストールが完了し、イメージがアクティブになった場合にのみイネーブルになります。

（注） Cisco IMC がセキュア モードになっている場合、次のことを意味します。

- 署名済みの Cisco IMC ファームウェア イメージのみがデバイスにインストールされ、起動できます。
- セキュア Cisco IMC モードは後でディセーブルにできません。
- いずれの Cisco IMC バージョンも最新バージョンに直接アップグレードできます。
- Cisco IMC のファームウェア バージョンは、バージョン 1.5(3x) より前のバージョンにインストールまたは起動できません。
- Cisco IMC バージョン 2.0 は、バージョン 1.4(x)、1.5、1.5(2x)、または 1.5(1)、1.5(2) または非セキュアのファームウェア バージョンにダウングレードできません。

最新バージョンからダウングレードする際にサポートされる Cisco IMC バージョン

次の表は、前のバージョンにダウングレードできるセキュア モードの Cisco IMC バージョンを示します。

Cisco IMC バージョンから	Cisco IMC バージョンへ	可能性
2.0(x)	1.5(1) よりも前	可能性なし
2.0(x)	1.5(3x) 以降	可能性あり
2.0(x)	1.5(3x) よりも前	可能性なし

（注） 使用している Cisco IMC のバージョンが非セキュア モードの場合、Cisco IMC を以前のバージョンにダウングレードすることができます。

（注） HUU を使用して 1.5(4) より前のバージョンに Cisco IMC バージョンをダウングレードする場合は、最初に Cisco IMC をダウングレードし、その後に他のファームウェアをダウングレードする必要があります。ファームウェアをアクティブにし、次に BIOS ファームウェアをダウングレードします。

Cisco IMC バージョン 2.0(1) に必要な更新回数

重要 この項は、Cisco IMC バージョン 2.0(1) 以前のリリースに有効です。

最新バージョンにアップグレードする際にサポートされる Cisco IMC バージョン

次の表に、最新バージョンのすべてのアプリケーションを正しくインストールするために Cisco IMC に必要な更新回数を示します。

Cisco IMC バージョンから	非セキュア Cisco IMC バージョン 2.0(x) へ	セキュア Cisco IMC バージョン 2.0(x) へ
1.5(2) よりも前	更新 2 回	更新 2 回
1.5（2）	更新 1 回	更新 2 回
1.5（3）	更新 1 回	更新 2 回
1.5(3x) 以降	更新 1 回	更新 2 回

非セキュア モードでの Cisco IMC の更新

重要 この項は、Cisco IMC バージョン 2.0(1) 以前のリリースに有効です。

すべての最新機能とアプリケーションが正常にインストールされた状態で、非セキュア モードで Cisco IMC を最新バージョンにアップグレードできます。Web UI または CLI を使用して Cisco IMC を最新バージョンにアップグレードするときは、使用しているバージョンによってはファームウェアを手動で 2 回更新する必要があります。「最新バージョンにアップグレードする際にサポートされる Cisco IMC バージョン」を参照してください。Cisco IMC バージョンにアップグレードするために HUU を使用すると、最新バージョンに自動的にアップグレードされます。

（注） 1.5(2x) よりも前のバージョンの Cisco IMC からインストールする場合は、次のメッセージが表示されます。

警告 "Some of the Cisco IMC firmware components are not installed properly! Please reinstall Cisco IMC firmware version 2.0(1) or higher to recover".

（注） （HUUによる）更新の最中は、KVM セッションに再接続して更新の現在のステータスを取
することを推奨します。

Cisco IMC が非セキュア モードで実行している場合は、次を意味します。

- 署名済みまたは未署名の Cisco ファームウェア イメージをデバイスにインストールできます。
- いずれの Cisco IMC バージョンも最新バージョンに直接アップグレードできます。
- Cisco IMC のファームウェア バージョンは以前のバージョンにインストールまたは起動できます。

リモート サーバからの Cisco IMC ファームウェアのインストール

はじめる前に

- admin 権限を持つユーザとして Cisco IMC にログインします。
- Cisco.com から Cisco Host Upgrade Utility ISO ファイルを入手し、シスコからのファームウェアの取得, （261 ページ） の説明に従ってファームウェア インストール ファイルを抽出します。

（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**	Cisco IMC コマンド モードを開始します。
ステップ 2	server /cimc # **scope firmware**	Cisco IMC 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***protocolIP Addresspath*	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 （注） Cisco UCS C シリーズ サーバでは、リモート サーバからファームウェアを更新すると、サーバのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバ タイプとして SCP または SFTP を選択した場合にのみ使用できます。 このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」というメッセージが表示されます。サーバ フィンガープリントの信頼性に応じて、[Y] または [N] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。
ステップ 4	server /cimc/firmware # **update-secure***protocolIP Addresspath*	（任意） Cisco IMC のセキュア ブート オプションに移行します。移行は次のことを意味します。 • 署名済された Cisco IMC ファームウェア イメーにのみをサーバ上でインストールおよびブートできます。 • バージョン 1.5(3x) 以前の Cisco IMC ファームウェアはインストールまたはブートできません。

	コマンドまたはアクション	目的
		• セキュア ブートを後でディセーブルにすることができません。 **重要** このアクションは、Cisco IMC 2.0(1) バージョンにのみ使用できます。以降のバージョンでは、デフォルトで有効になっています。 **警告** セキュア ブートの移行でファームウェアをインストールした後は、他の通常のサーバベースのタスクを実行する前にイメージをアクティブにする必要があります。このイメージがアクティブになっていない場合や、他のファームウェア イメージを再インストールした場合、Cisco IMC が応答不能になる場合があります。 Cisco IMC バージョン 2.0(1) の場合、セキュア ブートは、ファームウェアのインストールが完了し、イメージがアクティブになっている場合にのみイネーブルになります。
ステップ 5	server /cimc /firmware # **show detail**	（任意） 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、Cisco IMC ファームウェアを更新し、非セキュア ブートから Cisco IMC バージョン 2.0 のセキュア ブートに Cisco IMC を移行する例を示します。

```
server# scope cimc
server /cimc # scope firmware
server /cimc /firmware # update ftp 192.0.20.34 //test/dnld-ucs-k9-bundle.1.0.2h.bin
Firmware update has started.
Please check the status using "show detail"
Server /cimc /firmware # update-secure tftp 1.1.1.1 /cimc-pkg.bin
Migrating to Cisco IMC Secure Boot option implies:
-You can install and boot only signed Cisco IMC firmware images on the server.
-You cannot install and boot Cisco IMC firmware versions prior than 1.5(3x).
-You cannot disable Secure Boot later on.

After installing the firmware with the Secure Boot migration, you must
activate the image before performing any other regular server-based tasks.
The Secure Boot option is enabled only when the firmware installation
is complete and you have activated the image.

Continue?[y|N]y
Update to Secure Boot selected, proceed with update.
Firmware update initialized.
Please check the status using "show detail".
server /cimc /firmware # show detail
Firmware Image Information:
    Update Stage: DOWNLOAD
    Update Progress: 5
    Current FW Version: 2.0(0.29)
    FW Image 1 Version: 2.0(0.28)
    FW Image 1 State: BACKUP INACTIVATED
    FW Image 2 Version: 2.0(0.29)
    FW Image 2 State: RUNNING ACTIVATED
    Boot-loader Version: 2.0(0.9).35
```

```
    Secure Boot: DISABLED

*+-------------------------------------------------------------------------+
 + Some of the Cisco IMC firmware components are not installed properly! +
 + Please reinstall Cisco IMC firmware version 2.0 or higher to recover. +
 +-------------------------------------------------------------------------+
server /cimc /firmware #
```

次に、Cisco IMC を更新する例を示します。

```
server# scope cimc
server /cimc # scope firmware
server /cimc /firmware # update ftp 192.0.20.34 //test/dnld-ucs-k9-bundle.1.0.2h.bin
Firmware update has started.
Please check the status using "show detail"
server /cimc /firmware #
```

次の作業

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

はじめる前に

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。

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。
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。

	コマンドまたはアクション	目的
ステップ 5	プロンプトでyと入力し、選択したファームウェアイメージをアクティブ化します。	BMC がリブートし、リブートが完了するまですべての CLI セッションと GUI セッションが終了します。
ステップ 6	CLI にログインし、手順 1 ～ 3 を繰り返してアクティブ化されたことを確認します。	（任意）

この例では、ファームウェア イメージ 1 をアクティブ化し、BMC がリブートした後でアクティブ化されたことを確認します。

```
Server# scope cimc
Server /cimc # scope firmware
Server /cimc/firmware # show detail
Firmware Image Information:
    Update Stage: NONE
    Update Progress: 100
    Current FW Version: 1.3(3a)
    FW Image 1 Version: 1.4(3j)
    FW Image 1 State: BACKUP INACTIVATED
    FW Image 2 Version: 1.3(3a)
    FW Image 2 State: RUNNING ACTIVATED
    Boot-loader Version: 1.4(3.21).18

Server /cimc/firmware # activate 1
This operation will activate firmware 1 and reboot the BMC.
Continue?[y|N]y
.
.
 -- BMC reboot --
.
.
-- Log into CLI as Admin --

Server# scope cimc
Server /cimc # scope firmware
Server /cimc/firmware # show detail
Firmware Image Information:
    Update Stage: NONE
    Update Progress: 100
    Current FW Version: 1.4(3j)
    FW Image 1 Version: 1.4(3j)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 1.3(3a)
    FW Image 2 State: BACKUP INACTIVATED
    Boot-loader Version: 1.4(3.21).18
```

リモートサーバからのBIOSファームウェアのインストール

（注） この手順は、一部のサーバでは使用できません。他の BIOS インストール方法については、次の URL で入手できる『*Cisco UCS C-Series Rack-Mount Server BIOS Upgrade Guide*』を参照してください。http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/bios/b_Upgrading_BIOS_Firmware.html

はじめる前に

- admin 権限を持つユーザとして Cisco IMC にログインします。
- インストールした CIMC ファームウェアのアクティブ化, （269 ページ） の説明に従って、インストールする BIOS バージョンに対応する Cisco IMC ファームウェアをアクティブにします。
- サーバの電源を切ります。

（注） C220 M4、C240 M4 および C3160 の場合は、サーバの電源をオフにする必要はありません。

（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**	Cisco IMC 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。
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。

	コマンドまたはアクション	目的
ステップ 4	[Current FW Version] フィールドに表示されるファームウェア バージョンが、インストールする BIOS ファームウェア バージョンと一致するかどうか確認します。	**重要** Cisco IMC ファームウェア バージョンが一致しない場合は、この手順を続行する前に Cisco IMC ファームウェアをアクティブ化します。そうしないとサーバがブートしません。詳細については、インストールした CIMC ファームウェアのアクティブ化, （269 ページ）を参照してください。
ステップ 5	Server /cimc/firmware # **top**	サーバのルート レベルに戻ります。
ステップ 6	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 7	Server /bios # **update***protocolIP Addresspath*	次の情報を指定します。 • プロトコル。TFTP、FTP、SFTP、SCP、または HTTP が使用できます。 **（注）** Cisco UCS C シリーズ サーバでは、リモート サーバからファームウェアを更新すると、サーバのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバ タイプとして SCP または SFTP を選択した場合にのみ使用できます。 このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」というメッセージが表示されます。サーバ フィンガープリントの信頼性に応じて、[Y] または [N] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 • リモート サーバの IPv4 アドレスまたは IPv6 アドレス、あるいはホスト名。 • リモート サーバ上の BIOS ファームウェア ファイルへのファイル パス。

次に、BIOS ファームウェアを Cisco IMC ソフトウェア リリース 1.4(3j) に更新する例を示します。

```
Server# scope bios
Server /bios# show detail
BIOS:
    BIOS Version: C220M4.2.0.3.0.080720142114
    Backup BIOS Version: C220M4.2.0.2.68.073120141827
    Boot Order: (none)
    Boot Override Priority:
    FW Update/Recovery Status: None, OK
    UEFI Secure Boot: disabled
    Configured Boot Mode: None
    Actual Boot Mode: Unknown
    Last Configured Boot Order Source: UNKNOWN
Server /bios # update ftp 192.0.20.34 //upgrade_bios_files/C220-BIOS-1-4-3j-0.CAP
 <CR>  Press Enter key
Firmware update has started.
Please check the status using "show detail"
Server /bios #
```

インストールされているBIOSファームウェアのアクティブ化

（注） [Activate BIOS Firmware]（アクティブ化）オプションを使用できるのは一部の C シリーズ サーバだけです。このオプションがないサーバでは、サーバをリブートしてインストールされている BIOS ファームウェアをアクティブにします。

はじめる前に

- BIOS ファームウェアをサーバにインストールします。
- ホストの電源を切ります。

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。
- Cisco IMC のリブートまたはリセット。
- 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。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **show detail**	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 /bios # **activate**	現在非アクティブになっているイメージをアクティブにします。
ステップ 4	プロンプトで y と入力し、選択したファームウェア イメージをアクティブ化します。	

次に、ファームウェアをアクティブにしてから、アクティベーションを確認する例を示します。

```
Server# scope bios
Server /bios # show detail
BIOS
    Version: C240M4.2.0.2.67.072320142231
    Backup BIOS Version: C240M4.2.0.2.66.071820142034
    Boot Order: (none)
    Boot Override Priority:
    FW Update/Recovery Status: None, OK
    UEFI Secure Boot: disabled
    Configured Boot Mode: None
    Actual Boot Mode: Legacy
    Last Configured Boot Order Source: BIOS

Server /bios # activate
This operation will activate "C240M4.2.0.2.66.071820142034" after next host power off
Continue?[y|N]

Server# scope bios
Server /bios # show detail
BIOS
    Version: C240M4.2.0.2.66.071820142034
    Backup BIOS Version: C240M4.2.0.2.67.072320142231
    Boot Order: (none)
    Boot Override Priority:
    FW Update/Recovery Status: None, OK
    UEFI Secure Boot: disabled
    Configured Boot Mode: None
    Actual Boot Mode: Legacy
    Last Configured Boot Order Source: BIOS
```

リモートサーバからのCMCファームウェアのインストール

はじめる前に

- admin 権限を持つユーザとして Cisco IMC にログインします。

- Cisco.com から Cisco Host Upgrade Utility ISO ファイルを入手し、シスコからのファームウェアの取得, （261 ページ） の説明に従ってファームウェア インストール ファイルを抽出します。
- このアクションを使用できるのは一部の C シリーズ サーバだけです。
-

（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 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 cmc***1*|*2*	選択した SIOC コントローラ コマンド モードの CMC を開始します。
ステップ 3	server /chassis/cmc # **update***protocolIP Addresspath*	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 （注） Cisco UCS C シリーズ サーバでは、リモート サーバからファームウェアを更新すると、サーバのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバ タイプとして SCP または SFTP を選択した場合にのみ使用できます。 このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」というメッセージが表示されます。サーバ フィンガープリントの信頼性に応じて、[Y] または [N] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。

	コマンドまたはアクション	目的
ステップ 4	server /chassis/cmc # **show detail**	（任意） 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、CMC ファームウェアを更新する例を示します。

```
server # scope chassis
server /chassis # scope cmc 1
server /chassis/cmc # update  http 10.104.236.99 colusa_cmc.2.0.2a.img
CMC Firmware update initialized.
Please check the status using "show detail"
Server /chassis/cmc # show detail
Firmware Image Information:
    Name: CMC1
    Update Stage: DOWNLOAD
    Update Progress: 25
    Current FW Version: 2.0(2a)
    FW Image 1 Version: 2.0(2a)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 2.0(2a)
    FW Image 2 State: BACKUP INACTIVATED
server /chassis/cmc #
```

次の作業

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 CMC ファームウェアのアクティブ化

（注） CMC は 1 つをアクティブな状態にし、他はバックアップとして機能するように設定されています。バックアップ CMC をアクティブにすると、それまでアクティブだった CMC が、バックアップ CMC に変わり、もう一方がアクティブになります。

はじめる前に

CMC 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。
- Cisco IMC のリブートまたはリセット。
- 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。

- CMC-1 アクティベーションによって Cisco IMC ネットワーク接続が中断されます。

手順

	コマンドまたはアクション	目的
ステップ 1	server # **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server# **scope cmc** *1|2*	選択した SIOC スロット コマンド モードの CMC を開始します。
ステップ 3	Server /cmc # **activate**	選択した CMC に対して選択したイメージをアクティブにします。
ステップ 4	プロンプトで y と入力し、選択したファームウェア イメージをアクティブ化します。	CMC-1 がリブートし、そのリブートが完了するまではすべての CLI セッションと GUI セッションが終了しますが、CMC-2 リブートがアクティブなセッションに影響を与えることはありません。

次に、SIOC スロット 1 上の CMC ファームウェアをアクティブにする例を示します。

```
Server # scope chassis
Server /chassis # scope cmc 1
Server /chassis/cmc #  activate
Warning: The CMC will be rebooted immediately to complete the activation.
The network may go down temporarily till CMC boots up again
Continue?[y|N]y
```

第 15 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。

Fault Summary

障害およびログのサマリーの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scopefault**	障害コマンド モードを開始します。
ステップ 2	Server # **showfault-entries**	すべての障害のログを表示します。

次に、障害のサマリーの例を示します。

```
Server # scope fault
Server /fault # show fault-entries
Time                      Severity      Description
------------------------- ------------- -----------------
Sun Jun 27 04:00:52 2013  info          Storage Local disk 12 missing
Sat Jun 26 05:00:22 2013  warning       Power Supply redundancy is lost

Server /fault #
```

障害履歴

障害履歴の表示

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 # **show fault-history**	障害の履歴を表示します。

次に、障害の履歴を表示する例を示します。

```
Server # scope fault
Server /fault # show fault-history
Time                 Severity  Source  Cause                  Description
------------------- --------- ------  --------------------
----------------------------------------
2014 Feb 6 23:24:49 error     %CIMC   PSU_REDUNDANCY-FAIL
"[F0743][major][psu-redundancy-fail].....
2014 Feb 6 23:24:49 error     %CIMC   EQUIPMENT_INOPERABLE
"[F0374][major][equipment-inoperable]...
2014 Feb 6 23:24:19 debug     %CIMC   2014 Feb 6 23        "24:19:7:%CIMC::: SEL INIT DONE"


Server /fault #
```

Cisco IMC ログ

Cisco IMC 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# **scopecimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scopelog**	Cisco IMC ログ コマンド モードを開始します。
ステップ 3	Server /cimc/log # **showentries** [**detail**]	Cisco IMC 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、Cisco IMC 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                Severity      Source           Description

------------------- ------------- ---------------- ----------------------------------------

2012 Jan 30 05:20:45 Informational BMC:ciscoNET:961 " rpc_aim_callback_function_1_svc() -
result == SUCCESS, callbackData size: 600 "
2012 Jan 30 05:20:45 Informational BMC:ciscoNET:961 rpc_aim_callback_function_1_svc() -
returned from pFunctionCallback result:0
2012 Jan 30 05:20:45 Informational BMC:ciscoNET:961 " rpc_aim_callback_function_1_svc() -
szFunctionName:netGetCurrentIfConfig nSize:0 nMaxSize: 600 "
--More--

Server /cimc/log # show entries detail
Trace Log:
    Time: 2012 Jan 30 05:20:45
    Severity: Informational
    Source: BMC:ciscoNET:961
   Description: " rpc_aim_callback_function_1_svc() - result == SUCCESS, callbackData size:
 600 "
    Order: 0
Trace Log:
    Time: 2012 Jan 30 05:20:45
    Severity: Informational
    Source: BMC:ciscoNET:961
   Description: rpc_aim_callback_function_1_svc() - returned from pFunctionCallback result:0

    Order: 1
Trace Log:
    Time: 2012 Jan 30 05:20:45
    Severity: Informational
    Source: BMC:ciscoNET:961
   Description: " rpc_aim_callback_function_1_svc() - szFunctionName:netGetCurrentIfConfig
 nSize:0 nMaxSize: 600 "
    Order: 2
--More--

Server /cimc/log #
```

Cisco IMC 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# **scopecimc**	Cisco IMC コマンドモードを開始します。
ステップ 2	Server /cimc # **scopelog**	Cisco IMC ログ コマンド モードを開始します。
ステップ 3	Server /cimc/log # **clear**	Cisco IMC ログをクリアします。

次に、Cisco IMC 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
```

Cisco IMC ログしきい値の設定

Cisco IMC 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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope log**	Cisco IMC ログ コマンド モードを開始します。
ステップ 3	Server /cimc/log # **setlocal-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） Cisco IMC 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、Cisco IMC 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	Server /cimc/log # **showlocal-syslog-severity**	（任意） 設定された重大度レベルを表示します。

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 Cisco IMC ログの送信

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

はじめる前に

- リモート syslog サーバが、リモート ホストからログを受信するように設定されている必要があります。
- リモート syslog サーバが、認証関連のログを含め、すべてのタイプのログを受信するように設定されている必要があります。
- リモート syslog サーバのファイアウォールが、syslog メッセージが syslog サーバに到達するように設定され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**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope log**	Cisco IMC ログ コマンド モードを開始します。
ステップ 3	Server /cimc/log # **set remote-syslog-severity** *level*	（任意） 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

	コマンドまたはアクション	目的
		（注） Cisco IMC では、選択した重大度よりも低い重大度のメッセージは、リモートでログに記録されません。たとえば、**error** を選択した場合、リモート syslog サーバは重大度が Emergency、Alert、Critical、または Error のすべての Cisco IMC ログ メッセージを受信します。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 # **scope server** {**1** | **2**}	2 台のリモート syslog サーバ プロファイルのいずれかを選択し、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 5	Server /cimc/log/server # **set server-ip** *ipv4 or ipv6 address or domain name*	リモート syslog サーバのアドレスを指定します。 （注） リモート サーバのアドレスとして IPv4 アドレスまたは IPv6 アドレス、あるいはメイン名を設定できます。
ステップ 6	Server /cimc/log/server # **set server-port** *port number*	リモート syslog サーバの宛先ポート番号を設定します。
ステップ 7	Server /cimc/log/server # **set enabled** {**yes** | **no**}	この syslog サーバへの Cisco IMC ログ エントリの送信をイネーブルにします。
ステップ 8	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。

次に、リモート syslog サーバ プロファイルを設定し、重大度レベル Warning 以上の Cisco IMC 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 # set remote-syslog-severity warning
Server /cimc/log *# scope server 1
Server /cimc/log/server *# set server-ip www.abc.com
Server /cimc/log/server *# set server-port 514
Server /cimc/log/server *# set enabled yes
Server /cimc/log/server *# commit
Server /cimc/log/server # exit
Server /cimc/log # show server
Syslog Server 1:
    Syslog Server Address: www.abc.com
    Syslog Server Port: 514
    Enabled: yes

Server /cimc/log # show remote-syslog-severity
    Remote Syslog Severity: warning

Server /cimc/log #
```

システム イベント ログ

システム イベント ログの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope sel**	システム イベント ログ（SEL）コマンド モードを開始します。
ステップ 2	Server /sel # **show entries [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。
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
```

ロギング制御

Cisco IMC ログしきい値の設定

Cisco IMC 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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope log**	Cisco IMC ログ コマンド モードを開始します。
ステップ 3	Server /cimc/log # **setlocal-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

	コマンドまたはアクション	目的
		• warning • notice • informational • debug （注） Cisco IMC 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、Cisco IMC 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	Server /cimc/log # **showlocal-syslog-severity**	（任意） 設定された重大度レベルを表示します。

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 Cisco IMC ログの送信

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

はじめる前に

- リモート syslog サーバが、リモート ホストからログを受信するように設定されている必要があります。
- リモート syslog サーバが、認証関連のログを含め、すべてのタイプのログを受信するように設定されている必要があります。

- リモート syslog サーバのファイアウォールが、syslog メッセージが syslog サーバに到達するように設定され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**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope log**	Cisco IMC ログ コマンド モードを開始します。
ステップ 3	Server /cimc/log # **set remote-syslog-severity** *level*	（任意） 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） Cisco IMC では、選択した重大度よりも低い重大度のメッセージは、リモートでログに記録されません。たとえば、**error** を選択した場合、リモート syslog サーバは重大度が Emergency、Alert、Critical、または Error のすべての Cisco IMC ログ メッセージを受信します。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 # **scope server** {**1** | **2**}	2 台のリモート syslog サーバ プロファイルのいずれかを選択し、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 5	Server /cimc/log/server # **set server-ip** *ipv4 or ipv6 address or domain name*	リモート syslog サーバのアドレスを指定します。 （注） リモート サーバのアドレスとして IPv4 アドレスまたは IPv6 アドレス、あるいはメイン名を設定できます。

	コマンドまたはアクション	目的
ステップ 6	Server /cimc/log/server # **set server-port** *port number*	リモート syslog サーバの宛先ポート番号を設定します。
ステップ 7	Server /cimc/log/server # **set enabled** {**yes** | **no**}	この syslog サーバへの Cisco IMC ログ エントリの送信をイネーブルにします。
ステップ 8	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。

次に、リモート syslog サーバ プロファイルを設定し、重大度レベル Warning 以上の Cisco IMC 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 # set remote-syslog-severity warning
Server /cimc/log *# scope server 1
Server /cimc/log/server *# set server-ip www.abc.com
Server /cimc/log/server *# set server-port 514
Server /cimc/log/server *# set enabled yes
Server /cimc/log/server *# commit
Server /cimc/log/server # exit
Server /cimc/log # show server
Syslog Server 1:
    Syslog Server Address: www.abc.com
    Syslog Server Port: 514
    Enabled: yes

Server /cimc/log # show remote-syslog-severity
    Remote Syslog Severity: warning

Server /cimc/log #
```

リモート サーバへのテスト Cisco IMC ログの送信

はじめる前に

- リモート syslog サーバが、リモート ホストからログを受信するように設定されている必要があります。
- リモート syslog サーバが、認証関連のログを含め、すべてのタイプのログを受信するように設定されている必要があります。
- リモート syslog サーバのファイアウォールが、syslog メッセージが syslog サーバに到達するように設定され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**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope log**	Cisco IMC ログ コマンド モードを開始します。
ステップ 3	Server /cimc/log # **send-test-syslog**	テスト Cisco IMC ログを設定したリモート サーバに送信します。

次に、テスト Cisco IMC の syslog を設定したリモート サーバに送信する例を示します。

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # send-test-syslog

Syslog Test message will be sent to configured Syslog destinations.
If no Syslog destinations configured, this command will be silently ignored.
Syslog Test message has been requested.

Server /cimc/log #
```

第 16 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。

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。

重要 ファームウェアまたは BIOS の更新が進行中の場合は、それらのタスクが完了するまで、テクニカル サポート データをエクスポートしないでください。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scopetech-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 # **setremote-ip***ip-address*	テクニカル 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 # **setremote-path***path/filename*	リモート 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、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。 ヒント　システムにファイル名を自動生成させるには default.tar.gz というファイル名を入力します。
ステップ 5	Server /cimc/tech-support # **setremote-protocol***protocol*	リモート サーバに接続するためのプロトコルを指定します。次のいずれかのタイプを指定できます。 • TFTP • FTP • SFTP • SCP • HTTP （注）　Cisco UCS C シリーズ サーバでは、リモート サーバからファームウェアを更新すると、サーバのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバ タイプとして SCP または SFTP を選択した場合にのみ使用できます。 このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」というメッセージが表示されます。サーバ フィンガープリントの信頼性に応じて、[Y] または [N] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。

	コマンドまたはアクション	目的
ステップ 6	Server /cimc/tech-support # **setremote-username***name*	テクニカルサポートデータ ファイルを保存するリモート サーバのユーザ名を指定します。このフィールドは、プロトコルが 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 # **setremote-password***password*	テクニカルサポートデータ ファイルを保存するリモートサーバのパスワードを指定します。このフィールドは、プロトコルが 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**	（任意） リモート サーバへのデータ ファイルの転送の進捗状況が表示されます。
ステップ 11	Server /cimc/tech-support # **cancel**	（任意） リモート サーバへのデータ ファイルの転送をキャンセルします。

次に、テクニカル 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 192.0.20.41
Server /cimc/tech-support* # set remote-protocol tftp
Server /cimc/tech-support *# set remote-path /user/user1/default.tar.gz
Server /cimc/tech-support *# commit
Server /cimc/tech-support # start
Tech Support upload started.

Server /cimc/tech-support # show detail

Tech Support:
  Server Address: 192.0.20.41
  Path: default.tar.gz
  Protocol: tftp
  Username:
  Password: *******
  Progress (%): 5
  Status: Collecting

Server /cimc/tech-support #
```

次の作業

生成されたレポート ファイルを Cisco TAC に提供します。

Cisco IMC 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、Cisco IMC 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。Cisco IMC を再起動した後にログオフすると、Cisco IMC 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 Cisco IMC を再起動すると、サーバの電源は、Cisco IMC 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# **scopecimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **reboot**	Cisco IMC がリブートします。

次に、Cisco IMC 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

（注） この手順は、一部のサーバ モデルでは使用できません。

破損した BIOS のリカバリには、この手順の他に 3 種類の方法が存在します。

- Cisco Host Upgrade Utility（HUU）を使用します。これは推奨される方法です。
- Cisco IMC GUI インターフェイスを使用します。
- サーバのマザーボード上でハードウェア ジャンパの BIOS リカバリ機能を使用する（お使いのサーバ モデルでサポートされている場合）。手順については、お使いのサーバ モデルに対応した『Cisco UCS Server Installation and Service Guide』を参照してください。

はじめる前に

- 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# **scopebios**	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
```

次の作業

電源を再投入するか、サーバをリセットします。

Cisco IMC 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、Cisco IMC の出荷時の初期状態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。Cisco IMC 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。

バージョン 1.5(1) からバージョン 1.5(2) にアップグレードすると、Cisco IMC インターフェイスのホスト名はそのまま保持されます。ただし、バージョン 1.5(2) にアップグレードした後、工場出荷時の状態にリセットすると、ホスト名は CXXX-YYYYYY という形式に変更されます。（XXX はモデル番号、YYYYYY はサーバのシリアル番号）。

バージョン 1.5(2) からバージョン 1.5(1) にダウングレードすると、ホスト名はそのまま保持されます。ただし、工場出荷時の状態にリセットすると、ホスト名は ucs-cxx-mx という形式に変更されます。

（注） Cisco IMC 1.5(x)、2.0、および 2.0(3) バージョンを工場出荷時の初期状態にリセットすると、Shared LOM モードがデフォルトで設定されます。C3160 サーバの場合、Cisco IMC を工場出荷時の初期状態にリセットすると、Dedicated モードが Full デュプレックスに設定され、速度はデフォルトで 100 Mbps 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# **scopecimc**	Cisco IMC 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、Cisco IMC が出荷時デフォルトにリセットされます。

Cisco IMC の出荷時デフォルトには、次の条件が含まれます。

- Cisco IMC 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。
- Cisco IMC 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**）。

- 管理ポートで DHCP がイネーブルになっている。
- 前の実際のブート順序が保持される。
- 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、Cisco IMC 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]
```

Cisco IMC 設定のエクスポートとインポート

Cisco IMC 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。

重要 ファームウェアまたはBIOSの更新が進行中の場合は、それらのタスクが完了するまで、Cisco IMC 設定をエクスポートしないでください。

はじめる前に

バックアップ リモート サーバの IP アドレスを取得します。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	Cisco IMC 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***protocolip-addresspath-and-filename*	コンフィギュレーション ファイルは、指定した IPv4 または IPv6 アドレス、あるいはホスト名のリモート サーバに、指定したパスとファイル名で保存されます。

	コマンドまたはアクション	目的
		リモート サーバは次のいずれかのタイプになります。 • TFTP • FTP • SFTP • SCP • HTTP （注） Cisco UCS C シリーズ サーバでは、リモートサーバからファームウェアを更新すると、サーバのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバ タイプとして SCP または SFTP を選択した場合にのみ使用できます。 このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」というメッセージが表示されます。サーバフィンガープリントの信頼性に応じて、[Y] または [N] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。
ステップ 4	ユーザ名、パスワード、およびパス フレーズを入力します。	エクスポートするファイルのユーザ名、パスワード、およびパスフレーズを設定します。バックアップ操作を開始します。

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。

次に、Cisco IMC コンフィギュレーション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 tftp 192.0.2.34 /ucs/backups/cimc5.xml
Username:pynj
Password:****
Passphrase:***
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 #
```

Cisco IMC 設定のエクスポートとインポート

Cisco IMC 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 Cisco IMC 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 Cisco IMC 設定ファイルは、同じシステムで復元したり、別の Cisco IMC 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の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の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。

Cisco IMC 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 Cisco IMC 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。

次の機能でインポートまたはエクスポート操作を実行できます。

- Cisco IMC のバージョン

  （注） この情報のみをエクスポートできます。

- ネットワーク設定
- テクニカルサポート

- ローカル ログおよびリモート ログのロギング制御
- 電力ポリシー
- BIOS - BIOS パラメータ

（注） 高精度ブートはサポートされません。

- 通信サービス
- リモート プレゼンス
- ユーザ管理 - LDAP
- イベント管理
- SNMP

Cisco IMC 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。

重要 ファームウェアまたはBIOSの更新が進行中の場合は、それらのタスクが完了するまで、Cisco IMC 設定をエクスポートしないでください。

はじめる前に

バックアップ リモート サーバの IP アドレスを取得します。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	Cisco IMC 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***protocolip-addresspath-and-filename*	コンフィギュレーション ファイルは、指定した IPv4 または IPv6 アドレス、あるいはホスト名のリモート サーバに、指定したパスとファイル名で保存されます。

	コマンドまたはアクション	目的
		リモート サーバは次のいずれかのタイプになります。 • TFTP • FTP • SFTP • SCP • HTTP （注） Cisco UCS C シリーズ サーバでは、リモート サーバからファームウェアを更新すると、サーバのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバ タイプとして SCP または SFTP を選択した場合にのみ使用できます。 このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」というメッセージが表示されます。サーバ フィンガープリントの信頼性に応じて、[Y] または [N] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。
ステップ 4	ユーザ名、パスワード、およびパス フレーズを入力します。	エクスポートするファイルのユーザ名、パスワード、およびパスフレーズを設定します。バックアップ操作を開始します。

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。

次に、Cisco IMC コンフィギュレーション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 tftp 192.0.2.34 /ucs/backups/cimc5.xml
Username:pynj
Password:****
Passphrase:***
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 #
```

Cisco IMC 設定のインポート

重要 ファームウェアまたはBIOSの更新が進行中の場合は、それらのタスクが完了するまで、Cisco IMC 設定をインポートしないでください。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scopecimc**	Cisco IMC コマンドモードを開始します。
ステップ 2	Server /cimc # **scopeimport-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***protocolip-addresspath-and-filename*	指定した IPv4 アドレスまたは IPv6 アドレス、またはホスト名にあるリモートサーバ上の、指定したパスとファイル名のコンフィギュレーションファイルがインポートされます。リモートサーバは次のいずれかになります。 • TFTP • FTP • SFTP • SCP • HTTP

	コマンドまたはアクション	目的
		（注） Cisco UCS C シリーズ サーバでは、リモート サーバからファームウェアを更新すると、サーバのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバ タイプとして SCP または SFTP を選択した場合にのみ使用できます。 このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?」というメッセージが表示されます。サーバフィンガープリントの信頼性に応じて、[Y] または [N] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。
ステップ 4	ユーザ名、パスワード、およびパス フレーズを入力します。	インポートするファイルのユーザ名、パスワード、およびパスフレーズを設定します。インポート操作を開始します。

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。

次に、Cisco IMC コンフィギュレーションをインポートする例を示します。

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

Cisco IMC バナーの追加

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scopechassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **upload-banner**	バナーを入力するプロンプトが表示されます。
ステップ 3	バナーを入力し、CTRL+D キーを押します。	プロンプトで、y を入力します。これによって現在のセッションが失われ、もう一度ログインすると、バナーが表示されます。
ステップ 4	Server /chassis # **show-banner**	（任意） 追加したバナーが表示されます。

次に、Cisco IMC バナーを追加する例を示します。

```
Server # scope chassis
Server /chassis # upload-banner
Please paste your custom banner here, when finished, press enter and CTRL+D.
hello world
This will terminate all open SSH session to take an immediate action.
Do you wish to continue? [y/N] yy
Server /chassis # show-banner
hello world
Server /chassis #
```

Cisco IMC バナーの追加

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scopechassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **upload-banner**	バナーを入力するプロンプトが表示されます。
ステップ 3	バナーを入力し、CTRL+D キーを押します。	プロンプトで、y を入力します。これによって現在のセッションが失われ、もう一度ログインすると、バナーが表示されます。

	コマンドまたはアクション	目的
ステップ 4	Server /chassis # **show-banner**	（任意） 追加したバナーが表示されます。

次に、Cisco IMC バナーを追加する例を示します。

```
Server # scope chassis
Server /chassis # upload-banner
Please paste your custom banner here, when finished, press enter and CTRL+D.
hello world
This will terminate all open SSH session to take an immediate action.
Do you wish to continue? [y/N] yy
Server /chassis # show-banner
hello world
Server /chassis #
```

Cisco IMC バナーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scopechassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **delete-banner**	プロンプトで、y を入力します。これによって現在のセッションが失われ、もう一度ログインすると、バナーが削除されます。
ステップ 3	Server /chassis # **show-banner**	（任意） 追加したバナーが表示されます。

次に、Cisco IMC バナーを削除する例を示します。

```
Server # scope chassis
Server /chassis # delete-banner
This will terminate all open SSH session to take an immediate action.
Do you wish to continue? [y/N] yy
Server /chassis # show-banner

Server /chassis #
```

付 録 A

サーバ モデル別 BIOS パラメータ

この付録の内容は、次のとおりです。

C22 および C24 サーバ

C22 および C24 サーバの主要な BIOS パラメータ

名前	説明
[TPM Support] **set TPMAdminCtrl**	TPM（トラステッドプラットフォームモジュール）は、主に暗号キーを使用する基本的なセキュリティ関連機能を提供するように設計されたマイクロチップです。このオプションを使用すると、システムの TPM セキュリティ デバイス サポートを制御できます。次のいずれかを指定できます。 • [Disabled]：サーバは TPM を使用しません。 • [Enabled]：サーバは TPM を使用します。 （注） 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。

C22 および C24 サーバの高度な BIOS パラメータ

[Processor Configuration] のパラメータ

名前	説明
[Intel Hyper-Threading Technology] **set IntelHyperThread**	プロセッサで Intel Hyper-Threading Technology 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。
[Number of Enabled Cores] **set CoreMultiProcessing**	サーバ上の 1 つ以上の物理コアをディセーブルにできます。次のいずれかになります。 • [All]：すべての物理コアをイネーブルにします。これにより、関連付けられている論理プロセッサ コアで Hyper Threading もイネーブルになります。 • [1] ～ [*n*]：サーバで実行できる物理プロセッサ コアの数を指定します。各物理コアには、論理コアが関連付けられています。 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
[Execute Disable] **set ExecuteDisable**	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ディセーブルにします。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。
[Intel VT] **set IntelVT**	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-d] **set IntelVTD**	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。

名前	説明
[Intel VT-d Coherency Support] **set CoherencySupport**	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。
[Intel VT-d ATS Support] **set ATS**	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。
[CPU Performance] **set CPUPerformance**	サーバの CPU パフォーマンス プロファイルを設定します。パフォーマンス プロファイルは次のオプションで構成されます。 • DCU Streamer Prefetcher • DCU IP Prefetcher • Hardware Prefetcher • Adjacent Cache-Line Prefetch 次のいずれかになります。 • [Enterprise]：すべてのオプションがイネーブルです。 • [High Throughput][High_Throughput]：DCUIP Prefetcher のみがイネーブルです。残りのオプションはディセーブルになります。 • [HPC]：すべてのオプションがイネーブルです。この設定はハイ パフォーマンス コンピューティングとも呼ばれます。 • [Custom]：パフォーマンス プロファイルのすべてのオプションをサーバの BIOS セットアップから設定できます。また、Hardware Prefetcher オプションと Adjacent Cache-Line Prefetch オプションは、下記のフィールドで設定できます。

名前	説明
[Hardware Prefetcher] **set HardwarePrefetch**	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。
[Adjacent Cache Line Prefetcher] **set AdjacentCacheLinePrefetch**	プロセッサで必要な行のみを取得するのではなく、偶数または奇数のペアのキャッシュ行を取得するかどうか。次のいずれかになります。 • [Disabled]：プロセッサで必要な行のみを取得します。 • [Enabled]：プロセッサで必要な行およびペアの行の両方を取得します。
[DCU Streamer Prefetch] **set DcuStreamerPrefetch**	プロセッサで DCU IP Prefetch メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [Disabled]：プロセッサはキャッシュ読み取り要求を予測しようとせず、明示的に要求された行のみを取得します。 • [Enabled]：DCU Prefetcher でキャッシュ読み取りパターンを分析し、必要と判断した場合にキャッシュ内の次の行を事前に取得します。
[DCU IP Prefetcher] **set DcuIpPrefetch**	プロセッサで DCU IP Prefetch メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [Disabled]：プロセッサでキャッシュ データをプリロードしません。 • [Enabled]：DCU IP Prefetcher で最も関連性が高いと判断されたデータを含む L1 キャッシュをプリロードします。

名前	説明
[Direct Cache Access Support] **set DirectCacheAccess**	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。
[Power Technology] **set CPUPowerManagement**	次のオプションの CPU 電源管理設定を指定できます。 • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 [Power Technology] は次のいずれかになります。 • [Custom]：前述の BIOS パラメータの個々の設定が使用されます。これらの BIOS パラメータのいずれかを変更する場合は、このオプションを選択する必要があります。 • [Disabled]：サーバで CPU 電源管理は実行されず、前述の BIOS パラメータの設定が無視されます。 • Energy_Efficient：前述の BIOS パラメータに最適な設定が決定され、これらのパラメータの個々の設定は無視されます。

名前	説明
[Enhanced Intel Speedstep Technology] **set EnhancedIntelSpeedStep**	プロセッサで Enhanced Intel SpeedStep Technology 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。 （注） CPUPowerManagement を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[Intel Turbo Boost Technology] **set IntelTurboBoostTech**	プロセッサで Intel Turbo Boost Technology 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。 （注） CPUPowerManagement を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。

名前	説明
[Processor Power State C6] **set ProcessorC6Report**	BIOS 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。OS はレポートを受信すると、プロセッサを電力量の少ない C6 状態に移行してエネルギー使用量を減らし、最適なプロセッサパフォーマンスを維持できます。次のいずれかになります。 • [Disabled]：BIOS から C6 レポートを送信しません。 • [Enabled]：BIOS から C6 レポートを送信し、OS がプロセッサを電力量の少ない C6 状態に移行できるようにします。 （注） CPUPowerManagement を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[Processor Power State C1 Enhanced] **set ProcessorC1EReport**	C1 ステートに入ったときに、CPU が最小周波数に移行するかどうか。次のいずれかになります。 • [Disabled]：CPU は C1 ステートでも引き続き最大周波数で動作します。 • [Enabled]：CPU は最小周波数に移行します。このオプションでは C1 ステートで節約される電力量が最大になります。
[Frequency Floor Override] **set CpuFreqFloor**	アイドル時に、CPU がターボを除く最大周波数よりも低い周波数にできるようにするかどうか。次のいずれかになります。 • [Disabled]：アイドル中に CPU をターボを除く最大周波数よりも低くできます。このオプションでは電力消費が低下しますが、システムパフォーマンスが低下する可能性があります。 • [Enabled]：アイドル中に CPU をターボを除く最大周波数よりも低くできません。このオプションではシステムパフォーマンスが向上しますが、消費電力が増加することがあります。

名前	説明
[P-STATE Coordination] **set PsdCoordType**	BIOS がオペレーティング システムに P-state サポート モデルを通信する方法を定義できます。Advanced Configuration and Power Interface（ACPI）仕様で定義される 3 つのモデルがあります。 • [HW_ALL]：プロセッサ ハードウェアが、依存性のある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。 • [SW_ALL]：OS Power Manager（OSPM）が、依存性のある論理プロセッサ（物理パッケージ内のすべての論理プロセッサ）間の P-state を調整します。すべての論理プロセッサで遷移を開始する必要があります。 • [SW_ANY]：OS Power Manager（OSPM）が、依存性のある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。ドメイン内の任意の論理プロセッサで遷移を開始する場合があります。 （注） CPUPowerManagement を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[Energy Performance] **set CpuEngPerfBias**	システム パフォーマンスまたはエネルギー効率がこのサーバで重要かどうかを判断できます。次のいずれかになります。 • Balanced_Energy • Balanced_Performance • Energy_Efficient • Performance

[Memory Configuration] のパラメータ

名前	説明
[Select Memory RAS] **set SelectMemoryRAS**	サーバに対するメモリの Reliability, Availability, and Serviceability（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。 • [Lockstep]：サーバ内の DIMM ペアが、同一のタイプ、サイズ、および構成を持ち、SMI チャネルにまたがって装着されている場合、ロックステップモードをイネーブルにして、メモリ アクセス遅延の最小化およびパフォーマンスの向上を実現できます。このオプションを使用した場合、[Mirroring] よりもシステム パフォーマンスが向上し、[Maximum Performance] よりも信頼性が向上しますが、[Mirroring] よりも信頼性が低く、[Maximum Performance] よりもシステム パフォーマンスは低下します。
[DRAM Clock Throttling] **set DRAMClockThrottling**	メモリ帯域幅と消費電力に関してシステム設定を調整できます。次のいずれかになります。 • [Balanced]：DRAM クロック スロットリングを低下させ、パフォーマンスと電力のバランスをとります。 • [Performance]：DRAM クロック スロットリングはディセーブルです。追加の電力をかけてメモリ帯域幅を増やします。 • [Energy Efficient][Energy_Efficient]：DRAMのクロック スロットリングを上げてエネルギー効率を向上させます。

名前	説明
[NUMA] **set NUMAOptimize**	BIOS で Non-Uniform Memory Access（NUMA）がサポートされているかどうか。次のいずれかになります。 • [Disabled]：BIOS で NUMA をサポートしません。 • [Enabled]：NUMA に対応したオペレーティング システムに必要な ACPI テーブルを BIOS に含めます。このオプションをイネーブルにした場合は、一部のプラットフォームでシステムのソケット間メモリインターリーブをディセーブルにする必要があります。
[Low Voltage DDR Mode] **set LvDDRMode**	低電圧と高周波数のどちらのメモリ動作をシステムで優先するか。次のいずれかになります。 • [Power Saving Mode][Power_Saving_Mode]：低電圧のメモリ動作が高周波数のメモリ動作よりも優先されます。 このモードでは、電圧を低く維持するために、メモリの周波数が低下する可能性があります。 • [Performance Mode][Performance_Mode]：高周波数の動作が低電圧の動作よりも優先されます。
[DRAM Refresh rate] **set DramRefreshRate**	DRAM セルをリフレッシュするレートを設定できます。次のいずれかになります。 • [1x]：DRAM セルは、64ms ごとにリフレッシュされます。 • [2x]：DRAM セルは、32ms ごとにリフレッシュされます。 • [3x]：DRAM セルは、21ms ごとにリフレッシュされます。 • [4x]：DRAM セルは、16ms ごとにリフレッシュされます。 • [Auto]： DRAM セルのリフレッシュ レートは、システム設定に基づき BIOS によって自動的に選択されます。これは、このパラメータに推奨される設定です。

名前	説明
[Channel Interleaving] **set ChannelInterLeave**	CPUがメモリ ブロックを分割して、データの隣接部分をインターリーブされたチャネル間に分散し、同時読み取り動作をイネーブルにするかどうか。次のいずれかになります。 • [Auto]：実行するインターリーブを、CPUが決定します。 • [1_Way]：何らかのチャネル インターリーブが使用されます。 • [2_Way] • [3_Way] • [4_Way]：最大のチャネル インターリーブが使用されます。
[Rank Interleaving] **set RankInterLeave**	1 つのランクを更新中に別のランクにアクセスできるよう、CPUがメモリの物理ランクをインターリーブするかどうか。次のいずれかになります。 • [Auto]：実行するインターリーブを、CPUが決定します。 • [1_Way]：何らかのランク インターリーブが使用されます。 • [2_Way] • [4_Way] • [8_Way]：最大量のランク インターリーブが使用されます。

名前	説明
[Patrol Scrub] **set PatrolScrub**	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] **set DemandScrub**	CPU または I/O が読み取りを要求した場合に検出された 1 ビットのメモリ エラーを、システムが修正するかどうか。次のいずれかになります。 • [Disabled]：1 ビット メモリ エラーは修正されません。 • [Enabled]：1 ビット メモリ エラーがメモリ内部で修正され、修正されたデータが、読み取り要求に対する応答に設定されます。
[Altitude] **set Altitude**	物理サーバがインストールされているおおよその海抜（m）。次のいずれかになります。 • [Auto]：物理的な高度を CPU によって判別します。 • [300_M]：サーバは、海抜約 300 m です。 • [900_M]：サーバは、海抜約 900 m です。 • [1500_M]：サーバは、海抜約 1500 m です。 • [3000_M]：サーバは、海抜約 3000 m です。

[QPI Configuration] のパラメータ

名前	説明
[QPI Link Frequency Select] **set QPILinkFrequency**	Intel QuickPath Interconnect（QPI）リンク周波数（ギガトランスファー/秒（GT/s）単位）。次のいずれかになります。 • [Auto]：QPI リンク周波数は CPU によって決定されます。 • [6.4_GT/s] • [7.2_GT/s] • [8.0_GT/s]
[QPI Snoop Mode] **set QpiSnoopMode**	Intel QuickPath Interconnect（QPI）スヌープ モード。次のいずれかになります。 • [Auto]：CPU は自動的に早期スヌープ モードとして認識します。 • [Early Snoop]：分散キャッシュ リング停止で、別のキャッシング エージェントにスヌープ プローブまたは要求を直接送信できます。このモードは、遅延が少なく、スレッド全体でデータ セットを共有しているためにキャッシュ間転送からメリットが得られるワークロードや NUMA 最適化されていないワークロードに最適です。 • [Home Snoop]：スヌープは、常に、メモリ コントローラのホーム エージェント（集中型リング停止）によって起動されます。このモードは、早期スヌープよりローカル遅延が多いですが、未処理トランザクションが増えた場合に予備のリソースを使用できます。 • [Home Directory Snoop]：ホーム ディレクトリは、プロセッサ内の HA と iMC の両方のロジックに実装されたオプション機能です。このディレクトリの目的は、スケーラブルなプラットフォームと 2S および 4S 構成でスヌープをリモート ソケットとノード コントローラにフィルタリングすることです。 • [Home Directory Snoop with OSB]：Opportunistic Snoop Broadcast（OSB）ディレクトリ モードでは、HA は、ディレクトリ情報が収集されてチェックされる前であっても、非常に負荷の軽い状況下で推測的ホーム スヌープ ブロードキャストを選択できます。

[Onboard Storage] のパラメータ

名前	説明
[Onboard SCU Storage Support] **set DisableSCU**	オンボード ソフトウェア RAID コントローラをサーバに使用できるかどうか。次のいずれかになります。 • [Disabled]：ソフトウェア RAID コントローラを使用できません。 • [Enabled]：ソフトウェア RAID コントローラを使用できます。

[USB Configuration] のパラメータ

名前	説明
[Legacy USB Support] **set LegacyUSBSupport**	システムでレガシーUSBデバイスをサポートするかどうか。次のいずれかになります。 • [Disabled]：USBデバイスは、EFIアプリケーションでのみ使用できます。 • [Enabled]：レガシーUSBのサポートは常に使用できます。 • [Auto]：USB デバイスが接続されていない場合、レガシー USB のサポートがディセーブルになります。
[Port 60/64 Emulation] **set UsbEmul6064**	完全な USB キーボード レガシー サポートのために 60h/64h エミュレーションをシステムでサポートするかどうか。次のいずれかになります。 • [Disabled]：60h/64 エミュレーションはサポートされません。 • [Enabled]：60h/64エミュレーションはサポートされます。 サーバで USB 非対応オペレーティング システムを使用する場合は、このオプションを選択する必要があります。
[All USB Devices] **set AllUsbDevices**	すべての物理および仮想USBデバイスがイネーブルであるか、ディセーブルであるか。次のいずれかになります。 • [Disabled]：すべての USB デバイスがディセーブルです。 • [Enabled]：すべての USB デバイスがイネーブルです。

名前	説明
[USB Port: Rear] **set UsbPortRear**	背面パネルのUSBデバイスがイネーブルかディセーブルか。次のいずれかになります。 • [Disabled]：背面パネルの USB ポートをディセーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [Enabled]：背面パネルの USB ポートをイネーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。
[USB Port: Front] **set UsbPortFront**	前面パネルのUSBデバイスがイネーブルかディセーブルか。次のいずれかになります。 • [Disabled]：前面パネルの USB ポートをディセーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [Enabled]：前面パネルの USB ポートをイネーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。
[USB Port: Internal] **set UsbPortInt**	内部USBデバイスがイネーブルかディセーブルか。次のいずれかになります。 • [Disabled]：内部 USB ポートをディセーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [Enabled]：内部 USB ポートをイネーブルにします。これらのポートに接続されるデバイスは、BIOSおよびオペレーティング システムによって検出されます。
[USB Port: KVM] **set UsbPortKVM**	KVM ポートがイネーブルかディセーブルか。次のいずれかになります。 • [Disabled]： KVM キーボードおよびマウス デバイスをディセーブルにします。キーボードとマウスは KVM ウィンドウで機能しなくなります。 • [Enabled]： KVM キーボードおよびマウス デバイスをイネーブルにします。

名前	説明
[USB Port: vMedia] **set UsbPortVMedia**	仮想メディアデバイスがイネーブルかディセーブルか。次のいずれかになります。 • [Disabled]：vMedia デバイスをディセーブルにします。 • [Enabled]：vMedia デバイスをイネーブルにします。

[PCI Configuration] のパラメータ

名前	説明
[MMIO Above 4GB] **set MemoryMappedIOAbove4GB**	4GB を超える MMIO をイネーブルまたはディセーブルにするかどうか。次のいずれかになります。 • [Disabled]：サーバでは 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングしません。 • [Enabled]：サーバで 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングします。
[ASPM Support] **set ASPMSupport**	BIOS での ASPM （アクティブ電源状態管理）サポートのレベルを設定できます。次のいずれかになります。 • [Disabled]：ASPM サポートは、BIOS でディセーブルです。 • [Force L0s]：すべてのリンクを強制的に L0 スタンバイ（L0）状態にします。 • [Auto]：電力状態を CPU によって判別します。

名前	説明
[VGA Priority] **set VgaPriority**	システムに複数の VGA デバイスがある場合は、VGA グラフィックス デバイスのプライオリティを設定できます。次のいずれかになります。 • [Onboard]：プライオリティがオンボード VGA デバイスに与えられます。BIOS ポスト画面および OS ブートはオンボード VGA ポート経由で駆動されます。 • [Offboard]：プライオリティが PCIE グラフィックス アダプタに与えられます。BIOS ポスト画面および OS ブートは外部グラフィックス アダプタ ポート経由で駆動されます。 • [Onboard VGA Disabled][Onboard_VGA_Disabled]：プライオリティがPCIE グラフィックス アダプタに与えられ、オンボード VGA デバイスはディセーブルになります。 （注） オンボード VGA がディセーブルの場合、vKVM は機能しません。

[Serial Configuration] のパラメータ

名前	説明
[Console Redirection] **set ConsoleRedir**	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。 • [Enabled]：POST 中にシリアル ポート A でコンソール リダイレクションをイネーブルにします。

名前	説明
[Terminal Type] **set TerminalType**	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+]：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。
[Bits per second] **set BaudRate**	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] をディセーブルにした場合は、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。 • [9600]：9,600 ボー レートが使用されます。 • [19200]：19,200 ボー レートが使用されます。 • [38400]：38,400 ボー レートが使用されます。 • [57600]：57,600 ボー レートが使用されます。 • [115200]：115,200 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。
[Flow Control] **set FlowCtrl**	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）を使用すると、隠れた端末問題が原因で発生する可能性があるフレーム コリジョンを減らすことができます。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。 • Hardware_RTS/CTS：フロー制御に RTS/CTS 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
[Putty KeyPad] **set PuttyFunctionKeyPad**	PuTTY ファンクション キーおよびテンキーの最上段のキーのアクションを変更できます。次のいずれかになります。 • [VT100]：ファンクション キーが ESC OP ～ ESC O[を生成します。 • [LINUX]：Linux 仮想コンソールを模倣します。ファンクション キー F6 ～ F12 はデフォルト モードと同様に動作しますが、F1 ～ F5 は ESC [[A ～ ESC [[E を生成します。 • [XTERMR6]：ファンクション キー F5 ～ F12 がデフォルト モードと同様に動作します。ファンクション キー F1 ～ F4 が ESC OP ～ ESC OS を生成します。これはデジタル端末のキーパッドの上段によって生成されるシーケンスです。 • [SCO]：ファンクション キー F1 ～ F12 が ESC [M ～ ESC [X を生成します。ファンクションおよび Shift キーが ESC [Y ～ ESC [j を生成します。Ctrl およびファンクション キーが ESC [k ～ ESC [v を生成します。Shift、Ctrl およびファンクション キーが ESC [w ～ ESC [{ を生成します。 • [ESCN]：デフォルト モードです。ファンクション キーはデジタル端末の一般的な動作と一致します。ファンクション キーが ESC [11~ や ESC [12~ などのシーケンスを生成します。 • [VT400]：ファンクション キーがデフォルト モードと同様に動作します。テンキーの最上段のキーが ESC OP ～ ESC OS を生成します。
[Redirection After BIOS POST] **set RedirectionAfterPOST**	BIOS POST が完了し、OS ブートローダに制御が渡された後に、BIOS コンソール リダイレクションがアクティブであるかどうか。次のいずれかになります。 • [Always Enable][Always_Enable]：OSのブートおよび実行時に BIOS レガシー コンソール リダイレクションがアクティブになります。 • [Bootloader]：OS ブートローダに制御が渡される前に BIOS レガシー コンソール リダイレクションがディセーブルになります。

名前	説明
[Out-of-Band Mgmt Port] **set comSpcrEnable**	Windows 緊急管理サービスに使用可能な COM ポート 0 を設定することができます。このセットアップ オプションに基づいて ACPI SPCR テーブルが報告されます。次のいずれかになります。 • [Disabled]：Windows オペレーティング システムで使われる汎用ポートとして COM ポート 0 を設定します。 • [Enabled]：Windows 緊急管理サービス用のリモート管理ポートとして COM ポート 0 を設定します。

[LOM and PCIe Slots Configuration] のパラメータ

名前	説明
[All Onboard LOM Ports] **set AllLomPortControl**	すべての LOM ポートがイネーブルであるか、ディセーブルであるか。次のいずれかになります。 • [Disabled]：すべての LOM ポートがディセーブルです。 • [Enabled]：すべての LOM ポートがイネーブルです。
[LOM Port *n* OptionROM] **set LomOpromControlPort*n***	*n* で指定された LOM ポートでオプション ROM を使用できるかどうか。次のいずれかになります。 • [Disabled]：オプション ROM を LOM ポート *n* では使用できません。 • [Enabled]：LOM ポート *n* でオプション ROM を使用できます。 • [UEFI Only][UEFI_Only]：拡張スロット *n* をUEFI 用でのみ使用できます。 • [Legacy Only][Legacy_Only]：拡張スロット*n* をレガシー用でのみ使用できます。

名前	説明
[All PCIe Slots OptionROM] **set PcieOptionROMs**	PCIeカードのオプションROMをサーバが使用できるかどうか。次のいずれかになります。 • [Disabled]：すべての PCIe スロットの オプション ROM が使用できません。 • [Enabled]：すべての PCIe スロットの オプション ROM が使用可能です。 • [UEFI_Only]：スロット *n* のオプション ROM は UEFI にのみ使用できます。 • [Legacy_Only]：スロット *n* のオプション ROM はレガシーにのみ使用できます。
[PCIe Slot:*n* OptionROM] **set Slot-*n*-ROM**	PCIeカードのオプションROMをサーバが使用できるかどうか。次のいずれかになります。 • [Disabled]：スロット *n* のオプション ROM は使用できません。 • [Enabled]：スロット *n* のオプション ROM は使用可能です。 • [UEFI_Only]：スロット *n* のオプション ROM は UEFI にのみ使用できます。 • [Legacy_Only]：スロット *n* のオプション ROM はレガシーにのみ使用できます。
[PCIe Slot:*n* Link Speed] **PCIe Slot:*n*LinkSpeed**	このオプションを使用すると、PCIe スロット *n* に装着されているアダプタ カードの最大速度を制限できます。次のいずれかになります。 • [GEN1]：最大 2.5GT/s（ギガトランスファー/秒）までの速度が許可されます。 • [GEN2]：最大 5GT/s までの速度が許可されます。 • [GEN3]：最大 8GT/s までの速度が許可されます。 • [Disabled]：最大速度は制限されません。 たとえば、PCIe スロット 2 にある第 3 世代アダプタ カードの最大速度を、サポートされている 8GT/s の代わりに 5GT/s で実行する場合は、[PCIe Slot 2 Link Speed] を [GEN2] に設定します。この設定により、カードでサポートされている 8GT/s の最大速度が無視され、強制的に 5GT/s の最大速度で実行されます。

名前	説明
[CDN Support for LOM] **set CdnSupport**	イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [Disabled]：OS イーサネット ネットワーキング識別子には、デフォルトの規則に従って ETH0、ETH1 などの名前が付けられます。デフォルトで、CDN オプションはディセーブルになっています。 • [LOMS Only]：OS イーサネット ネットワーク識別子は、LOM ポート 0 や LOM ポート 1 のように物理的な LAN on Motherboard（LOM）のポート番号付けに基づく Consistent Device Naming（CDN）による名前が付けられます。 （注） CDN は LOM ポートに対しイネーブルであり、Windows 2012 または最新の OS のみで機能します。
[CDN Support for VIC] **set CdnEnable**	イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [Disabled]：VIC カードの CDN サポートがディセーブルになります。 • [Enabled]：VIC カードの CDN サポートがイネーブルになります。 （注） VIC カードの CDN サポートは、Windows 2012 または最新の OS でのみ機能します。

C22 および C24 サーバのサーバ管理 BIOS パラメータ

名前	説明
[FRB-2 Timer] **set FRB-2**	POST 中にシステムが停止した場合に、システムを回復するために Cisco IMC で FRB2 タイマーを使用するかどうか。次のいずれかになります。 • [Disabled]：FRB2 タイマーは使用されません。 • [Enabled]：POST 中に FRB2 タイマーが開始され、必要に応じてシステムの回復に使用されます。

名前	説明
[OS Watchdog Timer] **set OSBootWatchdogTimer**	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。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 **set OSBootWatchdogTimerTimeout** コマンドで指定された時間内にブートしない場合、Cisco IMC 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 Watchdog Timer Timeout] **set OSBootWatchdogTimerTimeOut**	OS が指定された時間内にブートしない場合、OS ウォッチドッグ タイマーの期限が切れ、システムはタイマーポリシーに基づいてアクションを実行します。次のいずれかになります。 • [5_Minutes]：OS ウォッチドッグ タイマーは、ブートが開始されてから 5 分後に期限が切れます。 • [10_Minutes]：OS ウォッチドッグ タイマーは、ブートが開始されてから 10 分後に期限が切れます。 • [15_Minutes]：OS ウォッチドッグ タイマーは、ブートが開始されてから 15 分後に期限が切れます。 • [20_Minutes]：OS ウォッチドッグ タイマーは、ブートが開始されてから 20 分後に期限が切れます。 （注） このオプションは [OS Boot Watchdog Timer] をイネーブルにした場合にのみ適用されます。

名前	説明
[OS Watchdog Timer Policy] **set OSBootWatchdogTimerPolicy**	ウォッチドッグ タイマーが切れた場合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 タイマーの期限が切れた場合、アクションは実行されません。 • Power_Down：OS のブート中にウォッチドッグ タイマーの期限が切れた場合、サーバの電源がオフになります。 • [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] をイネーブルにした場合にのみ適用されます。

C220 および C240 サーバ

C220 および C240 サーバの主要な BIOS パラメータ

名前	説明
[TPM Support] **set TPMAdminCtrl**	TPM（トラステッドプラットフォーム モジュール）は、主に暗号キーを使用する基本的なセキュリティ関連機能を提供するように設計されたマイクロチップです。このオプションを使用すると、システムの TPM セキュリティ デバイス サポートを制御できます。次のいずれかを指定できます。 • [Disabled]：サーバは TPM を使用しません。 • [Enabled]：サーバは TPM を使用します。 （注） 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。

C220 および C240 サーバの高度な BIOS パラメータ

[Processor Configuration] のパラメータ

名前	説明
[Intel Hyper-Threading Technology] **set IntelHyperThread**	プロセッサで Intel Hyper-Threading Technology 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。
[Number of Enabled Cores] **set CoreMultiProcessing**	サーバ上の 1 つ以上の物理コアをディセーブルにできます。次のいずれかになります。 • [All]：すべての物理コアをイネーブルにします。これにより、関連付けられている論理プロセッサ コアで Hyper Threading もイネーブルになります。 • [1] ～ [*n*]：サーバで実行できる物理プロセッサ コアの数を指定します。各物理コアには、論理コアが関連付けられています。 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
[Execute Disable] **set ExecuteDisable**	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ディセーブルにします。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。
[Intel VT] **set IntelVT**	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-d] **set IntelVTD**	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。

名前	説明
[Intel VT-d Coherency Support] **set CoherencySupport**	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。
[Intel VT-d ATS Support] **set ATS**	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。
[CPU Performance] **set CPUPerformance**	サーバの CPU パフォーマンス プロファイルを設定します。パフォーマンス プロファイルは次のオプションで構成されます。 • DCU Streamer Prefetcher • DCU IP Prefetcher • Hardware Prefetcher • Adjacent Cache-Line Prefetch 次のいずれかになります。 • [Enterprise]：すべてのオプションがイネーブルです。 • [High Throughput][High_Throughput]：DCUIP Prefetcher のみがイネーブルです。残りのオプションはディセーブルになります。 • [HPC]：すべてのオプションがイネーブルです。この設定はハイ パフォーマンス コンピューティングとも呼ばれます。 • [Custom]：パフォーマンス プロファイルのすべてのオプションをサーバの BIOS セットアップから設定できます。また、Hardware Prefetcher オプションと Adjacent Cache-Line Prefetch オプションは、下記のフィールドで設定できます。

名前	説明
[Hardware Prefetcher] **set HardwarePrefetch**	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。
[Adjacent Cache Line Prefetcher] **set AdjacentCacheLinePrefetch**	プロセッサで必要な行のみを取得するのではなく、偶数または奇数のペアのキャッシュ行を取得するかどうか。次のいずれかになります。 • [Disabled]：プロセッサで必要な行のみを取得します。 • [Enabled]：プロセッサで必要な行およびペアの行の両方を取得します。
[DCU Streamer Prefetch] **set DcuStreamerPrefetch**	プロセッサで DCU IP Prefetch メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [Disabled]：プロセッサはキャッシュ読み取り要求を予測しようとせず、明示的に要求された行のみを取得します。 • [Enabled]：DCU Prefetcher でキャッシュ読み取りパターンを分析し、必要と判断した場合にキャッシュ内の次の行を事前に取得します。
[DCU IP Prefetcher] **set DcuIpPrefetch**	プロセッサで DCU IP Prefetch メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [Disabled]：プロセッサでキャッシュ データをプリロードしません。 • [Enabled]：DCU IP Prefetcher で最も関連性が高いと判断されたデータを含む L1 キャッシュをプリロードします。

名前	説明
[Direct Cache Access Support] **set DirectCacheAccess**	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。
[Power Technology] **set CPUPowerManagement**	次のオプションの CPU 電源管理設定を指定できます。 • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 [Power Technology] は次のいずれかになります。 • [Custom]：前述の BIOS パラメータの個々の設定が使用されます。これらの BIOS パラメータのいずれかを変更する場合は、このオプションを選択する必要があります。 • [Disabled]：サーバで CPU 電源管理は実行されず、前述の BIOS パラメータの設定が無視されます。 • Energy_Efficient：前述の BIOS パラメータに最適な設定が決定され、これらのパラメータの個々の設定は無視されます。

名前	説明
[Enhanced Intel Speedstep Technology] **set EnhancedIntelSpeedStep**	プロセッサで Enhanced Intel SpeedStep Technology 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。 （注） CPUPowerManagement を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[Intel Turbo Boost Technology] **set IntelTurboBoostTech**	プロセッサで Intel Turbo Boost Technology 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。 （注） CPUPowerManagement を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。

名前	説明
[Processor Power State C6] **set ProcessorC6Report**	BIOS 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。OS はレポートを受信すると、プロセッサを電力量の少ない C6 状態に移行してエネルギー使用量を減らし、最適なプロセッサパフォーマンスを維持できます。次のいずれかになります。 • [Disabled]：BIOS から C6 レポートを送信しません。 • [Enabled]：BIOS から C6 レポートを送信し、OS がプロセッサを電力量の少ない C6 状態に移行できるようにします。 （注） CPUPowerManagement を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[Processor Power State C1 Enhanced] **set ProcessorC1EReport**	C1 ステートに入ったときに、CPU が最小周波数に移行するかどうか。次のいずれかになります。 • [Disabled]：CPU は C1 ステートでも引き続き最大周波数で動作します。 • [Enabled]：CPU は最小周波数に移行します。このオプションでは C1 ステートで節約される電力量が最大になります。
[Frequency Floor Override] **set CpuFreqFloor**	アイドル時に、CPU がターボを除く最大周波数よりも低い周波数にできるようにするかどうか。次のいずれかになります。 • [Disabled]：アイドル中に CPU をターボを除く最大周波数よりも低くできます。このオプションでは電力消費が低下しますが、システムパフォーマンスが低下する可能性があります。 • [Enabled]：アイドル中に CPU をターボを除く最大周波数よりも低くできません。このオプションではシステムパフォーマンスが向上しますが、消費電力が増加することがあります。

名前	説明
[P-STATE Coordination] **set PsdCoordType**	BIOS がオペレーティング システムに P-state サポート モデルを通信する方法を定義できます。Advanced Configuration and Power Interface（ACPI）仕様で定義される 3 つのモデルがあります。 • [HW_ALL]：プロセッサ ハードウェアが、依存性のある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。 • [SW_ALL]：OS Power Manager（OSPM）が、依存性のある論理プロセッサ（物理パッケージ内のすべての論理プロセッサ）間の P-state を調整します。すべての論理プロセッサで遷移を開始する必要があります。 • [SW_ANY]：OS Power Manager（OSPM）が、依存性のある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。ドメイン内の任意の論理プロセッサで遷移を開始する場合があります。 （注） CPUPowerManagement を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[Energy Performance] **set CpuEngPerfBias**	システム パフォーマンスまたはエネルギー効率がこのサーバで重要かどうかを判断できます。次のいずれかになります。 • Balanced_Energy • Balanced_Performance • Energy_Efficient • Performance

[Memory Configuration] のパラメータ

名前	説明
[Select Memory RAS] **set SelectMemoryRAS**	サーバに対するメモリの Reliability, Availability, and Serviceability（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。 • [Lockstep]：サーバ内の DIMM ペアが、同一のタイプ、サイズ、および構成を持ち、SMI チャネルにまたがって装着されている場合、ロックステップモードをイネーブルにして、メモリ アクセス遅延の最小化およびパフォーマンスの向上を実現できます。このオプションを使用した場合、[Mirroring] よりもシステム パフォーマンスが向上し、[Maximum Performance] よりも信頼性が向上しますが、[Mirroring] よりも信頼性が低く、[Maximum Performance] よりもシステム パフォーマンスは低下します。
[DRAM Clock Throttling] **set DRAMClockThrottling**	メモリ帯域幅と消費電力に関してシステム設定を調整できます。次のいずれかになります。 • [Balanced]：DRAM クロック スロットリングを低下させ、パフォーマンスと電力のバランスをとります。 • [Performance]：DRAM クロック スロットリングはディセーブルです。追加の電力をかけてメモリ帯域幅を増やします。 • [Energy Efficient][Energy_Efficient]：DRAMのクロック スロットリングを上げてエネルギー効率を向上させます。

名前	説明
[NUMA] **set NUMAOptimize**	BIOS で Non-Uniform Memory Access（NUMA）がサポートされているかどうか。次のいずれかになります。 • [Disabled]：BIOS で NUMA をサポートしません。 • [Enabled]：NUMA に対応したオペレーティング システムに必要な ACPI テーブルを BIOS に含めます。このオプションをイネーブルにした場合は、一部のプラットフォームでシステムのソケット間メモリインターリーブをディセーブルにする必要があります。
[Low Voltage DDR Mode] **set LvDDRMode**	低電圧と高周波数のどちらのメモリ動作をシステムで優先するか。次のいずれかになります。 • [Power Saving Mode][Power_Saving_Mode]：低電圧のメモリ動作が高周波数のメモリ動作よりも優先されます。 このモードでは、電圧を低く維持するために、メモリの周波数が低下する可能性があります。 • [Performance Mode][Performance_Mode]：高周波数の動作が低電圧の動作よりも優先されます。
[DRAM Refresh rate] **set DramRefreshRate**	DRAM セルをリフレッシュするレートを設定できます。次のいずれかになります。 • [1x]：DRAM セルは、64ms ごとにリフレッシュされます。 • [2x]：DRAM セルは、32ms ごとにリフレッシュされます。 • [3x]：DRAM セルは、21ms ごとにリフレッシュされます。 • [4x]：DRAM セルは、16ms ごとにリフレッシュされます。 • [Auto]： DRAM セルのリフレッシュ レートは、システム設定に基づき BIOS によって自動的に選択されます。これは、このパラメータに推奨される設定です。

名前	説明
[Channel Interleaving] **set ChannelInterLeave**	CPUがメモリ ブロックを分割して、データの隣接部分をインターリーブされたチャネル間に分散し、同時読み取り動作をイネーブルにするかどうか。次のいずれかになります。 • [Auto]：実行するインターリーブを、CPUが決定します。 • [1_Way]：何らかのチャネル インターリーブが使用されます。 • [2_Way] • [3_Way] • [4_Way]：最大のチャネル インターリーブが使用されます。
[Rank Interleaving] **set RankInterLeave**	1 つのランクを更新中に別のランクにアクセスできるよう、CPUがメモリの物理ランクをインターリーブするかどうか。次のいずれかになります。 • [Auto]：実行するインターリーブを、CPUが決定します。 • [1_Way]：何らかのランク インターリーブが使用されます。 • [2_Way] • [4_Way] • [8_Way]：最大量のランク インターリーブが使用されます。

名前	説明
[Patrol Scrub] **set PatrolScrub**	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] **set DemandScrub**	CPU または I/O が読み取りを要求した場合に検出された 1 ビットのメモリ エラーを、システムが修正するかどうか。次のいずれかになります。 • [Disabled]：1 ビット メモリ エラーは修正されません。 • [Enabled]：1 ビット メモリ エラーがメモリ内部で修正され、修正されたデータが、読み取り要求に対する応答に設定されます。
[Altitude] **set Altitude**	物理サーバがインストールされているおおよその海抜（m）。次のいずれかになります。 • [Auto]：物理的な高度を CPU によって判別します。 • [300_M]：サーバは、海抜約 300 m です。 • [900_M]：サーバは、海抜約 900 m です。 • [1500_M]：サーバは、海抜約 1500 m です。 • [3000_M]：サーバは、海抜約 3000 m です。

[QPI Configuration] のパラメータ

名前	説明
[QPI Link Frequency Select] **set QPILinkFrequency**	Intel QuickPath Interconnect（QPI）リンク周波数（ギガトランスファー/秒（GT/s）単位）。次のいずれかになります。 • [Auto]：QPI リンク周波数は CPU によって決定されます。 • [6.4_GT/s] • [7.2_GT/s] • [8.0_GT/s]
[QPI Snoop Mode] **set QpiSnoopMode**	Intel QuickPath Interconnect（QPI）スヌープ モード。次のいずれかになります。 • [Auto]：CPU は自動的に早期スヌープ モードとして認識します。 • [Early Snoop]：分散キャッシュ リング停止で、別のキャッシング エージェントにスヌープ プローブまたは要求を直接送信できます。このモードは、遅延が少なく、スレッド全体でデータ セットを共有しているためにキャッシュ間転送からメリットが得られるワークロードや NUMA 最適化されていないワークロードに最適です。 • [Home Snoop]：スヌープは、常に、メモリ コントローラのホーム エージェント（集中型リング停止）によって起動されます。このモードは、早期スヌープよりローカル遅延が多いですが、未処理トランザクションが増えた場合に予備のリソースを使用できます。 • [Home Directory Snoop]：ホーム ディレクトリは、プロセッサ内の HA と iMC の両方のロジックに実装されたオプション機能です。このディレクトリの目的は、スケーラブルなプラットフォームと 2S および 4S 構成でスヌープをリモート ソケットとノード コントローラにフィルタリングすることです。 • [Home Directory Snoop with OSB]：Opportunistic Snoop Broadcast（OSB）ディレクトリ モードでは、HA は、ディレクトリ情報が収集されてチェックされる前であっても、非常に負荷の軽い状況下で推測的ホーム スヌープ ブロードキャストを選択できます。

[Onboard Storage] のパラメータ

名前	説明
[Onboard SCU Storage Support] **set DisableSCU**	オンボード ソフトウェア RAID コントローラをサーバに使用できるかどうか。次のいずれかになります。 • [Disabled]：ソフトウェア RAID コントローラを使用できません。 • [Enabled]：ソフトウェア RAID コントローラを使用できます。
[Onboard SCU Storage SW Stack] **set PchScuOromSelect**	オンボード SCU ストレージ コントローラに関する Pre-boot ソフトウェア スタックを選択することができます。次のいずれかになります。 • Intel RSTe(1) • LSI SW RAID (0) （注） この設定パラメータは C220 サーバに関してのみ有効です。

[USB Configuration] のパラメータ

名前	説明
[Legacy USB Support] **set LegacyUSBSupport**	システムでレガシー USB デバイスをサポートするかどうか。次のいずれかになります。 • [Disabled]：USB デバイスは、EFI アプリケーションでのみ使用できます。 • [Enabled]：レガシー USB のサポートは常に使用できます。 • [Auto]：USB デバイスが接続されていない場合、レガシー USB のサポートがディセーブルになります。
[Port 60/64 Emulation] **set UsbEmul6064**	完全な USB キーボード レガシー サポートのために 60h/64h エミュレーションをシステムでサポートするかどうか。次のいずれかになります。 • [Disabled]：60h/64 エミュレーションはサポートされません。 • [Enabled]：60h/64 エミュレーションはサポートされます。 サーバで USB 非対応オペレーティング システムを使用する場合は、このオプションを選択する必要があります。

名前	説明
[All USB Devices] **set AllUsbDevices**	すべての物理および仮想USBデバイスがイネーブルであるか、ディセーブルであるか。次のいずれかになります。 • [Disabled]：すべての USB デバイスがディセーブルです。 • [Enabled]：すべての USB デバイスがイネーブルです。
[USB Port: Rear] **set UsbPortRear**	背面パネルのUSBデバイスがイネーブルかディセーブルか。次のいずれかになります。 • [Disabled]：背面パネルの USB ポートをディセーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [Enabled]：背面パネルの USB ポートをイネーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。
[USB Port: Front] **set UsbPortFront**	前面パネルのUSBデバイスがイネーブルかディセーブルか。次のいずれかになります。 • [Disabled]：前面パネルの USB ポートをディセーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [Enabled]：前面パネルの USB ポートをイネーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。
[USB Port: Internal] **set UsbPortInt**	内部USBデバイスがイネーブルかディセーブルか。次のいずれかになります。 • [Disabled]：内部 USB ポートをディセーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [Enabled]：内部 USB ポートをイネーブルにします。これらのポートに接続されるデバイスは、BIOSおよびオペレーティング システムによって検出されます。

名前	説明
[USB Port: KVM] **set UsbPortKVM**	KVM ポートがイネーブルかディセーブルか。次のいずれかになります。 • [Disabled]： KVM キーボードおよびマウス デバイスをディセーブルにします。キーボードとマウスは KVM ウィンドウで機能しなくなります。 • [Enabled]： KVM キーボードおよびマウス デバイスをイネーブルにします。
[USB Port: vMedia] **set UsbPortVMedia**	仮想メディア デバイスがイネーブルかディセーブルか。次のいずれかになります。 • [Disabled]：vMedia デバイスをディセーブルにします。 • [Enabled]：vMedia デバイスをイネーブルにします。
[USB Port: SD Card] **set UsbPortSdCard**	SD カード ドライブがイネーブルかディセーブルか。次のいずれかになります。 • [Disabled]：SD カード ドライブをディセーブルにします。SD カード ドライブは、BIOS およびオペレーティング システムによって検出されません。 • [Enabled]：SD カード ドライブをイネーブルにします。

[PCI Configuration] のパラメータ

名前	説明
[Memory Mapped I/O Above 4GB] **set MemoryMappedIOAbove4GB**	4GB を超える MMIO をイネーブルまたはディセーブルにするかどうか。次のいずれかになります。 • [Disabled]：サーバでは 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングしません。 • [Enabled]：サーバで 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングします。 （注） PCI デバイスが 64 ビット対応でも、レガシーなオプション ROM を使用する場合は、この設定をイネーブルにしても正しく機能しない場合があります。

名前	説明
[MMCFG BASE] **set MmcfgBaseSelect**	4GB 以内の PCIe アダプタの低ベース アドレスを設定します。次のいずれかになります。 • 1 GB • 2 GB • 2.5 GB • 3 GB • [Auto]：自動的に PCIe アダプタの低ベース アドレスを設定します。 （注） これは C240 サーバでのみ有効です。
[ASPM Support] **set ASPMSupport**	BIOS での ASPM （アクティブ電源状態管理）サポートのレベルを設定できます。次のいずれかになります。 • [Disabled]：ASPM サポートは、BIOS でディセーブルです。 • [Force L0s]：すべてのリンクを強制的に L0 スタンバイ（L0）状態にします。 • [Auto]：電力状態を CPU によって判別します。
[VGA Priority] **set VgaPriority**	システムに複数の VGA デバイスがある場合は、VGA グラフィックス デバイスのプライオリティを設定できます。次のいずれかになります。 • [Onboard]：プライオリティがオンボード VGA デバイスに与えられます。BIOS ポスト画面および OS ブートはオンボード VGA ポート経由で駆動されます。 • [Offboard]：プライオリティが PCIE グラフィックス アダプタに与えられます。BIOS ポスト画面および OS ブートは外部グラフィックス アダプタ ポート経由で駆動されます。 • [Onboard VGA Disabled][Onboard_VGA_Disabled]：プライオリティがPCIE グラフィックス アダプタに与えられ、オンボード VGA デバイスはディセーブルになります。 （注） オンボード VGA がディセーブルの場合、vKVM は機能しません。

[Serial Configuration] のパラメータ

名前	説明
[Out-of-Band Mgmt Port] **set comSpcrEnable**	Windows 緊急管理サービスに使用可能な COM ポート 0 を設定することができます。このセットアップ オプションに基づいて ACPI SPCR テーブルが報告されます。次のいずれかになります。 • [Disabled]：Windows オペレーティング システムで使われる汎用ポートとして COM ポート 0 を設定します。 • [Enabled]：Windows 緊急管理サービス用のリモート管理ポートとして COM ポート 0 を設定します。
[Console Redirection] **set ConsoleRedir**	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。 • [COM 0][COM_0]：POST中に COM ポート 0 でコンソール リダイレクションをイネーブルにします。 • [COM 1][COM_1]：POST中に COM ポート 1 でコンソール リダイレクションをイネーブルにします。
[Terminal Type] **set TerminalType**	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+]：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
[Bits per second] **set BaudRate**	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] をディセーブルにした場合は、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。 • [9600]：9,600 ボー レートが使用されます。 • [19200]：19,200 ボー レートが使用されます。 • [38400]：38,400 ボー レートが使用されます。 • [57600]：57,600 ボー レートが使用されます。 • [115200]：115,200 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。
[Flow Control] **set FlowCtrl**	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）を使用すると、隠れた端末問題が原因で発生する可能性があるフレーム コリジョンを減らすことができます。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。 • Hardware_RTS/CTS：フロー制御に RTS/CTS 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
[Putty KeyPad] **set PuttyFunctionKeyPad**	PuTTY ファンクション キーおよびテンキーの最上段のキーのアクションを変更できます。次のいずれかになります。 • [VT100]：ファンクション キーが ESC OP ～ ESC O[を生成します。 • [LINUX]：Linux 仮想コンソールを模倣します。ファンクション キー F6 ～ F12 はデフォルト モードと同様に動作しますが、F1 ～ F5 は ESC [[A ～ ESC [[E を生成します。 • [XTERMR6]：ファンクション キー F5 ～ F12 がデフォルト モードと同様に動作します。ファンクション キー F1 ～ F4 が ESC OP ～ ESC OS を生成します。これはデジタル端末のキーパッドの上段によって生成されるシーケンスです。 • [SCO]：ファンクション キー F1 ～ F12 が ESC [M ～ ESC [X を生成します。ファンクションおよび Shift キーが ESC [Y ～ ESC [j を生成します。Ctrl およびファンクション キーが ESC [k ～ ESC [v を生成します。Shift、Ctrl およびファンクション キーが ESC [w ～ ESC [{ を生成します。 • [ESCN]：デフォルト モードです。ファンクション キーはデジタル端末の一般的な動作と一致します。ファンクション キーが ESC [11~ や ESC [12~ などのシーケンスを生成します。 • [VT400]：ファンクション キーがデフォルト モードと同様に動作します。テンキーの最上段のキーが ESC OP ～ ESC OS を生成します。
[Redirection After BIOS POST] **set RedirectionAfterPOST**	BIOS POST が完了し、OS ブートローダに制御が渡された後に、BIOS コンソール リダイレクションがアクティブであるかどうか。次のいずれかになります。 • [Always Enable][Always_Enable]：OSのブートおよび実行時に BIOS レガシー コンソール リダイレクションがアクティブになります。 • [Bootloader]：OS ブートローダに制御が渡される前に BIOS レガシー コンソール リダイレクションがディセーブルになります。

[LOM and PCIe Slots Configuration] のパラメータ

名前	説明
[CDN Support for LOM] **set CdnSupport**	イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [Disabled]：OS イーサネット ネットワーキング識別子には、デフォルトの規則に従って ETH0、ETH1 などの名前が付けられます。デフォルトで、CDN オプションはディセーブルになっています。 • [LOMS Only]：OS イーサネット ネットワーク識別子は、LOM ポート 0 や LOM ポート 1 のように物理的な LAN on Motherboard（LOM）のポート番号付けに基づく Consistent Device Naming（CDN）による名前が付けられます。 （注） CDN は LOM ポートに対しイネーブルであり、Windows 2012 または最新の OS のみで機能します。
[CDN Support for VIC] **set CdnEnable**	イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [Disabled]：VIC カードの CDN サポートがディセーブルになります。 • [Enabled]：VIC カードの CDN サポートがイネーブルになります。 （注） VIC カードの CDN サポートは、Windows 2012 または最新の OS でのみ機能します。
[All Onboard LOM Ports] **set AllLomPortControl**	すべての LOM ポートがイネーブルであるか、ディセーブルであるか。次のいずれかになります。 • [Disabled]：すべての LOM ポートがディセーブルです。 • [Enabled]：すべての LOM ポートがイネーブルです。

名前	説明
[LOM Port *n* OptionROM] **set LomOpromControlPort*n***	*n* で指定された LOM ポートでオプション ROM を使用できるかどうか。次のいずれかになります。 • [Disabled]：スロット *n* のオプション ROM は使用できません。 • [Enabled]：スロット *n* のオプション ROM は使用可能です。 • [UEFI_Only]：スロット *n* のオプション ROM は UEFI にのみ使用できます。 • [Legacy_Only]：スロット *n* のオプション ROM はレガシーにのみ使用できます。
[All PCIe Slots OptionROM] **set PcieOptionROMs**	PCIe カードのオプション ROM をサーバが使用できるかどうか。次のいずれかになります。 • [Disabled]：スロット *n* のオプション ROM は使用できません。 • [Enabled]：スロット *n* のオプション ROM は使用可能です。 • [UEFI_Only]：スロット *n* のオプション ROM は UEFI にのみ使用できます。 • [Legacy_Only]：スロット *n* のオプション ROM はレガシーにのみ使用できます。
[PCIe Slot:*n* OptionROM] **set PcieSlot*n*OptionROM**	PCIe カードのオプション ROM をサーバが使用できるかどうか。次のいずれかになります。 • [Disabled]：スロット *n* のオプション ROM は使用できません。 • [Enabled]：スロット *n* のオプション ROM は使用可能です。 • [UEFI_Only]：スロット *n* のオプション ROM は UEFI にのみ使用できます。 • [Legacy_Only]：スロット *n* のオプション ROM はレガシーにのみ使用できます。

名前	説明
[PCIe Mezzanine OptionROM] **set PcieMezzOptionROM**	PCIe メザニン スロットの拡張 ROM をサーバで使用できるかどうか。次のいずれかになります。 • [Disabled]：スロット *n* のオプション ROM は使用できません。 • [Enabled]：スロット *n* のオプション ROM は使用可能です。 • [UEFI_Only]：スロット *n* のオプション ROM は UEFI にのみ使用できます。 • [Legacy_Only]：スロット *n* のオプション ROM はレガシーにのみ使用できます。
[PCIe Slot:*n* Link Speed] **PCIe Slot:*n*LinkSpeed**	このオプションを使用すると、PCIe スロット *n* に装着されているアダプタ カードの最大速度を制限できます。次のいずれかになります。 • [GEN1]：最大 2.5GT/s（ギガトランスファー/秒）までの速度が許可されます。 • [GEN2]：最大 5GT/s までの速度が許可されます。 • [GEN3]：最大 8GT/s までの速度が許可されます。 • [Disabled]：最大速度は制限されません。 たとえば、PCIe スロット 2 にある第 3 世代アダプタ カードの最大速度を、サポートされている 8GT/s の代わりに 5GT/s で実行する場合は、[PCIe Slot 2 Link Speed] を [GEN2] に設定します。この設定により、カードでサポートされている 8GT/s の最大速度が無視され、強制的に 5GT/s の最大速度で実行されます。

C220 および C240 サーバのサーバ管理 BIOS パラメータ

名前	説明
[FRB-2 Timer] **set FRB-2**	POST 中にシステムが停止した場合に、システムを回復するために Cisco IMC で FRB2 タイマーを使用するかどうか。次のいずれかになります。 • [Disabled]：FRB2 タイマーは使用されません。 • [Enabled]：POST 中に FRB2 タイマーが開始され、必要に応じてシステムの回復に使用されます。

名前	説明
[OS Watchdog Timer] **set OSBootWatchdogTimer**	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。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 **set OSBootWatchdogTimerTimeout** コマンドで指定された時間内にブートしない場合、Cisco IMC 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 Watchdog Timer Timeout] **set OSBootWatchdogTimerTimeOut**	OS が指定された時間内にブートしない場合、OS ウォッチドッグ タイマーの期限が切れ、システムはタイマーポリシーに基づいてアクションを実行します。次のいずれかになります。 • [5_Minutes]：OS ウォッチドッグ タイマーは、ブートが開始されてから 5 分後に期限が切れます。 • [10_Minutes]：OS ウォッチドッグ タイマーは、ブートが開始されてから 10 分後に期限が切れます。 • [15_Minutes]：OS ウォッチドッグ タイマーは、ブートが開始されてから 15 分後に期限が切れます。 • [20_Minutes]：OS ウォッチドッグ タイマーは、ブートが開始されてから 20 分後に期限が切れます。 （注） このオプションは [OS Boot Watchdog Timer] をイネーブルにした場合にのみ適用されます。

名前	説明
[OS Watchdog Timer Policy] **set OSBootWatchdogTimerPolicy**	ウォッチドッグタイマーが切れた場合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 タイマーの期限が切れた場合、アクションは実行されません。 • Power_Down：OS のブート中にウォッチドッグ タイマーの期限が切れた場合、サーバの電源がオフになります。 • [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] をイネーブルにした場合にのみ適用されます。

C460 サーバ

C460 サーバの主要な BIOS パラメータ

名前	説明
[POST Error Pause] **set POSTErrorPause**	POST 中にサーバで重大なエラーが発生した場合の処理。次のいずれかになります。 • [Enabled]：POST 中に重大なエラーが発生した場合、BIOS はサーバのブートを一時停止し、Error Manager を開きます。 • [Disabled]：BIOS はサーバのブートを続行します。
[Boot Option Retry] **set BootOptionRetry**	BIOS でユーザ入力を待機せずに非 EFI ベースのブート オプションを再試行するかどうか。次のいずれかになります。 • [Enabled]：ユーザ入力を待機せずに非 EFI ベースのブート オプションを継続的に再試行します。 • [Disabled]：ユーザ入力を待機してから非 EFI ベースのブート オプションを再試行します。

C460 サーバの高度な BIOS パラメータ

[Processor Configuration] のパラメータ

名前	説明
[Intel Turbo Boost Technology] **set IntelTurboBoostTech**	プロセッサで Intel Turbo Boost Technology 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。
[Enhanced Intel Speedstep Technology] **set EnhancedIntelSpeedStep**	プロセッサで Enhanced Intel SpeedStep Technology 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。

名前	説明
[Intel Hyper-Threading Technology] **set IntelHyperThread**	プロセッサで Intel Hyper-Threading Technology 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。
[Number of Enabled Cores] **set CoreMultiProcessing**	サーバ上の 1 つ以上の物理コアをディセーブルにできます。次のいずれかになります。 • [All]：すべての物理コアをイネーブルにします。これにより、関連付けられている論理プロセッサ コアで Hyper Threading もイネーブルになります。 • [1]～[*n*]：サーバで実行できる物理プロセッサ コアの数を指定します。各物理コアには、論理コアが関連付けられています。 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] **set ExecuteDisable**	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ディセーブルにします。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] **set IntelVT**	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] **set IntelVTD**	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] **set InterruptRemap**	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] **set CoherencySupport**	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] **set ATS**	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] **set PassThroughDMA**	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] **set DirectCacheAccess**	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] **set ProcessorC3Report**	BIOS 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。OS はレポートを受信すると、プロセッサを電力量の少ない C3 状態に移行してエネルギー使用量を減らし、最適なプロセッサ パフォーマンスを維持できます。次のいずれかになります。 • [Disabled]：BIOS から C3 レポートを送信しません。 • ACPI_C2：BIOS から ACPI C2 形式の C3 レポートを送信し、OS がプロセッサを電力量の少ない C3 状態に移行できるようにします。 • ACPI_C3：BIOS から ACPI C3 形式の C3 レポートを送信し、OS がプロセッサを電力量の少ない C3 状態に移行できるようにします。

名前	説明
[Processor C6 Report] **set ProcessorC6Report**	BIOS 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。OS はレポートを受信すると、プロセッサを電力量の少ない C6 状態に移行してエネルギー使用量を減らし、最適なプロセッサパフォーマンスを維持できます。次のいずれかになります。 • [Disabled]：BIOS から C6 レポートを送信しません。 • [Enabled]：BIOS から C6 レポートを送信し、OS がプロセッサを電力量の少ない C6 状態に移行できるようにします。

名前	説明
[Package C State Limit] **set PackageCStateLimit**	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。 • [C1 state][C1_state]：CPUのアイドル時に、システムは電力消費を少し減らします。 このオプションでは、必要な電力が C0 よりも少なく、サーバはすばやくハイ パフォーマンス モードに戻ることができます。 • [C3 state][C3_state]：CPUのアイドル時に、システムは C1 オプションの場合よりもさらに電力消費を減らします。この場合、必要な電力は C1 または C0 よりも少なくなりますが、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が少し長くなります。 • [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。このオプションを使用すると、C0、C1、または C3 よりも電力量が節約されますが、サーバがフルパワーに戻るまでに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
[CPU C State] **set ProcessorCcxEnable**	アイドル期間中にシステムが省電力モードに入ることができるかどうか。次のいずれかになります。 • [Disabled]：システムはアイドル時でもハイパフォーマンス状態のままになります。 • [Enabled]：システムは DIMM や CPU などのシステムコンポーネントへの電力を低減できます。電力低減量は、**set PackageCStateLimit** コマンドを使用して指定します。
[C1E] **set ProcessorC1eEnable**	C1 ステートに入ったときに、CPU が最小周波数に移行するかどうか。次のいずれかになります。 • [Disabled]：CPU は C1 ステートでも引き続き最大周波数で動作します。 • [Enabled]：CPU は最小周波数に移行します。このオプションでは C1 ステートで節約される電力量が最大になります。 （注） このオプションは、ProcessorCcxEnable がイネーブルの場合にのみ使用します。

[Memory Configuration] のパラメータ

名前	説明
[Select Memory RAS] **set SelectMemoryRAS**	サーバに対するメモリの Reliability, Availability, and Serviceability（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]：システムは、DIMM に障害が発生した場合に使用するためのメモリを予約します。障害が発生した場合、サーバは DIMM をオフラインにして、予約済みのメモリと置き換えます。このオプションは、ミラーリングよりも冗長性が低くなりますが、サーバで実行するプログラムに使用できるメモリの量が多くなります。

名前	説明
[NUMA Optimized] **set NUMAOptimize**	BIOS で Non-Uniform Memory Access（NUMA）がサポートされているかどうか。次のいずれかになります。 • [Disabled]：BIOS で NUMA をサポートしません。 • [Enabled]：NUMA に対応したオペレーティング システムに必要な ACPI テーブルを BIOS に含めます。このオプションをイネーブルにした場合は、一部のプラットフォームでシステムのソケット間メモリ インターリーブをディセーブルにする必要があります。
[Sparing Mode] **set SparingMode**	Cisco IMC で使用する予備モード。次のいずれかになります。 • [Rank Sparing][Rank_Sparing]：ランク レベルで予備メモリが割り当てられます。 • [DIMM Sparing]：DIMM レベルで予備メモリが割り当てられます。 （注） このオプションは、[Select Memory RAS][set SelectMemoryRAS]が [Sparing] に設定されている場合にのみ使用されます。
[Mirroring Mode] **set MirroringMode**	ミラーリングは Integrated Memory Controller（IMC）全体でサポートされ、1 つのメモリ ライザーが別のメモリ ライザーとミラーリングされます。次のいずれかになります。 • [Intersocket]：各 IMC は 2 つのソケット全体でミラーリングされます。 • [Intrasocket]：1 つの IMC が同じソケット内の別の IMC とミラーリングされます。 （注） このオプションは、SelectMemoryRAS が [Mirroring] に設定されている場合にのみ使用します。

名前	説明
[Patrol Scrub] **set PatrolScrub**	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。
[Patrol Scrub Interval] **set PatrolScrubDuration**	各パトロール スクラブによるメモリ アクセスの時間間隔を制御します。小さくすると、メモリのスクラブ頻度が高くなりますが、必要なメモリ帯域幅も多くなります。 5 ～ 23 の値を選択します。デフォルト値は 8 です。 （注） このオプションは、[Patrol Scrub] がイネーブルの場合にのみ使用します。
[CKE Low Policy] **set CkeLowPolicy**	DIMM の省電力モード ポリシーを制御します。次のいずれかになります。 • [Disabled]：DIMM は省電力モードに入りません。 • [Slow]：DIMM は省電力モードに入ることができますが、要件が厳しくなります。したがって、DIMM が省電力モードに入る頻度は低くなります。 • [Fast]：DIMM はできる限り頻繁に省電力モードに入ります。 • [Auto]：BIOS は DIMM の構成に基づいて DIMM が省電力モードに入るタイミングを制御します。

[Serial Port Configuration] のパラメータ

名前	説明
[Serial A Enable] **set Serial-PortA**	シリアル ポート A がイネーブルかディセーブルか。次のいずれかになります。 • [Disabled]：シリアル ポートはディセーブルになります。 • [Enabled]：シリアル ポートはイネーブルになります。

[USB Configuration] のパラメータ

名前	説明
[Make Device Non-Bootable] **set MakeUSBDeviceNonBootable**	サーバが USB デバイスからブートできるかどうか。次のいずれかになります。 • [Disabled]：サーバは USB デバイスからブートできます。 • [Enabled]：サーバは USB デバイスからブートできません。

[PCI Configuration] のパラメータ

名前	説明
[Memory Mapped I/O Above 4GB] **set MemoryMappedIOAbove4GB**	4GB を超える MMIO をイネーブルまたはディセーブルにするかどうか。次のいずれかになります。 • [Disabled]：サーバでは 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングしません。 • [Enabled]：サーバで 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングします。
[Onboard NIC *n* ROM] **set NIC-*n*-ROM**	*n* で指定されたオンボード NIC 用に組み込み PXE オプション ROM をシステムでロードするかどうか。次のいずれかになります。 • [Disabled]：PXE オプション ROM を NIC *n* に使用できません。 • [Enabled]：PXE オプション ROM を NIC *n* に使用できます。

名前	説明
[PCIe OptionROMs] **set PciOptRomsDisable**	PCIe カードのオプション ROM をサーバが使用できるかどうか。次のいずれかになります。 • [Disabled]：すべての PCIe スロットの オプション ROM が使用できません。 • [Enabled]：すべての PCIe スロットの オプション ROM が使用可能です。 • [UEFI_Only]：スロット *n* のオプション ROM は UEFI にのみ使用できます。 • [Legacy_Only]：スロット *n* のオプション ROM はレガシーにのみ使用できます。
[PCIe Slot *n* ROM] **set Slot-*n*-ROM**	PCIe カードのオプション ROM をサーバが使用できるかどうか。次のいずれかになります。 • [Disabled]：スロット *n* のオプション ROM は使用できません。 • [Enabled]：スロット *n* のオプション ROM は使用可能です。 • [UEFI_Only]：スロット *n* のオプション ROM は UEFI にのみ使用できます。 • [Legacy_Only]：スロット *n* のオプション ROM はレガシーにのみ使用できます。
[Onboard Gbit LOM] **set OnboardNic1**	サーバ上で Gbit LOM がイネーブルかディセーブルか。次のいずれかになります。 • [Disabled]：Gbit LOM を使用できません。 • [Enabled]：10Git LOM を使用できます。
[Onboard 10Gbit LOM] **set OnboardNic2**	サーバ上で 10Gbit LOM がイネーブルかディセーブルか。次のいずれかになります。 • [Disabled]：10Gbit LOM を使用できません。 • [Enabled]：10Gbit LOM を使用できます。

名前	説明
[Sriov] **set SrIov**	サーバ上で SR-IOV（Single Root I/O Virtualization）がイネーブルかディセーブルか。次のいずれかになります。 • [Disabled]：SR-IOV はディセーブルになります。 • [Enabled]：SR-IOV はイネーブルになります。 （注） デフォルトでは、SR-IOV オプションは C220、C240、C22 および C24 M3 サーバに対してイネーブルです。
[IOH Resource Allocation] **set IOHResource**	システム要件に応じて、IOH0 と IOH1 間で 16 ビット I/O リソースの 64 KB を分配できます。次のいずれかになります。 • [IOH0 24k IOH1 40k]：16 ビット I/O リソースの 24 KB を IOH0 に、16 ビット I/O リソースの 40 KB を IOH1 に割り当てます。 • [IOH0 32k IOH1 32k]：16 ビット I/O リソースの 32 KB を IOH0 に、16 ビット I/O リソースの 32 KB を IOH1 に割り当てます。 • [IOH0 40k IOH1 24k]：16 ビット I/O リソースの 40 KB を IOH0 に、16 ビット I/O リソースの 24 KB を IOH1 に割り当てます。 • [IOH0 48k IOH1 16k]：16 ビット I/O リソースの 48 KB を IOH0 に、16 ビット I/O リソースの 16 KB を IOH1 に割り当てます。 • [IOH0 56k IOH1 8k]：16 ビット I/O リソースの 56 KB を IOH0 に、16 ビット I/O リソースの 8 KB を IOH1 に割り当てます。

C460 サーバのサーバ管理 BIOS パラメータ

名前	説明
[Assert NMI on SERR] **set AssertNMIOnSERR**	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 をイネーブルにする場合は、この設定をイネーブルにする必要があります。
[Assert NMI on PERR] **set AssertNMIOnPERR**	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。
[Console Redirection] **set ConsoleRedir**	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中にシリアル ポート A でコンソール リダイレクションをイネーブルにします。 （注） このオプションをイネーブルにする場合は、POST 中に表示される Quiet Boot のロゴ画面もディセーブルにします。

名前	説明
[Flow Control] **set FlowCtrl**	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）を使用すると、隠れた端末問題が原因で発生する可能性があるフレーム コリジョンを減らすことができます。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。
[Baud Rate] **set BaudRate**	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] をディセーブルにした場合は、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。

名前	説明
[Terminal Type] **set TerminalType**	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。
[OS Boot Watchdog Timer Timeout] **set OSBootWatchdogTimerTimeOut**	OS が指定された時間内にブートしない場合、OS ウォッチドッグ タイマーの期限が切れ、システムはタイマーポリシーに基づいてアクションを実行します。次のいずれかになります。 • [5_Minutes]：OS ウォッチドッグ タイマーは、ブートが開始されてから 5 分後に期限が切れます。 • [10_Minutes]：OS ウォッチドッグ タイマーは、ブートが開始されてから 10 分後に期限が切れます。 • [15_Minutes]：OS ウォッチドッグ タイマーは、ブートが開始されてから 15 分後に期限が切れます。 • [20_Minutes]：OS ウォッチドッグ タイマーは、ブートが開始されてから 20 分後に期限が切れます。 （注） このオプションは [OS Boot Watchdog Timer] をイネーブルにした場合にのみ適用されます。
[OS Boot Watchdog Policy] **set OSBootWatchdogTimerPolicy**	ウォッチドッグ タイマーが切れた場合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。 • Power_Off：OS のブート中にウォッチドッグ タイマーの期限が切れた場合、サーバの電源がオフになります。 • [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] をイネーブルにした場合にのみ適用されます。

名前	説明
[Legacy OS Redirection] **set LegacyOSRedir**	シリアル ポートでレガシーなオペレーティング システム（DOS など）からのリダイレクションをイネーブルにするかどうか。次のいずれかになります。 • [Disabled]：コンソール リダイレクションがイネーブルになっているシリアルポートは、レガシーなオペレーティング システムから認識されません。 • [Enabled]：コンソール リダイレクションがイネーブルになっているシリアルポートは、レガシーなオペレーティング システムから認識できます。
[OS Boot Watchdog Timer] **set OSBootWatchdogTimer**	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。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 **set OSBootWatchdogTimerTimeout** コマンドで指定された時間内にブートしない場合、Cisco IMC 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。

C220 M4 および C240 M4 サーバ

C220M4 および C240M4 サーバの [Main] タブ

サーバ リブート オプション

[Save Changes] をクリックした後で変更内容を自動的に適用するには、[Reboot Host Immediately] チェックボックスをオンにします。Cisco IMC によってサーバがただちにリブートされて、変更が適用されます。

変更内容を後で適用するには、[Reboot Host Immediately] チェックボックスをオフにします。Cisco IMC によって変更が保存され、次回サーバがリブートするときに適用されます。

（注） 保留中の BIOS パラメータの変更がすでにある場合、Cisco IMC は、[変更を保存] をクリックしたときに、保存されている値を現在の設定で自動的に上書きします。

主要な BIOS パラメータ

名前	説明
[TPM Support] **set TPMAdminCtrl**	TPM（トラステッドプラットフォームモジュール）は、主に暗号キーを使用する基本的なセキュリティ関連機能を提供するように設計されたマイクロチップです。このオプションを使用すると、システムの TPM セキュリティ デバイス サポートを制御できます。次のいずれかを指定できます。 • [Disabled]：サーバは TPM を使用しません。 • [Enabled]：サーバは TPM を使用します。 （注） 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。

[BIOS Configuration] ダイアログボックスのボタン バー

重要 このダイアログ ボックスのボタンは、表示しているタブのパラメータのみでなく、使用可能なすべてのタブのすべての BIOS パラメータに影響します。

名前	説明
[Save Changes] ボタン	3 つのタブすべての BIOS パラメータの設定を保存し、ダイアログボックスを閉じます。 [Reboot Host Immediately] チェックボックスがオフの場合、サーバはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバが手動でリブートされるまで保存されます。
[Reset Values] ボタン	3 つのタブすべての BIOS パラメータの値を、このダイアログボックスを最初に開いたときに有効だった設定に復元します。
[Restore Defaults] ボタン	3 つのタブすべての BIOS パラメータをそのデフォルト値に設定します。
[Cancel] ボタン	変更を行わずにダイアログボックスを閉じます。

C220M4 および C240M4 サーバの [Advanced] タブ

サーバ リブート オプション

[Save Changes] をクリックした後で変更内容を自動的に適用するには、[Reboot Host Immediately] チェックボックスをオンにします。Cisco IMC によってサーバがただちにリブートされて、変更が適用されます。

変更内容を後で適用するには、[Reboot Host Immediately] チェックボックスをオフにします。Cisco IMC によって変更が保存され、次回サーバがリブートするときに適用されます。

（注） 保留中の BIOS パラメータの変更がすでにある場合、Cisco IMC は、[変更を保存] をクリックしたときに、保存されている値を現在の設定で自動的に上書きします。

[Processor Configuration] のパラメータ

名前	説明
[Intel Hyper-Threading Technology] **set IntelHyperThread**	プロセッサで Intel Hyper-Threading Technology 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] **set CoreMultiProcessing**	サーバ上の 1 つ以上の物理コアをディセーブルにできます。次のいずれかになります。 • [All]：すべての物理コアをイネーブルにします。これにより、関連付けられている論理プロセッサ コアで Hyper Threading もイネーブルになります。 • [1] ～ [*n*]：サーバで実行できる物理プロセッサ コアの数を指定します。各物理コアには、論理コアが関連付けられています。 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] **set ExecuteDisable**	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ディセーブルにします。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。
[Intel VT] **set IntelVT**	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。

名前	説明
[Intel VT-d] **set IntelVTD**	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] **set InterruptRemap**	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 PassThrough DMA] **set PassThroughDMA**	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。
[Intel VT-d Coherency Support] **set CoherencySupport**	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。
[Intel VT-d ATS Support] **set ATS**	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。

名前	説明
[CPU Performance] **set CPUPerformance**	サーバの CPU パフォーマンス プロファイルを設定します。パフォーマンス プロファイルは次のオプションで構成されます。 • DCU Streamer Prefetcher • DCU IP Prefetcher • Hardware Prefetcher • Adjacent Cache-Line Prefetch 次のいずれかになります。 • [Enterprise]：すべてのオプションがイネーブルです。 • [High Throughput][High_Throughput]：DCUIP Prefetcher のみがイネーブルです。残りのオプションはディセーブルになります。 • [HPC]：すべてのオプションがイネーブルです。 この設定はハイ パフォーマンス コンピューティングとも呼ばれます。 • [Custom]：パフォーマンス プロファイルのすべてのオプションをサーバの BIOS セットアップから設定できます。また、Hardware Prefetcher オプションと Adjacent Cache-Line Prefetch オプションは、下記のフィールドで設定できます。
[Hardware Prefetcher] **set HardwarePrefetch**	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。

名前	説明
[Adjacent Cache Line Prefetcher] **set AdjacentCacheLinePrefetch**	プロセッサで必要な行のみを取得するのではなく、偶数または奇数のペアのキャッシュ行を取得するかどうか。次のいずれかになります。 • [Disabled]：プロセッサで必要な行のみを取得します。 • [Enabled]：プロセッサで必要な行およびペアの行の両方を取得します。
[DCU Streamer Prefetch] **set DcuStreamerPrefetch**	プロセッサで DCU IP Prefetch メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [Disabled]：プロセッサはキャッシュ読み取り要求を予測しようとせず、明示的に要求された行のみを取得します。 • [Enabled]：DCU Prefetcher でキャッシュ読み取りパターンを分析し、必要と判断した場合にキャッシュ内の次の行を事前に取得します。
[DCU IP Prefetcher] **set DcuIpPrefetch**	プロセッサで DCU IP Prefetch メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [Disabled]：プロセッサでキャッシュ データをプリロードしません。 • [Enabled]：DCU IP Prefetcher で最も関連性が高いと判断されたデータを含む L1 キャッシュをプリロードします。
[Direct Cache Access Support] **set DirectCacheAccess**	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。

名前	説明
[Power Technology] **set CPUPowerManagement**	次のオプションの CPU 電源管理設定を指定できます。 • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 [Power Technology] は次のいずれかになります。 • [Custom]：前述の BIOS パラメータの個々の設定が使用されます。これらの BIOS パラメータのいずれかを変更する場合は、このオプションを選択する必要があります。 • [Disabled]：サーバで CPU 電源管理は実行されず、前述の BIOS パラメータの設定が無視されます。 • Energy_Efficient：前述の BIOS パラメータに最適な設定が決定され、これらのパラメータの個々の設定は無視されます。
[Enhanced Intel Speedstep Technology] **set EnhancedIntelSpeedStep**	プロセッサで Enhanced Intel SpeedStep Technology 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。 （注） CPUPowerManagement を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。

名前	説明
[Intel Turbo Boost Technology] **set IntelTurboBoostTech**	プロセッサで Intel Turbo Boost Technology 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。 （注） CPUPowerManagement を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[Processor C3 Report] **set ProcessorC3Report**	BIOS 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。OS はレポートを受信すると、プロセッサを電力量の少ない C3 状態に移行してエネルギー使用量を減らし、最適なプロセッサパフォーマンスを維持できます。次のいずれかになります。 • [Disabled]：BIOS は C3 レポートの送信を行いません。 • [Enabled]：BIOS から C3 レポートを送信し、OS がプロセッサを電力量の少ない C3 状態に移行できるようにします。 （注） CPUPowerManagement を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[Processor C6 Report] **set ProcessorC6Report**	BIOS 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。OS はレポートを受信すると、プロセッサを電力量の少ない C6 状態に移行してエネルギー使用量を減らし、最適なプロセッサパフォーマンスを維持できます。次のいずれかになります。 • [Disabled]：BIOS から C6 レポートを送信しません。 • [Enabled]：BIOS から C6 レポートを送信し、OS がプロセッサを電力量の少ない C6 状態に移行できるようにします。 （注） CPUPowerManagement を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。

名前	説明
[Processor Power State C1 Enhanced] **set ProcessorC1EReport**	C1 ステートに入ったときに、CPU が最小周波数に移行するかどうか。次のいずれかになります。 • [Disabled]：CPU は C1 ステートでも引き続き最大周波数で動作します。 • [Enabled]：CPU は最小周波数に移行します。このオプションでは C1 ステートで節約される電力量が最大になります。
[P-STATE Coordination] **set PsdCoordType**	BIOS がオペレーティング システムに P-state サポート モデルを通信する方法を定義できます。Advanced Configuration and Power Interface（ACPI）仕様で定義される 3 つのモデルがあります。 • [HW_ALL]：プロセッサ ハードウェアが、依存性のある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。 • [SW_ALL]：OS Power Manager（OSPM）が、依存性のある論理プロセッサ（物理パッケージ内のすべての論理プロセッサ）間の P-state を調整します。すべての論理プロセッサで遷移を開始する必要があります。 • [SW_ANY]：OS Power Manager（OSPM）が、依存性のある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。ドメイン内の任意の論理プロセッサで遷移を開始する場合があります。 （注） CPUPowerManagement を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[Energy Performance Tuning] **set PwrPerfTuning**	エネルギー効率のバイアス調整のために BIOS またはオペレーティング システムを選択できます。次のいずれかになります。 • [OS]：エネルギー効率の調整のために OS を選択します。 • [BIOS]：エネルギー効率の調整のために BIOS を選択します。

名前	説明
[Energy Performance] **set CpuEngPerfBias**	システム パフォーマンスまたはエネルギー効率がこのサーバで重要かどうかを判断できます。次のいずれかになります。 • Balanced_Energy • Balanced_Performance • Energy_Efficient • Performance
[Package C State Limit] **set PackageCStateLimit**	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。 • [C1 state][C1_state]：CPUのアイドル時に、システムは電力消費を少し減らします。 このオプションでは、必要な電力が C0 よりも少なく、サーバはすばやくハイ パフォーマンス モードに戻ることができます。 • [C3 state][C3_state]：CPUのアイドル時に、システムは C1 オプションの場合よりもさらに電力消費を減らします。この場合、必要な電力は C1 または C0 よりも少なくなりますが、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が少し長くなります。 • [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。このオプションを使用すると、C0、C1、または C3 よりも電力量が節約されますが、サーバがフルパワーに戻るまでに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。

名前	説明
[Extended APIC] **set LocalX2Apic**	拡張 APIC サポートをイネーブルまたはディセーブルにできます。次のいずれかになります。 • [XAPIC]：APIC サポートをイネーブルにします。 • [X2APIC]：APIC をイネーブルにして、Intel VT-d と Interrupt Remapping もイネーブルにします。
[Workload Configuration] **set WorkLdConfig**	ワークロードの特性を最適化するようにパラメータを設定できます。次のいずれかになります。 • [Balanced]：バランスをとる最適化オプションを選択します。 • [I/O Sensitive]：I/O を優先する最適化オプションを選択します。 （注） ワークロード構成は [Balanced] に設定することをお勧めします。

[Memory Configuration] のパラメータ

名前	説明
[Select Memory RAS] **set SelectMemoryRAS**	サーバに対するメモリの Reliability, Availability, and Serviceability（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。 • [Lockstep]：サーバ内の DIMM ペアが、同一のタイプ、サイズ、および構成を持ち、SMI チャネルにまたがって装着されている場合、ロックステップモードをイネーブルにして、メモリ アクセス遅延の最小化およびパフォーマンスの向上を実現できます。このオプションを使用した場合、[Mirroring] よりもシステム パフォーマンスが向上し、[Maximum Performance] よりも信頼性が向上しますが、[Mirroring] よりも信頼性が低く、[Maximum Performance] よりもシステム パフォーマンスは低下します。

名前	説明
[NUMA] **set NUMAOptimize**	BIOS で Non-Uniform Memory Access（NUMA）がサポートされているかどうか。次のいずれかになります。 • [Disabled]：BIOS で NUMA をサポートしません。 • [Enabled]：NUMA に対応したオペレーティング システムに必要な ACPI テーブルを BIOS に含めます。このオプションをイネーブルにした場合は、一部のプラットフォームでシステムのソケット間メモリ インターリーブをディセーブルにする必要があります。
[Channel Interleaving] **set ChannelInterLeave**	CPU がメモリ ブロックを分割して、データの隣接部分をインターリーブされたチャネル間に分散し、同時読み取り動作をイネーブルにするかどうか。次のいずれかになります。 • [Auto]：実行するインターリーブを、CPU が決定します。 • [1_Way]：何らかのチャネル インターリーブが使用されます。 • [2_Way] • [3_Way] • [4_Way]：最大のチャネル インターリーブが使用されます。
[Rank Interleaving] **set RankInterLeave**	1 つのランクを更新中に別のランクにアクセスできるよう、CPU がメモリの物理ランクをインターリーブするかどうか。次のいずれかになります。 • [Auto]：実行するインターリーブを、CPU が決定します。 • [1_Way]：何らかのランク インターリーブが使用されます。 • [2_Way] • [4_Way] • [8_Way]：最大量のランク インターリーブが使用されます。

名前	説明
[Patrol Scrub] **set PatrolScrub**	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] **set DemandScrub**	CPU または I/O が読み取りを要求した場合に検出された 1 ビットのメモリ エラーを、システムが修正するかどうか。次のいずれかになります。 • [Disabled]：1 ビット メモリ エラーは修正されません。 • [Enabled]：1 ビット メモリ エラーがメモリ内部で修正され、修正されたデータが、読み取り要求に対する応答に設定されます。
[Altitude] **set Altitude**	物理サーバがインストールされているおおよその海抜（m）。次のいずれかになります。 • [Auto]：物理的な高度を CPU によって判別します。 • [300_M]：サーバは、海抜約 300 m です。 • [900_M]：サーバは、海抜約 900 m です。 • [1500_M]：サーバは、海抜約 1500 m です。 • [3000_M]：サーバは、海抜約 3000 m です。

[QPI Configuration] のパラメータ

名前	説明
[QPI Link Frequency Select] **set QPILinkFrequency**	Intel QuickPath Interconnect（QPI）リンク周波数（ギガトランスファー/秒（GT/s）単位）。次のいずれかになります。 • [Auto]：QPI リンク周波数は CPU によって決定されます。 • [6.4_GT/s] • [7.2_GT/s] • [8.0_GT/s]
[QPI Snoop Mode] **set QpiSnoopMode**	Intel QuickPath Interconnect（QPI）スヌープ モード。次のいずれかになります。 • [Home Snoop]：スヌープは、常に、メモリ コントローラのホーム エージェント（集中型リング停止）によって起動されます。このモードは、早期スヌープよりローカル遅延が多いですが、未処理トランザクションが増えた場合に予備のリソースを使用できます。 • [Cluster on Die]：クラスタ オン ダイが有効になります。有効な LLC が 2 つの部分に分割され、それぞれに個別のキャッシュ エージェントが設定されます。これにより、一部のワークロードのパフォーマンスが向上します。このモードは、コアが 10 以上のプロセッサでのみ使用できます。高度にNUMA最適化されたワークロードに最適なモードです。 • [Early Snoop]：分散キャッシュ リング停止で、別のキャッシング エージェントにスヌープ プローブまたは要求を直接送信できます。このモードは、遅延が少なく、スレッド全体でデータ セットを共有しているためにキャッシュ間転送からメリットが得られるワークロードや NUMA 最適化されていないワークロードに最適です。

[USB Configuration] のパラメータ

名前	説明
[Legacy USB Support] **set LegacyUSBSupport**	システムでレガシーUSBデバイスをサポートするかどうか。次のいずれかになります。 • [Disabled]：USBデバイスは、EFIアプリケーションでのみ使用できます。 • [Enabled]：レガシーUSBのサポートは常に使用できます。 • [Auto]：USB デバイスが接続されていない場合、レガシー USB のサポートがディセーブルになります。
[Port 60/64 Emulation] **set UsbEmul6064**	完全な USB キーボード レガシー サポートのために 60h/64h エミュレーションをシステムでサポートするかどうか。次のいずれかになります。 • [Disabled]：60h/64 エミュレーションはサポートされません。 • [Enabled]：60h/64エミュレーションはサポートされます。 サーバで USB 非対応オペレーティング システムを使用する場合は、このオプションを選択する必要があります。
[xHCI Mode] **set PchUsb30Mode**	xHCI コントローラのレガシー サポートを有効または無効にします。次のいずれかになります。 • [Disabled]：xHCI コントローラのレガシー サポートが無効になります。 • [Enabled]：xHCI コントローラのレガシー サポートが有効になります。

[PCI Configuration] のパラメータ

名前	説明
[Memory Mapped I/O Above 4GB] **set MemoryMappedIOAbove4GB**	4GB を超える MMIO をイネーブルまたはディセーブルにするかどうか。次のいずれかになります。 • [Disabled]：サーバでは 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングしません。 • [Enabled]：サーバで 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングします。 （注） PCI デバイスが 64 ビット対応でも、レガシーなオプション ROM を使用する場合は、この設定をイネーブルにしても正しく機能しない場合があります。
[Sriov] **set SrIov**	サーバ上で SR-IOV（Single Root I/O Virtualization）がイネーブルかディセーブルか。次のいずれかになります。 • [Disabled]：SR-IOV はディセーブルになります。 • [Enabled]：SR-IOV はイネーブルになります。

[Serial Configuration] のパラメータ

名前	説明
[Out-of-Band Mgmt Port] **set comSpcrEnable**	Windows 緊急管理サービスに使用可能な COM ポート 0 を設定することができます。このセットアップ オプションに基づいて ACPI SPCR テーブルが報告されます。次のいずれかになります。 • [Disabled]：Windows オペレーティング システムで使われる汎用ポートとして COM ポート 0 を設定します。 • [Enabled]：Windows 緊急管理サービス用のリモート管理ポートとして COM ポート 0 を設定します。

名前	説明
[Console Redirection] **set ConsoleRedir**	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。 • [COM 0][COM_0]：POST中に COM ポート 0 でコンソール リダイレクションをイネーブルにします。 • [COM 1][COM_1]：POST中に COM ポート 1 でコンソール リダイレクションをイネーブルにします。
[Terminal Type] **set TerminalType**	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+]：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。
[Bits per second] **set BaudRate**	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] をディセーブルにした場合は、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。 • [9600]：9,600 ボー レートが使用されます。 • [19200]：19,200 ボー レートが使用されます。 • [38400]：38,400 ボー レートが使用されます。 • [57600]：57,600 ボー レートが使用されます。 • [115200]：115,200 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。

名前	説明
[Flow Control] **set FlowCtrl**	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）を使用すると、隠れた端末問題が原因で発生する可能性があるフレーム コリジョンを減らすことができます。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。 • Hardware_RTS/CTS：フロー制御に RTS/CTS 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。
[Putty KeyPad] **set PuttyFunctionKeyPad**	PuTTY ファンクション キーおよびテンキーの最上段のキーのアクションを変更できます。次のいずれかになります。 • [VT100]：ファンクション キーが ESC OP ～ ESC O[を生成します。 • [LINUX]：Linux 仮想コンソールを模倣します。ファンクション キー F6 ～ F12 はデフォルト モードと同様に動作しますが、F1 ～ F5 は ESC [[A ～ ESC [[E を生成します。 • [XTERMR6]：ファンクション キー F5 ～ F12 がデフォルト モードと同様に動作します。ファンクション キー F1 ～ F4 が ESC OP ～ ESC OS を生成します。これはデジタル端末のキーパッドの上段によって生成されるシーケンスです。 • [SCO]：ファンクション キー F1 ～ F12 が ESC [M ～ ESC [X を生成します。ファンクションおよび Shift キーが ESC [Y ～ ESC [j を生成します。Ctrl およびファンクション キーが ESC [k ～ ESC [v を生成します。Shift、Ctrl およびファンクション キーが ESC [w ～ ESC [{ を生成します。 • [ESCN]：デフォルト モードです。ファンクション キーはデジタル端末の一般的な動作と一致します。ファンクション キーが ESC [11~ や ESC [12~ などのシーケンスを生成します。 • [VT400]：ファンクション キーがデフォルト モードと同様に動作します。テンキーの最上段のキーが ESC OP ～ ESC OS を生成します。

名前	説明
[Redirection After BIOS POST] **set RedirectionAfterPOST**	BIOS POST が完了し、OS ブートローダに制御が渡された後に、BIOS コンソール リダイレクションがアクティブであるかどうか。次のいずれかになります。 • [Always Enable][Always_Enable]：OSのブートおよび実行時にBIOS レガシー コンソール リダイレクションがアクティブになります。 • [Bootloader]：OS ブートローダに制御が渡される前に BIOS レガシー コンソール リダイレクションがディセーブルになります。

[LOM and PCIe Slots Configuration] のパラメータ

名前	説明
[CDN Support for VIC] **set CdnEnable**	イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [Disabled]：VIC カードの CDN サポートがディセーブルになります。 • [Enabled]：VIC カードの CDN サポートがイネーブルになります。 （注） VIC カードの CDN サポートは、Windows 2012 または最新の OS でのみ機能します。
[PCI ROM CLP] **set PciRomClp**	PCI ROM Command Line Protocol（CLP）は、カード上の iSCSI や PxE などのさまざまなオプション ROM の実行を制御します。デフォルト設定は、ディセーブルです。 • [Enabled]：ポートごとに個別に、iSCSI や PxE などのさまざまなオプション ROM の実行を制御できるようにします。 • [Disabled]：デフォルト オプションです。異なるオプション ROM は選択できません。デフォルト オプション ROM は PCI 列挙中に実行されます。

名前	説明
[PCH Performance Mode] **set SataModeSelect**	このオプションでは、PCH SATA モードを選択することができます。次のいずれかになります。 • [AHCI]：SATA コントローラと sSATA コントローラの両方を AHCI モードに設定します。 • [Disabled]：SATA コントローラと sSATA コントローラを無効にします。 • [LSI SW Raid]：SATA コントローラと sSATA コントローラを LSI SW Raid の raid モードに設定します。
[All Onboard LOM Ports] **set AllLomPortControl**	すべての LOM ポートがイネーブルであるか、ディセーブルであるか。次のいずれかになります。 • [Disabled]：すべての LOM ポートがディセーブルです。 • [Enabled]：すべての LOM ポートがイネーブルです。
[LOM Port *n* OptionROM] **set LomOpromControlPort*n***	*n* で指定された LOM ポートでオプション ROM を使用できるかどうか。次のいずれかになります。 • [Disabled]：スロット *n* のオプション ROM は使用できません。 • [Enabled]：スロット *n* のオプション ROM は使用可能です。 • [UEFI_Only]：スロット *n* のオプション ROM は UEFI にのみ使用できます。 • [Legacy_Only]：スロット *n* のオプション ROM はレガシーにのみ使用できます。
[All PCIe Slots OptionROM] **set PcieOptionROMs**	PCIe カードのオプション ROM をサーバが使用できるかどうか。次のいずれかになります。 • [Disabled]：スロット *n* のオプション ROM は使用できません。 • [Enabled]：スロット *n* のオプション ROM は使用可能です。 • [UEFI_Only]：スロット *n* のオプション ROM は UEFI にのみ使用できます。 • [Legacy_Only]：スロット *n* のオプション ROM はレガシーにのみ使用できます。

名前	説明
[PCIe Slot:*n* OptionROM] **set PcieSlot*n*OptionROM**	PCIe カードのオプション ROM をサーバが使用できるかどうか。次のいずれかになります。 • [Disabled]：スロット *n* のオプション ROM は使用できません。 • [Enabled]：スロット *n* のオプション ROM は使用可能です。 • [UEFI_Only]：スロット *n* のオプション ROM は UEFI にのみ使用できます。 • [Legacy_Only]：スロット *n* のオプション ROM はレガシーにのみ使用できます。
[PCIe Slot:MLOM OptionROM] **set PcieSlotMLOMOptionROM**	このオプションでは、MLOM スロットに接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [Enabled]：レガシーおよび UEFI オプション ROM の両方を実行します。 • [Disabled]：レガシーおよび UEFI オプション ROM の両方を実行しません。 • [UEFI Only]：UEFI オプション ROM だけを実行します。 • [Legacy Only]：レガシー オプション ROM だけを実行します。
[PCIe Slot:HBA OptionROM] **set PcieSlotHBAOptionROM**	このオプションでは、HBA スロットに接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [Enabled]：レガシーおよび UEFI オプション ROM の両方を実行します。 • [Disabled]：レガシーおよび UEFI オプション ROM の両方を実行しません。 • [UEFI Only]：UEFI オプション ROM だけを実行します。 • [Legacy Only]：レガシー オプション ROM だけを実行します。

名前	説明
[PCIe Slot:N1 OptionROM] **set PcieSlotN1OptionROM**	このオプションでは、SSD:NVMe1 スロットに接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [Enabled]：レガシーおよび UEFI オプション ROM の両方を実行します。 • [Disabled]：レガシーおよび UEFI オプション ROM の両方を実行しません。 • [UEFI Only]：UEFI オプション ROM だけを実行します。 • [Legacy Only]：レガシー オプション ROM だけを実行します。
[PCIe Slot:N2 OptionROM] **set PcieSlotN2OptionROM**	このオプションでは、SSD:NVMe2 スロットに接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [Enabled]：レガシーおよび UEFI オプション ROM の両方を実行します。 • [Disabled]：レガシーおよび UEFI オプション ROM の両方を実行しません。 • [UEFI Only]：UEFI オプション ROM だけを実行します。 • [Legacy Only]：レガシー オプション ROM だけを実行します。
[PCIe Slot:N2 OptionROM] **set PcieSlotN2OptionROM**	このオプションでは、SSD:NVMe2 スロットに接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [Enabled]：レガシーおよび UEFI オプション ROM の両方を実行します。 • [Disabled]：レガシーおよび UEFI オプション ROM の両方を実行しません。 • [UEFI Only]：UEFI オプション ROM だけを実行します。 • [Legacy Only]：レガシー オプション ROM だけを実行します。

名前	説明
[PCIe Slot:HBA Link Speed] **PCIe SlotHBALinkSpeed**	このオプションを使用すると、PCIe HBA スロットに装着されているアダプタ カードの最大速度を制限できます。次のいずれかになります。 • [Auto]：システムは許容最大速度を選択します。 • [GEN1]：最大 2.5GT/s（ギガトランスファー/秒）までの速度が許可されます。 • [GEN2]：最大 5GT/s までの速度が許可されます。 • [GEN3]：最大 8GT/s までの速度が許可されます。 • [Disabled]：最大速度は制限されません。

[BIOS Configuration] ダイアログボックスのボタン バー

重要 このダイアログ ボックスのボタンは、表示しているタブのパラメータのみでなく、使用可能なすべてのタブのすべての BIOS パラメータに影響します。

名前	説明
[Save Changes] ボタン	3 つのタブすべての BIOS パラメータの設定を保存し、ダイアログボックスを閉じます。 [Reboot Host Immediately] チェックボックスがオフの場合、サーバはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバが手動でリブートされるまで保存されます。
[Reset Values] ボタン	3 つのタブすべての BIOS パラメータの値を、このダイアログボックスを最初に開いたときに有効だった設定に復元します。
[Restore Defaults] ボタン	3 つのタブすべての BIOS パラメータをそのデフォルト値に設定します。
[Cancel] ボタン	変更を行わずにダイアログボックスを閉じます。

C220M4 および C240M4 サーバの [Server Management] タブ

サーバ リブート オプション

[Save Changes] をクリックした後で変更内容を自動的に適用するには、[Reboot Host Immediately] チェックボックスをオンにします。Cisco IMC によってサーバがただちにリブートされて、変更が適用されます。

変更内容を後で適用するには、[Reboot Host Immediately] チェックボックスをオフにします。Cisco IMC によって変更が保存され、次回サーバがリブートするときに適用されます。

（注） 保留中の BIOS パラメータの変更がすでにある場合、Cisco IMC は、[変更を保存] をクリックしたときに、保存されている値を現在の設定で自動的に上書きします。

サーバ管理 BIOS パラメータ

名前	説明
[FRB-2 Timer] **set FRB-2**	POST 中にシステムが停止した場合に、システムを回復するために Cisco IMC で FRB2 タイマーを使用するかどうか。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。
[OS Watchdog Timer] **set OSBootWatchdogTimer**	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。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 **set OSBootWatchdogTimerTimeout** コマンドで指定された時間内にブートしない場合、Cisco IMC 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。

名前	説明
[OS Watchdog Timer Timeout] **set OSBootWatchdogTimerTimeOut**	OS が指定された時間内にブートしない場合、OS ウォッチドッグ タイマーの期限が切れ、システムはタイマーポリシーに基づいてアクションを実行します。次のいずれかになります。 • [5_Minutes]：OS ウォッチドッグ タイマーは、ブートが開始されてから 5 分後に期限が切れます。 • [10_Minutes]：OS ウォッチドッグ タイマーは、ブートが開始されてから 10 分後に期限が切れます。 • [15_Minutes]：OS ウォッチドッグ タイマーは、ブートが開始されてから 15 分後に期限が切れます。 • [20_Minutes]：OS ウォッチドッグ タイマーは、ブートが開始されてから 20 分後に期限が切れます。 （注） このオプションは [OS Boot Watchdog Timer] をイネーブルにした場合にのみ適用されます。
[OS Watchdog Timer Policy] **set OSBootWatchdogTimerPolicy**	ウォッチドッグ タイマーが切れた場合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 タイマーの期限が切れた場合、アクションは実行されません。 • Power_Down：OS のブート中にウォッチドッグ タイマーの期限が切れた場合、サーバの電源がオフになります。 • [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] をイネーブルにした場合にのみ適用されます。

[BIOS Configuration] ダイアログボックスのボタン バー

重要 このダイアログ ボックスのボタンは、表示しているタブのパラメータのみでなく、使用可能なすべてのタブのすべての BIOS パラメータに影響します。

名前	説明
[Save Changes] ボタン	3 つのタブすべての BIOS パラメータの設定を保存し、ダイアログボックスを閉じます。 [Reboot Host Immediately] チェックボックスがオフの場合、サーバはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバが手動でリブートされるまで保存されます。
[Reset Values] ボタン	3 つのタブすべての BIOS パラメータの値を、このダイアログボックスを最初に開いたときに有効だった設定に復元します。
[Restore Defaults] ボタン	3 つのタブすべての BIOS パラメータをそのデフォルト値に設定します。
[Cancel] ボタン	変更を行わずにダイアログボックスを閉じます。

C3160 サーバ

C3160 サーバの主要な BIOS パラメータ

主要な BIOS パラメータ

名前	説明
[TPM Support] **set TPMAdminCtrl**	TPM（トラステッドプラットフォームモジュール）は、主に暗号キーを使用する基本的なセキュリティ関連機能を提供するように設計されたマイクロチップです。このオプションを使用すると、システムの TPM セキュリティ デバイス サポートを制御できます。次のいずれかを指定できます。 • [Disabled]：サーバは TPM を使用しません。 • [Enabled]：サーバは TPM を使用します。 （注） 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。

C3160 サーバの高度な BIOS パラメータ

[Processor Configuration] のパラメータ

名前	説明
[Intel Hyper-Threading Technology] **set IntelHyperThread**	プロセッサで Intel Hyper-Threading Technology 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。
[Number of Enabled Cores] **set CoreMultiProcessing**	サーバ上の 1 つ以上の物理コアをディセーブルにできます。次のいずれかになります。 • [All]：すべての物理コアをイネーブルにします。これにより、関連付けられている論理プロセッサ コアで Hyper Threading もイネーブルになります。 • [1] ～ [*n*]：サーバで実行できる物理プロセッサ コアの数を指定します。各物理コアには、論理コアが関連付けられています。 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
[Execute Disable] **set ExecuteDisable**	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ディセーブルにします。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。
[Intel VT] **set IntelVT**	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-d] **set IntelVTD**	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。

名前	説明
[Intel VT-d Coherency Support] **set CoherencySupport**	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。
[Intel VT-d ATS Support] **set ATS**	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。
[CPU Performance] **set CPUPerformance**	サーバの CPU パフォーマンス プロファイルを設定します。パフォーマンス プロファイルは次のオプションで構成されます。 • DCU Streamer Prefetcher • DCU IP Prefetcher • Hardware Prefetcher • Adjacent Cache-Line Prefetch 次のいずれかになります。 • [Enterprise]：すべてのオプションがイネーブルです。 • [High Throughput][High_Throughput]：DCUIP Prefetcher のみがイネーブルです。残りのオプションはディセーブルになります。 • [HPC]：すべてのオプションがイネーブルです。 この設定はハイ パフォーマンス コンピューティングとも呼ばれます。 • [Custom]：パフォーマンス プロファイルのすべてのオプションをサーバの BIOS セットアップから設定できます。また、Hardware Prefetcher オプションと Adjacent Cache-Line Prefetch オプションは、下記のフィールドで設定できます。

名前	説明
[Hardware Prefetcher] **set HardwarePrefetch**	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。
[Adjacent Cache Line Prefetcher] **set AdjacentCacheLinePrefetch**	プロセッサで必要な行のみを取得するのではなく、偶数または奇数のペアのキャッシュ行を取得するかどうか。次のいずれかになります。 • [Disabled]：プロセッサで必要な行のみを取得します。 • [Enabled]：プロセッサで必要な行およびペアの行の両方を取得します。
[DCU Streamer Prefetch] **set DcuStreamerPrefetch**	プロセッサで DCU IP Prefetch メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [Disabled]：プロセッサはキャッシュ読み取り要求を予測しようとせず、明示的に要求された行のみを取得します。 • [Enabled]：DCU Prefetcher でキャッシュ読み取りパターンを分析し、必要と判断した場合にキャッシュ内の次の行を事前に取得します。
[DCU IP Prefetcher] **set DcuIpPrefetch**	プロセッサで DCU IP Prefetch メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [Disabled]：プロセッサでキャッシュ データをプリロードしません。 • [Enabled]：DCU IP Prefetcher で最も関連性が高いと判断されたデータを含む L1 キャッシュをプリロードします。

名前	説明
[Direct Cache Access Support] **set DirectCacheAccess**	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。
[Power Technology] **set CPUPowerManagement**	次のオプションの CPU 電源管理設定を指定できます。 • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 [Power Technology] は次のいずれかになります。 • [Custom]：前述の BIOS パラメータの個々の設定が使用されます。これらの BIOS パラメータのいずれかを変更する場合は、このオプションを選択する必要があります。 • [Disabled]：サーバで CPU 電源管理は実行されず、前述の BIOS パラメータの設定が無視されます。 • Energy_Efficient：前述の BIOS パラメータに最適な設定が決定され、これらのパラメータの個々の設定は無視されます。

名前	説明
[Enhanced Intel Speedstep Technology] **set EnhancedIntelSpeedStep**	プロセッサで Enhanced Intel SpeedStep Technology 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。 （注） CPUPowerManagement を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[Intel Turbo Boost Technology] **set IntelTurboBoostTech**	プロセッサで Intel Turbo Boost Technology 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。 （注） CPUPowerManagement を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。

名前	説明
[Processor Power State C6] **set ProcessorC6Report**	BIOS 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。OS はレポートを受信すると、プロセッサを電力量の少ない C6 状態に移行してエネルギー使用量を減らし、最適なプロセッサパフォーマンスを維持できます。次のいずれかになります。 • [Disabled]：BIOS から C6 レポートを送信しません。 • [Enabled]：BIOS から C6 レポートを送信し、OS がプロセッサを電力量の少ない C6 状態に移行できるようにします。 （注） CPUPowerManagement を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[Processor Power State C1 Enhanced] **set ProcessorC1EReport**	C1 ステートに入ったときに、CPU が最小周波数に移行するかどうか。次のいずれかになります。 • [Disabled]：CPU は C1 ステートでも引き続き最大周波数で動作します。 • [Enabled]：CPU は最小周波数に移行します。このオプションでは C1 ステートで節約される電力量が最大になります。
[Frequency Floor Override] **set CpuFreqFloor**	アイドル時に、CPU がターボを除く最大周波数よりも低い周波数にできるようにするかどうか。次のいずれかになります。 • [Disabled]：アイドル中に CPU をターボを除く最大周波数よりも低くできます。このオプションでは電力消費が低下しますが、システムパフォーマンスが低下する可能性があります。 • [Enabled]：アイドル中に CPU をターボを除く最大周波数よりも低くできません。このオプションではシステムパフォーマンスが向上しますが、消費電力が増加することがあります。

名前	説明
[P-STATE Coordination] **set PsdCoordType**	BIOS がオペレーティング システムに P-state サポート モデルを通信する方法を定義できます。Advanced Configuration and Power Interface（ACPI）仕様で定義される 3 つのモデルがあります。 • [HW_ALL]：プロセッサ ハードウェアが、依存性のある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。 • [SW_ALL]：OS Power Manager（OSPM）が、依存性のある論理プロセッサ（物理パッケージ内のすべての論理プロセッサ）間の P-state を調整します。すべての論理プロセッサで遷移を開始する必要があります。 • [SW_ANY]：OS Power Manager（OSPM）が、依存性のある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。ドメイン内の任意の論理プロセッサで遷移を開始する場合があります。 （注） CPUPowerManagement を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[Energy Performance] **set CpuEngPerfBias**	システム パフォーマンスまたはエネルギー効率がこのサーバで重要かどうかを判断できます。次のいずれかになります。 • Balanced_Energy • Balanced_Performance • Energy_Efficient • Performance

[Memory Configuration] のパラメータ

名前	説明
[Select Memory RAS] **set SelectMemoryRAS**	サーバに対するメモリの Reliability, Availability, and Serviceability（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。 • [Lockstep]：サーバ内の DIMM ペアが、同一のタイプ、サイズ、および構成を持ち、SMI チャネルにまたがって装着されている場合、ロックステップモードをイネーブルにして、メモリアクセス遅延の最小化およびパフォーマンスの向上を実現できます。このオプションを使用した場合、[Mirroring] よりもシステム パフォーマンスが向上し、[Maximum Performance] よりも信頼性が向上しますが、[Mirroring] よりも信頼性が低く、[Maximum Performance] よりもシステム パフォーマンスは低下します。
[DRAM Clock Throttling] **set DRAMClockThrottling**	メモリ帯域幅と消費電力に関してシステム設定を調整できます。次のいずれかになります。 • [Balanced]：DRAM クロック スロットリングを低下させ、パフォーマンスと電力のバランスをとります。 • [Performance]：DRAM クロック スロットリングはディセーブルです。追加の電力をかけてメモリ帯域幅を増やします。 • [Energy Efficient][Energy_Efficient]：DRAMのクロック スロットリングを上げてエネルギー効率を向上させます。

名前	説明
[NUMA] **set NUMAOptimize**	BIOS で Non-Uniform Memory Access（NUMA）がサポートされているかどうか。次のいずれかになります。 • [Disabled]：BIOS で NUMA をサポートしません。 • [Enabled]：NUMA に対応したオペレーティング システムに必要な ACPI テーブルを BIOS に含めます。このオプションをイネーブルにした場合は、一部のプラットフォームでシステムのソケット間メモリインターリーブをディセーブルにする必要があります。
[Low Voltage DDR Mode] **set LvDDRMode**	低電圧と高周波数のどちらのメモリ動作をシステムで優先するか。次のいずれかになります。 • [Power Saving Mode][Power_Saving_Mode]：低電圧のメモリ動作が高周波数のメモリ動作よりも優先されます。 このモードでは、電圧を低く維持するために、メモリの周波数が低下する可能性があります。 • [Performance Mode][Performance_Mode]：高周波数の動作が低電圧の動作よりも優先されます。
[DRAM Refresh rate] **set DramRefreshRate**	DRAM セルをリフレッシュするレートを設定できます。次のいずれかになります。 • [1x]：DRAM セルは、64ms ごとにリフレッシュされます。 • [2x]：DRAM セルは、32ms ごとにリフレッシュされます。 • [3x]：DRAM セルは、21ms ごとにリフレッシュされます。 • [4x]：DRAM セルは、16ms ごとにリフレッシュされます。 • [Auto]： DRAM セルのリフレッシュ レートは、システム設定に基づき BIOS によって自動的に選択されます。これは、このパラメータに推奨される設定です。

名前	説明
[Channel Interleaving] **set ChannelInterLeave**	CPUがメモリブロックを分割して、データの隣接部分をインターリーブされたチャネル間に分散し、同時読み取り動作をイネーブルにするかどうか。次のいずれかになります。 • [Auto]：実行するインターリーブを、CPUが決定します。 • [1_Way]：何らかのチャネル インターリーブが使用されます。 • [2_Way] • [3_Way] • [4_Way]：最大のチャネル インターリーブが使用されます。
[Rank Interleaving] **set RankInterLeave**	1つのランクを更新中に別のランクにアクセスできるよう、CPUがメモリの物理ランクをインターリーブするかどうか。次のいずれかになります。 • [Auto]：実行するインターリーブを、CPUが決定します。 • [1_Way]：何らかのランク インターリーブが使用されます。 • [2_Way] • [4_Way] • [8_Way]：最大量のランク インターリーブが使用されます。

名前	説明
[Patrol Scrub] **set PatrolScrub**	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] **set DemandScrub**	CPU または I/O が読み取りを要求した場合に検出された 1 ビットのメモリ エラーを、システムが修正するかどうか。次のいずれかになります。 • [Disabled]：1 ビット メモリ エラーは修正されません。 • [Enabled]：1 ビット メモリ エラーがメモリ内部で修正され、修正されたデータが、読み取り要求に対する応答に設定されます。
[Altitude] **set Altitude**	物理サーバがインストールされているおおよその海抜（m）。次のいずれかになります。 • [Auto]：物理的な高度を CPU によって判別します。 • [300_M]：サーバは、海抜約 300 m です。 • [900_M]：サーバは、海抜約 900 m です。 • [1500_M]：サーバは、海抜約 1500 m です。 • [3000_M]：サーバは、海抜約 3000 m です。

[QPI Configuration] のパラメータ

名前	説明
[QPI Link Frequency Select] **set QPILinkFrequency**	Intel QuickPath Interconnect（QPI）リンク周波数（ギガトランスファー/秒（GT/s）単位）。次のいずれかになります。 • [Auto]：QPI リンク周波数は CPU によって決定されます。 • [6.4_GT/s] • [7.2_GT/s] • [8.0_GT/s]

[SATA Configuration] のパラメータ

名前	説明
[SATA Mode] **set SataMode**	Serial Advanced Technology Attachment（SATA）ソリッドステートドライブ（SSD）の動作モード。 • [Disabled]：すべての SATA ポートが無効であり、ドライバは列挙されません。 • [IDE Mode]：動作モードは、以前のハードウェア標準である Integrated Drive Electronics（IDE）インターフェイスに従います。 • [AHCI Mode]：デフォルトモードです。ドライブは、新しい標準である Advance Host Controller Interface（AHCI）に基づいて動作します。

[USB Configuration] のパラメータ

名前	説明
[Legacy USB Support] **set LegacyUSBSupport**	システムでレガシーUSBデバイスをサポートするかどうか。次のいずれかになります。 • [Disabled]：USBデバイスは、EFIアプリケーションでのみ使用できます。 • [Enabled]：レガシーUSBのサポートは常に使用できます。 • [Auto]：USB デバイスが接続されていない場合、レガシー USB のサポートがディセーブルになります。
[Port 60/64 Emulation] **set UsbEmul6064**	完全な USB キーボード レガシー サポートのために 60h/64h エミュレーションをシステムでサポートするかどうか。次のいずれかになります。 • [Disabled]：60h/64 エミュレーションはサポートされません。 • [Enabled]：60h/64エミュレーションはサポートされます。 サーバで USB 非対応オペレーティング システムを使用する場合は、このオプションを選択する必要があります。
[All USB Devices] **set AllUsbDevices**	すべての物理および仮想USBデバイスがイネーブルであるか、ディセーブルであるか。次のいずれかになります。 • [Disabled]：すべての USB デバイスがディセーブルです。 • [Enabled]：すべての USB デバイスがイネーブルです。
[USB Port: Rear] **set UsbPortRear**	背面パネルのUSBデバイスがイネーブルかディセーブルか。次のいずれかになります。 • [Disabled]：背面パネルの USB ポートをディセーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [Enabled]：背面パネルの USB ポートをイネーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。

名前	説明
[USB Port: Internal] **set UsbPortInt**	内部USBデバイスがイネーブルかディセーブルか。次のいずれかになります。 • [Disabled]：内部 USB ポートをディセーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [Enabled]：内部 USB ポートをイネーブルにします。これらのポートに接続されるデバイスは、BIOSおよびオペレーティング システムによって検出されます。
[USB Port: KVM] **set UsbPortKVM**	KVM ポートがイネーブルかディセーブルか。次のいずれかになります。 • [Disabled]： KVM キーボードおよびマウス デバイスをディセーブルにします。キーボードとマウスは KVM ウィンドウで機能しなくなります。 • [Enabled]： KVM キーボードおよびマウス デバイスをイネーブルにします。
[USB Port: vMedia] **set UsbPortVMedia**	仮想メディア デバイスがイネーブルかディセーブルか。次のいずれかになります。 • [Disabled]：vMedia デバイスをディセーブルにします。 • [Enabled]：vMedia デバイスをイネーブルにします。

[PCI Configuration] のパラメータ

名前	説明
[PCI ROM CLP] **set PciRomClp**	PCI ROM Command Line Protocol（CLP）は、カード上の iSCSI や PxE などのさまざまなオプション ROM の実行を制御します。デフォルト設定は、ディセーブルです。 • [Enabled]：ポートごとに個別に、iSCSI や PxE などのさまざまなオプション ROM の実行を制御できるようにします。 • [Disabled]：デフォルト オプションです。異なるオプション ROM は選択できません。デフォルト オプション ROM は PCI 列挙中に実行されます。

名前	説明
[ASPM Support] **set ASPMSupport**	BIOS での ASPM （アクティブ電源状態管理）サポートのレベルを設定できます。次のいずれかになります。 • [Disabled]：ASPM サポートは、BIOS でディセーブルです。 • [Force L0s]：すべてのリンクを強制的に L0 スタンバイ（L0）状態にします。 • [Auto]：電力状態を CPU によって判別します。

[Serial Configuration] のパラメータ

名前	説明
[Out-of-Band Mgmt Port] **set comSpcrEnable**	Windows 緊急管理サービスに使用可能な COM ポート 0 を設定することができます。このセットアップ オプションに基づいて ACPI SPCR テーブルが報告されます。次のいずれかになります。 • [Disabled]：Windows オペレーティング システムで使われる汎用ポートとして COM ポート 0 を設定します。 • [Enabled]：Windows 緊急管理サービス用のリモート管理ポートとして COM ポート 0 を設定します。
[Console Redirection] **set ConsoleRedir**	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。 • [COM 0][COM_0]：POST中に COM ポート 0 でコンソール リダイレクションをイネーブルにします。 • [COM 1][COM_1]：POST中に COM ポート 1 でコンソール リダイレクションをイネーブルにします。

名前	説明
[Terminal Type] **set TerminalType**	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+]：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。
[Bits per second] **set BaudRate**	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] をディセーブルにした場合は、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。 • [9600]：9,600 ボー レートが使用されます。 • [19200]：19,200 ボー レートが使用されます。 • [38400]：38,400 ボー レートが使用されます。 • [57600]：57,600 ボー レートが使用されます。 • [115200]：115,200 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。
[Flow Control] **set FlowCtrl**	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）を使用すると、隠れた端末問題が原因で発生する可能性があるフレーム コリジョンを減らすことができます。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。 • Hardware_RTS/CTS：フロー制御に RTS/CTS 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
[Putty KeyPad] **set PuttyFunctionKeyPad**	PuTTY ファンクション キーおよびテンキーの最上段のキーのアクションを変更できます。次のいずれかになります。 • [VT100]：ファンクション キーが ESC OP ～ ESC O[を生成します。 • [LINUX]：Linux 仮想コンソールを模倣します。ファンクション キー F6 ～ F12 はデフォルト モードと同様に動作しますが、F1 ～ F5 は ESC [[A ～ ESC [[E を生成します。 • [XTERMR6]：ファンクション キー F5 ～ F12 がデフォルト モードと同様に動作します。ファンクション キー F1 ～ F4 が ESC OP ～ ESC OS を生成します。これはデジタル端末のキーパッドの上段によって生成されるシーケンスです。 • [SCO]：ファンクション キー F1 ～ F12 が ESC [M ～ ESC [X を生成します。ファンクションおよび Shift キーが ESC [Y ～ ESC [j を生成します。Ctrl およびファンクション キーが ESC [k ～ ESC [v を生成します。Shift、Ctrl およびファンクション キーが ESC [w ～ ESC [{ を生成します。 • [ESCN]：デフォルト モードです。ファンクション キーはデジタル端末の一般的な動作と一致します。ファンクション キーが ESC [11~ や ESC [12~ などのシーケンスを生成します。 • [VT400]：ファンクション キーがデフォルト モードと同様に動作します。テンキーの最上段のキーが ESC OP ～ ESC OS を生成します。
[Redirection After BIOS POST] **set RedirectionAfterPOST**	BIOS POST が完了し、OS ブートローダに制御が渡された後に、BIOS コンソール リダイレクションがアクティブであるかどうか。次のいずれかになります。 • [Always Enable][Always_Enable]：OSのブートおよび実行時にBIOS レガシー コンソール リダイレクションがアクティブになります。 • [Bootloader]：OS ブートローダに制御が渡される前に BIOS レガシー コンソール リダイレクションがディセーブルになります。

[LOM and PCIe Slots Configuration] のパラメータ

名前	説明
[CDN Support for VIC] **set CdnEnable**	イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [Disabled]：OS イーサネット ネットワーキング識別子には、デフォルトの規則に従って ETH0、ETH1 などの名前が付けられます。デフォルトで、CDN オプションはディセーブルになっています。 • [LOMS Only]：OS イーサネット ネットワーク識別子は、LOM ポート 0 や LOM ポート 1 のように物理的な LAN on Motherboard（LOM）のポート番号付けに基づく Consistent Device Naming（CDN）による名前が付けられます。 （注） CDN は LOM ポートに対しイネーブルであり、Windows 2012 または最新の OS のみで機能します。
[All PCIe Slots OptionROM] **set PcieOptionROMs**	PCIe カードのオプション ROM をサーバが使用できるかどうか。次のいずれかになります。 • [Disabled]：すべての PCIe スロットの オプション ROM が使用できません。 • [Enabled]：すべての PCIe スロットの オプション ROM が使用可能です。 • [UEFI_Only]：スロット *n* のオプション ROM は UEFI にのみ使用できます。 • [Legacy_Only]：スロット *n* のオプション ROM はレガシーにのみ使用できます。
[PCIe Slot:*n* OptionROM] **set PcieSlot*n*OptionROM**	PCIe カードのオプション ROM をサーバが使用できるかどうか。次のいずれかになります。 • [Disabled]：スロット *n* のオプション ROM は使用できません。 • [Enabled]：スロット *n* のオプション ROM は使用可能です。 • [UEFI_Only]：スロット *n* のオプション ROM は UEFI にのみ使用できます。 • [Legacy_Only]：スロット *n* のオプション ROM はレガシーにのみ使用できます。

名前	説明
[PCIe Mezzanine OptionROM] **set PcieMezzOptionROM**	PCIe メザニン スロットの拡張 ROM をサーバで使用できるかどうか。次のいずれかになります。 • [Disabled]：スロット *M* のオプション ROM は使用できません。 • [Enabled]：スロット *M* のオプション ROM は使用可能です。 • [UEFI_Only]：スロット *M* のオプション ROM は UEFI にのみ使用できます。 • [Legacy_Only]：拡張スロット *M* はレガシーにのみ使用できます。
[SIOC1 Link Speed] **Set PcieSlot1LinkSpeed**	System IO Controller 1（SIOC1）アドオン スロット 1 のリンク速度。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：デフォルトのリンク速度。リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。 • [Disabled]：スロットは無効であり、カードは列挙されません。
[SIOC2 Link Speed] **Set PcieSlot2LinkSpeed**	System IO Controller 2（SIOC2）アドオン スロット 2 のリンク速度。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：デフォルトのリンク速度。リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。 • [Disabled]：スロットは無効であり、カードは列挙されません。

名前	説明
[Mezz Link Speed] **set PcieSlotMLinkSpeed**	リンク速度を拡張（メザニン）します。次のいずれかになります。 • [GEN 1]：リンク速度は第 1 世代まで到達可能です。 • [GEN 2]：リンク速度は第 2 世代まで到達可能です。 • [GEN 3]：デフォルトのリンク速度。リンク速度は第 3 世代まで到達可能です。 • [Disabled]：スロットは無効であり、カードは列挙されません。

C3160 サーバの [Server Management] タブ

名前	説明
[FRB-2 Timer] **set FRB-2**	POST 中にシステムが停止した場合に、システムを回復するために Cisco IMC で FRB2 タイマーを使用するかどうか。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。
[OS Watchdog Timer] **set OSBootWatchdogTimer**	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。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 **set OSBootWatchdogTimerTimeout** コマンドで指定された時間内にブートしない場合、Cisco IMC 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。

名前	説明
[OS Watchdog Timer Timeout] **set OSBootWatchdogTimerTimeOut**	OS が指定された時間内にブートしない場合、OS ウォッチドッグ タイマーの期限が切れ、システムはタイマーポリシーに基づいてアクションを実行します。次のいずれかになります。 • [5_Minutes]：OS ウォッチドッグ タイマーは、ブートが開始されてから 5 分後に期限が切れます。 • [10_Minutes]：OS ウォッチドッグ タイマーは、ブートが開始されてから 10 分後に期限が切れます。 • [15_Minutes]：OS ウォッチドッグ タイマーは、ブートが開始されてから 15 分後に期限が切れます。 • [20_Minutes]：OS ウォッチドッグ タイマーは、ブートが開始されてから 20 分後に期限が切れます。 （注） このオプションは [OS Boot Watchdog Timer] をイネーブルにした場合にのみ適用されます。
[OS Watchdog Timer Policy] **set OSBootWatchdogTimerPolicy**	ウォッチドッグ タイマーが切れた場合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 タイマーの期限が切れた場合、アクションは実行されません。 • Power_Down：OS のブート中にウォッチドッグ タイマーの期限が切れた場合、サーバの電源がオフになります。 • [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] をイネーブルにした場合にのみ適用されます。

付 録 B

複数のインターフェイスのBIOSトークン名の比較

この付録は、次の項で構成されています。

複数のインターフェイスの BIOS トークン名の比較

次の表に、XML、CLI および Web GUI のインターフェイスで使用される BIOS トークン名を示します。このリストは、これらのインターフェイスに名前をマッピングするために使用できます。

（注） 使用可能なパラメータは、使用している Cisco UCS サーバのタイプによって異なります。

BIOS トークン グループ	BIOS トークン名	XML オブジェクト	CLI および Web GUI オブジェクト
Main	[TPM Support]	biosVfTPMSupport/ vpTPMSupport	TPMAdminCtrl
Process Configuration	Intel(R) Hyper-Threading Technology	biosVfIntelHyperThreadingTech/ vpIntelHyperThreadingTech	IntelHyperThread
	Number of Enable Cores	biosVfCoreMultiProcessing/ vpCoreMultiProcessing	CoreMultiProcessing
	Execute Disable	biosVfExecuteDisableBit/ vpExecuteDisableBit	ExecuteDisable

BIOS トークン グループ	BIOS トークン名	XML オブジェクト	CLI および Web GUI オブジェクト
	Intel(R) VT	biosVfIntelVirtualizationTechnology/ vpIntelVirtualizationTechnology	IntelVT
	Intel(R) VT-d	biosVfIntelVTForDirectedIO/ vpIntelVTForDirectedIO	IntelVTD
	Intel(R) VT-d Coherency Support	biosVfIntelVTForDirectedIO/ vpIntelVTDCoherencySupport	CoherencySupport
	Intel(R) VT-d ATS Support	biosVfIntelVTForDirectedIO/ vpIntelVTDATSSupport	ATS
	CPU Performance	biosVfCPUPerformance/ vpCPUPerformance	CpuPerformanceProfile
	Hardware Prefetcher	biosVfHardwarePrefetch/ vpHardwarePrefetch	HardwarePrefetch
	Adjacent Cache Line Prefetcher	biosVfAdjacentCacheLinePrefetch/ vpAdjacentCacheLinePrefetch	AdjacentCacheLinePrefetch
	DCU Streamer Prefetch	biosVfDCUPrefetch/ vvpStreamerPrefetch	DcuStreamerPrefetch
	DCU IP Prefetcher	biosVfDCUPrefetch/ vpIPPrefetch	DcuIpPrefetch
	Direct Cache Access Support	biosVfDirectCacheAccess/ vpDirectCacheAccess	DirectCacheAccess
	Power Technology	biosVfCPUPowerManagement/ vpCPUPowerManagement	CPUPowerManagement
	Enhanced Intel Speedstep(R) Technology	biosVfEnhancedIntelSpeedStepTech/ vpEnhancedIntelSpeedStepTech	EnhancedIntelSpeedStep
	Intel(R) Turbo Boost Technology	biosVfIntelTurboBoostTech/ vpIntelTurboBoostTech	IntelTurboBoostTech

BIOS トークン グループ	BIOS トークン名	XML オブジェクト	CLI および Web GUI オブジェクト
	Processor Power state C6	biosVfProcessorCState/ vpProcessorCState	ProcessorC6Report
	Processor Power state C1 Enhanced	biosVfProcessorC1E/ vpProcessorC1E	ProcessorC1E
	Frequency Floor Override	biosVfCPUFrequencyFloor/ vpCPUFrequencyFloor	CpuFreqFloor
	P-STATE Coordination	biosVfPStateCoordType/ vpPStateCoordType	PsdCoordType
	Energy Performance	biosVfCPUEnergyPerformance/ vpCPUEnergyPerformance	CpuEngPerfBias
メモリ構成	Select Memory RAS	biosVfSelectMemoryRASConfiguration/ vpSelectMemoryRASConfiguration	SelectMemoryRAS
	DRAM Clock Throttling	biosVfDRAMClockThrottling/ vpDRAMClockThrottling	DRAMClockThrottling
	NUMA	biosVfNUMAOptimized/ vpNUMAOptimized	NUMAOptimize
	Low Voltage DDR Mode	biosVfLvDIMMSupport/ vpNUMAOptimized	LvDDRMode
	DRAM Refresh rate	biosVfDramRefreshRate/ vpDramRefreshRate	DramRefreshRate
	Channel Interleaving	biosVfMemoryInterleave/ vpChannelInterLeave	ChannelInterLeave
	Rank Interleaving	biosVfMemoryInterleave/ vpRankInterLeave	RankInterLeave
	Patrol Scrub	biosVfPatrolScrub/ vpPatrolScrub	PatrolScrub
	Demand Scrub	biosVfDemandScrub/ vpDemandScrub	DemandScrub

BIOS トークン グループ	BIOS トークン名	XML オブジェクト	CLI および Web GUI オブジェクト
	高度	biosVfAltitude/ vpAltitude	高度
QPI の設定	QPI Link Frequency Select	biosVfQPIConfig/ vpQPILinkFrequency	QPILinkFrequency
	Cluster on Die	biosVfCODEnable/ vpCODEnable	CODEnable
	Snoop Mode	biosVfEarlySnoop/ vpEarlySnoop	EarlySnoop
[SATA Configuration]	SATA Mode	サポート対象外	SATAMode
オンボード ストレージ	Onboard SCU Storage Support	biosVfOnboardStorage/ vpOnboardSCUStorageSupport	DisableSCU
	オンボード SCU ストレージ SW スタック	biosVfOnboardStorageSWStack vpOnboardSCUStorageSWStack	PchScuOromSelect
USB 設定	Legacy USB Support	biosVfLegacyUSBSupport/ vpLegacyUSBSupport	LegacyUSBSupport
	Port 60/64 Emulation	biosVfUSBEmulation/ vpUSBEmul6064	UsbEmul6064
	All USB Devices	biosVfUSBPortsConfig/ vpAllUsbDevices	AllUsbDevices
	USB Port:Rear	biosVfUSBPortsConfig/ vpUsbPortRear	UsbPortRear
	USB Port:Front	biosVfUSBPortsConfig/ vpUsbPortFront	UsbPortFront
	USB Port:Internal	biosVfUSBPortsConfig/ vpUsbPortInternal	UsbPortInt
	USB Port:KVM	biosVfUSBPortsConfig/ vpUsbPortKVM	UsbPortKVM

BIOS トークン グループ	BIOS トークン名	XML オブジェクト	CLI および Web GUI オブジェクト
	USB Port:Vmedia	biosVfUSBPortsConfig/ vpUsbPortVMedia	UsbPortVMedia
	USB Port:SD Card	biosVfUSBPortsConfig/ vpUsbPortSDCard	UsbPortSdCard
	xHCI Mode	biosVfPchUsb30Mode/ vpPchUsb30Mode	PchUsb30Mode
PCI の設定	PCI ROM CLP	未サポート	PciRomClp
	MMIO above 4GB	biosVfMemoryMappedIOAbove4GB/ vpMemoryMappedIOAbove4GB	MemoryMappedIOAbove4GB
	ASPM Support	biosVfASPMSupport/ vpASPMSupport	ASPMSupport
	VGA Priority	biosVfVgaPriority/ vpVgaPriority	VgaPriority
シリアルの設定	Console Redirection	biosVfConsoleRedirection/ vpConsoleRedirection	ConsoleRedir
	Terminal Type	biosVfConsoleRedirection/ vpTerminalType	TerminalType
	ビット/秒	biosVfConsoleRedirection/ vpBaudRate	BaudRate
	Flow Control	biosVfConsoleRedirection/ vpFlowControl	FlowCtrl
	Putty KeyPad	biosVfConsoleRedirection/ vpPuttyKeyPad	PuttyFunctionKeyPad
	Redirection After BIOS POST	biosVfConsoleRedirection/ vpLegacyOSRedirection	RedirectionAfterPOST
LOM と PCIe スロットの設定	PCH SATA Mode	biosVfSataModeSelect/ vpSataModeSelect	SataModeSelect

BIOS トークン グループ	BIOS トークン名	XML オブジェクト	CLI および Web GUI オブジェクト
	All Onboard LOM Ports	biosVfSataModeSelect/ vpSataModeSelect	AllLomPortControl
	LOM Port 0 OptionROM	biosVfLOMPortOptionROM/ vpLOMPort0State	LomOpromControlPort0
	LOM Port 1 OptionROM	biosVfLOMPortOptionROM/ vpLOMPort1State	LomOpromControlPort1
	All PCIe Slots OptionROM	biosVfPCIOptionROMs/ vpPCIOptionROMs	PcieOptionROMs
	PCIe Slot:*n* OptionROM	biosVfPCISlotOptionROMEnable/ vpSlot*n*State	PcieSlot*n*OptionROM
	PCIe Mezzanine OptionROM	biosVfPCISlotOptionROMEnable/ vpSlotMezzState	PcieMezzOptionROM
	PCIe Slot:1 Link Speed または SIOC1 Link Speed	biosVfPCISlotOptionROMEnable/ vpSlot1LinkSpeed	PcieSlot1LinkSpeed
	PCIe Slot:2 Link Speed または SIOC2 Link Speed	biosVfPCISlotOptionROMEnable/ vpSlot2LinkSpeed	PcieSlot2LinkSpeed
	PCIe Slot:MLOM OptionROM	biosVfPCISlotOptionROMEnable/ vpSlotMLOMState	PcieSlotMLOMOptionROM
	PCIe Slot:HBA OptionROM	biosVfPCISlotOptionROMEnable/ vpSlotHBAState	PcieSlotHBAOptionROM
	PCIe Slot:N1 OptionROM	biosVfPCISlotOptionROMEnable/ vpSlotN1State	PcieSlotN1OptionROM
	PCIe Slot:N2 OptionROM	biosVfPCISlotOptionROMEnable/ vpSlotN2State	PcieSlotN2OptionROM

BIOS トークン グループ	BIOS トークン名	XML オブジェクト	CLI および Web GUI オブジェクト
サーバ管理	FRB-2 Timer	biosVfFRB2Enable/ vpFRB2Enable	FRB-2
	OS Watchdog Timer	biosVfOSBootWatchdogTimer/ vpOSBootWatchdogTimer	OSBootWatchdogTimer
	OS Watchdog Timer Timeout	biosVfOSBootWatchdogTimerPolicy/ vpOSBootWatchdogTimerPolicy	OSBootWatchdogTimerTimeout
	OS Watchdog Timer Policy	biosVfOSBootWatchdogTimerTimeOut/ vpOSBootWatchdogTimerPolicy	OSBootWatchdogTimerPolicy
	Boot Order Rules	biosVfUCSMBootOrderRuleControl/ vpUCSMBootOrderRule	UCSMBootOrderRule

複数のインターフェイスの BIOS トークン名の比較

索 引

D

F

H

I

K

L

M

N

O

P

S

T

U

V

X

Y

あ

い

え

か

く

こ

さ

し

す

せ

た

て

ね

は

ふ

ほ

ま

め

ゆ

り

ろ