Cisco UCS C シリーズ サーバ Integrated Management Controller リリース 4.3 CLI 設定ガイド

初版：2023 年 3 月 3 日

最終更新：2023 年 5 月 18 日

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

目 次

はじめに

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、**this font**で示しています。 CLI コマンド内の変数は、このフォント 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。

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。

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。

警告　安全上の重要事項

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

これらの注意事項を保管しておいてください。

Cisco UCS の関連資料

ドキュメント ロードマップ

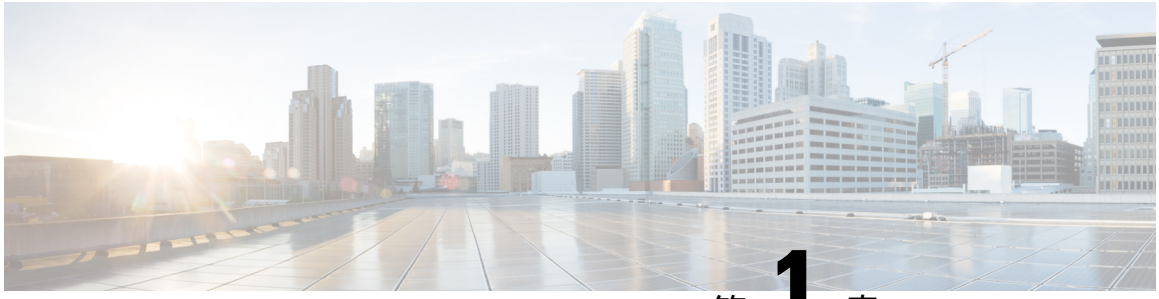
すべての B シリーズ マニュアルの完全なリストについては、次の URL で入手可能な『*Cisco UCS B-Series Servers Documentation Roadmap*』を参照してください。https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_roadmap.html

すべての C-Series マニュアルの完全なリストについては、次の URL で入手可能な『『*Cisco UCS C-Series Servers Documentation Roadmap*』』を参照してください。https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/ucs_rack_roadmap.html

管理用の UCS Manager に統合されたラック サーバでサポートされるファームウェアと UCS Manager のバージョンについては、『Release Bundle Contents for Cisco UCS Software』[英語] 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、次の内容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 サーバーには、次のモデルがあります。

- Cisco UCS C220 M7 ラックマウント サーバー
- Cisco UCS C240 M7 ラックマウント サーバー
- Cisco UCS C220 M6 ラックマウント サーバー
- Cisco UCS C240 M6 ラックマウント サーバー
- Cisco UCS C225 M6 ラックマウント サーバー
- Cisco UCS C245 M6 ラックマウント サーバー
- Cisco UCS C240 SD M5 ラックマウント サーバ
- Cisco UCS C125 ラックマウント サーバー
- Cisco UCS C220 M5 ラックマウント サーバー
- Cisco UCS C240 M5 ラックマウント サーバー
- Cisco UCS C480 M5 ラックマウント サーバー
- Cisco UCS C220 M4 ラックマウント サーバー
- Cisco UCS C240 M4 ラックマウント サーバー

- Cisco UCS C460 M4 ラックマウント サーバー

（注） このファームウェア リリースでサポートされている Cisco UCS C シリーズ ラック マウント サーバーを確認するには、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

Overview of the Server Software

The Cisco UCS C-Series Rack-Mount Server ships with the Cisco IMC firmware.

Cisco IMC Firmware

Cisco IMC is a separate management module built into the motherboard. A dedicated ARM-based processor, separate from the main server CPU, runs the Cisco IMC firmware. The system ships with a running version of the Cisco IMC firmware. You can update the Cisco IMC firmware, but no initial installation is needed.

Server OS

The Cisco UCS C-Series rack servers support operating systems such as Windows, Linux, Oracle and so on. For more information on supported operating systems, see the *Hardware and Software Interoperability for Standalone C-series servers* at http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html. You can use Cisco IMC to install an OS on the server using the KVM console and vMedia.

サーバ ポート

次に示すのは、サーバ ポートとそのデフォルトのポート番号のリストです。

表 *1:* サーバ ポート

ポート名	ポート番号
LDAP Port 1	389
LDAP Port 2	389
LDAP Port 3	389
LDAP Port 4	3268
LDAP Port 5	3268
LDAP Port 6	3268
SSHポート	22

ポート名	ポート番号
[HTTP ポート（HTTP Port）]	80
HTTPS ポート	443
SMTP ポート（SMTP Port）	25
KVM ポート	2068
Andromeda Management ポート	8889
Andromeda クラウド ポート	8888
SOL SSH ポート	2400
SNMPポート	161
SNMP トラップ	162
外部Syslog	514

Cisco Integrated Management Controller

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

（注） Cisco IMC 管理サービスは、サーバーがスタンドアロン 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。ほとんどのタスクがいずれかのインターフェイスを使用して実行できます。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を、他方のインターフェイスに表示することができます。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。

- サーバーの電源のオン、電源のオフ、電源再投入、リセット、およびシャットダウンを行う
- ロケータ LED を切り替える
- BIOS の設定
- サーバーのブート順を設定する
- サーバのプロパティとセンサーの表示
- リモート プレゼンスの管理
- ローカル ユーザ アカウントの作成と管理、および Active Directory を経由したリモート ユーザ認証の有効化
- NIC プロパティ、IPv4、VLAN、ネットワーク セキュリティなどのネットワーク関連の設定
- HTTP、SSH、IPMI over LAN、SNMP などのコミュニケーション サービスの設定
- 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のモニタ
- タイム ゾーンの設定と現地時刻の確認
- 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 ファームウェアのインストールと有効化

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 はサーバーのプロビジョニングを行うため、サーバー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、サーバでのオペレーティング システムやアプリケーションのプロビジョニングおよび管理には、これを使用できません。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 以外のユーザー 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。

Note 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コマンドの大部分は、関連する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	任意のモードで **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 #
dimm-summary	シャーシ モードから **scope dimm-summary** *index* コマンド	/chassis/dimm-summary #
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 #

モード名	アクセスするコマンド	モード プロンプト
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 #
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 #

モード名	アクセスするコマンド	モード プロンプト
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 #
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、目的のコマンドを再度呼び出し、Enterキー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 キー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。
- スマート アクセス機能は、OS の起動後、OS の grub 設定ファイルの `console` プロパティが **ttyS0** に設定されていない限り、期待どおりには動作しません。それが期待どおりに動作するには、OS の grub 設定ファイルの `console` プロパティを **ttyS0** に設定する必要があります。

CLI に関するオンラインヘルプ

? 文字を入力すれば、いつでもコマンド構文の現在の状態で使用可能なオプションを表示できます。

プロンプトに何も入力しなかった場合、**?** と入力すると、そのときのモードで使用できるコマンドがすべて表示されます。コマンドの一部を入力した場合、**?** と入力すると、コマンド構文のそのときの位置で使用できるキーワードと引数がすべて表示されます。

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。

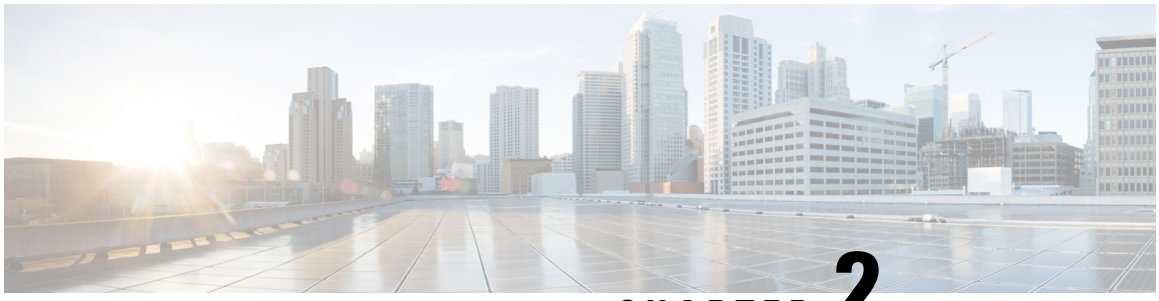
- Cisco IMC Web UI または CLI でデフォルトの管理者クレデンシャルを変更するまでは、操作を実行できません。

（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。スクリプトを実行する際にこのことが問題になる場合は、ユーザ管理オプションにログインし直すことによって、それをパスワードに変更することができますが、これは完全に自己責任において実行するようにしてください。シスコでは推奨していません。

例

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 #
```



CHAPTER 2

サーバー OS のインストール

この章は、次の内容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

Cisco UCS サーバ構成ユーティリティに関する詳細情報については、『Cisco UCS サーバ構成ユーティリティ ユーザー ガイド』を参照してください。

仮想 KVM コンソール

vKVM 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（vKVM）の直接接続をエミュレートします。vKVM 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。

Cisco KVM コンソールを使用する主な利点は次のとおりです。

- Cisco KVM コンソールは KVM、SOL、および vMedia への接続を提供しますが、Avocent KVM は KVM および vMedia への接続のみを提供します。
- KVM コンソールでは、vMedia 接続が KVM 起動マネージャで確立され、すべてのユーザーが使用できます。

- KVM コンソールには、ゲストからホストにテキストを貼り付ける際に、サポートされていない文字の高度な文字置換オプションが用意されています。
- KVM コンソールには、CIMC に vMedia マッピングを保存する機能があります。

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、vKVM 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

vKVM 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） vKVM コンソールの操作には、GUI 以外は使用できません。vKVM コンソールの起動手順については、『*Cisco UCS C* シリーズ サーバ統合管理コントローラ *GUI* 構成ガイド』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

始める前に

- VLAN 経由でサーバに到達できることを確認します。
- 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。

次のタスク

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。ソフトウェアの相互運用性とドライバの互換性を含め、常に OS ベンダ推奨の設定に従うようにします。ドライバの推奨事項とインストールについて詳しくは、こちらの Cisco UCS ハードウェア互換性リストに従ってください。

https://ucshcltool.cloudapps.cisco.com/public/

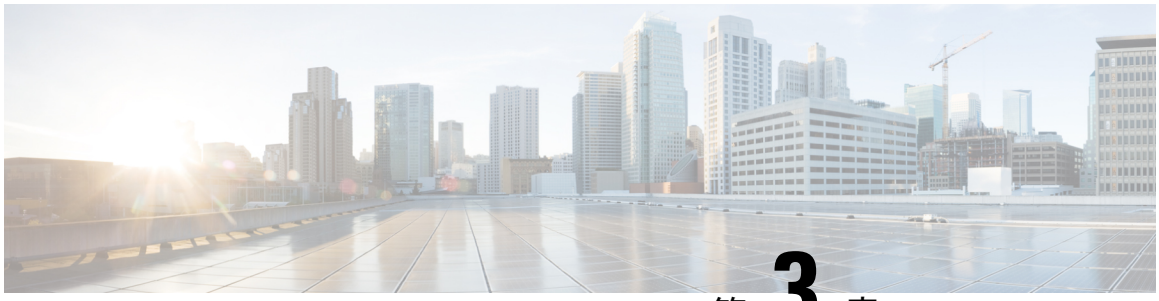
USB ポートからのオペレーティング システムの起動

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。



第 3 章

サーバーの管理

この章は、次の内容で構成されています。

ロケータ LED の切り替え

始める前に

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

手順

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

例

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。

始める前に

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

手順

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

例

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。

始める前に

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

手順

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

例

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 #
```

パーソナリティ構成のクリア

始める前に

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

手順

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 # **clear-personality**

パーソナリティ構成をクリアします。

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 log
- 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

始める前に

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

手順

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

例

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 #
```

サーバーのブート順の管理

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ー

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ーから設定されていないデバイスを追加した。

重要 Cisco UCS C220 M5 または C480 M5 サーバをリリース 4.1 (1x) にアップグレードする場合は、次の条件に従います。

- 4.0 よりも前のリリースからアップグレードする場合 (4x)
- **[レガシー ブート モード (Legacy Boot Mode)]** が有効になっていて、**[Cisco IMC のブート順序 (Cisco IMC Boot Order)]** が設定されていない場合
- サーバが Cisco HWRAID アダプタから起動している場合

その後、アップグレードする前に次のいずれかを実行する必要があります。

- ここに記載されている XML API スクリプトと UCSCFG ベースのスクリプトを実行します。

  または

- Cisco IMC GUI または CLI インターフェイスを使用して、目的のブート順序を手動で設定します。

（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 2.0(x) のアップグレード中に、レガシー ブート順は高精度ブート順に移行されます。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 **[構成されたブート順序 (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確認するには、**show boot-device** コマンドを入力します。この間に、サーバー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ーを設定した場合、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、**set boot-order HDD,PXE** コマンドを使用してこれを設定できます。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。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **show boot-device** [**detail**]	ブート デバイスの詳細情報を表示します。

例

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 TestUSB:
    Device Type: USB
    Device State: Enabled
    Device Order: 1
    Sub Type: HDD
Boot Device TestPXE:
    Device Type: PXE
    Device State: Enabled
    Device Order: 2
    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。

始める前に

リリース 4.1(3b) 以降、Cisco IMC は HTTP ブート機能をサポートしています。HTTP ブートは、UEFI ブート モードでのみサポートされます。

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** • **HTTP**
ステップ 3	Server /bios # **scope boot-device** はブートデバイス名を作成しました。	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。

	コマンドまたはアクション	目的
		• 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。 • macaddress：ネットワーク イーサネット インターフェイスの MAC アドレス • iptype：IP タイプ 必要な値のいずれかを入力します：IPv4 または IPv6 • ipconfig-type：IP 構成のタイプ 必要な値のいずれかを入力します：DHCP または静的 • uri：すべての OS iso および EFI ファイルが配置されている URI パス
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。

例

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
```

次に、ブート順序を構成し、IP タイプ：**[DHCP]** に HTTP 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 server 1
Server /server # scope bios
Server /server/bios #  create boot-device HTTP-Test HTTP
Server /server/bios #  scope boot-device HTTP-Test
Server /server/bios/boot-device # set status enabled
Server /server/bios/boot-device # set port 10
Server /server/server/bios /boot-device #  set order 1
Server /server/bios /boot-device #  set slot MLOM
Server /server/bios/boot-device # set iptype IPv4
Server /server/bios/boot-device # set macaddress 00:25:B5:00:01:2b
Server /server/bios/boot-device # set ipconfig-type DHCP
Server /server/bios/boot-device # set uri http://www.cloudboot.com:80/EFI/rhel_82_dvd.iso
Server /bios /boot-device #  commit
Commiting device configuration
Server /server/bios/boot-device # show detail
BBIOS:
    BIOS Version: server-name.2.0.7c.0.071620151216
    Backup BIOS Version: server-name.2.0.7c.0.071620151216
    Boot Order: (none)
    Boot Override Priority:
    FW Update/Recovery Status: None, OK
    UEFI Secure Boot: Enabled
    Last Configured Boot Order Source: CIMC

Server /server/bios/boot-device # show boot-device detail
Boot Device HTTP-Test:
    Device Type: HTTP-Test
    Device State: Enabled
    Device Order: 1
    Slot Id: MLOM
    Port Number: 10
    MAC Address: 00:25:B5:00:01:2b
    IP Type: IPv4
    IP Config Type: DHCP
    URI: http://www.cloudboot.com:80/EFI/rhel_82_dvd.iso
```

次に、ブート順序を構成し、IP タイプ：**[静的（Static）]** に HTTP 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 server 1
Server /server # scope bios
Server /server/bios #  create boot-device HTTP-Test HTTP
Server /server/bios #  scope boot-device HTTP-Test
Server /server/bios/boot-device # set status enabled
Server /server/bios/boot-device # set port 10
Server /server/server/bios /boot-device #  set order 1
Server /server/bios /boot-device #  set slot MLOM
Server /server/bios/boot-device # set macaddress 00:25:B5:00:01:2b
Server /server/bios/boot-device # set ipconfig-type Static
Server /server/bios/boot-device # set iptype IPv6C240-WZP21360Z1B /bios/boot-device *#
set ipaddress 2001:420:5446:2014::330:12
Server /server/bios/boot-device *# set netmask_or_ipv6prefix 64
Server /server/bios/boot-device *# set gateway 2001:420:5446:2014::330:1
Server /server/bios/boot-device *# set dnsserver 2001:420:c0e0:1008::118
Server /server/bios/boot-device *# commit
Server /server/bios/boot-device *# set uri http://cisco.com/a.iso
Server /server/bios/boot-device *# commit
Server /server/bios/boot-device # show detail
Boot Device http_test:
    Device Type: HTTP
    Device State: Disabled
    Device Order: 1
    Slot Id: MLOM
    Port Number: 10
    MAC Address: aa:aa:aa:aa:aa:aa
    IP Type: IPv6
    IP Config Type: Static
    URI: http://cisco.com/a.iso
    IP Address: 2001:420:5446:2014::330:12
    Netmask/IPV6 Prefix: 64
    Gateway: 2001:420:5446:2014::330:1
    DNS Server: 2001:420:c0e0:1008::118
Server /server/bios/boot-device #
```

次のタスク

サーバーを再起動して、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。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **scope boot-device** はブートデバイス名を作成しました。	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。
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 /server/bios /boot-device* # **set iptype** {*value* | *IPv4* | *IPv6*}.	デバイスの IP タイプを指定します。
ステップ 7	Server /server/bios /boot-device* # **set macaddress** {*value* }.	ネットワーク イーサネット インターフェイスの MAC アドレスを設定します。
ステップ 8	Server /server/bios /boot-device* # **set ipconfig-type** {*value* | *DHCP* | *Static* }.	デバイスの IP 構成タイプを指定します。

	コマンドまたはアクション	目的
ステップ 9	Server /server/bios /boot-device* # **set uri** {*value* }.	すべての OS iso および EFI ファイルが置かれている URI パスを指定します。
ステップ 10	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。

例

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 #
```

次に、既存の HTTP ブート デバイスの属性を変更する例を示します。

```
Server# scope server 1
Server /server # scope bios
Server /server/bios *# scope boot-device http-test
Server /server/bios/boot-device # show detail
Boot Device http-test:
    Device Type: HTTP
    Device State: Disabled
    Device Order: 3
    Slot Id: 1
    Port Number: 10
    MAC Address: 00:25:B5:00:01:2b
    IP Type: IPv4
    IP Config Type: DHCP
    URI: http://www.cloudboot.com:80/EFI/rhel_82_dvd.iso


Server /server/bios/boot-device # set iptype IPv6
Server /server/bios/boot-device *# set slot 34
Server /server/server/bios /boot-device #  set order 1
Server /server/bios/boot-device *# set macaddress 00:25:B5:00:01:2c
Server /server/bios/boot-device *# set uri http://www.cloudboot.com:80/dvd.iso
Server /server/bios/boot-device *# commit
Server /server/bios/boot-device # show detail
Boot Device http-test:
    Device Type: HTTP
    Device State: Disabled
    Device Order: 3
    Slot Id: 34
    Port Number: 10
    MAC Address: 00:25:B5:00:01:2c
    IP Type: IPv6
    IP Config Type: DHCP
    URI: http://www.cloudboot.com:80/dvd.iso

Server /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。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ2	Server /bios # **rearrange boot-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。

例

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 #
```

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。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **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。

例

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 #
```

次のタスク

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。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **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。

例

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 2019 • Windows Server 2016 • ESX 6.7 • ESX 6.5 • ESXi 7.0 • Linux

コンポーネント	種類
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

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。

	コマンドまたはアクション	目的
		（注） 有効にすると、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。 （注） RFD（Reset Factory Default）の場合は、UEFI セキュア ブートを再度有効にする必要があります。

例

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 #
```

次のタスク

サーバー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。

例

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 #
```

次のタスク

サーバー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# **scope bios**	bios コマンド モードを開始します。
ステップ 2	Server /bios # **show actual-boot-order** [**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。

例

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 #
```

ワンタイム ブート デバイスでブートするようにサーバーを設定する

現在設定されているブート順序を中断することなく、次回のサーバーのブートに対してのみ、特定のデバイスから起動するようにサーバーを設定できます。ワン タイム ブート デバイスからサーバーを起動すると、事前に設定されているブート順で以降のすべてのリブートが行われます。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server# /bios **show boot-device**	使用可能なブート ドライブのリストを表示します。
ステップ 3	Server #/bios **set one-time-boot-device** *device-order*	サーバのブート順を設定します。 （注） 無効になっている拡張ブート デバイスで設定されている場合でも、ホストはワンタイム ブート デバイスに対して起動します。
ステップ 4	Server# /bios * **commit**	トランザクションをコミットします。
ステップ 5	（任意） Server# /bios **show detail**	BIOS の詳細を表示します。

例

次に、ワンタイム ブート デバイスで起動するサーバを設定する例を示します。

```
Server scope bios
Server /bios # show boot-device
Boot Device                    Device Type  Device State       Device Order
------------------------------ ------------ ------------------ ----------------
KVMDVD                         VMEDIA       Enabled            1
vkvm                           VMEDIA       Enabled            2

Server /bios # set one-time-boot-device KVMDVD
Server /bios *# 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 # show detail
BIOS:
    BIOS Version: "C240M3.3.0.0.9 (Build Date: 10/02/16)"
    Boot Order: (none)
    FW Update/Recovery Status: None, OK
    UEFI Secure Boot: disabled
    Configured Boot Mode: Legacy
    Actual Boot Mode: Legacy
    Last Configured Boot Order Source: CIMC
    One time boot device: KVMDVD
Server /bios #
```

ユーザ定義のサーバの説明とアセット タグの割り当て

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 description** <*Server Description*>	サーバの説明を入力します。
ステップ 3	Server /chassis* # **set asset-tag** <*Asset Tag*>	アセット タグを入力します。
ステップ 4	Server /chassis* # **commit**	トランザクションをコミットします。
ステップ 5	（任意） Server /chassis # **show detail**	サーバの詳細を表示します。

例

この例は、ユーザ定義のサーバの説明とアセット タグを割り当てる方法を示しています。

```
Server# scope chassis
Server/chassis # set description DN1-server
```

```
Server/chassis* # set asset-tag powerpolicy
Server /chassis* # commit
Server /chassis # show detail
Chassis:
    Power: on
    Serial Number: FCH1834V23X
    Product Name: UCS C220 M4S
    PID : UCSC-C220-M4S
    UUID: 414949AC-22D6-4D0D-B0C0-F7950E9217C1
    Locator LED: off
    Description: DN1-server
    Asset Tag: powerpolicy
Server /chassis #
```

サーバーのリセット

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。

始める前に

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

手順

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

例

次に、サーバー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]
```

サーバーのシャットダウン

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。

始める前に

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

手順

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

例

次に、サーバをシャットダウンする例を示します。

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

サーバーの電源管理

サーバーの電源投入

（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。

始める前に

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

手順

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

例

次に、サーバの電源をオンにする例を示します。

```
Server# scope chassis
Server /chassis # power on
Warning: System is already powered ON, this action is ineffective.
Do you want to continue?[y|N]y
```

サーバーの電源オフ

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。

始める前に

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

手順

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

例

次に、サーバーの電源をオフにする例を示します。

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

Server /chassis # show
Power Serial Number Product Name  UUID
----- ------------- ------------- ------------------------------------
off   Not Specified Not Specified 208F0100020F000000BEA80000DEAD00
```

サーバー電源の再投入

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。

始める前に

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

手順

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

例

次に、サーバ電源を再投入する例を示します。

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

電力ポリシーの設定

電力制限

重要 このセクションは、一部の UCS C シリーズのサーバでのみ利用可能です。

パワー キャッピングによって、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。パワーキャッピング オプションを有効にすると、システムにより電力消費がモニタされ、割り当てられている電力制限を超えないように電力が維持されます。サーバが電力制限を維持できない場合、またはプラットフォームの電力を修正時間内に指定の電力制限に戻すことができない場合、**[電力プロファイル（Power Profile）]** 領域の **[アクション（Action）]**フィールドに指定したアクションがパワー キャッピングにより実行されます。

パワーキャッピングが有効になったら、定義された属性を持つ標準電力プロファイルまたは詳細電力プロファイルを使用できるように複数の電力プロファイルを設定できます。標準電力プロファイルを選択する場合は、電力制限、修正時間、修正アクション、中断期間、ハードキャップ、ポリシー状態（有効な場合）を設定できます。詳細電力プロファイルを選択する場合は、標準電力プロファイルの属性の他に、ドメイン固有の電力制限、安全スロットル レベル、周囲温度に基づくパワー キャッピング属性も設定できます。

（注） 次に示す変更は、Cisco UCS C シリーズ リリース 2.0(13) 以降に適用されます。

- 2.0(13) リリースへのアップグレード後、ホストの電源を初めてオンにするときに、電力特性評価が自動的に実行されます。それ以降は、電力特性評価は**[電力特性評価の実行（Run Power Characterization）]**セクションで指定されているとおりに開始する場合にのみ実行されます。
- また、サーバへの電源再投入が行われ、CPU または DIMM の設定が変更されている場合にも、初回ホスト ブート時に電力特性評価が自動的に実行されます。PCIe アダプタ、GPU、HDD などのハードウェアが変更されている場合は、電力特性評価は実行されません。特性評価された電力範囲は、ホストの電源再投入後に存在するコンポーネントに応じて変更されます。

Web UI の **[パワー キャッピング設定（Power Cap Configuration）]** タブの **[電力特性評価の実行（Run Power Characterization）]**オプションを選択すると、ホストの電源が再投入され、電力特性評価が開始されます。

電源の冗長性ポリシーの設定

始める前に

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 # **scope sensor**	センサー コマンドを入力します。
ステップ 2	Server /sensor # **scope psu-redundancy-policy**	psu冗長性ポリシー コマンドを入力します。
ステップ 3	Server /sensor/psu-redundancy-policy #**set psu-redundancy-policy***value*	設定する次の冗長性値のいずれか1つを選択します。 • **non-redundant** - N（使用可能なPSU出力性能）は、インストールされている PSU の数に等しくなります。この場合、PSU のエラー、またはグリッドのエラーはサポートされません。 • [N+1] : N（使用可能な PSU 出力性能）は、インストールされている PSU の数から 1 を引いた数に等しくなります。この場合、単一のPSUのエラーはサポートされますが、グリッドのエラーはサポートされません。 • **grid** - N（使用可能な PSU 出力性能）は、インストールされているPSUの数の半分に等しくなります。この場合、N 個の PSU のエラー、またはグリッドのエラーがサポートされます。このポリシーは、N個のPSU を 1 つのフィードに接続し、別の N 個の PSU を別のフィードに接続したことを暗黙的に示しています。
ステップ 4	Server /sensor/psu-redundancy-policy* #**commit**	トランザクションをサーバにコミットします。

	コマンドまたはアクション	目的
ステップ 5	（任意） Server /sensor/psu-redundancy-policy #**show detail**	パワー冗長性ステータスを表示します。

例

次に、サーバのパワー冗長性を設定する例を示します。

```
Server / #scope sensor
Server /sensor #scope psu-redundancy-policy
Server /sensor/psu-redundancy-policy # set psu-redundancy-policy grid
Server /sensor/psu-redundancy-policy* # commit
Server /sensor/psu-redundancy-policy # show detail
PSU Redundancy Policy: grid
Server /sensor/psu-redundancy-policy #
```

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。

始める前に

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

手順

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

例

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 # 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。

始める前に

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

手順

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

例

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 #
```

Power Cap 範囲の確認

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。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Chassis power-cap-config # **show detail**	power cap 範囲の詳細の表示します。 **[プラットフォーム最小値（スロットリングを許可）]** - CPU のスロットリング

	コマンドまたはアクション	目的
		が有効になっているときのシャーシの電力の下限です。プラットフォーム最小値としてこれを使用するには、標準または高度な電力プロファイル範囲**allow-throttle**フィールドを**enabled**に設定します。 **[プラットフォーム最小値（効率的）]** - CPU のスロットリングが無効になっているときのシャーシの電力の下限です。 **[CPU 最小値（スロットリングを許可）]** - スロットリングが有効になっているときに CPU ドメインの電力の下限です。CPU最小値としてこれを使用するには、標準または高度な電力プロファイル範囲内の **allow-throttle**フィールドを**enabled**に設定します。 **[CPU 最小値 (効率的)]** - これは、スロットリングが無効になっているときの、CPU ドメインの電力の下限です。

例

```
Power Characterization Enabled: yes
    Power Capping: yes
    Power Characterization Status: Completed
    Platform Min (Allow-Throttle)(W): 164
    Platform Min (Efficient)(W): 286
    Platform Max (W): 582
    Memory Min (W): 2
    Memory Max (W): 5
    CPU Min (Allow-Throttle)(W): 64
    CPU Min (Efficient)(W): 177
    CPU Max (W): 330
```

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。

始める前に

- 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# **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 power-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# **set pow-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# **scope power-profile standard**	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# **set allow-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 6	Server /chassis /power-cap-config# **set corr-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# **set except-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 にイベントを記録します。 • **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。
ステップ 8	Server /chassis /power-cap-config# **set hard-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 9	Server /chassis /power-cap-config# **set pow-limit** *value*	電力制限を指定します。

	コマンドまたはアクション	目的
		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# **set susp-pd** {*h:m-h:m* | |*All,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。

例

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 # show detail
Power Cap Config:
    Power Characterization Enabled: yes
    Power Capping: no
    Power Characterization Status: Completed
    Platform Min (Allow-Throttle)(W): 164
    Platform Min (Efficient)(W): 290
    Platform Max (W): 581
    Memory Min (W): 2
    Memory Max (W): 5
    CPU Min (Allow-Throttle)(W): 64
    CPU Min (Efficient)(W): 177
    CPU Max (W): 330
```

詳細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。

始める前に

- 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 # **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 power-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 # **set pow-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 # **scope power-profile advanced**	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/power-profile # **set allow-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/power-profile # **set corr-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/power-profile # **set cpu-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/power-profile # **set except-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 10	Server/chassis/power-cap-config/power-profile # **set hard-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 11	Server /chassis /power-cap-config/power-profile # **set mem-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 12	Server /chassis /power-cap-config/power-profile # **set fail-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 13	Server /chassis /power-cap-config/power-profile # **set plat-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 14	Server /chassis /power-cap-config/power-profile # **set plat-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 15	Server /chassis /power-cap-config/power-profile # **set pow-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 16	Server /chassis /power-cap-config/power-profile # **set susp-pd** {*h:m-h:m* | |*All,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 17	Server /chassis /power-cap-config/power-profile # **set thermal-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 18	Server /power-cap-config/power-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。

例

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

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。

始める前に

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

手順

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

例

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。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope 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 power-cap-config**	電力制限設定コマンド モードを開始します。
ステップ 3	Server /chassis/power-cap-config# **showdetail**	電力特性評価に関する情報を表示します。

例

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 # scope power-cap-config
Server /chassis/power-cap-config # show detail
Power Cap Config:
    Power Characterization Enabled: yes
    Power Capping: no
    Power Characterization Status: Completed
    Platform Min (Allow-Throttle)(W): 164
    Platform Min (Efficient)(W): 290
    Platform Max (W): 581
    Memory Min (W): 2
    Memory Max (W): 5
    CPU Min (Allow-Throttle)(W): 64
    CPU Min (Efficient)(W): 177
    CPU Max (W): 330
Server /chassis/power-cap-config #
```

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。

始める前に

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

手順

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

例

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。

始める前に

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

手順

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

	コマンドまたはアクション	目的
		ります。これがデフォルトのアクションになります。 • **power-on**：サーバの電源は、シャーシの電源が回復したときにオンになります。 • **restore-last-state**：サーバの電源は、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	（任意） Server /CIMC/power-restore-policy # **set delay** {**fixed** | **random**}	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	（任意） Server /CIMC/power-restore-policy # **set delay-value** *delay*	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。
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。

例

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。

- [バランス（Balanced）]：この設定はほとんどのサーバー構成を冷却できますが、PCIe カードは容易に過熱するため、これらのカードのあるサーバーには適していない可能性があります。
- **[低電力（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。
- **[高電力（High Power）]**：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ーに最適です。
- **[最大電力（Maximum Power）]**：この設定は、非常に高いファン速度を必要とするサーバー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。
- **Acoustic**：この設定は、ファンのノイズ レベルを設定するために使用できます。これにより、サーバのノイズ リダクションが可能になります。

このポリシーを適用すると、システム パフォーマンスに影響するパフォーマンス スロットリングが発生する可能性があります。過剰な温度またはパフォーマンスイベントがイベント ログに記録されている場合は、**低電力**などの標準のファン制御ポリシーを選択します。これは、中断のない変更です。

（注） このオプションは、Cisco UCS C220 M5、C240 SD M5、C240 M5、C220 M6、C240 M6、C245 M6、C225 M6、C220 M7、および C240 M7 サーバーでのみ使用できます。これらのサーバーでは、**[音響（Acoustic）]** がデフォルトのファン ポリシーです。

他のサーバーの場合、デフォルトのファンポリシーは、サーバー構成とサーバーに存在する PCIe カードの数によって異なります。

（注） Cisco UCS M5 サーバーの場合、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ーの構成要件により決定されます。PCIe カードには、温度要件に応じて最小ファン速度のタグが付けられています。サーバーにこれらの PCIe カードが装備されている場合、タグ付けされた要件を下回るファンポリシーを構成することはできません。

[構成ステータス（Configuration Status）] には、Cisco UCS M5 サーバーで構成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。この原因として、以下が考えられます。
  - 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
- [ファン ポリシーの上書き（FAN POLICY OVERRIDE）]：指定されたファン速度を、サーバー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。

（注）
- Cisco UCS C220 M7、C240 M7、C220 M6、C240 M6、UCS C220 M5、C240 M5、C240 SD M5、C125 M5、C480 M5、C480-M5ML の場合、**[適用されるファンポリシー（Applied fan policy）]** は、サーバーに存在する PCIe カードによって異なります。
- Cisco UCS C225 M6 および C245 M6 の場合、**[適用されるファン ポリシー（Applied fan policy）]** は、サーバーに存在する PCIe カードまたは特定の CPU タイプによって異なります。

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。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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。 • [バランス（Balanced）]：この設定はほとんどのサーバー構成を冷却できますが、PCIe カードは容易に過熱するため、これらのカードのあるサーバーには適していない可能性があります。 • **[低電力（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。 • **[高電力（High Power）]**：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ーに最適です。 • **[最大電力（Maximum Power）]**：この設定は、非常に高いファン速度を必要とするサーバー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。 • **Acoustic**：この設定は、ファンのノイズ レベルを設定するために使用できます。これにより、サーバのノ

	コマンドまたはアクション	目的
		イズ リダクションが可能になります。 このポリシーを適用すると、システム パフォーマンスに影響するパフォーマンス スロットリングが発生する可能性があります。過剰な温度またはパフォーマンス イベントがイベント ログに記録されている場合は、**低電力**などの標準のファン制御ポリシーを選択します。これは、中断のない変更です。 （注） このオプションは、Cisco UCS C220 M5、C240 SD M5、C240 M5、C220 M6、C240 M6、C245 M6、C225 M6、C220 M7、および C240 M7 サーバーでのみ使用できます。 これらのサーバーでは、**[Acoustic]** がデフォルトのファン ポリシーです。 他のサーバーの場合、デフォルトのファン ポリシーは、サーバー構成とサーバーに存在する PCIe カードの数によって異なります。
ステップ 4	Server /chassis/fan-policy # **set aggressive-cooling***no\yes*	このオプションを使用して、積極的な冷却を有効にします。
ステップ 5	Server /chassis/fan-policy # **commit**	サーバへの変更をコミットします。

例

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 # set aggressive-cooling yes
```

```
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 #
```

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。不良とマークされた 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 がマップから外されるかまたはブラックリストに追加されるのは、修正不可能なエラーが発生した場合だけです。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） 16000 修正可能エラーの場合、DIMM がマップから外されることや、ブラックリストに追加されることはありません。

DIMM のブラックリストのイネーブル化

始める前に

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。

	コマンドまたはアクション	目的
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。

例

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 # **show detail**	BIOS ステータスの詳細を表示します。

BIOS ステータス情報には、次のフィールドが含まれます。

名前	説明
BIOS Version	実行中の BIOS のバージョン文字列。
Boot Order	サーバが使用を試行する、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。
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 Secure Boot	UEFI セキュア ブートを有効または無効にします。

名前	説明
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。

Configuring BIOS Settings

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **scope** **input-output | main-memory | power-performance | processor | server-management**	設定コマンドモードを開始します。 各 BIOS 設定のオプションに関する説明および情報については、次のトピックを参照してください。 サーバー モデル別 BIOS パラメータ（515 ページ） 各設定タイプ間の変更をコミットする必要があります。 Server /bios/ # **commit**

例

次に、USB レガシー サポートを有効にするように BIOS 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 # scope input-output
Server /bios/input-output # set UsbLegacySupport enabled
Server /bios/input-output *# 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/input-output #
```

BIOS デフォルトの復元

始める前に

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

手順

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

例

次の例は、BIOS デフォルト設定を復元します。

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

BIOS セットアップの開始

始める前に

- 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。

例

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 サーバに対してのみ使用できます。

始める前に

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

例

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 #
```

BIOS プロファイル

Cisco UCS サーバでは、デフォルトのトークン ファイルはすべての S3260 サーバ プラットフォームに使用可能で、グラフィック ユーザ インターフェイス（GUI）、CLI インターフェイス、および XML API インターフェイスを使用して、これらのトークンの値を設定できます。

サーバーパフォーマンスを最適化するには、これらのトークン値を特定の組み合わせで設定する必要があります。

BIOS プロファイルを設定することで、正しい組み合わせのトークン値が設定された事前設定トークン ファイルを使用することができます。利用可能な事前設定プロファイルには、仮想化、高性能、低電力などがあります。シスコの Web サイトから事前設定トークン ファイルのさまざまなオプションをダウンロードし、BMC を介してサーバに適用できます。

ダウンロードしたプロファイルを編集し、トークンの値を変更したり、新しいトークンを追加したりできます。これにより、応答時間なしで、要件に合わせてプロファイルをカスタマイズできます。

BIOS プロファイルの有効化

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server# /bios **scope bios-profile**	BIOS プロファイル コマンド モードを開始します。
ステップ 3	Server# /bios/bios-profile **activate** *virtualization*	BIOS の設定をバックアップするように求めるメッセージが表示されます。**y** と入力します。
ステップ 4	BIOS のセットアップ パラメータの変更を適用するためシステムを再起動するように求められます。**y** と入力します。	システムの再起動を開始します。

例

次に、指定した BIOS プロファイルをアクティブにする例を示します。

```
Server # scope bios
Server /bios # scope bios-profile
Server /bios/bios-profile # activate virtualization
It is recommended to take a backup before activating a profile.
Do you want to take backup of BIOS configuration?[y/n] y
backup-bios-profile succeeded.
bios profile “virtualization” deleted
Changes to BIOS set-up parameters will require a reboot.
Do you want to reboot the system?[y|N]y
A system reboot has been initiated.
Server /bios/bios-profile #
```

BIOS プロファイルのバックアップの取得

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server# /bios **scope bios-profile**	BIOS プロファイル コマンド モードを開始します。
ステップ 3	Server# /bios/bios-profile **backup**	BIOS プロファイルのバックアップが成功したというメッセージが表示されます。

例

この例は、BIOS プロファイルをバックアップします。

```
Server # scope bios
Server /bios # scope bios-profile
Server /bios/bios-profile # backup
backup-bios-profile succeeded.
Server /bios #
```

BIOS プロファイルの削除

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server# /bios **scope bios-profile**	BIOS プロファイル コマンド モードを開始します。
ステップ 3	Server# /bios/bios-profile **delete** *BIOS profile*	指定した BIOS プロファイルを削除します。

例

この例では、指定した BIOS プロファイルを削除します。

```
Server # scope bios
Server /bios # scope bios-profile
Server /bios/bios-profile # delete performance
Server /bios/bios-profile #
```

BIOS プロファイルの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server# /bios **show bios-profile**	すべての BIOS プロファイルを表示します。

例

次に、BIOS プロファイルを表示する例を示します。

```
Server # scope bios
Server /bios # show bios-profile
ID     Name             Active
------ ---------------- -------- --------
1      performance      yes
2      virtualization   no
3      none             no
4      cisco_backup     no
Server /bios #scope bios-profile
Server /bios #
```

BIOS プロファイルの情報の表示

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 **scope bios-profile**	すべての BIOS プロファイルを表示します。
ステップ 3	Server# /bios/bios-profile **info** *performance*	トークンの名前、プロファイル値、およびアクティブな値など BIOS プロファイルの情報を表示します。

例

この例では、指定した BIOS プロファイルの情報を表示します。

```
Server # scope bios
Server /bios # scope bios-profile
Server /bios/bios-profile # info performance

TOKEN NAME                      PROFILE VALUE        ACTUAL VALUE
=================================================================
 TPMAdminCtrl                    Enabled              Enabled
 ASPMSupport                     Disabled             Disabled
Server /bios/bios-profile #
```

BIOS プロファイルの詳細の表示

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 **scope bios-profile**	BIOS プロファイル コマンド モードを開始します。
ステップ 3	Server# /bios/bios-profile **show detail**	BIOS プロファイルの詳細が表示されます。

例

次に、BIOS プロファイルの詳細を表示する例を示します。

```
Server # scope bios
Server /bios # scope bios-profile
Server /bios/bios-profile # show detail
Active Profile: Virtualization
Install Status: bios profile install done
Server /bios/bios-profile #
```

セキュアブート証明書の管理

4.2 (2a) リリース以降、Cisco IMC では、設定されたセキュア HTTP ブート デバイス用に最大 10 個の証明書をアップロードできます。構成された特定のブート デバイスの新しい証明書を削除してアップロードすることもできます。Cisco IMC では、最大 10 個のルート CA 証明書をアップロードできます。

セキュアブート証明書の表示

始める前に

このタスクを実行するには、admin 権限を持つユーザーとして 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 bios**	BIOS コマンド モードを開始します。
ステップ 2	Server / bios # **scope secure-boot-certificate** *certificate_ID*	ここで、*certificate_ID* は Cisco IMC によって割り当てられた ID です。
ステップ 3	Server / bios / secure-boot-certificate # **show detail**	証明書の詳細が表示されます。

例

この例は、セキュアブート証明書の詳細を表示する方法を示しています。

```
server # scope bios
server / bios # scope secure-boot-certificate 3
server /bios/secure-boot-certificate # show detail
Secure Boot CA Certificate:
    Certificate ID: 3
    Serial Number: 04
    Subject Country Code (CC): XX
    Subject State (S): XX
    Subject Locality (L): XX
    Subject Organization (O): XX
    Subject Organizational Unit (OU): XX
    Subject Common Name (CN): *.XX
    Issuer Country Code (CC): XX
    Issuer State (S): XX
    Issuer Locality (L): XX
    Issuer Organization (O): XX
    Issuer Organizational Unit (OU): XX
    Issuer Common Name (CN): .XX
    Valid From: Month Date Time_Stamp 20xx GMT
    Valid To: Month Date Time_Stamp 20xx GMT
```

貼り付けオプションをしようしてセキュアブート証明書をアップロードする

始める前に

このタスクを実行するには、admin 権限を持つユーザーとして 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 bios**	BIOS コマンド モードを開始します。
ステップ 2	Server / bios # **scope secure-boot-certificate** *certificate_ID*	ここで、*certificate_ID* は Cisco IMC によって割り当てられた ID です。 証明書がこの ID に既にアップロードされている場合は、証明書の詳細のみを表示できます。ステータスを確認するには、**show detail** コマンドを使用します。
ステップ 3	Server / bios / secure-boot-certificate # **upload-paste-secure-boot-certificate**	証明書を貼り付けるように求められます。 ここに証明書を貼り付けてください。完了したら、CTRL+D を押します。

証明書が正常にアップロードされると、次のメッセージが表示されます。

セキュアブート証明書が正常に貼り付けされました。

例

この例は、貼り付けオプションを使用してセキュアブート証明書をアップロードする方法を示しています。

```
server # scope bios
server / bios # scope secure-boot-certificate 3
server /bios/secure-boot-certificate # upload-paste-secure-boot-certificate
Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIIDzzCCAregAwIBAgIBBDANBgkqhkiG9w0BAQsFADCBnTELMAkGA1UEBhMCVVMx
EzARBgNVBAgMCkNhbGlmb3JuaWExEDAOBgNVBAcMB05ld3lvcmsxETAPBgNVBAoM
CERpZ2ljZXJ0MRAwDgYDVQQLDAdTU0xERVBUMR8wHQYDVQQDDBYqLmNhLnRlc3Rp
bmcuY28uYmxyLmluMSEwHwYJKoZIhvcNAQkBFhJhbm1pY2hhZUBjaXNjby5jb20w
HhcNMjAwNDI4MDQyNTM2WhcNMjIwNDI4MDQyNTM2WjCBoDELMAkGA1UEBhMCSU4x
EjAQBgNVBAgMCUJlbmdhbHVydTESMBAGA1UEBwwJa2FybmF0YWthMQ8wDQYDVQQK
DAZPUkdDU1IxEzARBgNVBAsMCk9SR1VOSVRDU1IxIDAeBgNVBAMMFyouY3NyLnRl
c3RpbmcuYmxyLmNvLmluMSEwHwYJKoZIhvcNAQkBFhJhbm1pY2hhZUBjaXNjby5j
b20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC4oBCGcFnw/wcHkitn
TshWScl5+yI2aCmiCcVCUfRCX96erdE+4QKW1UqClZ9lpL8CqnhKkKTWVl54mcw2
RcZto+SpDrCJLJNgcuvmaUu1sIoafNmc3DTLCDJvrlxE0ooJP8SgXdEngAm44DXz
Uw3/8nu3I7WLXu//tOxd0edHHv4V2ktFx5mLaU/QlRRBEyRuXtGyiRSE5h5YWWd0
TAZ0R2NZFHn7ymYg2GGMjEFKfDSK0mfspbfQI5SMNLVIeA3SqI98Y95o6y9UUbg0
2DQH4O9Z/F9w0NuNJz5vhtxSl3ScNFQwRMLho/lJErV0SvV9vtuio+j3btQ+1CsF
VM9lAgMBAAGjFTATMBEGCWCGSAGG+EIBAQQEAwIGQDANBgkqhkiG9w0BAQsFAAOC
AQEAUzW7p3YhiEZfgBvR8D4iNsuv4J18BdzZmhDqA852tLprnh4HoWgMRt1YBO5B
7D5wJ7mgQn/TCqIlIlrNX8KUbDs+UYYDQBTxCuRZcM2QNaFogOJiQqHFugtjJZ4H
kUX06s9JJmTNs68dySQVJhHrY0b3sQdvWhzL8ryxDyg5EUu/m+O/FnxqU9CTEWEf
7E8ATB4dH82NlecRCbh2su4bC1PnMMi5g/w6pIMahMKHPVVvRQBW/0PsB0rlRw2j
J6o61URlJ6L7bc8ij5ExX+UjYc1mR555jflNG+1Sty5H8oJtzDLoxNgOPzyb4U6C
ljPN+QPSVZOcLUjIMZYjB8qSDw==
```

```
-----END CERTIFICATE-----
Secure Boot Certificate pasted successfully.
```

次のタスク

show detail コマンドを使用して、証明書の詳細を確認できます。

リモートの場所からセキュアブート証明書をアップロードする

始める前に

- このタスクを実行するには、admin 権限を持つユーザーとして admin としてログインする必要があります。
- 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。
- 次の証明書形式がサポートされています。
  - .crt
  - .cer
  - .pem

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 secure-boot-certificate** *certificate_ID*	ここで、*certificate_ID* は Cisco IMC によって割り当てられた ID です。 証明書がこの ID に既にアップロードされている場合は、証明書の詳細のみを表示できます。ステータスを確認するには、**show detail** コマンドを使用します。
ステップ 3	Server / bios / secure-boot-certificate # **upload-remote-secure-boot-certificate tftp | ftp | sftp | scp | http** *IP_address|Hostname Remote_server_path_filename*	値は次のとおりです。 • **[tftp]、[ftp]、[sftp]、[scp]、[http]** はファイル転送用のプロトコルです • **[サーバー IP アドレスまたはホスト名（Server IP Address or Hostname）]**：証明書ファイルの保管先とするサーバーの IP アドレスまたはホスト名。

	コマンドまたはアクション	目的
		• **[パスおよびファイル名（Path and Filename）]**：リモート サーバーにファイルをアップロードする際に Cisco IMC が使用する必要があるパスおよびファイル名。 ファイル転送プロトコルによっては、ユーザー名とパスワードの入力を求められる場合があります

証明書が正常にアップロードされると、次のメッセージが表示されます。

セキュアブート証明書が正常にアップロードされました

例

次の例は、リモートロケーションオプションを使用してセキュアブート証明書をアップロードする方法を示しています（scp ファイル転送プロトコルを使用）。

```
server # scope bios
server / bios # scope secure-boot-certificate 3
server /bios/secure-boot-certificate # upload-remote-secure-boot-certificate scp
10.10.10.10
/home/username/certificate.pem
Server (RSA) key fingerprint is xx:xx:8b:36:5a:53:14:d3:85:d0:xx:xx:e0:xx:24:51
Do you wish to continue? [y/N]y
Username: username
Password: password
Secure Boot Certificate uploaded successfully
```

次のタスク

show detail コマンドを使用して、証明書の詳細を確認できます。

セキュアブート証明書の削除

始める前に

このタスクを実行するには、admin 権限を持つユーザーとして 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 bios**	BIOS 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 / bios # **scope secure-boot-certificate** *certificate_ID*	ここで、*certificate_ID* は Cisco IMC によって割り当てられた ID です。
ステップ 3	Server / bios / secure-boot-certificate # **delete-secure-boot-certificate**	**[y]** と入力して **[Enter]** を押して確定します。

次のメッセージが表示されます。

セキュアブート証明書：*ID* は削除されました

例

この例は、セキュアブート証明書を削除する方法を示しています。

```
server # scope bios
server / bios # scope secure-boot-certificate 3
Server /bios/secure-boot-certificate # delete-secure-boot-certificate
Do you want to delete the existing secure boot certificate? [y|N]y
Secure Boot Certificate - 3 is deleted
```

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。

始める前に

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

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 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 firmware**	ファームウェア コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	Server /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。

例

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
```

製品 ID（PID）カタログの詳細の表示

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 cpu-pid**	CPU PID の詳細を表示します。
ステップ 3	Server /chassis # **show dimm-pid**	メモリ PID の詳細を表示します。
ステップ 4	Server /chassis # **show pciadapter-pid**	PCI アダプタ PID の詳細を表示します。
ステップ 5	Server /chassis # **show hdd-pid**	HDD PID の詳細を表示します。

例

次に、PID の詳細を表示する例を示します

```
Server # scope chassis
Viewing CPU PID details
Server /chassis # show cpu-pid
Socket Product ID           Model
------ -------------------- ----------------------------------------
```

```
CPU1   UCS-CPU-E52660B      Intel(R) Xeon(R) CPU E5-2660 v2 @ 2.2...
CPU2   UCS-CPU-E52660B      Intel(R) Xeon(R) CPU E5-2660 v2 @ 2.2...
Viewing memory PID details
Server /chassis # show dimm-pid
Name              Product ID           Vendor ID  Capacity  Speed
----------------- -------------------- ---------- --------- ------
DIMM_A1           UNKNOWN              NA         Failed    NA
DIMM_A2           UNKNOWN              NA         Ignore... NA
DIMM_B1           UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_B2           UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_C1           UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_C2           UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_D1           UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_D2           UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_E1           UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_E2           UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_F1           UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_F2           UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_G1           UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_G2           UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_H1           UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
DIMM_H2           UCS-MR-1X162RZ-A     0xCE00     16384 MB  1866
Viewing PCI adapters PID details
Server /chassis # show pciadapter-pid
Slot   Product ID           Vendor ID  Device ID   SubVendor ID  SubDevice ID
------ -------------------- ---------- ----------- ------------- -------------
1      UCSC-MLOM-CSC-02     0x1137     0x0042      0x1137        0x012e
Viewing HDD PID details
Server /chassis # show hdd-pid
Disk Controller  Product ID           Vendor     Model
---- ----------- -------------------- ---------- ------------
1    SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
2    SLOT-MEZZ   UCS-C3X60-HD4TB      SEAGATE    ST4000NM0023
3    SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
4    SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
5    SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
6    SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
7    SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
8    SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
9    SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
10   SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
11   SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
12   SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
13   SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
14   SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
15   SLOT-MEZZ   UCS-C3X60-HD4TB      SEAGATE    ST4000NM0023
16   SLOT-MEZZ   UCS-C3X60-HD4TB      SEAGATE    ST4000NM0023
19   SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
28   SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
54   SLOT-MEZZ   UCSC-C3X60-HD6TB     SEAGATE    ST6000NM0014
55   SLOT-MEZZ   UCSC-C3X60-HD6TB     SEAGATE    ST6000NM0014
56   SLOT-MEZZ   UCSC-C3X60-HD4TB     TOSHIBA    MG03SCA400
57   SLOT-MEZZ   UCS-HD4T7KS3-E       WD         WD4001FYY...
58   SLOT-MEZZ   UCS-HD4T7KS3-E       WD         WD4001FYY...
59   SLOT-MEZZ   UCS-HD4T7KS3-E       WD         WD4001FYY...
60   SLOT-MEZZ   UCS-HD4T7KS3-E       WD         WD4001FYY...

Server /chassis #
```

PID カタログのアップロードとアクティブ化

注意 PID カタログがアクティブになると、BMC が自動的に再起動します。

PID カタログをアクティブ化した後、サーバを再起動する必要があります。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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 pid-catalog**	PID カタログ コマンド モードを開始します。
ステップ 3	Server /chassis/pid-catalog # **upload-pid-catalog** *remote-protocol IP Address PID Catalog file*	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

	コマンドまたはアクション	目的
		（注） Cisco UCS C シリーズ サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバー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 サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[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	（任意） Server# /chassis/pid-catalog **show detail**	アップロードのステータスが表示されます。
ステップ 5	Server# /chassis/pid-catalog **activate**	アップロードされた PID カタログをアクティブにします。
ステップ 6	Server# /chassis/pid-catalog **show detail**	アクティベーションのステータスが表示されます。

例

次に、PID カタログをアップロードし、アクティブにする例を示します。

```
Server # scope chassis
Server /chassis # scope pid-catalog
Uploading PID Catalog
Server /chassis/pid-catalog # upload-pid-catalog tftp 10.10.10.10
```

```
pid-ctlg-2_0_12_78_01.tar.gz
upload-pid-catalog initialized.
Please check the status using "show detail".
Server /chassis/pid-catalog #
Server /chassis/pid-catalog # show detail
    Upload Status: Upload Successful
    Activation Status: Please Activate Catalog
    Current Activated Version: N/A
Activating the uploaded PID catalog
Server /chassis/pid-catalog # activate
Successfully activated PID catalog
Server /chassis/pid-catalog # show detail
    Upload Status:
    Activation Status: Activation Successful
    Current Activated Version: 2.0(12.78).01
Server /chassis/pid-catalog #
```

PID カタログを削除

⚠

注意 PID カタログが削除されると、BMC が自動的に再起動します。

PID カタログを削除した後、サーバを再起動する必要があります。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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 **scopepid-catalog**	PID カタログ コマンド モードを開始します。
ステップ 3	Server /chassis/pid-catalog # **delete**	確認プロンプトで**y**と入力し、PID カタログを削除します。 （注） PID カタログは、以前に更新およびアクティブ化されている場合にのみ削除できます。
ステップ 4	（任意） Server# /chassis/pid-catalog **show detail**	PID カタログのステータスを表示します。

例

次に、PID カタログをアップロードし、アクティブにする例を示します。

```
Server # scope chassis
Server /chassis # scope pid-catalog
Server /chassis/pid-catalog # delete
CIMC will be automatically rebooted after successful deletion of the uploaded catalog
file.
Once this is complete, a host reboot will be required for the catalog changes to be
reflected in
the BIOS and host Operating System Continue?[y|N]y
Server /chassis/pid-catalog # show detail
PID Catalog:
    Upload Status: N/A
    Activation Status: N/A
    Current Activated Version: 4.1(0.41)
Server /chassis/pid-catalog #
```

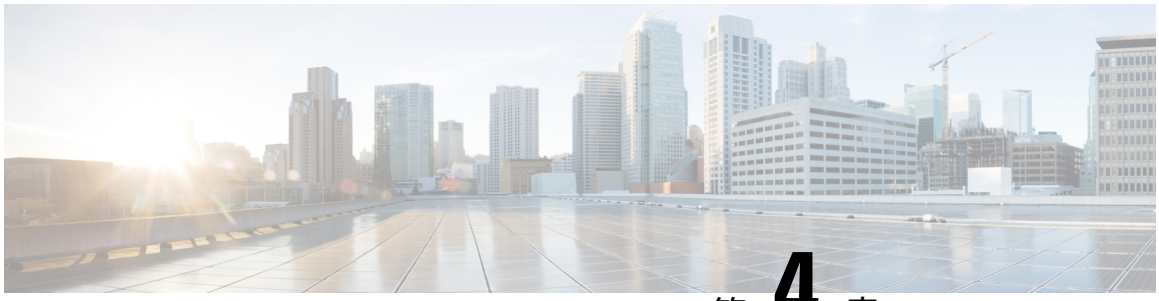
永続メモリ モジュール

永続メモリ モジュール

Cisco UCS C シリーズ リリース 4.0(4) は、Intel® Optane™ Data Center 永続メモリ モジュール (第二世代インテル® Xeon® Scalable プロセッサに基づく UCM M5 サーバ上) のサポートを導入します。永続メモリ モジュールは、第二世代インテル® Xeon® Scalable プロセッサでのみ使用できます。

永続メモリ モジュールは、メモリの低遅延とストレージの永続化を実現する不揮発性メモリ モジュールです。永続メモリ モジュールに保存されているデータは、他のストレージ デバイスに比べてすぐにアクセスでき、電源サイクルで保持されます。

永続メモリ モジュールの設定の詳細については、『Cisco UCS: Intel® Optane™ Data Center 永続メモリモジュールの設定と管理』を参照してください。



第 4 章

サーバーのプロパティの表示

この章は、次の内容で構成されています。

サーバー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# **show chassis** [**detail**]	サーバーのプロパティを表示します。

例

次に、サーバーのプロパティを表示する例を示します。

```
Server# 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#
```

システム情報の表示

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 sku-details**	システム情報を表示します。

例

次に、システムの詳細を表示する例を示します。

```
Server# scope chassis
Server /chassis # show sku-details
    SAS Expander: Not-Present
    HDD: 10-SFF_drive_back_plane
    Riser1: (1 Slot x16)
    Riser2: (1 Slot x16)
    M.2 SATA/NVMe: Not-Present
    M.2 SD Card Controller: Not-Present
    CPU1 PKG-ID: Non-MCP
    CPU2 PKG-ID: Non-MCP
    Intrusion Sensor: Not-Equipped
Server /chassis #
```

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。

例

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 から現在の日付と時刻を取得します。この情報を変更するには、サーバーをリブートし、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# **show cimc** [**detail**]	Cisco IMC プロパティを表示します。

例

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

始める前に

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

手順

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

例

次に、CPU のプロパティを表示する例を示します。

```
Server# scope chassis
Server /chassis # show cpu
Name         Cores    Version
------------ -------- ----------------------------------------------------
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

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **show dimm** [**detail**]	メモリのプロパティを表示します。
ステップ 3	Server /chassis # **show dimm-summary**	DIMM サマリー情報を表示します。

例

次に、メモリのプロパティを表示する例を示します。

```
Server# scope chassis
Server /chassis # show dimm
Name                 Capacity        Channel Speed (MHz) Channel Type
-------------------- --------------- ------------------- ---------------
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

始める前に

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

手順

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

例

次に、電源のプロパティを表示する例を示します。

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

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **show storageadapter** [*slot*] [**detail**]	インストールされているストレージ カードを表示します。 （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** スロット	装着されているストレージカードに対してコマンド モードを開始します。
ステップ 4	Server /chassis/storageadapter # **show bbu** [**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 # **show capabilites** [**detail**]	ストレージ カードでサポートされる RAID レベルを表示します。

	コマンドまたはアクション	目的
ステップ 6	Server /chassis/storageadapter # **show error-counters** [**detail**]	ストレージカードによって認識されたエラーの数を表示します。
ステップ 7	Server /chassis/storageadapter # **show firmware-versions** [**detail**]	ストレージ カードのファームウェア バージョン情報を表示します。
ステップ 8	Server /chassis/storageadapter # **show hw-config** [**detail**]	ストレージカードのハードウェア情報を表示します。
ステップ 9	Server /chassis/storageadapter # **show mfg-data** [**detail**]	ストレージカードの製造元のデータを表示します。
ステップ 10	Server /chassis/storageadapter # **show pci-info** [**detail**]	ストレージカードのディスプレイ アダプタの PCI 情報が表示されます。
ステップ 11	Server /chassis/storageadapter # **show running-firmware-images** [**detail**]	ストレージカードの実行中のファームウェアの情報を表示します。
ステップ 12	Server /chassis/storageadapter # **show settings** [**detail**]	ストレージカードのアダプタ ファームウェアの設定を表示します。
ステップ 13	Server /chassis/storageadapter # **show startup-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。

例

次に、ストレージのプロパティを表示する例を示します。

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

始める前に

- 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	必須: 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	必須: 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。

例

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** スロット	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** [ドライブ番号] [**detail**]	ストレージ カードの物理ドライブの情報を表示します。
ステップ 4	Server /chassis/storageadapter # **show physical-drive-count** [**detail**]	ストレージ カードの物理ドライブの数を表示します。
ステップ 5	Server /chassis/storageadapter # **scope physical-drive** ドライブ番号	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。

例

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

例

次に、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。

始める前に

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** スロット番号	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。

例

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

始める前に

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

手順

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

例

次に、PCI アダプタのプロパティを表示する例を示します。

```
Server# scope chassis
Server /chassis # show pci-adapter
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…

Option ROM Status
----------
Loaded
Not-Loaded
Not-Loaded
Loaded

Server /chassis #
```

（注） **[オプション ROM ステータス（Option ROM Status）]** は、レガシー ブート モードにのみ適用され、UEFI ブート モードには適用されません。

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。

	コマンドまたはアクション	目的
ステップ 2	Server /chassis # **scope network-adapter** スロット *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。
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。

例

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

始める前に

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

手順

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

例

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 #
```

SAS エクスパンダでの 6G または 12G 混合モード速度の有効化

Cisco IMC は、SAS エクスパンダに 6 ギガバイトまたは 12 ギガバイトの混合モード速度をサポートしています。6 ギガバイトのソリッド ステート ドライブ（SSD）が現在 12 ギガバイトの SSD に移行しているため、このサポートが追加されました。この機能を使用すると、[Dynamic Storage] タブで SAS エクスパンダを選択し、要件に基づいていずれかのモードを有効にすることができます。

SAS エクスパンダでの 6G または 12G 混合モードの有効化

この機能は、一部のサーバでのみ使用できます。

始める前に

このタスクを実行するには、admin 権限でログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope 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 sas-expander sas-expander ID**	SAS エクスパンダ コマンド モードを開始します。
ステップ 3	Server /chassis/sas-expander # **scope 6G-12G-Mixed-Mode-status**	6 G または 12 G の混在モード コマンド モードを開始します。
ステップ 4	Server /chassis/sas-expander/6G-12G-Mixed-Mode-status # **set set-6G-12G-mixed-mode Enabled**	SAS エクスパンダでの 6 G または 12 G 混合モードを有効化します。
ステップ 5	Server /chassis/sas-expander/6G-12G-Mixed-Mode-status * # **commit**	プロンプトで **y** と入力します。トランザクションをシステム設定にコミットします。
ステップ 6	（任意） Server /chassis/sas-expander/6G-12G-Mixed-Mode-status # **show detail**	6 G または 12 G 混合モードの状態が表示されます。

例

この例は、SAS エクスパンダで 6 G または 12 G 混合モードを有効にする方法を示しています。

```
Server# scope chassis
Server /chassis # scope sas-expander 1
Server /chassis/sas-expander # scope 6G-12G-Mixed-Mode-status
Server /chassis/sas-expander/6G-12G-Mixed-Mode-status # set set-6G-12G-mixed-mode Enabled
Server /chassis/sas-expander/6G-12G-Mixed-Mode-status *# commit
Are you sure you want to change the enable-mixed-mode setting to Enable mode?[y|N]y
Setting enable-mixed-mode setting to Enable ..
Successfully set enable-6G-12G-mixed-mode to Enable..
Server /chassis/sas-expander/6G-12G-Mixed-Mode-status # show detail
6G/12G Mixed Mode Settings:
    Mixed 6G/12G Drive Support: Enabled
Server /chassis/sas-expander/6G-12G-Mixed-Mode-status #
```

ストレージコントローラでのデュアルエンクロージャーの有効化

この機能は、UCS S3260 12G デュアル パススルー コントローラ（UCS-S3260-DHBA）を備えたサーバー ノードでのみサポートされます。この機能を使用すると、[ダイナミック ストレージ（Dynamic Storage）] タブで SAS エクスパンダを選択し、要件に基づいて SAS エクスパンダ上でデュアル エンクロージャのサポートを有効にすることができます。

始める前に

- サーバーの電源がオフになっていることを確認します。

手順

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 # **dynamic-storage**

ダイナミック ストレージ コマンド モードを開始します。

ステップ 3 Server /chassis/dynamic-storage # **show expander-hw-detail**

SAS エクスパンダ ハードウェアの詳細のリストを表示します。

- エクスパンダ ID
- ハードウェア リビジョン

- SAS アドレス
- SAS エクスパンダのエンクロージャ ID

ステップ 4 Server /chassis/dynamic-storage # **set-dual-enclosure**

デュアル エンクロージャ のサポートを有効化します。また、yes を選択して、SAS エクスパンダごとに異なるエンクロージャ ID を設定します。

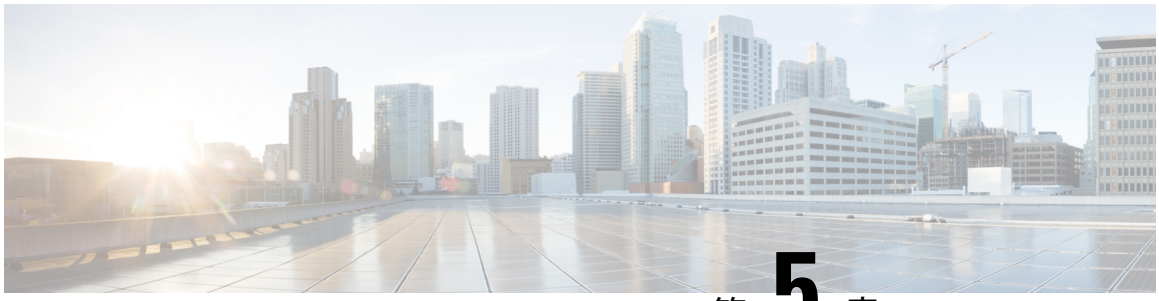
ステップ 5 Server /chassis/dynamic-storage # **show expander-hw-detail**

SAS エクスパンダ ハードウェアの詳細のリストを表示します。デュアル エンクロージャのサポートを有効にした後、各 SAS エクスパンダのエンクロージャ ID を書き留めます。

例

この例では、SASエクスパンダでデュアルエンクロージャのサポートを設定します。

```
Server # scope chassis
Server /chassis # scope dynamic-storage
Server /chassis # show expander-hw-detail
Name       Id    ExpanderHwRev   SasAddress           EnclosureId
---------- ----- --------------- -------------------- -------------------------
SASEXP1    1     2               52cd02db305cba00     52cd02db305cb000
Name       Id    ExpanderHwRev   SasAddress           EnclosureId
---------- ----- --------------- -------------------- -------------------------
SASEXP2    2     2               52cd02db305ccb00     52cd02db305cb000

Server /chassis/dynamic-storage # set-dual-enclosure
Do you want to set different enclosure id to SAS Expanders?
Enter 'yes' --> to set different enclosure id
Enter 'no' --> to set same enclosure id
Enter your option 'yes/no' to continue-->yes
This dual enclosure feature should be applied only when the server nodes has UCS-S3260-DHBA
 adaptor and single path is zoned for each drives.
make sure both server blades are powered off.
Do you want to continue? Enter 'yes' to continue-->yes
set-dual-enclosure operation success

Server /chassis # show expander-hw-detail
Name       Id    ExpanderHwRev   SasAddress           EnclosureId
---------- ----- --------------- -------------------- -------------------------
SASEXP1    1     2               52cd02db305cba00     52cd02db305cb000
Name       Id    ExpanderHwRev   SasAddress           EnclosureId
---------- ----- --------------- -------------------- -------------------------
SASEXP2    2     2               52cd02db305ccb00     52cd02db305cb100
```



第 5 章

センサーの表示

この章は、次の内容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# **scope sensor**	センサー コマンド モードを開始します。
ステップ 2	Server /sensor # **show psu**	サーバの電源センサーの統計情報を表示します。
ステップ 3	Server /sensor # **show psu-redundancy**	サーバーの電源冗長センサーのステータスを表示します。

例

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# **scope sensor**	センサー コマンド モードを開始します。

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

例

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**]	サーバーの温度センサーの統計情報を表示します。

例

次に、温度センサーの統計情報を表示する例を示します。

```
Server# scope sensor
Server /sensor # show temperature
Name                     Sensor Status  Reading    Units      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**]	サーバーの電圧センサーの統計情報を表示します。

例

次に、電圧センサーの統計情報を表示する例を示します。

```
Server# scope sensor
Server /sensor # show voltage
Name                     Sensor Status  Reading    Units      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**]	サーバーの電流センサーの統計情報を表示します。

例

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。
[LED ステータス（LED Status）] 列	現在の LED の色（LED 付きの場合）。 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 [点灯（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、[消灯（Turn Off）] を選択します。 （注） この情報は、一部のCシリーズ サーバのみで表示されます。

例

次に、ストレージ センサーの情報を表示する例を示します。

```
Server# scope chassis
Server /chassis # show hdd
Name                 Status
-------------------- --------------------
HDD_01_STATUS        present
HDD_02_STATUS        present
HDD_03_STATUS        present
HDD_04_STATUS        present

Server /chassis #
```

前面パネルの動的温度しきい値の設定

始める前に

管理者権限を持つユーザとしてログインします。

手順

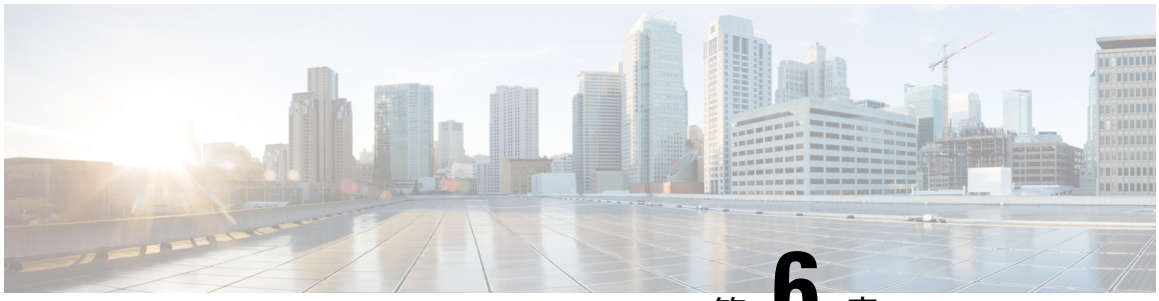
	コマンドまたはアクション	目的
ステップ 1	server # **scope sensor**	センサー コマンド モードを開始します
ステップ 2	server /sensor # **set fp-critical-temp** 臨界温度上限のしきい値	臨界温度上限のしきい値を設定します。有効な範囲は、8 ～ 50 です。
ステップ 3	server /sensor * # **commit**	温度のしきい値の値の変更をコミットします。

例

次に、ダイナミック フロント パネルの温度しきい値を設定する例を示します。

```
Server # scope sensor
Valid value for "fp-critical-temp" is from 8 to 50
Server /sensor # set fp-critical-temp 44
Server /sensor *# commit
Server /sensor # show temperature
Name                     Sensor Status  Reading    Units   Critical Min  Critical Max
 Non-Recoverable Min   Non-Recoverable Max
------------------       -------------  -------   ------   ------------  ------------
 --------------------  --------------------
VIC_SLOT1_TEMP             Normal         58.0       C          N/A          90.0
  N/A                  95.0
TEMP_SENS_FRONT            Normal         27.0       C          N/A          40.0
  N/A                  50.0
DDR4_P1_A1_TMP             Normal         29.0       C          N/A          85.0
  N/A                  90.0
DDR4_P2_G1_TMP             Normal         28.0       C          N/A          85.0
  N/A                  90.0
P1_TEMP_SENS               Normal         39.5       C          N/A          103.0
  N/A                  113.0
P2_TEMP_SENS               Normal         39.5       C          N/A          103.0
  N/A                  113.0
PSU1_TEMP                  Normal         27.0       C          N/A          65.0
  N/A                  70.0
PSU2_TEMP                  Normal         26.0       C          N/A          65.0
  N/A                  70.0
PCH_TEMP_SENS              Normal         36.0       C          N/A          85.0
  N/A                  90.0
RISER2_INLET_TMP           Normal         37.0       C          N/A          70.0
  N/A                  80.0
RISER1_INLET_TMP           Normal         36.0       C          N/A          70.0
```

```
                N/A                     80.0
```



第 6 章

リモート プレゼンスの管理

この章は、次の内容で構成されています。

仮想 KVM の管理

仮想 KVM コンソール

vKVM 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（vKVM）の直接接続をエミュレートします。vKVM 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。

Cisco KVM コンソールを使用する主な利点は次のとおりです。

- Cisco KVM コンソールは KVM、SOL、および vMedia への接続を提供しますが、Avocent KVM は KVM および vMedia への接続のみを提供します。
- KVM コンソールでは、vMedia 接続が KVM 起動マネージャで確立され、すべてのユーザーが使用できます。
- KVM コンソールには、ゲストからホストにテキストを貼り付ける際に、サポートされていない文字の高度な文字置換オプションが用意されています。
- KVM コンソールには、CIMC に vMedia マッピングを保存する機能があります。

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、vKVM 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

vKVM 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） vKVM コンソールの操作には、GUI 以外は使用できません。vKVM コンソールの起動手順については、『*Cisco UCS C* シリーズ サーバ統合管理コントローラ *GUI* 構成ガイド』を参照してください。

仮想 KVM のイネーブル化

始める前に

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

手順

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

例

次に、仮想 KVM をイネーブルにする例を示します。

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

Server /kvm #
```

仮想 KVM のディセーブル化

始める前に

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

手順

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

例

次に、仮想 KVM をディセーブルにする例を示します。

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

Server /kvm #
```

仮想 KVM の設定

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope kvm**	KVM コマンド モードを開始します。
ステップ 2	Server /kvm # **set enabled** {**yes** | **no**}	仮想KVMをイネーブルまたはディセーブルにします。
ステップ 3	Server /kvm # **set encrypted** {**yes** | **no**}	暗号化をイネーブルにすると、サーバーは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ーに接続されているすべてのモニターにも表示されます。
ステップ 6	Server /kvm # **set max-sessions** *sessions*	許可されているKVMの同時セッションの最大数を指定します。*sessions* 引数は、1 ～ 4 の範囲の整数になります。
ステップ 7	Server /kvm # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 8	Server /kvm # **show** [**detail**]	（任意）仮想 KVM の設定を表示します。

例

次に、仮想 KVM を設定し、その設定を表示する例を示します。

```
Server# scope kvm
Server /kvm # set enabled yes
Server /kvm *# set encrypted no
Server /kvm *# set kvm-port 2068
Server /kvm *# set max-sessions 4
Server /kvm *# set local-video yes
Server /kvm *# commit
Server /kvm # show detail
KVM Settings:
    Encryption Enabled: no
    Max Sessions: 4
    Local Video: yes
    Active Sessions: 0
    Enabled: yes
    KVM Port: 2068

Server /kvm #
```

次のタスク

GUI から仮想 KVM を起動します。

仮想メディアの設定

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope vmedia**	仮想メディア コマンド モードを開始します。
ステップ 2	Server /vmedia # **set enabled** {**yes** | **no**}	仮想メディアをイネーブルまたはディセーブルにします。デフォルトでは、仮想メディアはディセーブルになります。 （注） 仮想メディアをディセーブルにすると、仮想CD、仮想フロッピー、および仮想HDDデバイスがホストから切断されます。
ステップ 3	Server /vmedia # **set encryption** {**yes** | **no**}	仮想メディアの暗号化をイネーブルまたはディセーブルにします。
ステップ 4	Server /vmedia # **set low-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。

	コマンドまたはアクション	目的
		（注） UCS VIC P81E カードを持つサーバーに 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。

例

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 #
```

次のタスク

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

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope 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** [マウント オプション]	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 • サーバーに接続するためのユーザー名とパスワード
ステップ 3	Server /vmedia # **map-nfs** {**volume-name** |**remote-share** |**remote-file-path**} [マウント オプション]	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 • 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

	コマンドまたはアクション	目的
ステップ 4	Server /vmedia # **map-www** {**volume-name** |**remote-share** |**remote-file-path** [マウントオプション]	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 • サーバーに接続するためのユーザー名とパスワード

例

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

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope 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** 詳細	設定されたすべての vMedia マッピングの情報を表示します。

例

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
```

既存の Cisco IMC vMedia イメージの再マッピング

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope vmedia**	vMedia コマンド モードを開始します。
ステップ 2	Server /vmedia # **show saved-mappings**	利用可能な保存済みのマッピングを表示します。
ステップ 3	Server /vmedia # **remap** マッピング ボリューム	VMedia を再マッピングします。 （注） このコマンドの変数として保存されているマッピングのボリューム名を使用する必要があります。
ステップ 4	（任意） Server /vmedia # **show mappings**	マッピングされた vMedia の詳細を表示します。

例

次に、保存されているマッピングに vMedia イメージを再マッピングする例を示します。

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

```
Volume           Map-Status               Drive-Type Remote-Share             Remote-File
              Mount-Type
---------------- ------------------------ ---------- ------------------------
------------------------ --------
huu              OK                        CD         https://10.104.236.99...
ucs-c240-huu-3.0.0.33... www
Server/vmedia # show saved-mappings
Volume           Drive-Type Remote-Share             Remote-File              Mount-Type
---------------- ---------- ------------------------ ------------------------ --------
huu              CD         https://10.104.236.99... ucs-c240-huu-3.0.0.33... www
Server/vmedia #
```

Cisco IMC vMedia イメージの削除

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope vmedia**	vMedia コマンド モードを開始します。
ステップ 2	Server /vmedia # **delete-saved-mappings**	確認プロンプトで **yes** と入力します。保存済みのマッピングを削除します。
ステップ 3	Server /vmedia # **show saved-mappings**	削除されたので、保存されたマッピングは表示されません。

例

次の例は、保存されたマッピングの削除方法を示します。

```
Server # scope vmedia
Server/vmedia # show saved-mappings
Volume           Drive-Type Remote-Share             Remote-File              Mount-Type
---------------- ---------- ------------------------ ------------------------ --------
huu              CD         https://10.104.236.99... ucs-c240-huu-3.0.0.33... www
Server/vmedia # delete-saved-mappings
Purge saved mappings? Enter 'yes' to confirm -> yes
Server/vmedia # show saved-mappings
Server/vmedia #
```

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。

- シリアル　ポート A へのコンソール リダイレクション
- フロー制御なし
- SoL に設定されたのと同じボー レート
- VT-100 端末タイプ
- レガシー OS のリダイレクションが無効

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

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

Serial over LAN の設定

始める前に

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**}	このサーバーで SoL をイネーブルまたはディセーブルにします。

	コマンドまたはアクション	目的
ステップ 3	Server /sol # **set baud-rate** {**9600** | **19200** | **38400** | **57600** | **115200**}	システムが SoL 通信に使用するシリアル ボー レートを設定します。 （注） このボー レートは、サーバーのシリアル コンソールで設定したボー レートと一致する必要があります。
ステップ 4	（任意） Server /sol # **set comport** {**com0** | **com1**	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） このオプションを使用できるのは一部の C シリーズ サーバーだけです。使用できない場合、サーバは常に、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 を有効にして、RJ45 接続を無効にします。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 COM ポート 1 経由でルーティングされます。このポートは、SoL のみを介してアクセスできる内部ポートです。 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。

	コマンドまたはアクション	目的
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。

例

次に、SoL を設定する例を示します。

```
Server# scope sol
Server /sol # set enabled yes
Server /sol *# set baud-rate 115200
Server /sol *# commit
Server /sol # show
Enabled Baud Rate(bps)  Com Port
------- --------------- --------
yes     115200          com2
Server /sol # show detail
Serial Over LAN:
    Enabled: yes
    Baud Rate(bps): 115200
    Com Port: com2
Server /sol #
```

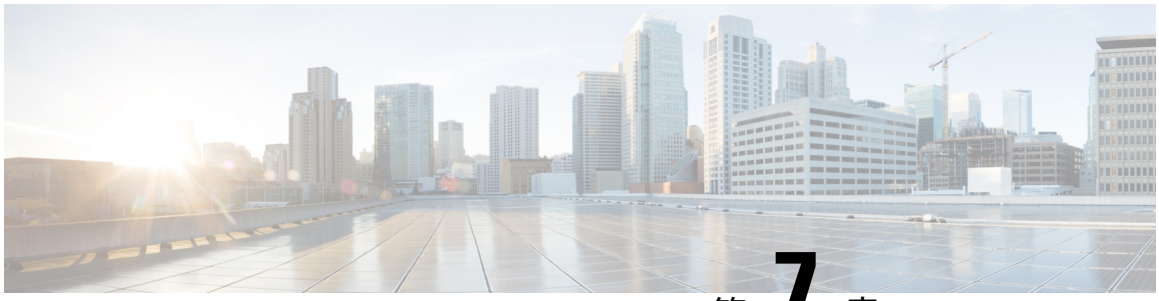
Serial Over LAN の起動

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。

次のタスク

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

ユーザー アカウントの管理

この章は、次の内容で構成されています。

Cisco USC C シリーズ M7 および以降のサーバー向けローカル ユーザーの構成

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope user** *usernumber*	ユーザー番号 *usernumber* に対するユーザー コマンド モードを開始します。
ステップ 2	Server /user # **set enabled** {**yes** |**no**\\	Cisco IMC でユーザー アカウントを有効または無効にします。
ステップ 3	Server /user # **set name** *username*	ユーザーのユーザー名を指定します。
ステップ 4	Server /user # **set role** {**readonly** |**user** |**admin**\\	ユーザーに割り当てるロールを指定します。ロールには、次のものがあります。 • readonly：このユーザーは情報を表示できますが、変更することはできません。 • user：このユーザーは、次の操作を実行できます。 • すべての情報を表示する • 電源のオン、電源再投入、電源のオフなどの電力制御オプションを管理する • KVM コンソールと仮想メディアを起動する • すべてのログをクリアする • ロケータ LED の点灯・消灯（リモート作業者に場所を示す） • タイム ゾーンを設定する • IP アドレスを ping する • admin：このユーザーは、GUI、CLI、IPMI で可能なすべての処理を実行できます。
ステップ 5	Server /user # **set user-typeCIMC|SNMP|IPMI**	ユーザーに割り当てるユーザー タイプを指定します。1 人のユーザーに対して 1 つまたは複数のユーザー タイプを選択できます。

	コマンドまたはアクション	目的
ステップ 6	Server /user # **set password**	パスワードを 2 回入力するように求められます。 （注） 強力なパスワードを有効にすると、ガイドラインに従ってパスワードを設定する必要があります。 • パスワードは 8 ～ 14 文字とすること。 • パスワードにユーザ名を含めることはできません。 • パスワードには次の 4 つのカテゴリの中から 3 つに該当する文字を含めること。 • 大文字の英字（A ～ Z） • 小文字の英字（a ～ z） • 10 進数の数字（0 ～ 9） • アルファベット以外の文字（!、@、#、$、%、^、&、*、 強力なパスワードを無効にすると、1 ～ 20 文字の範囲で任意の文字（英数字、特殊文字または整数）を使用してパスワードを設定できます。
ステップ 7	Server /user # **set ipmi-password** *password*	IPMI ユーザー タイプのパスワードを設定します。
ステップ 8	Server /user # **set v3priv-proto***None*|*CFB128_AES128*	この値は、SNMP ユーザー タイプに設定します。

	コマンドまたはアクション	目的
ステップ 9	Server /user # **set v3proto***HMAC128_SHA224*| *HMAC192_SHA256*| *HMAC256_SHA384* |*HMAC384_SHA512* |*HMAC_SHA96* |*None*	この値は、SNMP ユーザー タイプに設定します。
ステップ 10	Server /user # **set v3priv-auth-key***Priv_Auth_key*	必要に応じてキーを設定します。
ステップ 11	Server /user # **set v3auth-key***Auth_key*	必要に応じてキーを設定します。
ステップ 12	Server /user # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、ユーザー 5 を 1 つの admin と 3 つすべてのユーザー タイプとして構成する例を示します。

```
Server# scope user 5
Server /user # set enabled yes
Server /user *# set name UserName
Server /user *# set role readonly
Server /user *# set user-type CIMC,SNMP,IPMI
Server /user *# set password
Warning:
Strong Password Policy is enabled!

For CIMC protection your password must meet the following requirements:
        The password must have a minimum of 8 and a maximum of 14 characters.
        The password must not contain the User's Name.
       The password must contain characters from three of the following four categories.

            English uppercase characters (A through Z)
            English lowercase characters (a through z)
            Base 10 digits (0 through 9)
Please enter password:
Please confirm password:
Server /user *# set ipmi-password
Warning:
Strong Password Policy is enabled!

For CIMC protection your password must meet the following requirements:
        The password must have a minimum of 8 and a maximum of 20 characters for IPMI
users and
maximum 127 characters for Non IPMI users.
        The password must not contain the User's Name.
       The password must contain characters from three of the following four categories.

            English uppercase characters (A through Z)
            English lowercase characters (a through z)
            Base 10 digits (0 through 9)
            Non-alphabetic characters (!, @, #, $, %, ^, &, *, -, _, +, =)
Please enter ipmi-password:
Server /user *# set v3proto None
Server /user *# set v3priv-proto None
Server /user *# commit
```

ユーザーアカウントでの SSH キーの管理

SSH キーの設定

リリース 4.1.2 では、Cisco IMC はパスワード認証に加えて SSH RSA キーベースの認証を提供します。SSH キーは、認証に使用できる公開キーおよび秘密キーの RSA キー ペアのセットです。公開キーベースの認証は、パスワードベースの認証よりも強化されたセキュリティを提供します。

すべてのユーザーの SSH キーを構成するには、管理者権限を持つユーザーとしてログインする必要があります。管理者以外のユーザーの場合は、自分のアカウントにのみ認証してログインできる SSH キーを構成することができます。アカウントには、公開と秘密の SSH RSA キーペアを 1 つだけ構成できます。SSH キーは .pem または .pub フォーマットにする必要があります。

公開キーを使用して認証された Cisco IMC セッションは、パスワードの有効期限が切れてもアクティブのままです。また、パスワードの有効期限が切れた後に、公開 SSH キーを使用して新しいセッションを開始することもできます。一部の C シリーズ サーバで使用可能な**アカウント ロックアウト**オプションは、公開キー認証を使用するアカウントには適用されません。

SSH キーの追加

始める前に

- すべてのユーザーの SSH キーを追加するには、管理者権限を持つユーザーとしてログインする必要があります。
- 管理者以外のユーザーの場合は、自分のアカウントの公開キーのみを追加できます。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope user** *user-number*	ユーザーのコマンドモードを開始します。
ステップ 2	Server /user # **show-detail**	ユーザーアカウントの詳細を表示します。ユーザーに構成されている SSH キーの数を確認するには、`[SSH キー数（SSH Key Count）]` フィールドを参照します。
ステップ 3	Server /user # **scope ssh-keys**	SSH キー コマンドモードを開始します。
ステップ 4	Server /user/ssh-keys # **add-key 1 remote**	このオプションを使用して、リモート サーバーから SSH キーを追加します。

	コマンドまたはアクション	目的
		次の詳細を入力します。 **1.** リモート サーバー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） FTP、SCP または SFTP を選択した場合は、ユーザ名とパスワードの入力が求められます。 **2.** リモート サーバーのアドレスを指定します。 **3.** リモート ファイルのパスを指定します。 **4.** ユーザー名とパスワードを指定します。
ステップ 5	（任意） Server /user/ssh-keys # **add-key 2 paste**	このオプションを使用して、貼り付け方式で SSH キーを追加します。 SSH 公開キーを入力するためのダイアログを起動します。プロンプトが表示されたら、SSH キーの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 を押します。
ステップ 6	（任意） Server /user/ssh-keys # **show-detail**	アカウントに追加した公開 SSH キーを表示します。

例

1. この例では、リモート サーバーから SSH キーを追加します。

```
Server# scope user 1
Server /user # scope ssh-keys
Server /user/ssh-keys # add-key 1 remote
```

```
Enter the remote Protocol [tftp | ftp | sftp | scp | http]: scp
Enter the remote Server: 10.10.10.10
Enter the remote file Path: /home/xyz/publickey.pem
Server (RSA) key fingerprint is dd:b5:2b:07:ad:c0:30:b2:d5:6a:6a:78:80:85:93:b0
Do you wish to continue? [y/N]y
Username: xyz
Password:
SSH Public key added successfully
Server /user/ssh-keys #
```

2. この例では、貼り付け方式で SSH キーを追加します。

```
Server# scope user 1
Server /user # scope ssh-keys
Server /user/ssh-keys # add-key 2 paste
Please paste your ssh key here, when finished, press CTRL+D.
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDFOK17ZYbMMfGcxGrfxlupMqFyl1ZNIJohPxAStu41
OkItF9VrrhrfF1ZKOpogJinx3s0OcPfGLMSWEQkUq1zGlL8rAESZbi6z36WGFeZ93amJ3nfxDU7JWD9K
HmINixpX5XbbZeKQJvfSTptanmkjTQ8sq2iSMK0HL+G35i8BXmwIBLuEM+SWIEYjLaDAZ6aLKPxxddTr
FxWTP9QpzJAfQGlXXZSYauYb6OMNUxjgqFtB2XCiROZTzcj4n1XQRbzU+56HvHmowcOPhO81Btbun+xv
ksTeXbV3e9DVymjQK1qD2yY5h/EJdC0+9wGPyVmaT2bAOu4HbTsz8u4HFkTf
SSH Public key added successfully
Server /user/ssh-keys #
```

次のタスク

SSH キーを変更または削除します。

SSH キーの変更

始める前に

- すべてのユーザの SSH キーを変更するには、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。
- 管理者以外のユーザーの場合は、自分のアカウントの公開キーのみを変更できます。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope user** *user-number*	ユーザーのコマンドモードを開始します。
ステップ 2	Server /user # **show-detail**	ユーザーアカウントの詳細を表示します。ユーザーに構成されている SSH キーの数を確認するには、[SSH キー数（SSH Key Count）] フィールドを参照します。
ステップ 3	Server /user # **scope ssh-keys**	SSH キー コマンドモードを開始します。

	コマンドまたはアクション	目的
ステップ 4	Server /user/ssh-keys # **modify-key 1 remote**	このオプションを使用して、リモート サーバーから変更されたキーを追加します。次の詳細を入力します。 **1.** リモート サーバー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） FTP、SCP または SFTP を選択した場合は、ユーザ名とパスワードの入力が求められます。 **2.** リモート サーバーのアドレスを指定します。 **3.** リモート ファイルのパスを指定します。 **4.** ユーザー名とパスワードを指定します。
ステップ 5	（任意） Server /user/ssh-keys # **modify-key 2 paste**	このオプションを使用して、貼り付け方式で変更した SSH キーを追加します。 更新された公開 SSH キーを入力するためのダイアログを起動します。プロンプトが表示されたら、SSH キーの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 を押します。
ステップ 6	（任意） Server /user/ssh-keys # **show-detail**	アカウントで変更した更新済みの公開 SSH キーを表示します。

例

1. この例では、リモート サーバーから変更された SSH キーを追加します。

```
Server# scope user 1
Server /user # scope ssh-keys
Server /user/ssh-keys # modify-key 1 remote
Enter the remote Protocol [tftp | ftp | sftp | scp | http]: scp
Enter the remote Server: 10.10.10.10
Enter the remote file Path: /home/xyz/publickey.pem
Server (RSA) key fingerprint is dd:b5:2b:07:ad:c0:30:b2:d5:6a:6a:78:80:85:93:b0
Do you wish to continue? [y/N]y
Username: xyz
Password:
SSH Public key modified successfully
Server /user/ssh-keys #
```

2. この例では、貼り付け方法によって変更された SSH キーを追加します。

```
Server# scope user 1
Server /user # scope ssh-keys
Server /user/ssh-keys # modify-key 2 paste
Please paste your ssh key here, when finished, press CTRL+D.
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDFOK17ZYbMMfGcxGrfxlupMqFyl1ZNIJohPxAStu41
OkItF9VrrhrfF1ZKOpogJinx3s0OcPfGLMSWEQkUq1zGlL8rAESZbi6z36WGFeZ93amJ3nfxDU7JWD9K
HmINixpX5XbbZeKQJvfSTptanmkjTQ8sq2iSMK0HL+G35i8BXmwIBLuEM+SWIEYjLaDAZ6aLKPxxddTr
FxWTP9QpzJAfQGlXXZSYauYb6OMNUxjgqFtB2XCiROZTzcj4n1XQRbzU+56HvHmowcOPhO81Btbun+xv
ksTeXbV3e9DVymjQK1qD2yY5h/EJdC0+9wGPyVmaT2bAOu4HbTsz8u4HFkTf
SSH Public key modified successfully
Server /user/ssh-keys #
```

次のタスク

SSH キーを削除します。

SSH キーの削除

始める前に

- すべてのユーザの SSH キーを削除するには、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。
- 管理者以外のユーザーの場合は、自分のアカウントの公開キーのみを削除できます。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope user** *user-number*	ユーザーのコマンドモードを開始します。
ステップ 2	Server /user # **show-detail**	ユーザーアカウントの詳細を表示します。`SSH Key Count` フィールドには、ユーザーに対して構成されている SSH キーの数が表示されます。
ステップ 3	Server /user # **scope ssh-keys**	SSH キー コマンドモードを開始します。

	コマンドまたはアクション	目的
ステップ 4	Server /user/ssh-keys # **delete-key 1**	続行しますか？というメッセージがプロンプト表示されます。[y/N] が表示されます。
ステップ 5	y を押して削除を確定します。	
ステップ 6	（任意） Server /user/ssh-keys # **show-detail**	更新されたユーザーの詳細と SSH キーの数を表示します。

例

この例では、SSH キーを削除します。

```
Server# scope user 1
Server /user # scope ssh-keys
Server /user/ssh-keys # delete-key 1
This operation will delete the SSH key -
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDFOK17ZYbMMfGcxGrfxlupMqFyl1ZNIJohPxAStu41
OkItF9VrrhrfF1ZKOpogJinx3s0OcPfGLMSWEQkUq1zGlL8rAESZbi6z36WGFeZ93amJ3nfxDU7JWD9K
HmINixpX5XbbZeKQJvfSTptanmkjTQ8sq2iSMK0HL+G35i8BXmwIBLuEM+SWIEYjLaDAZ6aLKPxxddTr
FxWTP9QpzJAfQGlXXZSYauYb6OMNUxjgqFtB2XCiROZTzcj4n1XQRbzU+56HvHmowcOPhO81Btbun+xv
ksTeXbV3e9DVymjQK1qD2yY5h/EJdC0+9wGPyVmaT2bAOu4HbTsz8u4HFkTf
Do you wish to continue? [y/N]y
SSH Public key deleted successfully
Server /user/ssh-keys #
```

非 IPMI ユーザー モード

リリース4.1 では、IPMI と非 IPMI の両方のユーザー モードを切り替えることができる**ユーザー モード**と呼ばれる新しいユーザー設定オプションが導入されています。非 IPMI ユーザー モードの導入では、ユーザー向けに強化されたパスワードセキュリティと、IPMI 2.0 標準による制約により以前のリリースで制限された BMC データベースに対してセキュリティ強化を提供します。非 IPMI ユーザー モードでは、127 文字を使用してユーザー パスワードを設定できますが、IPMI モードのユーザーはパスワードの長さが 20 文字に制限されます。非 IPMI ユーザー モードでは、このモードで設定されたユーザーに対してより強力なパスワードを設定できます。

次の場合に、ユーザー モードの切り替え中に発生する次の設定変更を考慮する必要があります。

- 非 IPMI モードに切り替えると、IPMI 経由の IPMI はサポートされません。
- 非 IPMI から IPMI モードに切り替えて、すべてのローカル ユーザーを削除し、ユーザー クレデンシャルをデフォルトのユーザー名とパスワードに戻します。続いてログインすると、デフォルトのパスワードを変更するように求められます。

  IPMI から非 IPMI モードに切り替えた場合、ユーザー データは影響を受けません。
- ファームウェアを 4.1 よりも低いバージョンにダウングレードします。ユーザー モードが非 IPMI の場合、はすべてのローカル ユーザーを削除し、ユーザー クレデンシャルをデ

フォルトのユーザー名とパスワードに戻します。続いてログインすると、デフォルトのパスワードを変更するように求められます。

（注） 工場出荷時の初期状態にリセットすると、ユーザー モードは IPMI モードに戻ります。

IPMI から非 IPMI へのユーザー モードの切り替え

始める前に

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# **scope user-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 # **scope user-mode**	ユーザー モード コマンド モードを開始します。
ステップ 3	Server /user-policy/user-mode # **set user-mode non-ipmi**	IPMI 以外のユーザー モードに切り替えるには、確認プロンプトでyを入力します。
ステップ 4	Server /user-policy/user-mode * # **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 /user-policy/user-mode # **show detail**	ユーザー モードを表示します。

例

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 # scope user-mode
Server /user-policy/user-mode # set user-mode non-ipmi
Server /user-policy/user-mode *# commit
Warning: This will enable NON-IPMI based user mode.
         Converting to Non-IPMI User Mode disables IPMI Services and removes IPMI user
support.
         SSH, KVM, Webserver, XMAPI and Redfish sessions will be disconnected.
Do you wish to continue? [y/N] y
Connection to 10.10.10.10 closed by remote host.
Connection to 10.10.10.10 closed.
Server /user-policy/user-mode # show detail
User Mode:
```

```
    User mode for IPMI accessibility: non-ipmi
Server /user-policy/user-mode #
```

非 IPMI から IPMI へのユーザー モードの切り替え

始める前に

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# **scope user-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 # **scope user-mode**	ユーザー モード コマンド モードを開始します。
ステップ 3	Server /user-policy/user-mode # **set user-mode ipmi**	IPMI ユーザー モードに切り替えるには、確認プロンプトでyを入力します。 （注） IPMIユーザーモードに切り替えると、すべての UCS ユーザーが削除され、デフォルトのユーザー名とパスワードに戻ります。
ステップ 4	Server /user-policy/user-mode * # **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 /user-policy/user-mode # **show detail**	ユーザー モードを表示します。

例

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 # scope user-mode
Server /user-policy/user-mode # set user-mode ipmi
Server /user-policy/user-mode *# commit
Warning: This will enable IPMI based user mode.
         Converting to IPMI User Mode deletes all UCS users and reverts to default
userid/password.
         SSH, KVM, Webserver, XMAPI and Redfish sessions will be disconnected.
Do you wish to continue? [y/N] y
Connection to 10.10.10.10 closed by remote host.
Connection to 10.10.10.10 closed.
Server /user-policy/user-mode # show detail
User Mode:
```

```
    User mode for IPMI accessibility: ipmi
Server /user-policy/user-mode #
```

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。

始める前に

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# **scope user-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 # **set password-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。

例

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 #
```

パスワードの有効期限切れ

パスワードが期限切れになる有効期限を設定できます。管理者はこの期間を日単位で設定できます。この設定はすべてのユーザに対して共通です。パスワードが期限切れになると、ユーザに対してログイン時にこのことが通知され、パスワードをリセットするまではログインできなくなります。

（注） 古いデータベースにダウングレードすると、既存のユーザが削除されます。データベースはデフォルト設定に戻ります。以前に設定されたユーザが消去され、データベースは空になります。つまり、データベースにはデフォルトのユーザ名「admin」とパスワード「password」が設定されます。サーバにはデフォルトのユーザ データベースが残るため、デフォルト クレデンシャル変更機能が有効になります。つまり、「admin」ユーザはダウングレード後にデータベースに初めてログインするときに、デフォルトのクレデンシャルを変更する必要があります。

パスワード設定時刻

既存のすべてのユーザの「パスワード設定時刻」は、移行またはアップグレードの実行時刻に設定されます。新しいユーザ（アップグレード後に作成されるユーザ）の場合、パスワード設定時刻はそのユーザが作成され、パスワードが設定された時刻に設定されます。ユーザ全般（新規および既存）について、パスワードが変更されるたびにパスワード設定時刻が更新されます。

ユーザー認証の優先順位の構成

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope user-policy**	TACACS+ コマンド モードを開始します。
ステップ 2	Server/user-policy # **set authentication-precedence** *User Database name*	ユーザー データベースのコンマ区切りリストを入力します。
ステップ 3	Server/user-policy # **commit**	

例

```
Server # scope user-policy
Server /user-policy # set authentication-precedence DB1,DB2
Server /user-policy* # commit
```

ユーザ パスワードのリセット

[パスワードの変更（Change Password）] オプションを使用してパスワードを変更できます。

（注）
- このオプションは、admin としてログインしているときには使用できません。読み取り専用の権限をもつ設定済みのユーザのパスワードだけが変更できます。
- パスワードを変更すると、Cisco IMC からログアウトされます。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope user** *user ID*	選択したユーザ コマンド モードを開始します。
ステップ 2	Server /chassis/user # **set password**	パスワードの要件の指示を読み、現在のパスワード、新しいパスワード、パスワードの確認をそれぞれのプロンプトで入力します。
ステップ 3	Server /chassis/user * # **commit**	トランザクションをシステムの設定にコミットします。

例

この例では、設定されているユーザのパスワードを変更する方法を示します。

```
Server # scope user 2
Server /chassis/user # set password
Warning:
Strong Password Policy is enabled!
For CIMC protection your password must meet the following requirements:
      The password must have a minimum of 8 and a maximum of 20 characters.
       The password must not contain the User's Name.
       The password must contain characters from three of the following four categories.

            English uppercase characters (A through Z)
            English lowercase characters (a through z)
            Base 10 digits (0 through 9)
            Non-alphabetic characters (!, @, #, $, %, ^, &, *, -, _, +, =)
Please enter current password:Testabcd1
Please enter password: Testabcd2
Please confirm password: Testabcd2
Server /chassis/user * # commit
Server /chassis/user #
```

ユーザに対するパスワード期限切れの設定

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope user-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 # **scope password-expiration**	パスワードの有効期限コマンド モードを開始します。
ステップ 3	Server /user-policy/password-expiration # **set password-expiry-duration** *0 ～ 3650* の整数	既存のパスワードに設定できる有効期間（その時間以後、新しいパスワードを設定するか、または既存のパスワードを変更します。）範囲は 0 ～ 3650 日です。0 を入力すると、このオプションが無効になります。
ステップ 4	Server /user-policy/password-expiration * # **set notification-period** *0 ～ 15* の整数	パスワードの期限が切れる時間を通知します。0 日から 15 日までの値を入力します。0 を入力すると、このオプションが無効になります。
ステップ 5	Server /user-policy/password-expiration * # **set grace-period** *0 ～ 5* の整数	既存のパスワードをまだ使用できる期間。この期間の後、パスワードは期限切れになります。0 日から 5 日までの値を入力します。0 を入力すると、このオプションが無効になります。
ステップ 6	Server /user-policy/password-expiration * # **set password-history** *0 ～ 5* の整数	パスワードが入力された回数。このフィールドを有効にすると、指定された回数を超えてパスワードを繰り返し使用することができなくなります。0 ～ 5 の間の値を入力します。0 を入力すると、このオプションが無効になります。
ステップ 7	Server /user-policy/password-expiration *# **commit**	トランザクションをコミットします。
ステップ 8	（任意） Server /user-policy/password-expiration # **show detail**	パスワードの有効期限の詳細を表示します。
ステップ 9	（任意） Server /user-policy/password-expiration # **restore**	確認のプロンプトで、**yes** と入力してパスワード有効期限の設定をデフォルト値に復元します。

例

この例では、パスワードの有効期限を設定し、設定をデフォルト値に戻します。

```
Server # scope user-policy
Server /user-policy # scope password-expiration
Server /user-policy/password-expiration # set password-expiry-duration 5
Server /user-policy/password-expiration * # set notification-period 2
Server /user-policy/password-expiration *# set grace-period 1
Server /user-policy/password-expiration *# set password-history 4
Server /user-policy/password-expiration *# commit
Server /user-policy/password-expiration # show detail
Password expiration parameters:
 Valid password duration: 5
 Number of stored old passwords: 4
 Notification period: 2
 Grace period: 1
Server /user-policy/password-expiration #
Restoring the password expiry parameters to default values:
Server /user-policy/password-expiration # restoreAre you sure you want to restore
User password expiration parameters to defaults?
Please enter 'yes' to confirm:yes
Server /user-policy/password-expiration #
```

LDAP サーバー

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持する軽量ディレクトリ アクセス プロトコル（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 ユーザー データベース内に見つからないユーザー アカウントに関するユーザー認証とロール許可は、LDAP サーバーによって実行されます。LDAP ユーザー認証の形式は username@domain.com です。

サーバの Active Directory 設定で暗号化を有効にすると、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。

Configuring the LDAP Server

The Cisco IMC can be configured to use LDAP for user authentication and authorization. To use LDAP, configure users with an attribute that holds the user role and locale information for the Cisco IMC. You can use an existing LDAP attribute that is mapped to the Cisco IMC user roles and locales or you can modify the LDAP schema to add a new custom attribute, such as the CiscoAVPair attribute, which has an attribute ID of 1.3.6.1.4.1.9.287247.1.

Important For more information about altering the schema, see the article at http://technet.microsoft.com/en-us/library/bb727064.aspx.

Note This example creates a custom attribute named CiscoAVPair, but you can also use an existing LDAP attribute that is mapped to the Cisco IMC user roles and locales.

If you are using Group Authorization on the Cisco IMC LDAP configuration, then you can skip Steps 1-4 and perform the steps listed in the *Configuring LDAP Settings and Group Authorization in Cisco IMC* section.

The following steps must be performed on the LDAP server.

Procedure

ステップ 1 Ensure that the LDAP schema snap-in is installed.

ステップ 2 Using the schema snap-in, add a new attribute with the following properties:

Properties	Value
Common Name	`CiscoAVPair`
LDAP Display Name	`CiscoAVPair`
Unique X500 Object ID	`1.3.6.1.4.1.9.287247.1`
Description	`CiscoAVPair`
Syntax	`Case Sensitive String`

ステップ 3 Add the CiscoAVPair attribute to the user class using the snap-in:

a) Expand the **Classes** node in the left pane and type `U` to select the user class.
b) Click the **Attributes** tab and click **Add**.
c) Type `C` to select the CiscoAVPair attribute.
d) Click **OK**.

ステップ 4 Add the following user role values to the CiscoAVPair attribute, for the users that you want to have access to Cisco IMC:

Role	CiscoAVPair Attribute Value
admin	`shell:roles="admin"`
user	`shell:roles="user"`
read-only	`shell:roles="read-only"`

Note For more information about adding values to attributes, see the article at http://technet.microsoft.com/en-us/library/bb727064.aspx.

What to do next

Use the Cisco IMC to configure the LDAP server.

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。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ldap**	LDAP コマンド モードを開始します。
ステップ 2	Server /ldap # **set enabled** {**yes** |**no**\\	LDAP セキュリティをイネーブルまたはディセーブルにします。LDAPセキュリティがイネーブルの場合、ローカル ユーザーデータベースにないユーザー アカウントに対し、ユーザー認証とロール許可が LDAP によって実行されます。
ステップ 3	Server /ldap # **set domain***LDAP* ドメイン名	LDAP ドメイン名を指定します。
ステップ 4	Server /ldap # **set timeout** *seconds*	LDAP 検索操作がタイムアウトするまで 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 # **set base-dn** *domain-name*	LDAP サーバーで検索するベース DN を指定します。
ステップ 6	Server /ldap # **set attribute** 名	ユーザーのロールとロケール情報を保持する LDAP 属性を指定します。このプロパティは、常に、名前と値のペアで指定されます。システムは、ユーザ

	コマンドまたはアクション	目的
		レコードで、この属性名と一致する値を検索します。 Cisco IMC ユーザのロールおよびロケールにマップされた既存の LDAP 属性を使用するか、CiscoAVPair 属性など、次の属性 ID を持つカスタム属性を作成できます。 `1.3.6.1.4.1.9.287247.1` （注） このプロパティを指定しない場合、ユーザーアクセスが拒否されます。
ステップ 7	Server /ldap # **set filter-attribute**	アカウント名属性を指定します。Active Directory を使用している場合は、このフィールドに **sAMAccountName** を指定します。
ステップ 8	Server /ldap # **scope secure**	セキュリティ LDAP モードを開始します。
ステップ 9	セキュア LDAP を有効にして、証明書をリモートでダウンロードするか、証明書を貼り付けます。	次のいずれかの操作を行います。 1. Server /ldap # **secure-ldap** *disabled|enabled paste tftp | ftp | sftp | scp | http* 証明書の内容を貼り付け るよう求められます。 2. 証明書の内容を貼り付けて **CTRL+D** キーを押します。 確認のプロンプトが表示されます。 3. 確認プロンプトで、**y** と入力します。 これにより LDAP CA 証明書のダウンロードが開始されます。 または 1. Server /ldap # **secure-ldap** *disabled|enabled remote tftp | ftp | sftp | scp | http IP Address LDAP CA Certificate file*

	コマンドまたはアクション	目的
		（注） Cisco UCS C シリーズ サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバー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 サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[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。 **2.** 確認プロンプトで、**y** と入力します。 これにより LDAP CA 証明書のダウンロードが開始されます。
ステップ 10	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 11	Server /ldap # **show** [**detail**]	（任意）LDAP の設定を表示します。

例

この例では、リモート ダウンロード オプションを使用して LDAP を構成します。

```
Server# scope ldap
Server /ldap # set enabled yes
Server /ldap *# set domain sample-domain
Server /ldap *# set timeout 60
Server /ldap *# set base-dn example.com
Server /ldap *# set attribute CiscoAVPair
Server /ldap *# set filter-attribute sAMAccountName
Server /ldap *# scope secure
Server /ldap/secure *# secure-ldap enabled remote ftp xx.xx.xx.xx filename
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1282  100  1282    0     0   1247      0  0:00:01  0:00:01 --:--:--  1635
100  1282  100  1282    0     0   1239      0  0:00:01  0:00:01 --:--:--  1239
  You are going to overwrite the LDAP CA Certificate.
  Are you sure you want to proceed and overwrite the LDAP CA Certificate? [y|N]y
LDAP CA Certificate is downloaded successfully
Server /ldap/secure *# commit
Server /ldap # exit
Server /ldap # show detail
LDAP Settings:
    Enabled: yes
    Domain: sample-domain
    BaseDN: example.com
    Timeout: 60
    Filter-Attribute: sAMAccountName
Server /ldap #
```

この例では、証明書の貼り付けオプションを使用してセキュア LDAP を構成します。

```
Server# scope ldap
Server /ldap # set enabled yes
Server /ldap *# set domain sample-domain
Server /ldap *# set timeout 60
Server /ldap *# set base-dn example.com
Server /ldap *# set attribute CiscoAVPair
Server /ldap *# set filter-attribute sAMAccountName
Server /ldap *# scope secure
Server /ldap/secure *# secure-ldap enabled ftp paste

 Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIIDdzCCAl+gAwIBAgIQV06yJcJPAYNO8Cp+FYQttjANBgkqhkiG9w0BAQsFADBO
MRIwEAYKCZImiZPyLGQBGRYCaW4xGzAZBgoJkiaJk/IsZAEZFgs0T0JKUkEySkhC
UTEbMBkGA1UEAxMSV0lOLTRPQkpSQTJKSEJRLUNBMB4XDTE2MDIyNTE3MDczNloX
DTIxMDIyNTE3MTczM1owTjESMBAGCgmSJomT8ixkARkWAmluMRswGQYKCZImiZPy
LGQBGRYLNE9CSlJBMkpIQlExGzAZBgNVBAMTEldJTi00T0JKUkEySkhCUS1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMM2cdgmrPTkZe4K2zI+EbeZ
mfQnjfiUz8OIY97w8lC/2S4qK46T+fnX13rXe8vvVHAO5wgPDVQTGS4nlF46A6Ba
FK+krKcIgFrQB1gnF74qs/ln1YtKHNBjrvg5KyeWFrA7So6Mi2XEw8w/zMPL0d8T
b+LM1YnhnuXA9G8gVCJ/iUhXfMpB20L8sv30Mek7bw8x2cxJYTuJAviVIrjSwU5j
fO3WKttRuyFpeOIi00weklpF0+8D3Z9mBinoTbL2pl0U32am6wTI+8WmtJ+8W68v
jH4Y8YBY/kzMHdpwjpdZkC5pE9BcM0rL9xKoIu6X0kSNEssoGnepFyNaH3t8vnMC
AwEAAaNRME8wCwYDVR0PBAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYE
FBAUulHTAWBT1OBz8IgAEzXsfcCsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3
DQEBCwUAA4IBAQAzUMZr+0r1dWkVfFNBd7lu8tQbAEJf/A7PIKnJGNoUq8moAGs4
pMndoxdpNGZhYCWDWX3GWdeF1HqZHhb38gGQ9ylu0pIK7tgQufZmeCBH6T7Tzq/w
Dq+TMFGIjXF84xW3N665y4ePgUcUI7e/6aBGcGkGeUYodBPtExe28tQyeuYwD4Zj
nLuZKkT+I4PAYygVCqxDGsvfRHDpGneb3R+GeonOf4ED/0tn5PLSL9khb9qkHu/V
```

```
dO3/HmKVzUhloTDBuAMq/wES2WZAWhGr3hBc4nWQNjZWEMOKDpYZVK/GhBmNF+xi
eRcFqgh64oEmH9qAp0caGS1e7UyYaN+LtPRe
-----END CERTIFICATE-----
CTRL+D
  You are going to overwrite the LDAP CA Certificate.
  Are you sure you want to proceed and overwrite the LDAP CA Certificate? [y|N]
y

Server /ldap/secure *# commit
Server /ldap # exit
Server /ldap # show detail
LDAP Settings:
    Enabled: yes
    Domain: sample-domain
    BaseDN: example.com
    Timeout: 60
    Filter-Attribute: sAMAccountName
Server /ldap #
```

次のタスク

グループ許可用にLDAPグループを使用する場合は、「*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。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ldap**	LDAP コマンド モードを開始して、AD を設定します。
ステップ 2	Server /ldap# **scope ldap-group-rule**	LDAP グループ ルール コマンド モードを開始して、AD を設定します。
ステップ 3	Server /ldap/ldap-group-rule # **set group-auth** {**yes** |**no**}	LDAP グループ許可をイネーブルまたはディセーブルにします。

	コマンドまたはアクション	目的
ステップ 4	Server /ldap # **scope role-group** *index*	設定に使用可能なグループ プロファイルのいずれかを選択します。ここで、*index* は 1 から 28 までの数字です。
ステップ 5	Server /ldap/role-group # **set name** *group-name*	サーバーへのアクセスが許可されているグループの名前を AD データベースに指定します。
ステップ 6	Server /ldap/role-group # **set domain** *domain-name*	グループが存在する必要がある AD ドメインを指定します。
ステップ 7	Server /ldap/role-group # **set role** {**admin** | **user** | **readonly**}	この AD グループのすべてのユーザーに割り当てられる権限レベル（ロール）を指定します。次のいずれかになります。 • **admin**：ユーザーは使用可能なすべてのアクションを実行できます。 • **user**：ユーザーは、次のタスクを実行できます。 • すべての情報を表示する • 電源のオン、電源再投入、電源のオフなどの電力制御オプションを管理する • KVM コンソールと仮想メディアを起動する • すべてのログをクリアする • ロケータ LED の点灯・消灯（リモート作業者に場所を示す） • **readonly**：ユーザーは情報を表示できますが、変更することはできません。
ステップ 8	Server /ldap/role-group # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、LDAP グループの許可を設定する例を示します。

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

Server /ldap/role-group #
```

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# **scope ldap**	LDAP コマンド モードを開始して、AD を設定します。
ステップ 2	Server /ldap# **scope ldap-group-rule**	LDAP グループ ルール コマンド モードを開始して、AD を設定します。
ステップ 3	Server /ldap/ldap-group-rule # **set group-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。

例

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 #
```

TACACS+ 認証

4.1（3b） リリース以降、Cisco IMC は Terminal Access Controller Access-Control System Plus（TACACS+）ユーザー認証をサポートします。Cisco IMC は、最大 6 つの TACACS+ リモート サーバーをサポートします。ユーザーが正常に認証されると、ユーザー名に **[（TACACS+）]** が追加されます。これは Cisco IMC インターフェースにも表示されます。

TACACS+ 認証のイネーブル化 （149 ページ） を参照して TACACS+ 認証を有効化します。
Cisco IMC はまた、TACACS+ リモート サーバーにアクセスできない場合のユーザー認証の優先順位もサポートします。ユーザー認証の優先順位の構成 （136 ページ） を使用してユーザー認証の優先順位の構成が行えます。

TACACS+サーバ設定

ユーザーの特権レベルは、そのユーザーに設定された **[cisco-av-pair]** 値に基づいて計算されます。TACACS+ サーバに **[cisco-av-pair]** を作成する必要があります。ユーザーは既存の TACACS+ 属性は使用できません。

cisco-av-pair 属性のサポートされる 3 つのシンタックスは、次のとおりです。

- **admin** 特権の場合：**[cisco-av-pair=shell:roles=”admin”]**
- **user** 権限の場合：**[cisco-av-pair=shell:roles=”user”]**
- **read-only** 権限の場合：**[cisco-av-pair=shell:roles=”read-only”]**

必要に応じて、**[comma]** を区切り文字として使用して、さらにロールを追加できます。

（注） **[cisco-av-pair]** が TACACS+ サーバーで構成されていない場合、そのサーバーのユーザーには **[read-only]** 権限があります。

TACACS+ 認証のイネーブル化

始める前に

Terminal Access Controller Access-Control System（TACACS+）ベースのユーザ認証を構成する前に、ユーザーの特権レベルが **[cisco-av-pair]** 値に基づいて TACACS+ サーバーで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# **scope tacacs+**	TACACS+ コマンド モードを開始します。
ステップ 2	Server/tacacs+ # **set enabled** *yes*|*no*	
ステップ 3	Server/tacacs+ # **set fallback-only-on-no-connectivity** *yes*|*no*	**fallback-only-on-no-connectivity** を有効にする場合は、**Y** を入力して確認します。
ステップ 4	Server/tacacs+ # **set timeout** タイムアウト時間（秒）	5 ～ 30の値を入力してください
ステップ 5	Server/tacacs+ # **restore**	タイム アウトした場合に TACACS+ 構成をデフォルトに復元したい場合、**yes** と入力して確定してください。
ステップ 6	Server/tacacs+ # **commit**	システムで変更を保存します。

例

```
Server # scope tacacs+
Server /tacacs+ # set enabled yes
Server /tacacs+ # set fallback-only-on-no-connectivity yes

Warning: If TACACS+ and fallback option is enabled, then the fallback to the next
         precedence database happens only when CIMC is not able to connect to any
         of the configured TACACS+ servers.
Do you wish to continue? [y/N] y
Server /tacacs+ # set timeout 5
Server /tacacs+ # restore
Are you sure you want to restore TACACS+ configuration to defaults?
Please enter 'yes' to confirm: yes
Restored TACSCS+ default configuration.

Server /tacacs+ # commit
```

TACACS+ リモート サーバー設定の構成

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope tacacs+**	TACACS+ コマンド モードを開始します。
ステップ 2	Server# **scope tacacs-server***Server Number*	TACACS サーバー コマンド モードを開始します。
ステップ 3	Server/tacacs+/tacacs-server # **set tacacs-port** *Port Number*	1 ～ 65535 の値を入力します。
ステップ 4	Server/tacacs+/tacacs-server # **set tacacs-key** *Server Key*	リモート TACACS+ サーバーで構成されているのと同じキーを入力します。
ステップ 5	Server/tacacs+/tacacs-server # **set tacacs-server** *Server IP Address*	リモート TACACS+ サーバーの IP アドレスを入力します。
ステップ 6	Server/tacacs+/tacacs-server # **restore**	タイム アウトした場合に TACACS+ 構成をデフォルトに復元したい場合、**[yes]** と入力して確定してください。

例

```
Server # scope tacacs+
Server # scope tacacs-server 1
Server /tacacs+/tacacs-server # set tacacs-port 6
Server /tacacs+/tacacs-server # set tacacs-key xxx
Server /tacacs+/tacacs-server # set tacacs-server xx.xx.xx.xx
Server /tacacs+/tacacs-server # restore
Are you sure you want to restore TACACS+ configuration to defaults?
Please enter 'yes' to confirm: yes
Restored TACSCS+ default configuration.

Server /tacacs+/tacacs-server # commit
```

LDAP 証明書の概要

Cisco C シリーズ サーバでは、LDAP バインディング ステップ時に、LDAP クライアントがインストール済み CA 証明書またはチェーン CA 証明書に対してディレクトリ サーバ証明書を検証できるようになっています。リモートユーザー認証のために信頼されたポイントまたはチェーン証明書を Cisco IMC に入力できないことにより、誰でもユーザー認証用のディレクトリ サーバーを複製してセキュリティ違反が発生する恐れがある場合は、この機能を導入します。

LDAP クライアントには、暗号化 TLS/SSL 通信中にディレクトリ サーバ証明書を検証できる新しい設定オプションが必要です。

LDAP CA 証明書のエクスポート

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ldap**	LDAP コマンド モードを開始します。
ステップ 2	Server# /ldap **scope binding-certificate**	LDAP CA 証明書バインド コマンド モードを開始します。
ステップ 3	Server /ldap/binding-certificate # **export-ca-certificate** *remote-protocol IP アドレス LDAP CA 証明書ファイル*	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

	コマンドまたはアクション	目的
		（注） Cisco UCS C シリーズ サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバー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 サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[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。 証明書のエクスポートを開始します。

例

この例では、LDAP 証明書をエクスポートします。

```
Server # scope ldap
Server /ldap # scope binding-certificate
Server /ldap/binding-certificate #  export-ca-certificate tftp 172.22.141.66 test.csv
 Initiating Export
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1262    0     0  100  1262      0   1244  0:00:01  0:00:01 --:--:--  1653
100  1262    0     0  100  1262      0   1237  0:00:01  0:00:01 --:--:--  1237
LDAP CA Certificate is exported successfully
Server /ldap/binding-certificate #
```

LDAP バインディングのテスト

始める前に

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

（注） [Enable Encryption] チェックボックスと [Enable Binding CA Certificate] チェックボックスをオンにする場合は、[LDAP Server] フィールドに LDAP サーバーの完全修飾ドメイン名（FQDN）を入力します。LDAP サーバーの FQDN を解決するには、Cisco IMC ネットワークの優先 DNS を設定して適切な DNS IP アドレスを指定します。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ldap**	LDAP コマンド モードを開始します。
ステップ 2	Server# /ldap **scope binding-certificate**	LDAP CA 証明書バインド コマンド モードを開始します。
ステップ 3	Server /ldap/binding-certificate # **test-ldap-binding** ユーザ名	パスワードのプロンプトが表示されます。
ステップ 4	対応するパスワードを入力します。	ユーザを認証します。

例

次に、LDAP ユーザ バインドをテストする例を示します。

```
Server # scope ldap
Server /ldap # scope binding-certificate
Server /ldap/binding-certificate # test-ldap-binding user
Password:
diagldapbinding: Authenticated by LDAP
User user authenticated successfully.
Server /ldap/binding-certificate #
```

LDAP CA 証明書の削除

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ldap**	LDAP コマンド モードを開始します。
ステップ 2	Server# /ldap **scope binding-certificate**	LDAP CA 証明書バインド コマンド モードを開始します。
ステップ 3	Server /ldap/binding-certificate # **delete-ca-certificate**	確認のプロンプトが表示されます。
ステップ 4	確認プロンプトで、**y** と入力します。	これで LDAP CA 証明書が削除されます。

例

この例は、LDAP 証明書を削除します。

```
Server # scope ldap
Server /ldap # scope binding-certificate
Server /ldap/binding-certificate # delete-ca-certificate
You are going to delete the LDAP CA Certificate.
 Are you sure you want to proceed and delete the LDAP CA Certificate? [y|N]y
LDAP CA Certificate is deleted successfully
Server /ldap/binding-certificate #
```

ユーザ セッションの表示

手順

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

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

名前	説明
[Session ID] カラム	セッションの固有識別情報。
BMC セッション ID	BMC セッションの識別子。
[User name (ユーザー名)] カラム	ユーザーのユーザー名。
[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。

名前	説明
[Session Type] カラム	ユーザーがサーバー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。 • [Web GUI（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] : ユーザーがシリアル ポートを使用してサーバーに接続されていることを示します。 • **[XML API]** — ユーザーが XML API を使用してサーバーに接続していることを示します。 • **[Redfish]** — ユーザーが Redfish API を使用してサーバーに接続していることを示します。
[Action] カラム	このカラムには、SoL が有効である場合は [該当なし（N/A）] が表示され、SoL が無効である場合は [終了（Terminate）] が表示されます。Web UI で [終了（Terminate）] をクリックすると、セッションを終了できます。

例

次に、現在のユーザー セッションに関する情報を表示する例を示します。

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

Server /user #
```

ユーザー セッションの終了

始める前に

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

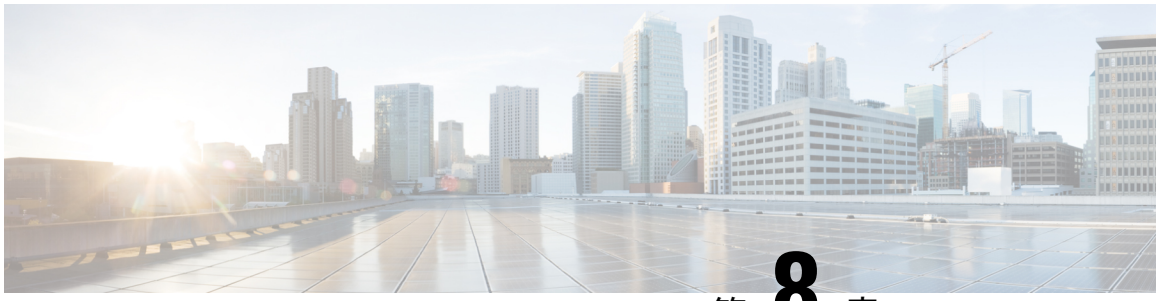
手順

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

例

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

```
Server# show user-session
ID     Name              IP Address        Type         Killable
------ ---------------- ----------------- ------------ --------
10     admin            10.20.41.234      CLI          yes
15     admin            10.20.30.138      CLI          yes
Server# scope user-session 15
Server /user-session # terminate
User session 15 terminated.

Server /user-session #
```



第 8 章

ネットワーク関連の設定

この章は、次の内容で構成されています。

サーバ NIC の設定

サーバー NIC

NIC モード

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

- **[専用（Dedicated）]**：Cisco IMC へのアクセスに管理ポートを使用します。
- **[Cisco カード（Cisco Card）]**：アダプタ カード上の任意のポートを Cisco IMC へのアクセスに使用できます。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。
- **[共有 LOM（Shared LOM）]**：Cisco IMC にアクセスするために使用できる LOM（LAN On Motherboard）ポート。

- **[共有 LOM 拡張（Shared LOM Extended）]**：Cisco IMC へのアクセスに使用できる 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 をサポートするスロットに装着する必要があります。

（注） [共有 LOM（Shared LOM）] ポートおよび [共有 LOM 拡張（Shared LOM Extended）] ポートは、一部の C シリーズ サーバでのみ使用できます。

（注） その他の UCS C シリーズ M4、M5、C220 M6、および C240 M6 サーバーでは、NIC のモードは、デフォルトで **[共有 LOM 拡張（Shared LOM Extended）]** に設定されます。

- **共有 OCP**：OCP アダプタ カード LOM ポートは、Cisco IMC にアクセスするために使用されます。次のステップで、[アクティブ-アクティブ（Active-active）] または [アクティブ-スタンバイ（Active-standby）] のいずれかの NIC 冗長化設定を選択する必要があります。
- **共有 OCP 拡張**：この NIC モードでは、DHCP 応答が OCP アダプタ カード LOM ポートと Cisco 仮想インターフェイス カード (VIC) ポートの両方に返されます。サーバがスタンドアロン モードであるために、Cisco VIC 接続でその IP アドレスが Cisco UCS Manager システムから取得されないと判別された場合は、その Cisco VIC からのその後の DHCP 要求は無効になります。

（注） **[共有 OCP（Shared OCP）]** および **[共有 OCP 拡張（Shared OCP Extended）]** ポートは、Cisco UCS C225 M6、C245 M6、C220 M7、および C240 M7 サーバーでのみ使用できます。

デフォルトのNICモード設定：

- UCS C シリーズ C125 M5 サーバーおよび S3260 サーバーの場合、**[NIC モード（NIC Mode）]** はデフォルトで **[Cisco カード（Cisco Card）]** に設定されています。

Cisco UCS C225 M6、C245 M6、C220 M7、および C240 M7 サーバーの場合：

- サーバーに Cisco VIC カードと OCP カードがある場合、デフォルトの NIC モードは**共有 OCP 拡張**になり、**NIC 冗長性**は **active-active** に設定されます。
- サーバーの NCSI 対応スロットに VIC カードが装着されているものの、OCP カードがない場合、デフォルトの NIC モードは **Cisco Card** になります。
- サーバーに VIC カードも OCP カードもない場合、デフォルトの NIC モードは**専用モード**に設定され、**NIC 冗長性**は**なし**に設定されます。

NIC 冗長化

選択した NIC モードとご使用の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。

- **[アクティブ-アクティブ（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が同時に動作します。これにより、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。
- **[アクティブ-スタンバイ（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。

- **[なし（None）]**：専用（*Dedicated*） モードでは、NIC 冗長性は なし（*None*） に設定されます。

使用できる冗長化モードは、選択されているネットワーク モードとプラットフォームによって異なります。使用できるモードについては、次を参照してください、『*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

VIC スロット

Cisco カード モードで管理機能に使用できる VIC スロット。

C240 M6、C245 M6、および C240 M7 の場合、VIC スロット オプションは次のとおりです。

- **[ライザー 1（Riser 1）]**：スロット 1 およびスロット 2
- **[ライザー 2（Riser 2）]**：スロット 4 およびスロット 5
- **mLOM**

（注） C240 M6 および C245 M6 C240 M6、C245 M6、および C240 M7 の場合、工場出荷時のデフォルト設定にリセットした後、スロットの優先順位は次のとおりです。

1. mLOM
2. ライザー 1：スロット 2、およびライザー 2 ～ スロット 5
3. ライザー 1：スロット 1、およびライザー 2 ～ スロット 4

C220 M6 および C225 M6 C220 M6、C225 M6、および C220 M7 の場合、VIC スロット オプションは次のとおりです。

- [ライザー 1（Riser 1）]：スロット 1 が選択されます。
- **[ライザー 3 (Riser 3)]**：スロット 3 が選択されます。
- **mLOM**

（注） C220 M6、C225 M6、および C220 M7 の場合、工場出荷時のデフォルト設定にリセットした後、スロットの優先順位は次のとおりです。

1. mLOM
2. ライザー 1 ：スロット 1
3. ライザー 3 ：スロット 3

C125 M5 の場合、VIC スロット オプションは **[ライザー 2（Riser 2）]** です。

C220 M4、C220 M5 および C240 M5 サーバーでは、VIC スロット オプションは次のとおりです。

- [ライザー 1（Riser 1）]：スロット 1 が選択されます。
- **[ライザー 2（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 M5 SD サーバーでは、VIC スロット オプションは次のとおりです。

- [ライザー 2（Riser 2）]：スロット 2 が選択されます。
- **[mLOM]**：mLOM スロットの VIC カードが選択されています。

C240 M4 サーバーでは、VIC スロット オプションは次のとおりです。

- [Riser 1]：スロット 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。
- **[ライザー 2（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。

C480 M5 ML サーバーの場合、Cisco カード モード スロットはスロット 11 およびスロット 12 です。

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

- **4**
- **5**

- **9**
- **10**

（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 サーバーだけです。

サーバー NIC の設定

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

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope network**	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 # **set mode** {**dedicated** | **shared_lom** | **shared_lom_10g** | **shipping** | **cisco_card** | **share_lom_ext** | **shared_ocp** | **shared_ocp_ext**}	NIC モードを次のいずれかに設定します。 • **[専用（Dedicated）]**：Cisco IMC へのアクセスに管理ポートを使用します。 • **[Cisco カード（Cisco Card）]**：アダプタ カード上の任意のポートを Cisco IMC へのアクセスに使用できます。Cisco アダプタ カードは、Network Communications Services Interface プロトコル（NCSI）をサポートするスロットに装着する必要があります。 • **[共有 LOM（Shared LOM）]**：Cisco IMC にアクセスするために使用できる LOM（LAN On Motherboard）ポート。 • **[共有 LOM 拡張（Shared LOM Extended）]**：Cisco IMC へのアクセ

	コマンドまたはアクション	目的
		スに使用できる 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 をサポートするスロットに装着する必要があります。 （注） [共有 LOM（Shared LOM）] ポートおよび [共有 LOM 拡張（Shared LOM Extended）] ポートは、一部の C シリーズ サーバでのみ使用できます。 （注） その他の UCS C シリーズ M4、M5、C220 M6、および C240 M6 サーバーでは、NIC のモードは、デフォルトで **[共有 LOM 拡張（Shared LOM Extended）]** に設定されます。 • **共有 OCP**：OCP アダプタ カード LOM ポートは、Cisco IMC にアクセスするために使用されます。次のステップで、[アクティブ-アクティブ（Active-active）] または [アクティブ-スタンバイ（Active-standby）] のいずれかの NIC 冗長化設定を選択する必要があります。 • **共有 OCP 拡張**：この NIC モードでは、DHCP 応答が OCP アダプタ カード LOM ポートと Cisco 仮想インターフェイス カード (VIC) ポートの両方に返されます。サーバがスタンドアロン モードであるために、Cisco VIC 接続でその IP アドレスが Cisco UCS Manager システムから取得されないと判別された場合は、そ

	コマンドまたはアクション	目的
		の Cisco VIC からのその後の DHCP 要求は無効になります。 （注） **[共有 OCP（Shared OCP）]** および **[共有 OCP 拡張（Shared OCP Extended）]** ポートは、Cisco UCS C225 M6、C245 M6、C220 M7、および C240 M7 サーバーでのみ使用できます。 **デフォルトのNICモード設定**： • UCS C シリーズ C125 M5 サーバーおよびS3260サーバーの場合、**[NIC モード（NIC Mode）]** はデフォルトで **[Cisco カード（Cisco Card）]** に設定されています。 • Cisco UCS C225 M6、C245 M6、C220 M7、およびC240 M7サーバーの場合： • サーバーに Cisco VIC カードと OCP カードがある場合、デフォルトの NIC モードは**共有 OCP 拡張**になり、**NIC 冗長性**は **active-active** に設定されます。 • サーバーの NCSI 対応スロットに VIC カードが装着されているものの、OCP カードがない場合、デフォルトの NIC モードは **Cisco Card** になります。 • サーバーに VIC カードも OCP カードもない場合、デフォルトの NIC モードは**専用モード**に設定され、**NIC冗長性**は**なし**に設定されます。
ステップ 4	Server /cimc/network # **set vic-slot** {**none** | **riser1** | **riser2** | **mlom**}	VIC スロットは、MLON またはサポートされるライザーで使用可能な Cisco カードに設定できます。

	コマンドまたはアクション	目的
		C240 M6、C245 M6、および C240 M7 の場合、VIC スロット オプションは次のとおりです。 • **[ライザー 1（Riser 1）]**：スロット 1 およびスロット 2 • **[ライザー 2（Riser 2）]**：スロット 4 およびスロット 5 • **mLOM** （注） C240 M6、C245 M6、および C240 M7 の場合、工場出荷時のデフォルト設定にリセットした後、スロットの優先順位は次のとおりです。 **1.** mLOM **2.** ライザー 1：スロット 2、およびライザー 2 ～ スロット 5 **3.** ライザー 1：スロット 1、およびライザー 2 ～ スロット 4 C220 M6、C225 M6、および C220 M7 の場合、VIC スロット オプションは次のとおりです。 • [ライザー 1（Riser 1）]：スロット 1 が選択されます。 • **[ライザー 3 (Riser 3)]**：スロット 3 が選択されます。 • **mLOM**

	コマンドまたはアクション	目的
		（注） C220 M6、C225 M6、および C220 M7 の場合、工場出荷時のデフォルト設定にリセットした後、スロットの優先順位は次のとおりです。 **1.** mLOM **2.** ライザー 1 ：スロット 1 **3.** ライザー 3 ：スロット 3 C125 M5 の場合、VIC スロット オプションは **[ライザー 2（Riser 2）]** です。 C220 M4、C220 M5 および C240 M5 サーバーでは、VIC スロット オプションは次のとおりです。 • [ライザー 1（Riser 1）] : スロット 1 が選択されます。 • **[ライザー 2（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 SD M5 サーバでは、VIC スロット オプションは次のとおりです。 • PCIe ライザー 1 と 2B を組み合わせたサーバの場合： • [Riser1] を選択した場合は、スロット 2 に VIC を取り付ける必要があります。 • [Riser2] を選択した場合は、スロット 5 に VIC を取り付ける必要があります。 • PCIe ライザー 1C と 2E を組み合わせたサーバの場合：

	コマンドまたはアクション	目的
		• [ライザー1（Riser1）] を選択した場合は、スロット 1 に VIC を取り付ける必要があります。 • [ライザー2（Riser2）] を選択した場合は、スロット 2 に VIC を取り付ける必要があります。 • [Flex-LOM] を選択した場合は、mLOM スロットに mLOM タイプの VIC を取り付ける必要があります。 C480 M5 ML サーバーの場合、Cisco カードモードスロットはスロット 11 およびスロット 12 です。 次のオプションを使用できるのは一部の UCS C シリーズ サーバーだけです。 • **4** • **5** • **9** • **10** C240 M4 サーバーでは、VIC スロットオプションは次のとおりです。 • [Riser 1]：スロット 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。 • **[ライザー 2（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 # **set redundancy** {**none** | **active-active** | **active-standby**}	NIC モードが Shared LOM である場合に、NIC 冗長モードを設定します。冗長モードは、次のいずれかになります。

	コマンドまたはアクション	目的
		• 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。サーバーでサポートされていないモードを選択すると、変更を保存するときにエラー メッセージが表示されます。
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

例

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 <mlom>
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 #
```

Cisco VIC mLOM および OCP カードの交換に関する考慮事項

Cisco UCS C220 M7、C240 M7、C225 M6 および C245 M6 サーバーで、Cisco VIC mLOM および OCP カードを交換する際には、次の状況で Cisco IMC ネットワークとの接続が失われることがあります。

- MLOM スロットの OCP カードを Cisco VIC カードと交換し、NIC モードを**共有 OCP** または**共有 OCP 拡張** に設定している場合。
- MLOM スロットの Cisco VIC カードを OCP カードと交換し、NIC モードを **Cisco カード MLOM** に設定している場合。

Cisco UCS C220 M7、C240 M7、C225 M6 または C245 M6 サーバーの Cisco VIC mLOM または OCP カードを交換する際は、次の推奨事項に従ってください。

- カードを交換する前に、ネットワークと接続している NIC のモードを、**Cisco カード MLOM**、**共有 OCP**、または **共有 OCP 拡張** 以外のいずれかに設定しておきます。カードの交換後に、適切な NIC モードを設定します。

  NIC モードの設定方法については、ご使用の Cisco IMC リリースの *Server NIC Configuration* の項を参照してください。これは Configuration Guides に記載されています。

- または、カードを交換した後、Cisco IMC Configuration Utility/（F8 キー）を使用して適切な NIC モードを設定します。

  ご使用のサーバーの *Connecting to the Server Locally For Setup* の項を参照してください。これは「」セクションを参照してください。これは Install and Upgrade Guides に記載されています。

- または、カードを交換した後、Cisco IMC Configuration Utility/（F8 キー）を使用して工場出荷時のデフォルト設定に戻してから、次の手順を実行します。

  1. サーバーが再起動を開始したら、F8 キーを押してシステムを Cisco IMC Configuration で起動し、デフォルトのパスワードを変更します。
  2. 適切な NIC モードに設定します。

表 *2*: 工場出荷時設定

mLOM スロットの VIC	mLOM スロットの Intel OCP 3.0 NIC	ライザー スロットの VIC	専用管理ポート。	CIMC アクセスのための NIC モード
はい	いいえ	いいえ	はい	mLOM スロットのカードを使用する **Cisco Card** モード
いいえ	はい	いいえ	はい	**Shared OCP Extended**

mLOM スロットの VIC	mLOM スロットの Intel OCP 3.0 NIC	ライザー スロットの VIC	専用管理ポート。	CIMC アクセスのための NIC モード
いいえ	はい	はい	はい	**Shared OCP Extended**
いいえ	いいえ	はい	はい	優先順位に基づく VIC スロットでの **Cisco カード**： **C220 M7 および C225 M6 の場合**： **1.** ライザー 1：スロット 1 **2.** ライザー 3：スロット 3 **C240 M7 および C245 M6 の場合**： **1.** ライザー 1：スロット 2 **2.** ライザー 2：スロット 5 **3.** ライザー 1：スロット 1 **4.** ライザー 2：スロット 4
いいえ	いいえ	いいえ	はい	**専用**

共通プロパティの設定

共通プロパティの設定の概要

ホスト名

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 サーバーから 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製造者から提供されるデフォルト シリアル番号は、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 サーバーのリソース 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 を有効にできます。[DDNS] オプションを有効にすると、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 サーバーのリソース 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。

- ホスト名
- LDAP 設定のドメイン名
- DDNS と DHCP が有効な場合に、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** コマンドを入力する場合。

[**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

サーバーを説明するには、共通プロパティを使用します。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope network**	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 # **set hostname** *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	（任意） Server /cimc/network # **set ddns-enabled**	Cisco IMC に対して DDNS サービスを有効にします
ステップ 5	（任意） Server /cimc/network # **set ddns-update-domain** *value*	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。

例

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 #
```

次のタスク

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

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope network**	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 # **set 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 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 # **set v4-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 # **set v4-netmask** *ipv4-netmask*	IPアドレスのサブネットマスクを指定します。
ステップ 6	Server /cimc/network # **set v4-gateway** *gateway-ipv4-address*	IP アドレスのゲートウェイを指定します。
ステップ 7	Server /cimc/network # **set dns-use-dhcp** {**yes** |**no**}	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 # **set preferred-dns-server** *dns1-ipv4-address*	プライマリ DNS サーバーの IP アドレスを指定します。
ステップ 9	Server /cimc/network # **set alternate-dns-server** *dns2-ipv4-address*	セカンダリ DNS サーバーの IP アドレスを指定します。
ステップ 10	Server /cimc/network # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 11	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。

例

次に、IPv4 ネットワークの設定を実行し、表示する例を示します。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set dhcp-enabled 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

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope network**	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 # **set v6-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 # **set v6-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 # **set v6-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 # **set v6-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 # **set v6-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 # **set v6-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# **set v6-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 # **set v6-alternate-dns-server** *dns2-ipv6-address*	セカンダリ DNS サーバーの IP アドレスを指定します。
ステップ 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。

例

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 #
```

ICMP の設定

このリリース 4.1（3b） では、Cisco IMC を使用して、BMC での着信 ICMP リダイレクトおよび接続先到達不能パケットの処理を有効または無効にすることができます。

（注） このオプションは一部の UCS M5 サーバーにのみ使用できます。

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 network**	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 # **scope icmp-configuration**	ICMP 構成モードを開始します。
ステップ 4	Server /cimc/network/icmp-configuration # **show-detail**	ICMP 構成設定を表示します。
ステップ 5	Server /cimc/network/icmp-configuration # **set destination-unreachable-enabled yes**	ICMP の **[接続先到達不能（Destination Unreachable）]** 構成設定を有効にします。
ステップ 6	Server /cimc/network/icmp-configuration # **set redirect-enabled yes**	ICMP の **[リダイレクト（Redirect）]** 構成設定を有効にします。
ステップ 7	Server /cimc/network/icmp-configuration # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 8	Server /cimc/network/icmp-configuration # **show-detail**	更新された ICMP 構成設定を表示します。

例

次の例は、ICMP 構成設定を構成する方法を示しています。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # scope icmp-configuration
Server /network/icmp-configuration # show detail
ICMP Settings:
    Destination Unreachable Enabled: no
    Redirect Enabled: no
Server /cimc/network/icmp-configuration # set destination-unreachable-enabled yes
Server /cimc/network/icmp-configuration # set redirect yes
Server /cimc/network/icmp-configuration # commit
Server /cimc/network/icmp-configuration # show detail
ICMP Settings:
    Destination Unreachable Enabled: yes
    Redirect Enabled: yes
Server /cimc/network/icmp-configuration #
```

サーバー VLAN の設定

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope network**	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 # **set vlan-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 # **set vlan-id** *id*	VLAN 番号を指定します。
ステップ 5	Server /cimc/network # **set vlan-priority** *priority*	VLAN でのこのシステムのプライオリティを指定します。
ステップ 6	Server /cimc/network # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 7	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。

例

次に、サーバー VLAN を設定する例を示します。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set vlan-enabled yes
Server /cimc/network *# set vlan-id 10
Server /cimc/network *# set vlan-priority 32
Server /cimc/network *# commit
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。

始める前に

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# **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**	Cisco IMC ネットワーク コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	Server /cimc/network # **set port-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 _（アンダーバー）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	（任意） Server /cimc/network # **show** [**detail**]	ネットワーク設定を表示します。

例

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。

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 # **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* # **set mode dedicated**	dedicated コマンドモードを開始します。
ステップ 4	Server/cimc/network # **set auto-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 ポート速度とデュプレックス値を設定できます。
ステップ 5	Server/cimc/network # **set net-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のみ、使用可能です。ポート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。**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。

	コマンドまたはアクション	目的
ステップ 6	Server/cimc/network* # **set duplex** {**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。
ステップ 7	Server/cimc/network* # commit	トランザクションをシステムにコミットします。

例

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 サーバー、またはその他のインターネット サーバーへの不要な接続を効果的に禁止します。

禁止 IP の設定は、一般的に、サービス拒否（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。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope network**	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 # **scope ipblocking**	IP ブロッキング コマンド モードを開始します。
ステップ 4	Server /cimc/network/ipblocking # **set enabled** {**yes** | **no**}	IP ブロッキングをイネーブルまたはディセーブルにします。
ステップ 5	Server /cimc/network/ipblocking # **set fail-count** *fail-count*	指定された時間ユーザーがロックアウトされる前に、ユーザーが試行できるログインの失敗回数を設定します。 この回数のログイン試行失敗は、[IP Blocking Fail Window] フィールドで指定されている期間内に発生する必要があります。 3 ～ 10 の範囲の整数を入力します。
ステップ 6	Server /cimc/network/ipblocking # **set fail-window** *fail-seconds*	ユーザーをロックアウトするためにログイン試行の失敗が発生する必要のある期間（秒数）を設定します。 60 ～ 120 の範囲の整数を入力します。
ステップ 7	Server /cimc/network/ipblocking # **set penalty-time** *penalty-seconds*	ユーザーが指定されている期間内にログイン試行の最大回数を超えた場合に、ユーザーがロックアウトされている秒数を設定します。 300 ～ 900 の範囲の整数を入力します。
ステップ 8	Server /cimc/network/ipblocking # **commit**	トランザクションをシステムの設定にコミットします。

	コマンドまたはアクション	目的
ステップ 9	Server /cimc/network/ipblocking # **exit**	IP ブロッキング コマンド モードを終了し、ネットワーク コマンドモードを開始します。
ステップ 10	Server /cimc/network # **scope ipfiltering**	IP フィルタリング コマンド モードを開始します。
ステップ 11	Server /cimc/network/ipfiltering # **set enabled** {**yes** | **no**}	IP フィルタリングをイネーブルまたはディセーブルにします。プロンプトに **y** を入力して IP フィルタリングをイネーブルにします。
ステップ 12	Server /cimc/network/ipfiltering # **set filter-1** *IPv4* または *IPv6* アドレスまたは一定範囲の *IP* アドレス	4 つの IP フィルタを設定できます。IPv4 または IPv6 IP アドレスまたは IP アドレス範囲を割り当てることができます。
ステップ 13	Server /cimc/network/ipfiltering # **commit**	トランザクションをシステム設定にコミットします。

例

次の例はネットワーク セキュリティを設定します。

```
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 #  exit
Server /cimc/network # scope ipfiltering
Server /cimc/network/ipfiltering # set enabled yes
This will enable IP Filtering
Do you wish to continue? [y/N] y
Server /cimc/network/ipfiltering *# set filter-1 1.1.1.1-255.255.255.255
                                    set filter-2 10.10.10.10
                                    set filter-3 2001:xxx::-2xxx:xx8::0001
                                    set filter-4
2001:xxx::-2xxx:xx8::0001-2001:xxx::-2xxx:xx8::0020
Server /cimc/network/ipfiltering *# commit
Changes to the ipfiltering will be applied immediately.
You may lose connectivity to the Cisco IMC and may have to log in again.
Do you wish to continue? [y/N] Y
```

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 サーバーで時刻を同期することができます。デフォルトでは、NTP サーバーは 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 サービスを有効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 サーバー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 サービスを有効にするには、DNS アドレスではなく、サーバの IP アドレスを指定することを推奨します。

始める前に

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

手順

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

	コマンドまたはアクション	目的
		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。

例

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。

始める前に

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

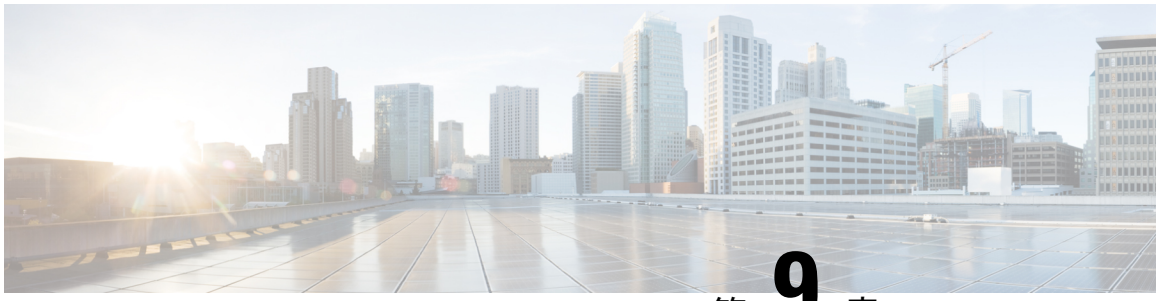
	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。

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

例

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、次の内容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 VIC 15238 仮想インターフェイス カード
- Cisco UCS VIC 15428 仮想インターフェイス カード
- Cisco UCS VIC 1497 仮想インターフェイス カード
- Cisco UCS VIC 1495 仮想インターフェイス カード
- Cisco UCS VIC 1477 仮想インターフェイス カード
- Cisco UCS VIC 1467 仮想インターフェイス カード
- Cisco UCS VIC 1457 仮想インターフェイス カード

- Cisco UCS VIC 1455 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
- 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 1225 仮想インターフェイス カード
- Cisco UCS P81E Virtual Interface Card

（注） VIC カードをサーバで同じの生成は必須です。たとえば、1 つのサーバで第 3 世代と第 4 世代 VIC カードの組み合わせを持つことはできません。

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 VIC 15238 仮想インターフェイス カード

Cisco UCS VIC 15238 は、Cisco UCS C シリーズ ラック サーバーの M6 および M7 世代用に設計された、デュアルポート クワッド Small Form-Factor Pluggable（QSFP/QSFP28/QSFP56）mLOM カードです。このカードは、40/100/200 Gbps イーサネットまたは FCoE をサポートします。PCIe 標準準拠のインターフェイスをホストに提示可能で、NIC または HBA として動的に構成できます。

Cisco UCS VIC 15428 仮想インターフェイス カード

Cisco VIC 15428 は、Cisco UCS C シリーズ ラック サーバーの M6 および M7 世代用に設計された、クワッドポート Small Form-Factor Pluggable（SFP+/SFP28/SFP56）mLOM カードです。このカードは、10/25/50 Gbps イーサネットまたは FCoE をサポートします。PCIe 標準準拠のインターフェイスをホストに提示可能で、NIC または HBA として動的に構成できます。

Cisco UCS VIC 1497 仮想インターフェイス カード

Cisco UCS 仮想インターフェイスカード (VIC) 1497 は、Cisco UCS C シリーズ ラックサーバの M5 世代用に設計された、デュアルポート Small Form-Factor (QSFP28) mLOM カードです。このカードは、40/100 Gbps イーサネットおよび FCoE をサポートします。PCIe 標準準拠のインターフェイスをホストに提示可能で、NIC および HBA として動的に構成できます。

Cisco UCS VIC 1495 仮想インターフェイス カード

Cisco UCS 仮想インターフェイスカード (VIC) 1495 は、Cisco UCS C シリーズ ラックサーバの M5 世代用に設計された、デュアルポート Small Form-Factor (QSFP28) PCIe カードです。このカードは、40/100 Gbps イーサネットおよび FCoE をサポートします。PCIe 標準準拠のインターフェイスをホストに提示可能で、NIC および HBA として動的に構成できます。

Cisco UCS VIC 1477 仮想インターフェイス カード

Cisco UCS VIC 1477 は、Cisco UCS C シリーズ ラック サーバーの M6 世代用に設計された、デュアルポート クアッド Small Form-Factor（QSFP28）mLOM カードです。このカードは、40/100 Gbps イーサネットまたは FCoE をサポートします。PCIe 標準準拠のインターフェイスをホストに提示可能で、NIC または HBA として動的に構成できます。

Cisco UCS VIC 1467 仮想インターフェイス カード

Cisco UCS VIC 1467 は、Cisco UCS C シリーズ ラック サーバーの M6 世代用に設計された、クワッドポート Small Form-Factor Pluggable（SFP28）mLOM カードです。このカードは、10/25 Gbps イーサネットまたは FCoE をサポートします。PCIe 標準準拠のインターフェイスをホストに提示可能で、NIC または HBA として動的に構成できます。

Cisco UCS VIC 1457 仮想インターフェイス カード

Cisco UCS 仮想インターフェイス カード（VIC）1457 は、Cisco UCS C シリーズ ラック サーバの M5 世代用に設計された、クワッドポート Small Form-Factor Pluggable（SFP28）mLOM カードです。このカードは、10/25 Gbps イーサネットまたは FCoE をサポートします。これは Cisco の次世代 CNA テクノロジーを組み込み、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。PCIe 標準準拠のインターフェイスをホストに提示可能で、NIC および HBA として動的に構成できます。

Cisco UCS VIC 1455 仮想インターフェイス カード

Cisco UCS 仮想インターフェイス カード（VIC）1455 は、Cisco UCS C シリーズ ラック サーバの M5 世代用に設計された、クワッドポート Small Form-Factor Pluggable（SFP28）ハーフハイト PCIe カードです。このカードは、10/25 Gbps イーサネットまたは FCoE をサポートします。これは Cisco の次世代 CNA テクノロジーを組み込み、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。PCIe 標準準拠のインターフェイスをホストに提示可能で、NIC および HBA として動的に構成できます。

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。

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。

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。

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 P81E Virtual Interface Card

Cisco UCS P81E Virtual Interface Card 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。

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。

例

- 次に、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 adapter
PCI Slot Product Name   Serial Number  Product ID     Vendor
-------- -------------- -------------- -------------- --------------------
11       UCS VIC 1455   FCH233770S8    UCSC-PCIE-C... Cisco Systems Inc
Server /chassis # show adapter detail
PCI Slot 11:
    Product Name: UCS VIC 1455
    Serial Number: FCH233770S8
    Product ID: UCSC-PCIE-C25Q-04
    Adapter Hardware Revision: 5
    Current FW Version: 5.1(1.64)
    VNTAG: Disabled
    FIP: Enabled
    LLDP: Enabled
    PORT CHANNEL: Enabled
    Configuration Pending: no
    Cisco IMC Management Enabled: no
    VID: V04
    Vendor: Cisco Systems Inc
    Description:
    Bootloader Version: 5.0(3c)
    FW Image 1 Version: 5.1(1.64)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 5.1(1.59)
    FW Image 2 State: BACKUP INACTIVATED
    FW Update Status: Fwupdate never issued
    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

始める前に

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

	コマンドまたはアクション	目的
ステップ 5	Server /chassis/adapter # **set lldp** {**disable** | **enable**}	（注） LLDP の変更を有効にするは、サーバーの再起動が必要です。 S3260 シャーシに 2 つのノードがある場合、プライマリ ノードで LLDP の変更を行った後にセカンダリ ノードを再起動するようにしてください。 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 # **set vntag-mode** {**disabled** | **enabled**}	アダプタ カードで VNTAG を有効または無効にします。VNTAG はデフォルトにより無効にされます。 （注） VNTAG モードがイネーブルな場合、以下の操作を実行できます。 • 特定のチャネルに vNIC と vHBA を割り当てることができます。 • ポート プロファイルに vNIC と vHBA を関連付けることができます。 • 通信に問題が生じた場合、vNIC を他の vNIC にフェールオーバーする。
ステップ 7	Server /chassis/adapter # **set portchannel** *disabled*	ポート チャネルを有効または無効にすることができます。ポート チャネルを

	コマンドまたはアクション	目的
		無効にすると、4 個の vNIC と vHBA はアダプタで使用できます。 ポート チャネルを有効にすると、次のようになります。 • 2 個の vNIC と vHBA のみを使用できます。 • ポート 0 と 1 は 1 つのポート チャネルとしてバンドルされ、ポート 2 および 3 はもう一方のポート チャネルとしてバンドルされます。 （注） • このオプションは、Cisco UCS VIC 1455 および 1457 ではデフォルトで有効になっています。 • ポート チャネル設定を変更するとき、すべての以前に作成した vNIC および vHBA が削除され、設定は工場出荷時のデフォルトに復元されます。 • VNTAG モードは、ポート チャネル モードでのみサポートされます。
ステップ 8	Server /chassis/adapter # **set physical-nic-mode** *enabled*	物理 NIC モードを有効または無効にすることができます。このオプションは、デフォルトで無効です。 物理 NIC モードが有効になっている場合、VIC のアップリンク ポートはパススルー モードに設定されます。これにより、ホストは変更を行わずにパケットを送信できます。VIC ASIC は、vNIC の VLAN と CoS の設定に基づいてパケットの VLAN タグをリライトしません。

	コマンドまたはアクション	目的
		（注） このオプションは、Cisco UCS VIC 14xx シリーズおよび 15xxx シリーズ アダプタでのみ使用できます。 VIC 構成の変更を有効にするには、ホストを再起動する必要があります。 次のようなアダプタでは、このオプションを有効にすることはできません。 • **[ポート チャネル モード (Port Channel mode)]** が有効になっています • **[VNTAG モード (VNTAG mode)]** が有効になっているもの • **[LLDP]** が有効になっているもの • **[FIP モード (FIP mode)]** が有効になっているもの • **[CISCO IMC 管理が有効 (Cisco IMC Management Enabled)]** 値が **[はい (Yes)]** に設定されています • 複数のユーザーが作成した vNIC
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。

例

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 *# set vntag-mode enabled
Server /chassis/adapter *# commit
```

```
Warning: Enabling VNTAG mode
All the vnic configuration will be reset to factory defaults
New VNIC adapter settings will take effect upon the next server reset
Server /chassis/adapter # show detail
PCI Slot 1:
    Product Name: UCS VIC xxxx
    Serial Number: FCHXXXXXZV4
    Product ID: UCSC-PCIE-xxx-04
    Adapter Hardware Revision: 3
    Current FW Version: x.0(0.345)
    VNTAG: Enabled
    FIP: Enabled
    LLDP: Enabled
    PORT CHANNEL: Disabled
    Configuration Pending: yes
    Cisco IMC Management Enabled: no
    VID: V00
    Vendor: Cisco Systems Inc
    Description:
    Bootloader Version: xxx
    FW Image 1 Version: x.0(0.345)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: bodega-dev-170717-1500-orosz-ET
    FW Image 2 State: BACKUP INACTIVATED
    FW Update Status: Fwupdate never issued
    FW Update Error: No error
    FW Update Stage: No operation (0%)
    FW Update Overall Progress: 0%
Server /chassis/adapter #
```

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # set fip-mode enable
Server /chassis/adapter *# set vntag-mode enabled
Server /chassis/adapter* # set portchannel disabled
Server /chassis/adapter *# commit
Warning: Enabling VNTAG mode
All the vnic configuration will be reset to factory defaults
New VNIC adapter settings will take effect upon the next server reset
Server /chassis/adapter # show detail
PCI Slot 1:
    Product Name: UCS VIC xxxx
    Serial Number: FCHXXXXXZV4
    Product ID: UCSC-PCIE-xxx-04
    Adapter Hardware Revision: 3
    Current FW Version: x.0(0.345)
    VNTAG: Enabled
    FIP: Enabled
    LLDP: Enabled
    PORT CHANNEL: Disabled
    Configuration Pending: no
    Cisco IMC Management Enabled: no
    VID: V00
    Vendor: Cisco Systems Inc
    Description:
    Bootloader Version: xxx
    FW Image 1 Version: x.0(0.345)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: gafskl-dev-170717-1500-orosz-ET
    FW Image 2 State: BACKUP INACTIVATED
    FW Update Status: Fwupdate never issued
    FW Update Error: No error
    FW Update Stage: No operation (0%)
```

```
    FW Update Overall Progress: 0%
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 仮想インターフェイス カードについている には、デフォルトで 2 個の vHBA と 2 個の vNIC が用意されています。これらのアダプタ カードに最大 14 個の vHBA または vNIC を追加作成できます。

  Cisco UCS1455、1457、および 1467 仮想インターフェイス カードは、非ポートチャネル モードで、デフォルトで 4 個の vHBAs と4 個の Vhbas を提供します。これらのアダプタ カードに最大 10 個の vHBA または vNICs を追加作成できます。

（注） アダプタに対して VNTAG モードが有効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 仮想インターフェイス カードを使用する場合は、vHBA を FCoE VLAN に関連付ける必要があります。VLAN を割り当てるには、「**vHBA のプロパティの変更**」で説明されている手順に従います。
- 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。

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。

	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、サーバー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。

例

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: 10:00:70:0F:6A:C0:97:43
    World Wide Port Name: 20:00:70:0F:6A:C0:97:43
    FC SAN Boot: disabled
    FC Type: fc-initiator
    Persistent LUN Binding: disabled
    Uplink Port: 0
    PCI Link: 0
    MAC Address: 70:0F:6A:C0:97:43
    CoS: 3
    VLAN: NONE
    Rate Limiting: OFF
    PCIe Device Order: 2
    EDTOV: 2000
    RATOV: 10000
    Maximum Data Field Size: 2112
    Channel Number: N/A
    Port Profile: N/A

Server /chassis/adapter #
```

vHBA のプロパティの変更

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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、サーバー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。

	コマンドまたはアクション	目的
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。
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 ～ 100000 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-data-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

	コマンドまたはアクション	目的
		（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 # **set channel-number** *channel number*	この vHBA に割り当てるチャネル番号。1 ～ 1,000 の整数を入力します。 （注） このオプションには VNTAG モードが必要です。
ステップ 18	Server /chassis/adapter/host-fc-if # **set pci-link** *0|1*	vNIC を接続できるリンク。値は次のとおりです。 • 0：vNIC が配置されている最初の cross-edged リンク。 • 1：vNIC が配置されている 2 番目の cross-edged リンク。 （注） 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。
ステップ 19	Server /chassis/adapter/host-fc-if # **set uplink** *Port number*	vHBA に関連付けられたアップリンク ポート。 （注） この値は、システム定義の vHBA である fc0 と fc1 については変更できません。
ステップ 20	Server /chassis/adapter/host-fc-if # **set vhba-type** *fc-initiator|fc-target|fc-nvme-initiator|fc-nvme-target*	このポリシーで使用される vHBA タイプ。サポートされている FC と FC NVMe Vhba は、同じアダプタでここで作成できます。このポリシーで使用される vHBA タイプには、次のいずれかを指定できます。 • fc-initiator：レガシー SCSI FC vHBA イニシエータ • fc-target：SCSI FC ターゲット機能をサポートする vHBA （注） このオプションは、技術プレビューとして使用可能です。

	コマンドまたはアクション	目的
		• fc-nvme-initiator：FC NVME イニシエータ、FC NVME ターゲットを検出し、それらに接続する vHBA • fc-nvme-target：FC NVME ターゲットとして機能し、NVME ストレージへ接続する vHBA
ステップ 21	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。
ステップ 22	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 23	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 24	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 25	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 26	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。

	コマンドまたはアクション	目的
ステップ 27	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 28	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。
ステップ 29	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 30	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 31	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 32	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 33	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 34	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 35	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 ～

	コマンドまたはアクション	目的
		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 36	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 37	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 38	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 39	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 40	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 41	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 42	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 43	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。Cisco UCS VIC 14xx シリーズ アダプタの場合、1 ～ 64 の整数を入力します。その他の VIC アダプタの場合は、1 ～ 245 の整数を入力します。
ステップ 44	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

	コマンドまたはアクション	目的
		の範囲は 64 ～ 512 です。デフォルトは 512 です。
ステップ 45	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 46	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 47	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 48	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 49	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 50	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 51		
ステップ 52	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。
ステップ 53	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。

例

この例では、vHBA のプロパティを設定します(いくつかのオプションのみが表示されます) :

```
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 #
```

次のタスク

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。

（注） 追加の vHBA は、**[VNTAG]** モードでのみ作成できます。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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、サーバー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-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*	この vHBA にチャネル番号を割り当てます。指定できる範囲は 1 ～ 1000 です。

	コマンドまたはアクション	目的
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。

例

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 #
```

次のタスク

- サーバーをリブートして 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 （202 ページ）の説明に従って、新しい vHBA を設定します。

vHBA の削除

始める前に

デフォルトの vHBA は削除できません。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope 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、サーバー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。

例

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、サーバー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 # **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。

例

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、サーバー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。

	コマンドまたはアクション	目的
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* — hh:hh:hh:hh:hh:hh:hh:hh の形式でブート ターゲットの ワールドワイドポート名 (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。

例

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、サーバー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 # **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。

例

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 #
```

次のタスク

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、サーバー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。

例

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、サーバー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。

例

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

始める前に

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、サーバー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。

例

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 仮想インターフェイス カードには、デフォルトで 2 個の vHBA と 2 個の vNIC が用意されています。これらのアダプタ カードに最大 14 個の vHBA または vNIC を追加作成できます。

追加の vHBA は、VNTAG モードを使用して作成できます。

Cisco UCS 1455、1457、および 1467 仮想インターフェイス カードは、非ポートチャネル モードで、デフォルトで 4 個の vHBAs と4 個の Vhbas を提供します。これらのアダプタ カードに最大 10 個の vHBA または vNICs を追加作成できます。

（注） アダプタに対して VNTAG モードが有効になっている場合は、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、サーバー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-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 # **show ext-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。

例

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。

（注） これらの例は、特定のリリースでのみ使用可能な機能を示している場合があります。

```
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: B0:8B:CF:4C:ED:FF
    CoS: 0
    Trust Host CoS: disabled
    PCI Link: 0
    PCI Order: 0
    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: N/A
    Uplink Failback Timeout: N/A
    aRFS: disabled
    VMQ: disabled
    NVGRE: disabled
    VXLAN: disabled
    CDN Name: VIC-MLOM-eth0
    RoCE Version1: disabled
    RoCE Version2: disabled
    RDMA Queue Pairs: 0
    RDMA Memory Regions: 0
    RDMA Resource Groups: 0
    RDMA COS: 0
    Multi Queue: disabled
    No of subVnics:
    Multi Queue Transmit Queue Count:
    Multi Queue Receive Queue Count:
    Multi Que Completion Queue Count:
    Multi Queue RoCE Version1:
    Multi Queue RoCE Version2:
    Multi Queue RDMA Queue Pairs:
    Multi Queue RDMA Memory Regions:
    Multi Queue RDMA Resource Groups:
    Multi Queue RDMA COS:
    Advanced Filters: disabled
    Geneve Offload: disabled

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

始める前に

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

手順

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

	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、サーバー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 # **set mtu** *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 # **set uplink** {**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 # **set mac-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 # **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、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） • RDMA が有効になっているインターフェイスの 5 分、**COS**値を設定する必要があります。 • 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 # **set trust-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 # **set order** {**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 # **set vlan** {**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 # **set vlan-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。

	コマンドまたはアクション	目的
ステップ 13	Server /chassis/adapter/host-eth-if # **set rate-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。 VIC 13xx コントローラの場合、1 ～ 40,000 の整数を入力できます。 VIC 1455 および 1457 コントローラの場合: • アダプタがスイッチ上の 25 Gbps リンクに接続されている場合は、1 ~ 25000 Mbps の整数を入力できます。 • アダプタがスイッチ上の 10 Gbps リンクに接続されている場合は、1 ~ 10000 Mbps の整数を入力できます。 VIC 1495 および 1497 コントローラの場合: • アダプタがスイッチ上の 40 Gbps リンクに接続されている場合は、1 ~ 40,000 Mbps の整数を入力できます。 • アダプタがスイッチ上の 100 Gbps リンクに接続されている場合は、1 ~ 100,000 Mbps の整数を入力できます。 （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。
ステップ 14	Server /chassis/adapter/host-eth-if # **set boot** {**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。デフォルト値は、デフォルト vNIC およびユーザー作成の vNIC に対しては無効に設定されています。
ステップ 15	Server /chassis/adapter/host-eth-if # **set channel-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

	コマンドまたはアクション	目的
		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 # **set port-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 # **set uplink-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 # **set uplink-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 # **set vmq** {**disabled** | **enabled**}	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。

	コマンドまたはアクション	目的
		（注） • SR-IOV がアダプタで有効化されている場合は、VMQ が有効化されていないことを確認してください。 • このオプションは、1495 または 1497 アダプタを備えたいくつかの Cisco UCS C-シリーズサーバーでのみ使用できます。
ステップ 20	Server /chassis/adapter/host-eth-if # **set multi-queue** {**disabled** | **enabled**}	このアダプタのマルチキューオプションを有効または無効にして、次のマルチキューパラメータを設定することができます。 • **mq-rq-count**—割り当てる受信キューリソースの数。1 ～ 1000 の整数を入力します。 • **mq-wq-count**—割り当てる送信キューリソースの数。1 ～ 1000 の整数を入力します。 • **mq-cq-count**—割り当てる完了キューリソースの数。通常、割り当てなければならない完了キューリソースの数は、送信キュー リソースの数に受信キューリソースの数を加えたものと等しくなります。1 ～ 2000 の整数を入力します。

	コマンドまたはアクション	目的
		（注） • マルチキューは、14xx アダプタを備えた C-Seriesサーバーでのみサポートされます。 • このオプションを有効にするには、VMQ が有効な状態である必要があります。 • いずれか 1 つの vNIC でこのオプションを有効にすると、他の vNIC での VNQ のみの設定（マルチキューを選択しない）はサポートされません。 • このオプションを有効にすると、usNIC の設定は無効になります。
ステップ 21	Server /chassis/adapter/host-eth-if # **set arfs** {**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。
ステップ 22	Server /chassis/adapter/host-eth-if # **set geneve** {**disable** | **enable**}	リリース 4.1(2a) 以降、Cisco IMC では、ESX 7.0 (NSX-T 3.0) および ESX 6.7U3(NSX-T 2.5) OS の Cisco VIC 14xx シリーズ アダプタを使用した、汎用ネットワーク仮想カプセル化（Geneve）オフロード機能がサポートされています。 Geneveは、ネットワーク トラフィックのトンネル カプセル化機能です。Cisco VIC 14xx シリーズ アダプタで Geneve オフロードのカプセル化を有効にする場合は、この機能を有効化します。 Geneve オフロードを無効にするには、この機能を無効化します。これにより、接続先ポート番号が Geneve宛て先ポートと一致するカプセル化されてい

	コマンドまたはアクション	目的
		ないUDPパケットが、トンネルパケットとして扱われないようにします。 Geneve Offload 機能を有効にすると、次の設定が推奨されます。 • 送信キュー数 = 1 • 送信キュー リング サイズ = 4096 • 受信キュー数 = 8 • 受信キュー リング サイズ = 4096 • 完了キュー数 = 9 • 割り込み数 = 11 （注） Geneve Offload が有効になっている場合は、次を有効にできません。 • 同じ vNIC 上の RDMA • 同じ vNIC 上の usNIC • 非ポート チャネル モード • aRFS • 詳細フィルタ • NetQueue （注） Cisco UCS C220 M7 および C240 M7 サーバーは、Cisco 14xx シリーズ VIC アダプタをサポートしていません。 外部 IPV6 は、GENEVE Offload 機能ではサポートされていません。 **ダウングレードの制限**：Geneve Offload が有効になっている場合、4.1(2a) より前のリリースにダウングレードすることはできません。
ステップ 23	Server /chassis/adapter/host-eth-if # **scope interrupt**	割り込みコマンド 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 24	Server /chassis/adapter/host-eth-if/interrupt # **set interrupt-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 25	Server /chassis/adapter/host-eth-if/interrupt # **set coalescing-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 26	Server /chassis/adapter/host-eth-if/interrupt # **set coalescing-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 27	Server /chassis/adapter/host-eth-if/interrupt # **set interrupt-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 28	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 29	Server /chassis/adapter/host-eth-if # **scope recv-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 30	Server /chassis/adapter/host-eth-if/recv-queue # **set rq-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 31	Server /chassis/adapter/host-eth-if/recv-queue # **set rq-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 ～ 16384 です。デフォルトは 512 です。 VIC 14xx シリーズ アダプタは、最大 4K（4096）のリング サイズをサポートします。 VIC15xxx シリーズのアダプタは、最大 16K のリング サイズをサポートします。
ステップ 32	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 33	Server /chassis/adapter/host-eth-if # **scope trans-queue**	送信キューのコマンドモードを開始します。
ステップ 34	Server /chassis/adapter/host-eth-if/trans-queue # **set wq-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 35	Server /chassis/adapter/host-eth-if/trans-queue # **set wq-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 ～ 16384 です。デフォルトは 256 です。 VIC 14xx シリーズ アダプタは、最大 4K（4096）のリング サイズをサポートします。 VIC15xxx シリーズのアダプタは、最大 16K のリング サイズをサポートします。
ステップ 36	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 37	Server /chassis/adapter/host-eth-if # **scope comp-queue**	完了キューのコマンドモードを開始します。
ステップ 38	Server /chassis/adapter/host-eth-if/comp-queue # **set cq-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。

	コマンドまたはアクション	目的
		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 39	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 40	Server /chassis/adapter/host-eth-if/ # **set rdma_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 41	Server /chassis/adapter/host-eth-if/ # **set rdma_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 42	Server /chassis/adapter/host-eth-if/ # **set rdma_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。 （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 43	Server /chassis/adapter/host-eth-if # **scope offload**	TCP オフロードのコマンドモードを開始します。
ステップ 44	Server /chassis/adapter/host-eth-if/offload # **set tcp-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** ：大きい TCP パケットは、CPU からハードウェアに送信されて分割されます。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。

	コマンドまたはアクション	目的
ステップ 45	Server /chassis/adapter/host-eth-if/offload # **set tcp-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 46	Server /chassis/adapter/host-eth-if/offload # **set tcp-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 47	Server /chassis/adapter/host-eth-if/offload # **set tcp-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** ：すべての分割パケットは、CPU に送信される前にハードウェアによって再構築されます。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 48	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。

	コマンドまたはアクション	目的
ステップ 49	Server /chassis/adapter/host-eth-if # **scope rss**	Receive Side Scaling（RSS）のコマンドモードを開始します。
ステップ 50	Server /chassis/adapter/host-eth-if/rss # **set rss** {**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 51	Server /chassis/adapter/host-eth-if/rss # **set rss-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 52	Server /chassis/adapter/host-eth-if/rss # **set rss-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 53	Server /chassis/adapter/host-eth-if/rss # **set rss-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 54	Server /chassis/adapter/host-eth-if/rss # **set rss-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 55	Server /chassis/adapter/host-eth-if/rss # **set rss-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。
ステップ 56	Server /chassis/adapter/host-eth-if/rss # **set rss-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 57	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 58	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。
ステップ 59	Server /chassis/adapter/host-eth-if # **set vf-count***Count*	PF ごとに VF の数を指定します。

	コマンドまたはアクション	目的
		1 ～ 64 の整数を入力します。デフォルトは 0 です。 （注） リリース 4.3(1) 以降、Cisco IMC は、ESXi 7.0 U3 および 8.0 用の UCS VIC 15xxx シリーズアダプタを備えた Cisco UCS C シリーズ M7 サーバーで、シングルルート I/O 仮想化のサポートを提供します。
ステップ 60	Server /chassis/adapter/host-eth-if* # **set vf-intr-count***Count*	VF ごとの割り込み数を指定します。 1 ～ 16 の整数を入力します。
ステップ 61	Server /chassis/adapter/host-eth-if* # **set vf-rq-count***Count*	VF ごとの受信キューの数を指定します。 1 ～ 8 の整数を入力します。
ステップ 62	Server /chassis/adapter/host-eth-if* # **set vf-wq-count***Count*	VF ごとの送信キューの数を指定します。 1 ～ 8 の整数を入力します。
ステップ 63	Server /chassis/adapter/host-eth-if* # **set vf-cq-count***Count*	VF ごとの完了キューの数を指定します。 1 ～ 16 の整数を入力します。デフォルトは 0 です。 値は wq と rq の合計です。
ステップ 64	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。

例

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 # set vmq enabled
```

```
Server /chassis/adapter/host-eth-if # set multi-queue enabled
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 # set vf-count 8
Server /chassis/adapter/host-eth-if *# set vf-intr-count 8
Server /chassis/adapter/host-eth-if *# set vf-cq-count 8
Server /chassis/adapter/host-eth-if *# set vf-rq-count 4
Server /chassis/adapter/host-eth-if *# set vf-wq-count 4
Server /chassis/adapter/host-eth-if *# commit
Server /chassis/adapter/host-eth-if #
```

次のタスク

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 インターフェイスの Admin リンク トレーニングの設定

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 Admin 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。

始める前に

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

（注） このオプションは、一部のアダプタおよびサーバーでのみ使用可能です。

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。

	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、サーバー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 ext-eth-if 0** | **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 # **set admin-link-training on** | **off** |**auto**	指定された vNIC の選択されたオプションに Admin リンク トレーニングを設定します。 管理者リンク トレーニングは、デフォルトで `auto` に設定されています。 4.2(2a) 以降、次の異なる設定は、Cisco UCS VIC 15xxx アダプタと、速度 10G/25G/50G の銅線ケーブルにのみ適用されます。 • `admin-link-training` が `auto` に設定されている場合、アダプタ ファームウェアは、トランシーバに応じて `oper-link-training` 値を `on` または `off` に設定します。 • 25G 銅線では `Auto Negotiate` が無効です • 50G 銅線では `Auto Negotiate` が有効です • `admin-link-training` が `on` に設定されている場合、アダプタ ファームウェアは `oper-link-training` を `on` に設定します。 • 25G 銅線では `Auto Negotiate` が有効です • 50G 銅線では `Auto Negotiate` が有効です • `admin-link-training` が `off` の場合、アダプタ ファームウェアは

	コマンドまたはアクション	目的
		oper-link-training を off に設定します。 • 25G 銅線では Auto Negotiate が無効です • 50G 銅線では Auto Negotiate が無効です （注） • すべての非パッシブ銅線ケーブルでは、admin-link-training モードに関係なく、oper-link-training モードが off に設定されています。 • admin-link-training 設定を変更すると、oper-link-training 値が同じであっても、そのポートのシリーズがリセットされます。
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。

例

この例は、外部のイーサネットインターフェイスでAdminリンク トレーニングを auto に設定する方法を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # scope ext-eth-if 1
Server /chassis/adapter/ext-eth-if # set admin-link-training auto
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: -
    Admin Link Training: Auto
    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/ext-eth-if
```

Setting Admin FEC Mode on External Ethernet Interfaces

Before you begin

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。

Procedure

	Command or Action	Purpose
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**	(Optional) Displays the available adapter devices.
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。 **Note** アダプタの設定を表示または変更する前に、サーバー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 ext-eth-if** {**0** | **1** *name*}	Enters the external ethernet interface command mode for the specified vNIC.
ステップ 5	Server /chassis / adapter / ext-eth-if # **set admin-fec-mode** {|**cl108** |**cl91-cons16**| **cl91**|**cl74** | **off**}	Sets the admin FEC mode. The default value is **cl91**. **Note** Admin Forward Error Correction (FEC) mode apply only to Cisco UCS VIC 14xx adapters at speed 25/100G and Cisco UCS VIC 15xxx adapters at speeds 25G/50G. **Operating FEC Mode—**

	Command or Action	Purpose
		The value of **Operating FEC Mode** is the same as **Admin FEC mode** with these exceptions: • The value is Off when the speed is 10 Gbps or 40 Gbps. This is because FEC is not supported. • The value is Off for QSFP-100G-LR4-S transceiver. • The value is Off for QSFP-40/100-SRBD transceiver.
ステップ 6	Server /chassis / adapter / ext-eth-if * # **commit**	At the prompt, select **y**. Commits the transaction to the system configuration.

Example

This example shows how to set the admin FEC mode on the external ethernet interface.

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # scope ext-eth-if 1
Server /chassis/adapter/ext-eth-if # set admin-fec-mode cl74
Server /chassis/adapter/ext-eth-if* # 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
Port 1:
    MAC Address: 00:5D:73:1C:6C:58
    Link State: LinkDown
    Encapsulation Mode: CE
    Admin Speed: Auto
    Operating Speed: -
    Admin Link Training: N/A
    Admin FEC Mode: cl74
    Operating FEC Mode: Off
    Connector Present: NO
    Connector Supported: N/A
    Connector Type: N/A
    Connector Vendor: N/A
    Connector Part Number: N/A
    Connector Part Revision: N/A
Server /chassis/adapter/ext-eth-if #
```

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。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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、サーバー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	（任意） Server /chassis/adapter/host-eth-if # **set channel-number** *number*	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。

例

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、サーバー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。

例

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） [usNIC のプロパティ（usNIC properties）] ダイアログボックスには、Cisco usNIC の複数のプロパティが一覧表示されますが、次のプロパティのみを設定する必要があります。その他のプロパティは現在使用されていません。

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

始める前に

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# **scope host-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 個の vNIC のみを設定した場合、**eth0** を指定します。
ステップ 4	server/chassis/adapter/host-eth-if# **create usnic-config 0**	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

	コマンドまたはアクション	目的
		デックス値を必ず 0 に設定してください。 （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 （245 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# **set cq-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# **set rq-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# **set tq-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

	コマンドまたはアクション	目的
		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。
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。

例

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

始める前に

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。

	コマンドまたはアクション	目的
ステップ 3	server/chassis/adapter# **scope host-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 個の vNIC のみを設定した場合、**eth0** を指定します。
ステップ 4	server/chassis/adapter/host-eth-if# **scope usnic-config 0**	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。

例

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

始める前に

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

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、サーバー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。

例

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

始める前に

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。 （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# **scope host-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 個の vNIC のみを設定した場合、**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。

例

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

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 オプションを有効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。

始める前に

- 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 オプションを有効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。

	コマンドまたはアクション	目的
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、サーバー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。
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。

例

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

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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、サーバー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。
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。

例

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 #
```

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。

始める前に

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、サーバー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** プロトコル リモート サーバ *IP* アドレス	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

	コマンドまたはアクション	目的
		• FTP • SFTP • SCP • HTTP （注） Cisco UCS C シリーズ サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバー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 サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[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。

例

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。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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、サーバー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 サーバーから、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、サーバーが次にリブートされたときにインストールされます。

例

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 #
```

次のタスク

サーバーをリブートして、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

始める前に

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

手順

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

例

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。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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	（任意） Server /chassis # **recover-adapter-update** [*pci-slot*] [*pci-slot*]	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。

例

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 #
```

次のタスク

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（257 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 IMCCisco 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。

始める前に

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

手順

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

例

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 #
```

次のタスク

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

始める前に

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

手順

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

例

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、次の内容で構成されています。

未使用の物理ドライブからの仮想ドライブの作成

始める前に

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

一部の C シリーズ サーバーでのみ有効になります。

（注） Cisco IMC は、既存のデュアル ドライブ サポートに加えて、M.2 RAID コントローラでシングル ドライブ サポートを提供するようになりました。

シングル ドライブのサポートでは、仮想ディスクを作成できません。

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。

	コマンドまたはアクション	目的
ステップ 2	Server/chassis # **scope storageadapter** スロット	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。確認をする場合は **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。

例

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

始める前に

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

手順

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

	コマンドまたはアクション	目的
		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。確認をする場合は **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。

例

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 #
```

トランスポート可能としての仮想ドライブの設定

始める前に

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

- 仮想ドライブをトランスポート可能にするには、仮想ドライブが最適な状態になっていなければなりません。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope storageadapter** スロット *ID*	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** ドライブ番号	指定された仮想ドライブのコマンドモードを開始します。
ステップ 4	Server /chassis/storageadapter/virtual-drive # **set-transport-ready** *{include-all | exclude-all | include-dhsp}*	仮想ドライブをトランスポート可能に設定し、選択したプロパティを割り当てます。 選択した仮想ドライブをトランスポート可能として設定するために使用する初期化タイプを入力します。次のいずれかになります。 • exlude-all：専用ホット スペア ドライブをすべて除外します。 • include-all：排他的に使用可能な専用ホット スペア ドライブまたは共有される専用ホット スペア ドライブをすべて含めます。 • include-dhsp：排他的な専用ホット スペア ドライブを含めます。 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**y**を入力します。 （注） 仮想ドライブをトランスポート可能として設定すると、その仮想ドライブに関連付けられているすべての物理ドライブが [削除準備完了（Ready to remove）] として表示されます。

	コマンドまたはアクション	目的
ステップ 5	（任意） Server /chassis/storageadapter/virtual-drive # **show detail**	変更した仮想ドライブのプロパティを表示します。

例

次に、仮想ドライブ 5 をトランスポート可能に設定する例を示します。

```
Server # scope chassis
Server /chassis # scope storageadapter SLOT-HBA
Server /chassis/storageadapter # scope virtual-drive 5
Server /chassis/storageadapter/virtual-drive # set-transport-ready exclude-all
Since they belong to same drive group, all these virtual drives will be set to Transport
 Ready - 0
Are you sure you want to proceed?[y|N]y
Server /chassis/storageadapter/virtual-drive # show detail
Virtual Drive 0:
    Health: Good
    Status: Optimal
    Visibility : Visible
    Name: RAID0_124_RHEL
    Size: 2858160 MB
    Physical Drives: 1, 2, 4
    RAID Level: RAID 0
    Boot Drive: false
    FDE Capable: 0
    FDE Enabled: 0
    Target ID: 0
    Strip Size: 64 KB
    Drives Per Span: 3
    Span Depth: 1
    Access Policy: Transport Ready
    Cache Policy: Direct
    Read Ahead Policy: None
    Requested Write Cache Policy: Write Through
    Current Write Cache Policy: Write Through
    Disk Cache Policy: Unchanged
    Auto Snapshot: false
    Auto Delete Oldest: true
    Allow Background Init: true
Server /chassis/storageadapter/virtual-drive #
```

トランスポート可能としての仮想ドライブのクリア

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope 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** スロット *ID*	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** ドライブ番号	指定された仮想ドライブのコマンドモードを開始します。
ステップ 4	Server /chassis/storageadapter/virtual-drive # **clear-transport-ready**	これにより、選択したトランスポート可能な仮想ドライブが元の状態に戻されます。 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**y**を入力します。
ステップ 5	（任意） Server /chassis/storageadapter/virtual-drive # **show detail**	変更した仮想ドライブのプロパティを表示します。

例

次の例は、選択したトランスポート可能な仮想ドライブを元の状態に戻す方法を示しています。

```
Server # scope chassis
Server /chassis # scope server 1
Server /chassis # scope storageadapter SLOT-HBA
Server /chassis/storageadapter # scope virtual-drive 5
Server /chassis/storageadapter/virtual-drive # clear-transport-ready
Since they belong to same drive group, all these virtual drives will be moved out of
Transport Ready - 0
Are you sure you want to proceed?[y|N]y
Server /chassis/storageadapter/virtual-drive # show detail
Virtual Drive 0:
    Health: Good
    Status: Optimal
    Visibility : Visible
    Name: RAID0_124_RHEL
    Size: 2858160 MB
    Physical Drives: 1, 2, 4
    RAID Level: RAID 0
    Boot Drive: false
    FDE Capable: 0
    FDE Enabled: 0
    Target ID: 0
    Strip Size: 64 KB
    Drives Per Span: 3
    Span Depth: 1
    Access Policy: Read-Write
    Cache Policy: Direct
    Read Ahead Policy: None
```

```
    Requested Write Cache Policy: Write Through
    Current Write Cache Policy: Write Through
    Disk Cache Policy: Unchanged
    Auto Snapshot: false
    Auto Delete Oldest: true
    Allow Background Init: true
Server /chassis/storageadapter/virtual-drive #
```

ストレージコントローラ用に物理ドライブステータス自動構成モードに構成する

Cisco UCS C220 M6、C240 M6、C220 M7、および C240 M7 サーバーでは、自動構成により、コントローラはブートのたびにドライブを JBOD またはシングル ドライブ RAID0 VD に自動構成できます。手動で構成されたドライブは、自動構成の一部とは見なされません。

以下の表は、さまざまなシナリオでの自動構成の動作を示しています。

物理ドライブステータス自動設定モード	再起動または **OCR**	ホットプラグ	ユーザアクション
未構成良好（UG）	すべての **[未構成良好（unconfigured-good）]** ドライブは、**[未構成良好（unconfigured-good）]** のままです。 以前に構成されたすべての **[jbod]** は **[jbod]** のままです。	• 挿入されたドライブは **[unconfigured-good]** のままです。 • 別のサーバーからの JBOD は、このコントローラで **[unconfigured-good]** のままです。	• 挿入されたドライブは **[unconfigured-good]** のままです。 • 自動構成を無効にしても、既存の構成には影響しません。 • すべての **[jbod]** デバイスは、コントローラの起動後も **[jbod]** のままです。 • **[unconfigured-good]** は、コントローラの起動後も **[unconfigured-good]** のままです。

物理ドライブステータス自動設定モード	再起動または OCR	ホットプラグ	ユーザアクション
jbod	すべての **[unconfigured-good]** は **[jbod]** に変換されます。	新しく挿入された未構成のデバイスは、**[jbod]** に変換されます。	コントローラ上のすべての **[unconfigured-good]** のドライブ（ユーザーが作成したものではない）は、**[jbod]** に変換されます。 ユーザーが作成した **[unconfigured-good]** ドライブは、次回の再起動まで **[unconfigured-good]** のままです。再起動中に、**[unconfigured-good]** は **[jbod]** に変換されます。
[raid-0-writeback]	すべての **[unconfigured-good]** は、**[raid-0-writeback]** に変換されます。	新しく挿入された未構成のデバイスは、**[raid-0-writeback]** に変換されます。	コントローラー上のすべての **[unconfigured-good]** のドライブ（ユーザーが作成したものではない）は、**[raid-0-writeback]** に変換されます。 ユーザーが作成した **[unconfigured-good]** は、コントローラの再起動後も **[unconfigured-good]** のままです。 すべての **[raid-0-writeback]** デバイスは、コントローラの再起動後も **[raid-0-writeback]** として残ります。

[jbod] をデフォルト構成として選択すると、ホストの再起動後、**[unconfigured-good]** の状態は保持されません。ドライブの状態は、自動構成機能を無効にすることで保持できます。**[set-auto-cfg-option]** 構成オプションが使用されている場合、デフォルトの自動構成は常にドライブを **[unconfigured-good]** としてマークします。

自動構成を選択すると、ドライブは目的のドライブ状態に構成されます。また、JBOD および未構成のドライブは、次のコントローラのブートまたは OCR に応じてドライブの状態を設定します。

次の表は、さまざまな自動構成シナリオのサンプル ユースケースを示しています。

ユースケースのシナリオ	物理ドライブステータス自動設定モード
サーバーを JBOD のみに使用する	**jbod**

ユースケースのシナリオ	物理ドライブステータス自動設定モード
RAID ボリュームのサーバーの使用	**未構成良好（UG）**
JBOD と RAID ボリュームが混在するサーバーの使用	**未構成良好（UG）**
ドライブの RAID0 書き戻しごとにサーバーを使用する	**[raid-0-writeback]**

物理ドライブ ステータス自動構成モードの設定

次の手順では、コントローラで物理ドライブ ステータス自動構成モードを設定する方法について説明します。

始める前に

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

（注） 一部の UCS C シリーズ サーバーでのみ、物理ドライブ ステータス自動構成モードを設定できます。

手順

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**

ストレージ アダプタのコマンド モードを開始します。

ステップ 3 Server /chassis/storageadapter# **set-auto-cfg-option** *unconfigured-good*

次のメッセージが表示されます。

自動構成オプションを変更しますか？

[yes] と入力して確定します -> [yes]

確認プロンプトに [yes] と入力します。**[unconfigured-good]** モードを有効にします。これがデフォルトのオプションです。

名前	説明
[物理ドライブ ステータス自動構成モード（Physical Drive Status Auto Config Mode）] オプション	次のいずれかになります。 • **[unconfigured-good]**：デフォルトのオプション。サーバーを RAID ボリュームおよび混合 JBOD に使用している場合は、このオプションを選択します。 • **[raid-0-writeback]**：ドライブごとの R0 WB にサーバーを使用している場合は、このオプションを選択します。 • **[jbod]**：サーバーを JBOD のみに使用している場合は、このオプションを選択します。

（注） **[自動構成（Auto Config）]** モードで適切なオプションを選択すると、未使用の物理ドライブのすべてのステータスが変更されます。

例

この例では、**[物理ドライブ ステータス自動構成モード（physical drive status auto config mode）]** を **[unconfigured-good]** に設定します。

```
Server# scope chassis
Server /chassis # scope storageadapter
Server /chassis/storageadapter # set-auto-cfg-option unconfigured-good
Enter 'yes' to confirm -> yes
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。

重要 次の 2 つのシナリオでは外部設定をインポートすることはできません。

1. セキュアな仮想ドライブがリモート キーを使用してサーバー 1（設定のインポート元）で作成され、ローカル キーを使用してサーバー 2（インポート先）で作成された場合。
2. サーバー 2 が、サーバー 1 の KMIP サーバー クラスタの一部でない別の KMIP サーバーで構成されている場合。

これらのシナリオで外部設定をインポートするには、サーバー 2 のコントローラ セキュリティをローカル キー管理からリモート キー管理に変更し、サーバー 1 の KMIP が設定されている同じクラスタから同じ KMIP サーバーを使用します。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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** スロット	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。 （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。

例

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。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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** スロット	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	（任意） 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 5	（任意） Server /chassis/storageadapter/physicsl-drive # **show detail**	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。

例

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がクリアされます。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。

始める前に

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

手順

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

例

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** スロット	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。

例

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。

始める前に

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** スロット	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。

例

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。

始める前に

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

手順

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

例

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。

始める前に

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

手順

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

	コマンドまたはアクション	目的
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	（任意） Server /chassis/storageadapter/physicsl-drive # **show detail**	物理ドライブの詳細が表示されます。

例

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。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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** スロット	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	（任意） Server /chassis/storageadapter/physicsl-drive # **show detail**	物理ドライブの詳細を表示します。

例

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。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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** スロット	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	（任意） Server /chassis/storageadapter/physicsl-drive # **show detail**	物理ドライブの詳細を表示します。

例

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 #
```

コントローラのストレージ ファームウェア ログの取得

このタスクでは、コントローラのストレージ ファームウェア ログを取得して /var/log 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。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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** スロット	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-storage-fw-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** コントローラのストレージ ファームウェア ログの取得には、2～4分かかることがあります。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。

例

次に、スロット 3 の MegaRAID コントローラのストレージ ファームウェア 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-storage-fw-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)
```

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

デュアルまたは複数のコントローラの環境でコントローラ セキュリティを設定する場合に考慮すべきシナリオ

（注） デュアルまたは複数のコントローラの接続は一部のサーバーでのみ使用できます。

コントローラのセキュリティは、個別に有効、無効、または変更できます。ただし、ローカル キー管理とリモート キー管理は、サーバー上のすべてのコントローラに適用されます。したがって、キー管理モードの切り替えを伴うセキュリティ アクションは慎重に行う必要があります。両方のコントローラが安全で、コントローラの 1 つを別のモードに移動する場合は、もう一方のコントローラでも同じ操作を実行する必要があります。

次の 2 つのシナリオを考えてみましょう。

- シナリオ 1：キー管理はリモートに設定されています。両方のコントローラは安全で、リモート キー管理を使用します。ローカル キー管理に切り替える場合は、各コントローラのキー管理を切り替えて、リモート キー管理を無効にします。
- シナリオ2：キー管理はローカルに設定されています。両方のコントローラは安全で、ローカル キー管理を使用します。リモート キー管理に切り替える場合は、リモート キー管理を有効にして、各コントローラのキー管理を切り替えます。

いずれかのコントローラでコントローラ セキュリティ方式を変更しないと、セキュアなキー管理がサポートされていない設定状態になります。

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

始める前に

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

手順

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

例

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

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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** スロット	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、**n** (no) と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。

例

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

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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** スロット	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、**n** (no) と入力して操作をキャンセルします。

例

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。

始める前に

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

手順

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

例

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 #
```

リモート キー管理からローカル キー管理へのコントローラ セキュリティの切り替え

このタスクによって、コントローラ セキュリティをローカル管理からリモート管理に切り替えたり、リモート管理からローカル管理に切り替えることができます。

始める前に

- このタスクを実行するには、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。
- KMIP が有効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 storageadapter** スロット *ID*	ストレージ アダプタ コマンド モードを開始します。
ステップ 3	Server /chassis/storageadapter # **switch-to-local-key-mgmt**	プロンプトで **y** と入力します。 （注） 複数のコントローラがある場合はそれらのセキュリティも同様に切り替える必要があります。
ステップ 4	Server /chassis/server/storageadapter # *key id*	プロンプトで新しい ID を入力します。ローカル キー管理に切り替えます。

例

次に、コントローラ セキュリティをリモート キー管理からローカル キー管理へ切り替える例を示します。

```
Server # scope chassis
Server /chassis # scope storageadapter SLOT-HBA 1
Server /chassis/storageadapter # switch-to-local-key-mgmt
Executing this command will require you to disable remote key management once switch is
 complete.
Do you want to continue(y or n)?y
Proceeding to switch to local key management.
Enter new security-key: test
Will change security-key to 'test'
```

```
Switch to local key management complete on controller in SLOT-HBA.
***Remote key management needs to be disabled***
Please disable remote key management.
Server /chassis/server/storageadapter #
```

次のタスク

リモート キー管理からローカル キー管理に切り替えた後、必ず KMIP セキュア キー管理を無効にしてください。

ローカル キー管理からリモート キー管理へのコントローラ セキュリティの切り替え

このタスクによって、コントローラセキュリティをローカル管理からリモート管理に切り替えたり、リモート管理からローカル管理に切り替えることができます。

始める前に

このタスクを実行するには、admin 権限でログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope storageadapter** スロット *ID*	ストレージ アダプタ コマンド モードを開始します。
ステップ 3	Server /chassis/storageadapter # **switch-to-remote-key-mgmt**	プロンプトで **y** と入力します。
ステップ 4	Server /chassis/storageadapter # *security id*	プロンプトでセキュリティ キーを入力します。リモート キー管理に切り替えます。

例

次に、コントローラ セキュリティをローカル キー管理からリモート キー管理へ切り替える例を示します。

```
Server # scope chassis
Server /chassis # scope storageadapter SLOT-HBA 1
Server /chassis/server/storageadapter # switch-to-remote-key-mgmt
Changing the security key requires existing security key.
Please enter current security-key --> test
Switch to remote key management complete on controller in SLOT-HBA.
Server /chassis/server/storageadapter #
```

仮想ドライブの削除

重要　このタスクでは、仮想ドライブ（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）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。

始める前に

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

手順

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

例

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。

始める前に

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

手順

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

例

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 ドライブとして設定

始める前に

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

手順

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

例

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

始める前に

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

手順

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

例

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。

始める前に

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

手順

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

例

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

始める前に

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

手順

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

例

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

始める前に

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

手順

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

例

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

始める前に

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

手順

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

例

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。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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** スロット	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**	

例

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

始める前に

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

	コマンドまたはアクション	目的
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。

例

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

始める前に

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

例

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

始める前に

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

手順

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

例

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

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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** スロット	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**	

例

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

始める前に

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

手順

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

例

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

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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** スロット	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 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

例

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

始める前に

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** スロット	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。

例

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

始める前に

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** スロット	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。

例

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 #
```

コントローラ設定のクリア

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope 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** スロット *ID*	ストレージアダプタ コマンド モードを開始します。
ステップ 3	Server /chassis/storageadapter # **clear-all-config**	プロンプトで **yes** と入力します。コントローラ設定をクリアします。

例

次に、コントローラ設定をクリアする例を示します。

```
Server # scope chassis
Server /chassis # scope storageadapter SLOT-HBA 1
Server /chassis/storageadapter # clear-all-config
Are you sure you want to clear the controller's config and delete all VDs?
Enter 'yes' to confirm -> yes
Enter administrative password to proceed with operation\n
Password -> Password accepted. Performing requested operation.
Server /chassis/storageadapter #
```

ストレージコントローラの工場出荷時の初期状態への復元

始める前に

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

手順

	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** スロット *ID*	ストレージアダプタ コマンド モードを開始します。
ステップ 3	Server /chassis/storageadapter # **set-factory-defaults**	プロンプトで **yes** と入力します。コントローラの設定パラメータを出荷時のデフォルトに復元します。

例

次に、コントローラの設定パラメータを出荷時のデフォルトに復元する例を示します。

```
Server # scope chassis
Server /chassis # scope storageadapter SLOT-HBA 1
Server /chassis/storageadapter # set-factory-defaults
This operation will restore controller settings to factory default values. Do you want
to proceed?
Enter 'yes' to confirm -> yes
Server /chassis/storageadapter #
```

ストレージ コントローラのログの表示

始める前に

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

手順

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

例

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 #
```

物理ドライブの詳細の表示

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** スロット	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 # **show detail**	物理ドライブの詳細を表示します。

例

次に、物理ドライブの情報を表示する例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope physical-drive 202
Server /chassis/storageadapter/physical-drive # show detail
Physical Drive Number 202:
    Controller: SLOT-HBA
    Info Valid: Yes
    Info Invalid Cause:
    Enclosure Device ID: 252
    Device ID: 8
    Drive Number: 202
    Health: Good
    Status: Online
    Boot Drive: false
    Manufacturer: ATA
    Model: INTEL SSDSC2BB480G4
    Predictive Failure Count: 0
    Drive Firmware: 0370
    Type: SSD
    Block Size: 512
    Physical Block Size: 4096
    Negotiated Link Speed: 6.0 Gb/s
    Locator LED: false
    FDE Capable: 0
    FDE Enabled: 0
    FDE Secured: 0
    FDE Locked: 0
    FDE Locked Foreign Config: 0
    Enclosure Association: Direct Attached
    Enclosure Logical ID: N/A
    Enclosure SAS Address[0]: N/A
    Enclosure SAS Address[1]: N/A
    Power Cycle Count: 106
```

```
    Power On Hours: 10471
    Percentage Life Left: 100
    Wear Status in Days: 1825
    Percentage Reserved Capacity Consumed: 0
    Time of Last Refresh : 2017-03-04 13:47
    Operating Temperature: 34
    Media Error Count: 0
    Other Error Count: 0
    Interface Type: SATA
    Block Count: 937703088
    Raw Size: 457862 MB
    Non Coerced Size: 457350 MB
    Coerced Size: 456809 MB
    SAS Address 0: 4433221108000000
    SAS Address 1: 0x0
    Power State: active
```

NVMe コントローラの詳細の表示

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 nvmeadapter**	使用可能な NVMe アダプタを表示します。
ステップ 3	Server /chassis/nvmeadapter # **scope nvmeadapter** *NVMe アダプタ名*	選択した NVMe ダプタ コマンド モードを入力します。
ステップ 4	Server /chassis/nvmeadapter # **show detail**	NVMe コントローラの詳細を表示します。

例

この例は、コントローラ情報を表示する方法を示します。

```
Server# scope chassis
Server /chassis # show nvmeadapter
PCI Slot
----------------------------
NVMe-direct-U.2-drives
PCIe-Switch
Server /chassis # scope nvmeadapter PCIe-Switch
Server /chassis/nvmeadapter # show detail
PCI Slot: PCIe-Switch
    Health: Good
    Drive Count: 8
    Vendor ID: MICROSEM
    Product ID: PFX 48XG3
    Component ID: 8533
```

```
    Product Revision: RevB
    P2P Vendor ID: f811
    P2P Device ID: efbe
    Running Firmware Version: 1.8.0.58-24b1
    Pending Firmware Version: 1.8.0.58
    Switch temperature: 49 degrees C
    Switch status: Optimal
    Link Status: Optimal
Server /chassis/nvmeadapter #
```

NVMe 物理ドライブの詳細の表示

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 nvmeadapter**	使用可能な NVMe アダプタを表示します。
ステップ 3	Server /chassis/nvmeadapter # **scope nvmeadapter** *NVMe アダプタ名*	選択した NVMe ダプタ コマンド モードを入力します。
ステップ 4	Server /chassis/nvmeadapter # **show nvme-physical-drive**	使用可能な物理ドライブが表示されます。
ステップ 5	サーバ/シャーシ/nvmeadapter # **scope nvme-physical-drive** 物理ドライブ番号	選択した物理ドライブ コマンド モードを開始します。
ステップ 6	Server /chassis/nvmeadapter/nvme-physical-drive # **show detail**	NVMe 物理ドライブの詳細を表示します。

例

次に、物理ドライブの情報を表示する例を示します。

```
Server# scope chassis
Server /chassis # scope nvmeadapter NVMe-direct-U.2-drives
Server /chassis/nvmeadapter # show nvme-physical-drive
Physical Drive Number Product Name Manufacturer Serial Number Temperature % Drive Life
Used Performance Level LED Fault status % Power on Hours
--------------------- ----- ------------ ------------- ----------- -----------------
----------------- ---------------- ----------------
REAR-NVME-1           Ci... HGST         SDM00000E5EC  48 degre... 3                 100
              Healthy. Driv... 2
REAR-NVME-2           Ci... HGST         SDM00000DC90  47 degre... 2                 100
              Healthy          3
Server /chassis/nvmeadapter # scope nvme-physical-drive REAR-NVME-1
Server /chassis/nvmeadapter/nvme-physical-drive # show detail
```

```
Physical Drive Number REAR-NVME-1:
    Product Name: Cisco UCS (SN200) 2.5 inch 800 GB NVMe based PCIe SSD
    Manufacturer: HGST
    Serial Number: SDM00000E5EC
    Temperature: 48 degrees C
    % Drive Life Used: 3
    Performance Level: 100
    LED Fault status: Healthy. Drive is overused based on current write pattern
    % Power on Hours: 2
    Firmware Revision:
    PCI Slot: REAR-NVME-1
    Managed Id: 10
    Controller Type: NVME-SFF
    Controller Temperature: 48 degrees C
    Fault State: 0
    Throttle Start Temperature: 70 degrees C
    Shutdown Temperature: 75 degrees C
Server /chassis/nvmeadapter/nvme-physical-drive #
```

SIOC NVMe ドライブの詳細の表示

その CMC に関連付けられている SIOC の NVMe ドライブを表示するために、特定の CMC のスコープを設定する必要があります。

（注） この機能は、一部の S シリーズ サーバでのみ使用できます。

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 cmc** *[1 | 2]*	CMC コマンド モードを開始します。
ステップ 3	Server /chassis/CMC # **scope nvmeadapter** *adapter name*	NVMe アダプタ コマンド モードを開始します。
ステップ 4	Server /chassis/CMC/nvmeadapter # **show nvme-physical-drive detail**	SIOC NVMe 物理ドライブの詳細を表示します。

例

この例では、SIOC NVMe ドライブの詳細を表示する方法を示します。

```
Server # scope chassis
Server /chassis # scope cmc
Server /chassis/cmc # show detail
Firmware Image Information:
    ID: 1
```

```
    Name: CMC1
    SIOC PID: UCS-S3260-PCISIOC
    Serial Number: FCH21277K8T
    Update Stage: ERROR
    Update Progress: OS_ERROR
    Current FW Version: 4.0(0.166)
    FW Image 1 Version: 0.0(4.r17601)
    FW Image 1 State: BACKUP INACTIVATED
    FW Image 2 Version: 4.0(0.166)
    FW Image 2 State: RUNNING ACTIVATED
    Reset Reason: ac-cycle
    Secure Boot: ENABLED
Server /chassis # scope cmc 1
Server /chassis/cmc # scope nvmeadapter NVMe-direct-U.2-drives
Server /chassis/cmc/nvmeadapter # show nvme-physical-drive detail
Physical Drive Number SIOCNVMe1:
    Product Name: Cisco 2.5 inch  1TB Intel P4501 NVMe Med. Perf. Value Endurance
    Manufacturer: Intel
    Serial Number: PHLF7303008G1P0KGN
    Temperature: 39 degrees C
    % Drive Life Used: 1
    Performance Level: 100
    LED Fault status: Healthy
    Drive Status: Optimal
    % Power on Hours: 8
    Firmware Version: QDV1CP03
    PCI Slot: SIOCNVMe1
    Managed Id: 1
    Controller Type: NVME-SFF
    Controller Temperature: 39
    Throttle State: 0
    Throttle Start Temperature: 70
    Shutdown Temperature: 80
Physical Drive Number SIOCNVMe2:
    Product Name: Cisco 2.5 inch 500GB Intel P4501 NVMe Med. Perf. Value Endurance
    Manufacturer: Intel
    Serial Number: PHLF73440068500JGN
    Temperature: 39 degrees C
    % Drive Life Used: 1
    Performance Level: 100
    LED Fault status: Healthy
    Drive Status: Optimal
    % Power on Hours: 7
    Firmware Version: QDV1CP03
    PCI Slot: SIOCNVMe2
    Managed Id: 2
    Controller Type: NVME-SFF
    Controller Temperature: 39
    Throttle State: 0
    Throttle Start Temperature: 70
    Shutdown Temperature: 80
Server /chassis/cmc/nvmeadapter #
```

PCI スイッチの詳細の表示

この機能は、いくつかの C シリーズ サーバのみで使用可能です。

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 pci-switch**	システムで利用可能な PCI スイッチのリストが表示されます。
ステップ 3	Server /chassis # **show pci-switch detail**	システムで利用可能な PCI スイッチの詳細を表示します。

例

この例では、PCI スイッチの詳細を表示する方法を示します。

```
Server # scope chassis
Server /chassis # show pci-switch
Slot-ID                  Product Name         Manufacturer
------------------------ -------------------- --------------------
PCI-Switch-1             PEX 8764             PLX
PCI-Switch-2             PEX 8764             PLX
PCI-Switch-3             PEX 8764             PLX
PCI-Switch-4             PEX 8764             PLX
Server /chassis # show pci-switch detail
PCI SWITCH:
    Slot-ID: PCI-Switch-1
    Product Name: PEX 8764
    Product Revision: 0xab
    Manufacturer: PLX
    Device Id: 0x8764
    Vendor Id: 0x10b5
    Sub Device Id: 0x8764
    Sub Vendor Id: 0x10b5
    Temperature: 43
    Composite Health: Good
    Adapter Count: 3
PCI SWITCH:
    Slot-ID: PCI-Switch-2
    Product Name: PEX 8764
    Product Revision: 0xab
    Manufacturer: PLX
    Device Id: 0x8764
    Vendor Id: 0x10b5
    Sub Device Id: 0x8764
    Sub Vendor Id: 0x10b5
    Temperature: 43
    Composite Health: Good
    Adapter Count: 3
PCI SWITCH:
    Slot-ID: PCI-Switch-3
    Product Name: PEX 8764
    Product Revision: 0xab
    Manufacturer: PLX
    Device Id: 0x8764
    Vendor Id: 0x10b5
    Sub Device Id: 0x8764
    Sub Vendor Id: 0x10b5
```

```
    Temperature: 42
    Composite Health: Good
    Adapter Count: 3
PCI SWITCH:
    Slot-ID: PCI-Switch-4
    Product Name: PEX 8764
    Product Revision: 0xab
    Manufacturer: PLX
    Device Id: 0x8764
    Vendor Id: 0x10b5
    Sub Device Id: 0x8764
    Sub Vendor Id: 0x10b5
    Temperature: 43
    Composite Health: Degraded
    Adapter Count: 3
C480-FCH2213WH02 /chassis #
Server /chassis/ #
```

特定の PCI スイッチの詳細の表示

この機能は、いくつかの C シリーズ サーバのみで使用可能です。

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 pci-switch**	システムで利用可能な PCI スイッチのリストが表示されます。
ステップ 3	Server/chassis # **scope pci-switch** *PCI-Switch Number*	選択したスイッチの PCI スイッチ コマンド モードを開始します。
ステップ 4	Server /chassis/pci-switch # **show detail**	PCI スイッチの詳細を表示します。
ステップ 5	Server /chassis/pci-switch # **show adapter-list**	PCI スイッチに存在する、アダプタの詳細を表示します。

例

この例では、特定の PCI スイッチの詳細を表示する方法を示します。

```
Server # scope chassis
Server /chassis # show pci-switch
Slot-ID                  Product Name         Manufacturer
------------------------ -------------------- --------------------
PCI-Switch-1             PEX 8764             PLX
PCI-Switch-2             PEX 8764             PLX
PCI-Switch-3             PEX 8764             PLX
PCI-Switch-4             PEX 8764             PLX
Server /chassis # scope pci-switch PCI-Switch-1
```

```
Server /chassis/pci-switch show detail
PCI SWITCH:
    Slot-ID: PCI-Switch-1
    Product Name: PEX 8764
    Product Revision: 0xab
    Manufacturer: PLX
    Device Id: 0x8764
    Vendor Id: 0x10b5
    Sub Device Id: 0x8764
    Sub Vendor Id: 0x10b5
    Temperature: 43
    Composite Health: Good
    Adapter Count: 3
Server /chassis/pci-switch # show adapter-list
Slot                 Link Status          Link Speed           Link Width
Status
-------------------- -------------------- -------------------- --------------------
--------------------
GPU-3                up                   8.0                  16                   Good
GPU-4                up                   8.0                  16                   Good
12                   up                   8.0                  16                   Good
Server /chassis/pci-switch #
```

Flexible Flash コントローラの管理

Cisco Flexible Flash

M5 サーバでは、Flexible Flash コントローラはミニ ストレージ モジュール ソケットに挿入されます。ミニストレージ ソケットはマザーボードの M.2 スロットに挿入されます。M.2 スロットは SATA M.2 SSD スロットもサポートしています。

（注） M.2 スロットは、このリリースでは NVMe をサポートしていません。

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。

M.2 ドライブのインストールおよび設定の詳細については、次の URL にある C240 M5 サーバ用の『Cisco UCS サーバ インストレーションおよびサービス ガイド』の**「ストレージ コントローラに関する考慮事項（組み込み SATA RAID の要件）」**および**「M.2 用ミニストレージ キャリア内の M.2 SSD の交換」**のセクションを参照してください。

https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/products-installation-guides-list.html

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 の上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 ファームウェアの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。

アクション	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。

- サーバーに空の FlexFlash カードを追加し、最新バージョンにファームウェアをアップグレードします。
- 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ーに追加します。

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、サーバーに追加される空のカードのサイズが、サーバー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 サーバーでは、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 M5 および C240 M5 サーバの Flexible Flash コントローラ プロパティの設定

始める前に

- このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。
- 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	必須: 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 operational-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 # **set read-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。 読み取りエラーしきい値を指定するには、1 以上 255 以下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 # **set read-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。 読み取りエラーしきい値を指定するには、1 以上 255 以下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 6	Server /chassis/flexflash/operational-profile # **set write-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

	コマンドまたはアクション	目的
		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。 書き込みエラーしきい値を指定するには、1 以上 255 以下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 # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、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 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。

始める前に

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

• 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	必須: 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。

例

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。

始める前に

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

• 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。

	コマンドまたはアクション	目的
ステップ 2	必須: 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 # **configure-cards-mirror SLOT-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 Partition Name(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 Mirror Partition 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。
ステップ 7	**Set Virtual Drive as non-removable (Default is removable)?[y|N]** プロンプトで **y** を入力します。	非リムーバブルとして VD を設定することができます。 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 8	**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 9	（任意） Server /chassis/flexflash # **show physical-drive**	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、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。

例

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 :HV
Set Virtual Drive as non-removable (Default is removable)?[y|N]y
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 #
```

仮想ドライブの有効化

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。
- 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	必須: 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	必須: Server /chassis/ flexflash # **scope virtual-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 # **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。

例

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

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。
- 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	必須: 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	必須: Server /chassis/ flexflash # **scope virtual-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。

例

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

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。
- 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	必須: 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	必須: Server /chassis/ flexflash # **scope virtual-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。

例

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)10% done
    Last Operation completion status: none

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

FlexFlash ログの表示

始める前に

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	必須: Server /chassis # **scope flexflash** *index*	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 # **show logs**	Flexible Flash コントローラのログを表示します。

例

Flexible Flash コントローラのログの例です。

```
Server # scope chassis
Server /chassis # scope chassis flexflash FlexFlash-0
Server /chassis/flexflash # show logs
TimeStamp                   Severity      Description
---------                   --------      -----------
2017 July 10 07:16:17 UTC    warning       "CYWB_LOG: CYWB: USB connection status, 3.0
```

```
enable=1, 3.0 mode=1"
2017 July 10 07:46:05 UTC    warning       "CYWB_LOG: CYWB: USB connection status, 3.0
enable=1, 3.0 mode=1"
2017 July 10 07:46:05 UTC    warning       "CYWB_LOG: CYWB FWLOG (usbapp): USB HSChirp
event, data=1"
2017 July 10 07:45:07 UTC    warning       "CYWB_LOG: CYWB FWLOG (usbapp): USB Suspend
event, data=0"
2017 July 10 07:45:06 UTC    warning      "CYWB_LOG: CYWB FWLOG (usbapp): USB VbusValid
 event, data=0"
2017 July 10 07:44:23 UTC    warning       "CYWB_LOG: CYWB FWLOG (usb): connect done,
usb_state=4 ctrl_reg=0"
2017 July 10 07:44:23 UTC    info          "cywb_blkdev_create_disks: Finished changing
 disks: S0=0 S1=0 RAID=0 TOTAL=0"
2017 July 10 07:44:23 UTC    info          "cywbblkdev_blk_put: disk=cd3ad400
queue=cd3bd360 port=0 unit=0 usage=0"
2017 July 10 07:44:23 UTC    info          "cywb_blkdev_create_disks: S2 unit 0 has
become unavailable"
2017 July 10 07:44:23 UTC    info         "CYWB_LOG: Found 0 RAID partitions, 0 partitions
 on port0 and 0 partitions on port 1"
2017 July 10 07:44:23 UTC    info           cywb_blkdev_create_disks called
2017 July 10 07:44:23 UTC    info          "cywb_blkdev_create_disks: Scheduling driver
 callback"
2017 July 10 07:44:23 UTC    info         "cywbblkdev: Added disk=cd3ad400 queue=cd3bd360
 port=0 unit=0"
2017 July 10 07:44:23 UTC    info         "cywbblkdev: Registered block device cydiskraida
 with capacity 124727295 (major=254, minor=0)"
2017 July 10 07:44:23 UTC    info           cywbblkdev_blk_release exit
2017 July 10 07:44:23 UTC    info           "cywbblkdev_blk_put: disk=cd3ad400
queue=cd3bd360 port=0 unit=0 usage=1"
2017 July 10 07:44:23 UTC    info           cywbblkdev_blk_release entry
2017 July 10 07:44:23 UTC    warning      "CYWB_LOG: CyWb: Disk on port0, unit0 is busy,
 waiting"
2017 July 10 07:44:23 UTC    warning       "CYWB_LOG: CYWB: No device found on storage
port 0"
2017 July 10 07:44:23 UTC    info          cywbblkdev_revalidate_disk called
2017 July 10 07:44:23 UTC    info          cywbblkdev_blk_open exit
2017 July 10 07:44:23 UTC    info          cywbblkdev_media_changed called
2017 July 10 07:44:23 UTC    info          cywbblkdev_blk_open entry
2017 July 10 07:44:23 UTC    info          "cywb_blkdev_create_disks: Finished changing
 disks: S0=0 S1=0 RAID=1 TOTAL=1"
```

FlexUtil コントローラの管理

C シリーズ M5 ラックマウント サーバーは、サーバー 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用に microSD メモリ カードをサポートします。ライザー 1 にはこの microSD メモリ カード スロットがあります。Cisco FlexUtil は、32 GB の microSD カードのみをサポートします。

次のユーザー認識可能なパーティションが microSD カードに存在します。

- Server Configuration Utility（SCU）–1.25 GB
- 診断-0.25 GB
- Host Update Utility（HUU）–1.5 GB
- ドライバ–8 GB

- ユーザー（User）

（注） MicroSD の各パーティションの数とサイズは固定されています。

いつでも、ホストに2つのパーティションをマップできます。（ユーザーパーティションを除く）これらのパーティションは、CIFS または NFS 共有により更新できます。第 2 レベルの BIOS ブート順序のサポートは、すべての起動可能なパーティションにも使用できます。

（注） ユーザーパーティションはストレージにのみ使用する必要があります。このパーティションは OS のインストールをサポートしていません。

FlexUtil 運用プロファイルの設定

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。
- お使いのプラットフォームで Cisco FlexUtil 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	必須: Server /chassis # **scope flexutil**	FlexUtil コントローラ コマンド モードを開始します。
ステップ 3	必須: Server /chassis/flexutil # **scope operational-profile**	Operational Profile コマンド モードを開始します。
ステップ 4	Server /chassis/flexutil/operational-profile # **set read-err-count-threshold** *count*	読み取りエラーのしきい値のカウントを設定します。 （注） しきい値の値がゼロの場合は、特殊なケースとして扱われますが、カードはエラー カウントがゼロのしきい値を超えても異常とマークされません。

	コマンドまたはアクション	目的
ステップ 5	Server /chassis/flexutil/operational-profile* # **set write-err-count-threshold** *count*	書き込みエラーのしきい値のカウントを設定します。 （注） しきい値の値がゼロの場合は、特殊なケースとして扱われますが、カードはエラー カウントがゼロのしきい値を超えても異常とマークされません。
ステップ 6	Server /chassis/flexutil/operational-profile* # **commit**	トランザクションをシステムにコミットします。

例

次に、FlexUtil 運用プロファイルを設定する例を示します。

```
Server# scope chassis
Server /chassis # scope flexutil
Server /chassis/flexutil # scope operational-profile
Server /chassis/flexutil/operational-profile # set read-err-count-threshold 49
Server /chassis/flexutil/operational-profile* # set write-err-count-threshold 49
Server /chassis/flexutil/operational-profile* # commit
Server /chassis/flexutilServer /chassis/flexutil/operational-profile
```

FlexUtil カード設定のリセット

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。
- お使いのプラットフォームで Cisco FlexUtil 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	必須: Server /chassis # **scope flexutil**	FlexUtil 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/flexutil # **reset-card-config**	確認プロンプトで、**y** と入力します。FlexUtil カードの構成をリセットします。

例

次の例は、FlexUtil カード構成をリセットする方法を示しています。

```
Server# scope chassis
Server /chassis # scope flexutil
Server /chassis/flexutil # reset-card-config
This operation will wipe all the data on the card.
Any VD connected to host (except UserPartition) will be disconnected from host.
This task will take few minutes to complete.
Do you want to continue?[y|N]y
Server /chassis/flexutil #
```

FlexUtil プロパティの表示

始める前に

お使いのプラットフォームで Cisco FlexUtil 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	必須: Server /chassis # **scope flexutil**	FlexUtil 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/flexutil # **show detail**	FlexUtil コントローラのプロパティを表示します。

例

次の例では、FlexUtil コントローラのプロパティを表示します。

```
Server# scope chassis
Server /chassis # scope flexutil
Server /chassis/flexutil # show detail
Controller Flexutil:
    Product Name: Cisco Flexutil
    Internal State: Connected
    Controller Status: OK
    Physical Drive Count: 1
    Virtual Drive Count: 5
Server /chassis/flexutil #
```

FlexUtil 物理ドライブの詳細の表示

始める前に

お使いのプラットフォームで Cisco FlexUtil 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	必須: Server /chassis # **scope flexutil**	FlexUtil 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/flexutil # **show physical-drive detail**	FlexUtil 物理ドライブのプロパティを表示します。

例

次の例では、FlexUtil 物理ドライブのプロパティを表示します。

```
Server# scope chassis
Server /chassis # scope flexutil
Server /chassis/flexutil # show physical-drive detail
Physical Drive microSD:
    Status: present
    Controller: Flexutil
    Health: healthy
    Capacity: 30624 MB
    Write Enabled: true
    Read Error Count: 0
    Read Error Threshold: 49
    Write Error Count: 0
    Write Error Threshold : 49
    Product Name: SD32G
    Product Revision: 3.0
    Serial#: 0x1cafb
    Manufacturer Id: 39
    OEM Id: PH
    Manufacturing Date : 12/2016
    Block Size: 512 bytes
    Partition Count: 5
    Drives Enabled: SCU Diagnostics HUU Drivers UserPartition
Server /chassis/flexutil #
```

FlexUtil 仮想ドライブの詳細の表示

始める前に

お使いのプラットフォームで Cisco FlexUtil 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	必須: Server /chassis # **scope flexutil**	FlexUtil コントローラ コマンド モードを開始します。
ステップ 3	必須: Server /chassis/flexutil # **scope virtual-drive**	仮想ドライブ コマンド モードを開始します。
ステップ 4	Server /chassis/flexutil/virtual-drive # **show detail**	FlexUtil 物理ドライブのプロパティを表示します。

例

次の例では、FlexUtil 物理ドライブのプロパティを表示します。

```
Server# scope chassis
Server /chassis # scope flexutil
Server /chassis/flexutil # scope virtual-drive
Server /chassis/flexutil/virtual-drive # show detail
Virtual Drive SCU:
    ID: 1
    LUN ID: NA
    Size: 1280 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 Diagnostics:
    ID: 2
    LUN ID: 0
    Size: 256 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:
    ID: 3
    LUN ID: NA
    Size: 1536 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 Drivers:
```

```
    ID: 4
    LUN ID: NA
    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 UserPartition:
    ID: 5
    LUN ID: NA
    Size: 11159 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/flexutil/virtual-drive #
```

FlexUtil 仮想ドライブへのイメージの追加

始める前に

- このタスクを実行するには、admin 権限でログインします。
- お使いのプラットフォームで Cisco FlexUtil 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	必須: Server /chassis # **scope flexutil**	FlexUtil コントローラ コマンド モードを開始します。
ステップ 3	必須: Server /chassis/flexutil # **scope vd-image-configs**	仮想ドライブ イメージ 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/flexutil/vd-image-configs # **vd-image-cifs** {**virtual-drive-name remote-share remote-file-path** [*mount options*]	FlexUtil 仮想ドライブに CIFS ファイルをマップします。次を指定する必要があります。 • 仮想ドライブの名前

	コマンドまたはアクション	目的
		• IP アドレス（IPv4 または IPv6 アドレス）と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 • サーバーに接続するためのユーザー名とパスワード
ステップ 5	Server /chassis/flexutil/vd-image-configs # **vd-image-nfs** {**virtual-drive-name remote-share remote-file-path** [*mount options*]	FlexUtil 仮想ドライブに NFS ファイルをマップします。次を指定する必要があります。 • 仮想ドライブの名前 • IP アドレス（IPv4 または IPv6 アドレス）を含むリモート共有 • 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 6	Server /chassis/flexutil/vd-image-configs # **vd-image-www** {**virtual-drive-name** | **remote-share** | **remote-file-path** [*mount options*]	HTTPS ファイル仮想ドライブを示しています。次を指定する必要があります。 • マップする仮想ドライブの名前 • 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 • サーバーに接続するためのユーザー名とパスワード
ステップ 7	Server /chassis/flexutil/vd-image-configs # **show detail**	FlexUtil 仮想ドライブ イメージの詳細が表示されます。

例

次の例に、イメージを FlexUtil 仮想ドライブにマップする方法を示します。

```
Server# scope chassis
Server /chassis # scope flexutil
Server /chassis/flexutil # scope vd-image-configs
Server /chassis/flexutil/vd-image-configs # vd-image-nfs HUU 10.10.10.10:/nfsdata
ucs-c240m5-huu-3.1.0.182.iso
Server /chassis/flexutil/vd-image-configs # show detail
Virtual drive: SCU
    mount-type: nfs
    remote-share: 10.10.10.10:/nfsshare
    remote-file: ucs-cxx-scu-4.0.12.3.iso
    mount-options: 'nolock,noexec,noac,soft,timeo=60,retry=2,rsize=3072,wsize=3072'

Virtual drive: Diagnostics
    mount-type: nfs
    remote-share: 10.10.10.10:/nfsshare
    remote-file: ucs-cxx-diag.5.0.1a.iso
    mount-options: 'nolock,noexec,noac,soft,timeo=60,retry=2,rsize=3072,wsize=3072'

Virtual drive: HUU
    mount-type: nfs
    remote-share: 10.10.10.10:/nfsdata
    remote-file: ucs-c240m5-huu-3.1.0.182.iso
    mount-options: "nolock,noexec,noac,soft,timeo=60,retry=2,rsize=3072,wsize=3072"

Virtual-drive: Drivers
    mount-type: None
    remote-share: None
    remote-file: None
    mount-options: None
Server /chassis/flexutil/vd-image-configs #
```

FlexUtil 仮想ドライブの更新

始める前に

- このタスクを実行するには、admin 権限でログインする必要があります。
- お使いのプラットフォームで Cisco FlexUtil 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	必須: Server /chassis # **scope flexutil**	FlexUtil コントローラ コマンド モードを開始します。
ステップ 3	必須: Server /chassis/flexutil # **scope virtual-drive**	仮想ドライブ コマンド モードを開始します。
ステップ 4	Server /chassis/flexutil/virtual-drive # **update-vds** *virtual-drive*	選択した仮想ドライブを更新します。

	コマンドまたはアクション	目的
ステップ 5	（任意） Server /chassis/flexutil/virtual-drive # **update-vds-cancel**	進行中の仮想ドライブの更新をキャンセルします。
ステップ 6	Server /chassis/flexutil/virtual-drive # **show detail**	FlexUtil 仮想ドライブ イメージの詳細が表示されます。

例

次に、FlexUtil 仮想ドライブを更新する例を示します。

```
Server# scope chassis
Server /chassis # scope flexutil
Server /chassis/flexutil # scope virtual-drive
Server /chassis/flexutil/virtual-drive # update-vds HUU
Server /chassis/flexutil/virtual-drive # show detail

Virtual-drive: SCU
    partition-id: 1
    lun-id: NA
    size: 1280 MB
    partition-scope: Non-RAID
    partition-status: Healthy
    partition-type: Removable
    writable: R/W
    host-accessible: Not-Connected
    operation-in-progress: NA
    operation-completion-status: none

 Virtual-drive: Diagnostics
    partition-id: 2
    lun-id: NA
    size: 256 MB
    partition-scope: Non-RAID
    partition-status: Healthy
    partition-type: Removable
    writable: R/W
    host-accessible: Not-Connected
    operation-in-progress: NA
    operation-completion-status: none

Virtual-drive: HUU
    partition-id: 3
    lun-id: NA
    size: 1536 MB
    partition-scope: Non-RAID
    partition-status: Healthy
    partition-type: Removable
    writable: R/W
    host-accessible: Not-Connected
    operation-in-progress: Updating
    operation-completion-status: none

Virtual-drive: Drivers
    partition-id: 4
    lun-id: NA
    size: 8192 MB
    partition-scope: Non-RAID
```

```
    partition-status: Healthy
    partition-type: Removable
    writable: R/W
    host-accessible: Not-Connected
    operation-in-progress: NA
    operation-completion-status: none

 Virtual drive: UserPartition
    partition-id: 5
    lun-id: NA
    size: 11159 MB
    partition-scope: Non-RAID
    partition-status: Healthy
    partition-type: Removable
    writable: R/W
    host-accessible: Not-Connected
    operation-in-progress: NA
    operation-completion-status: none
Server /chassis/flexutil/virtual-drive #
```

FlexUtil 仮想ドライブの有効化

始める前に

- このタスクを実行するには、admin 権限でログインする必要があります。
- お使いのプラットフォームで Cisco FlexUtil がサポートされている必要があります。
- ホストにドライブをマッピングする前に、仮想ドライブのイメージを更新します。

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	必須: Server /chassis # **scope flexutil**	FlexUtil コントローラ コマンド モードを開始します。
ステップ 3	必須: Server /chassis/flexutil # **scope virtual-drive**	仮想ドライブ コマンド モードを開始します。
ステップ 4	Server /chassis/flexutil/virtual-drive # **enable-vds** *virtual-drive*	仮想ドライブをホストにマップします。
ステップ 5	Server /chassis/flexutil/virtual-drive # **show detail**	FlexUtil 仮想ドライブ イメージの詳細が表示されます。

例

次の例は、仮想ドライブ イメージのホストへのマップ方法を示します。

```
Server# scope chassis
Server /chassis # scope flexutil
Server /chassis/flexutil # scope virtual-drive
Server /chassis/flexutil/virtual-drive # enable-vds HUU
Server /chassis/flexutil/virtual-drive # show detail
Virtual Drive  ID     LUN ID Size     VD Status    Host Accessible   Operation in
Last Operation
               progress  completion status
-------------- ------ ------ -------- ------------ ----------------- ------------
-----------------
SCU            1      NA     1280 MB  Healthy      Not-Connected     NA         none
Diagnostics    2      0      256 MB   Healthy      Connected         NA
Update-Success
HUU            3      1      1536 MB  Healthy      Connected         NA
Update-Success
Drivers        4      NA     8192 MB  Healthy      Not-Connected     NA
none
UserPartition  5      NA     11159 MB Healthy      Not-Connected     NA
none
Server /chassis/flexutil/vd-image-configs #
```

仮想ドライブへのイメージのマッピング

始める前に

- このタスクを実行するには、admin 権限でログインする必要があります。
- お使いのプラットフォームで Cisco FlexUtil 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	必須: Server /chassis # **scope flexutil**	FlexUtil コントローラ コマンド モードを開始します。
ステップ 3	必須: Server /chassis/flexutil # **scope vd-image-configs**	仮想ドライブ イメージ 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	必須: /chassis/flexutil/vd-image-configs # **vd-image-nfs HUU** *nfs/cifs share IP and path ISO image file*	IP と nfs/cifs 共有のパス、および ISO イメージ ファイルを指定します。
ステップ 5	/chassis/flexutil/vd-image-configs # **show detail**	FlexUtil 仮想ドライブ イメージの詳細が表示されます。

例

次の例に、イメージを FlexUtil 仮想ドライブに追加する方法を示します。

```
Server# scope chassis
Server /chassis # scope flexutil
Server /chassis/flexutil # scope vd-image-configs
Server /chassis/flexutil/vd-image-configs #  vd-image-nfs HUU 10.127.54.176:/nfsdata
ucs-c240m5-huu-3.1.0.182.iso
Server /chassis/flexutil/vd-image-configs # show detail

    virtual-drive: SCU
    mount-type: nfs
    remote-share: 10.104.236.81:/nfsshare
    remote-file: ucs-cxx-scu-4.0.12.3.iso
    mount-options: 'nolock,noexec,noac,soft,timeo=60,retry=2,rsize=3072,wsize=3072'

    virtual-drive: Diagnostics
    mount-type: nfs
    remote-share: 10.104.236.81:/nfsshare
    remote-file: ucs-cxx-diag.5.0.1a.iso
    mount-options: 'nolock,noexec,noac,soft,timeo=60,retry=2,rsize=3072,wsize=3072'

    virtual-drive: HUU
    mount-type: nfs
    remote-share: 10.127.54.176:/nfsdata
    remote-file: ucs-c240m5-huu-3.1.0.182.iso
    mount-options: "nolock,noexec,noac,soft,timeo=60,retry=2,rsize=3072,wsize=3072"

    virtual-drive: Drivers
    mount-type: None
    remote-share: None
    remote-file: None
    mount-options: None

Server /chassis/flexutil/vd-image-configs
```

仮想ドライブからのイメージのマッピング解除

始める前に

- このタスクを実行するには、admin 権限でログインする必要があります。
- お使いのプラットフォームで Cisco FlexUtil 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。

	コマンドまたはアクション	目的
ステップ 2	必須: Server /chassis # **scope flexutil**	FlexUtil コントローラ コマンド モードを開始します。
ステップ 3	必須: Server /chassis/flexutil # **scope vd-image-configs**	仮想ドライブ イメージ 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/flexutil/vd-image-configs # **unmap** *virtual-drive*	選択した仮想ドライブのイメージをマッピング解除します。
ステップ 5	Server /chassis/flexutil/vd-image-configs # **show detail**	FlexUtil 仮想ドライブ イメージの詳細が表示されます。

例

次に、FlexUtil 仮想ドライブのマッピングを解除する例を示します。

```
Server# scope chassis
Server /chassis # scope flexutil
Server /chassis/flexutil # scope vd-image-configs
Server /chassis/flexutil/vd-image-configs # unmap HUU
Server /chassis/flexutil/vd-image-configs # show detail
Virtual drive: SCU
    mount-type: nfs
    remote-share: 10.10.10.10:/nfsshare
    remote-file: ucs-cxx-scu-4.0.12.3.iso
    mount-options: 'nolock,noexec,noac,soft,timeo=60,retry=2,rsize=3072,wsize=3072'

Virtual drive: Diagnostics
    mount-type: nfs
    remote-share: 10.10.10.10:/nfsshare
    remote-file: ucs-cxx-diag.5.0.1a.iso
    mount-options: 'nolock,noexec,noac,soft,timeo=60,retry=2,rsize=3072,wsize=3072'

Virtual drive: HUU
    mount-type: None
    remote-share: None
    remote-file: None
    mount-options: None

Virtual-drive: Drivers
    mount-type: None
    remote-share: None
    remote-file: None
    mount-options: None
Server /chassis/flexutil/vd-image-configs #
```

仮想ドライブ上の画像の消去

始める前に

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

- お使いのプラットフォームで Cisco FlexUtil 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	必須: Server /chassis # **scope flexutil**	FlexUtil コントローラ コマンド モードを開始します。
ステップ 3	必須: Server /chassis/flexutil # **scope virtual-drive**	仮想ドライブ コマンド モードを開始します。
ステップ 4	Server /chassis/flexutil/virtual-drive # **erase-vds** *virtual-drive*	仮想ドライブのイメージを消去します。
ステップ 5	Server /chassis/flexutil/virtual-drive # **show detail**	FlexUtil 仮想ドライブ イメージの詳細が表示されます。

例

次の例は、仮想ドライブの削除方法を示します。

```
Server# scope chassis
Server /chassis # scope flexutil
Server /chassis/flexutil # scope virtual-drive
Server /chassis/flexutil/virtual-drive # erase-vds SCU
This operation will erase data on the VD
Continue?[y|N]y
Server /chassis/flexutil/virtual-drive # show detail
Virtual Drive  ID     LUN ID Size     VD Status    Host Accessible   Operation in
Last Operation
               progress  completion status
-------------- ------ ------ -------- ------------ ----------------- ------------
-----------------
SCU            1      NA     1280 MB  Healthy      Not-Connected     Erasing
none
Diagnostics    2      0      256 MB   Healthy      Connected         NA
Update-Success
HUU            3      1      1536 MB  Healthy      Connected         NA
Update-Success
Drivers        4      NA     8192 MB  Healthy      Not-Connected     NA
none
UserPartition  5      NA     11159 MB Healthy      Not-Connected     NA
none
C220-WZP210606A7 /chassis/flexutil/virtual-drive #
```

Cisco ブート最適化 M.2 Raid コントローラ

Cisco ブート最適化 M. 2 Raid コントローラの詳細の表示

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 MSTOR-RAID**	Cisco ブート最適化 M.2 Raid 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/storageadapter # **show detail**	Cisco ブート最適化 M.2 Raid コントローラの詳細を表示します。

例

この例は、コントローラ情報を表示する方法を示します。

```
Server# scope chassis
Server /chassis # show storageadapter MSTOR-RAID
Server /chassis/storageadapter # show detail
PCI Slot MSTOR-RAID:
    Health: Good
    Controller Status: Optimal
    Product Name: Cisco Boot optimized M.2 Raid controller
    Serial Number: FCH222877A7
    Firmware Package Build: 2.3.17.1009
    Product ID: Marvell
    Flash Memory Size: 2 MB
    Product PID: UCS-M2-HWRAID
Server /chassis/storageadapter #
```

Cisco ブート最適化 M.2 Raid コントローラ物理ドライブの詳細の表示

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 MSTOR-RAID**	Cisco ブート最適化 M.2 Raid コントローラ 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** *Physical Drive Number*	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 # **show general**	一般的な物理ドライブ情報を表示します。
ステップ 5	Server /chassis/storageadapter/physical-drive # **show detail**	物理ドライブの詳細を表示します。
ステップ 6	Server /chassis/storageadapter/physical-drive # **show inquiry-data**	物理ドライブのシリアル番号を表示します。
ステップ 7	Server /chassis/storageadapter/physical-drive # **show status**	物理ドライブの健全性状況が表示されます。

例

次に、物理ドライブの情報を表示する例を示します。

```
Server# scope chassis
Server /chassis # show storageadapter MSTOR-RAID
Server /chassis/storageadapter # scope physical-drive 253
Server /chassis/storageadapter/physical-drive # show general
PCI Slot MSTOR-RAID:
    Health: Good
    Controller Status: Optimal
    Product Name: Cisco Boot optimized M.2 Raid controller
    Serial Number: FCH222877A7
    Firmware Package Build: 2.3.17.1009
    Product ID: Marvell
    Flash Memory Size: 2 MB
    Product PID: UCS-M2-HWRAID
Server /chassis/storageadapter/physical-drive # show detail
Physical Drive Number 253:
    Controller: MSTOR-RAID
    Info Valid: Yes
    Info Invalid Cause:
    Drive Number: 253
    Health: Good
    Status: Online
    Manufacturer: ATA
    Model: Micron_5100_MTFDDAV240TCB
    Drive Firmware: D0MU054
    Type: SSD
    Block Size: 512
    Physical Block Size: 512
    Negotiated Link Speed: 6.0 Gb/s
    State: online
    Operating Temperature: 32
    Enclosure Association: Direct Attached
    Interface Type: SATA
    Block Count: 468862127
    Raw Size: 228936 MB
    Non Coerced Size: 228936 MB
    Coerced Size: 228936 MB
    Power State: active
```

```
Server /chassis/storageadapter/physical-drive # show inquiry-data
Physical Drive Number 253:
    Controller: MSTOR-RAID
    Info Valid: Yes
    Info Invalid Cause:
    Vendor: ATA
    Product ID: Micron_5100_MTFDDAV240TCB
    Drive Firmware: D0MU054
    Drive Serial Number: 18201CB94A2C
Server /chassis/storageadapter/physical-drive # show status
Physical Drive Number 253:
    Controller: MSTOR-RAID
    Info Valid: Yes
    Info Invalid Cause:
    State: online
    Online: true
    Fault: false
Server /chassis/storageadapter/physical-drive #
```

Cisco ブート最適化 M.2 Raid コントローラ仮想ドライブの詳細の表示

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 MSTOR-RAID**	Cisco ブート最適化 M.2 Raid 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/storageadapter # **scope virtual-drive** *Virtual Drive Number*	仮想ドライブ コマンド モードを開始します。
ステップ 4	Server /chassis/storageadapter/virtual-drive # **show detail**	仮想ドライブ情報を表示します。
ステップ 5	Server /chassis/storageadapter/virtual-drive # **show lrop-info**	仮想ドライブの再構築のステータスを表示します。

例

次に、仮想ドライブの情報を表示する例を示します。

```
Server# scope chassis
Server /chassis # show storageadapter MSTOR-RAID
Server /chassis/storageadapter # scope virtual-drive 0
Server /chassis/storageadapter/virtual-drive # show detail
Virtual Drive 0:
    Health: Good
    Status : Optimal
    Name: test
    Size: 228872 MB
    Physical Drives: 253, 254
```

```
    RAID Level: RAID 1
    Target ID: 0
    Strip Size: 32 KB
Server /chassis/storageadapter/virtual-drive # show detail
LROP:
    LROP In Progress: false
    Current Long-Running Op: No operation in progress
    Percent Complete: 0
Server /chassis/storageadapter/virtual-drive #
```

Cisco ブート最適化 M.2 Raid コントローラ仮想ドライブの作成

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 MSTOR-RAID**	Cisco ブート最適化 M.2 Raid 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/storageadapter # **create-virtual-drive**	それぞれのプロンプトで、仮想ドライブ名とストライプサイズを入力します。これにより仮想ドライブを作成します。

例

この例は、仮想ドライブの作成方法を示します。

```
Server# scope chassis
Server /chassis # show storageadapter MSTOR-RAID
Server /chassis/storageadapter # create-virtual-drive
Please enter Virtual Drive name (15 characters maximum, hit return to skip name)--> test


Unused physical drives available 2:
    ID  Size(MB)       Model        Interface  Type
   253  228936         ATA          SATA       SSD
   254  915715         ATA          SATA       SSD

PD sizes NOT equal. NOT Assigning VD_size for RAID1

Optional attribute:

  stripsize: defaults to 64K Bytes

     0: 32K Bytes
    1: 64K Bytes
  Choose number from above options or hit return to pick default--> 0
stripsize will be set to 32K Bytes (4 and 'strip-size\:32k')

New virtual drive will have the following characteristics:
  - RAID level: '1'
  - Name: 'test'
```

```
  - stripsize: 32K Bytes

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

Cisco ブート最適化 M.2 Raid コントローラ仮想ドライブの削除

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 storageadapter MSTOR-RAID**	Cisco ブート最適化 M.2 Raid 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/storageadapter # **delete-virtual-drive**	確認プロンプトで **[はい (yes)]** と入力します。これにより仮想ドライブを削除します。

例

次の例は、仮想ドライブの削除方法を示します。

```
Server# scope chassis
Server /chassis # show storageadapter MSTOR-RAID
Server /chassis/storageadapter # delete-virtual-drive
Are you sure you want to delete virtual drive 0?
All data on the drive will be lost.  Enter 'yes' to confirm -> yes
Server /chassis/storageadapter #
```

Cisco ブート最適化 M.2 Raid コントローラ外部設定のインポート

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope storageadapter MSTOR-RAID**	Cisco ブート最適化 M.2 Raid 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/storageadapter # **import-foreign-config**	確認プロンプトで **[はい (yes)]** と入力し、コントローラ設定をインポートします。

例

次に、コントローラ設定をインポートする方法の例を示します。

```
Server# scope chassis
Server /chassis # show storageadapter MSTOR-RAID
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 #
```

Cisco ブート最適化 M.2 Raid コントローラ外部設定の消去

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 MSTOR-RAID**	Cisco ブート最適化 M.2 Raid 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/storageadapter # **clear-foreign-config**	確認プロンプトで **[はい(yes)]** と入力し、コントローラ設定を消去します。

例

次に、コントローラ設定を消去する例を示します。

```
Server# scope chassis
Server /chassis # show storageadapter MSTOR-RAID
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 #
```

Cisco FlexMMC

Cisco FlexMMC の詳細の表示

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 flexmmc**	FlexMMC モードを開始します。
ステップ 3	Server/chassis/flexmmc # **show detail**	FlexMMC の詳細を表示します。

例

この例は、コントローラ情報を表示する方法を示します。

```
Server# scope chassis
Server /chassis # scope flexmmc
Server /chassis/flexmmc # show detail
Cisco FlexMMC Storage:
    Total Memory For IMC Utilities: 2048 MB
    Available Memory For IMC Utilities: 1970 MB
    Total Memory For User Files: 6144 MB
    Available Memory For User Files: 6144 MB
```

新しいイメージ ファイルのアップロード

始める前に

アップロード進行中のファイルがないことを確認してください。一度にアップロードできるイメージファイルは1つだけです。新しいファイルをアップロードするには、まず既存のファイルをマッピング解除して削除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 flexmmc**	FlexMMC 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/flexmmc # **download-file** *location mount_type serverip/remote_share remote_file option_string*	マッピング用のイメージファイルをアップロードします。

例

この例は、イメージ ファイルをアップロードする方法を示しています。

```
Server# scope chassis
Server /chassis # scope flexmmc
Server /chassis/flexmmc # download-file file location
```

イメージ ファイルの削除

始める前に

次の点を確認します。

- アップロード進行中のファイルはありません。アップロード進行中のファイルは削除できません。
- マッピングされているファイルはありません。すでにマッピングされているファイルは削除できません。ファイルを削除する前に、まずファイルのマッピングを解除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 flexmmc**	FlexMMC モードを開始します。
ステップ 3	Server/chassis/flexmmc # **delete-file** *file_ID*	イメージ ファイルを削除します。

例

次の例では、イメージ ファイルの削除方法を示します。

```
Server# scope chassis
Server /chassis # scope flexmmc
Server /chassis/flexmmc # delete-file file ID
```

イメージのマッピング

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 flexmmc**	FlexMMC モードを開始します。
ステップ 3	Server/chassis/flexmmc # **scope flexmmc-file** *file_ID*	マッピングするファイルを選択します。
ステップ 4	Server/chassis/flexmmc/flexmmc-file # **map**	

例

この例は、アップロード済みのイメージ ファイルをマッピングする方法を示しています。

```
Server# scope chassis
Server /chassis # scope flexmmc
Server /chassis/flexmmc # scope flexmmc-file file ID
Server /chassis/flexmmc/flexmmc-file # map
```

FlexMMC をデフォルト設定へリセット

この手順を実行して、FlexMMC をデフォルトの Cisco IMC 設定にリセットします。

（注） この手順を実行すると、アップロードされたすべてのイメージが削除されます。

始める前に

次の点を確認します。

- アップロード進行中のファイルはありません。ファイルのアップロードが進行中は、FlexMMC をデフォルト設定にリセットできません。
- マッピングされているファイルはありません。ファイルがすでにマッピングされている場合、FlexMMC をリセットすることはできません。FlexMMC をリセットする前に、まずファイルのマッピングを解除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 flexmmc**	FlexMMC モードを開始します。
ステップ 3	Server/chassis/flexmmc # **reset-to-default**	
ステップ 4	確認するには、**[yes]** と入力します。	FlexMMC をデフォルト設定にリセットします。

例

この例では、FlexMMC をデフォルト設定にリセットする方法を示します。

```
Server# scope chassis
Server /chassis # scope flexmmc
Server /chassis/flexmmc # reset-to-default
Are you sure you want to reset the Cisco FlexMMC to default? All the files will be
deleted/wiped
Please enter 'yes' to confirm: yes
Server /chassis/flexmmc
```

ドライブ診断の構成

ドライブ 診断の概要

ドライブ診断機能は、HDD/SSD および SAS/SATA ドライブ タイプでの診断の実行をサポートします。この機能を使用すると、デバイスから情報を取得して、使用状況、温度、エージング、メディアの摩耗、リソースの消費量などを判断することで、デバイスの正常性を判断できます。さらに、ドライブによって維持されるログページを収集および読み取りして、診断データを収集し、分析を実行することができます。

リリース 4.2 (2a) 以降、SATA ドライブでドライブ診断セルフテストを実行できます。

リリース 4.1（3b） 以降、SSD ドライブでドライブ診断セルフテストを実行できます。

デバイスのセルフテストは、次の 2 つのモードで実行できます。

- オンデマンドのデバイスセルフテスト：このモードでは、コマンドを実行してドライブのセルフテストを実行し、テクニカル サポート ユーティリティを使用して診断レポートを表示できます。
- バックグラウンド デバイス セルフテスト：このモードでは、ドライブの定期的なセルフテストをスケジュールし、テクニカル サポート ユーティリティを使用して診断レポートを表示できます。

次の頻度で定期的なバックグラウンド セルフテスト モードをスケジュールできます。

- 毎日
- 毎週
- 2 週に 1 回
- 毎月

（注） デフォルトでは、この頻度は毎週に設定されています。

コントローラが Unconfigured Good で、ホットスペア HDD ドライブが省電力モードの場合、診断セルフテストはドライブ上で開始できません。そのため、診断ドライブ セルフテストを実行するためにドライブはスピンアップする必要があります。省電力モードにある HDD で診断ドライブ セルフテスト ポリシーを設定するには、パラメータ **[bg_diag_powersave_override]** を使用できます。詳細については、省電力モードの HDD での診断ドライブ セルフテスト ポリシーの設定 （360 ページ）を参照してください。

デバイスのセルフテストの全体的な結果セットを使用して、デバイスの実際の状態と正常性を評価できます。Cisco IMC の 2 つのインターフェイス（CLI と Redfish API）を使用して、コマンドを実行して診断データを収集できます。

（注） この機能は、すべての UCS C シリーズ M5 および M6 サーバーで使用できます。

オンデマンド ドライブ セルフ テストの開始

オンデマンドのデバイス セルフ テストを開始し、テクニカル サポート ユーティリティを使用して診断データをダウンロードできます。

始める前に

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

手順

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**

ストレージ アダプタ コマンドモードを開始します。

ステップ 3 Server chassis storageadapter# **show physical-drive** {*1*}

ストレージアダプタの物理ドライブのリストを表示し、オンデマンドデバイス セルフ テストを実行する megaraid コントローラの物理ドライブを選択します。

ステップ 4 Server chassis storageadapter# **scope physical-drive** {*1*}

物理ドライブ 1 のコマンドモードを開始します。

ステップ 5 Server chassis storageadapter physical-drive# **start-diag**

診断データを収集するために、megaraid コントローラに接続された物理ドライブ 1 でオンデマンド セルフ デバイス テストを初期化します。

オンデマンド診断セルフテストジョブは、物理ドライブのバックグラウンドで実行されます。

（注） ドライブのセルフテストで `bg_diag_powersave_override` パラメータが `false` に設定されている場合、ドライブのセルフテストは省電力モードのドライブで実行されません。

例

この例では、診断データを収集するために、SATA ドライブでオンデマンドのデバイス セルフ テストを初期化します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope physical-drive drive-number
Server /chassis/storageadapter/physical-drive # start-diag
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
You are initiating drive self test diagnostics via Cisco IMC.
This task will take a few minutes to complete. You may monitor the status
  of the retrieval by running the 'get-diag-status' command.
When the self test is finished, the 'selftest-percent-complete' value shows
  '100%'.
You may then download the diag report using the Technical Support facility
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Do you want to proceed?
Enter 'yes' to confirm -> yes
Self test operation on drive: MRAID/10 initiated successfully

Server /chassis/storageadapter/physical-drive # get-diag-status
  selftest-type: Self test immediate offline
  selftest-status: Self test in progress
  selftest-percent-complete: 20

Server /chassis/storageadapter/physical-drive # get-diag-status
  selftest-type: Self test immediate offline
  selftest-status: Self test completed without error
  selftest-percent-complete: 100
Server /chassis/storageadapter/physical-drive #
```

次のタスク

- ドライブ セルフテストのステータスを表示 （356 ページ）を参照：現在実行中のデバイス セルフテストのステータスを表示できます。
- 診断セルフ テスト レポートの表示 （361 ページ）を参照：テクニカル サポート ユーティリティを使用して診断レポートを表示できます。

ドライブ セルフ テストのステータスを表示

物理ドライブでセルフ デバイス テストを実行し、`selftest-percent-complete` フィールドに値 `100` が表示され、テストがエラーなしで完了するまで、セルフテストのステータスが完了していることを確認します。その後、テクニカル サポート ユーティリティを使用して診断データをダウンロードできます。

始める前に

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

手順

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**

ストレージ アダプタ コマンド モードを開始します。

ステップ 3 Server chassis storageadapter# **scope physical-drive**

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# **get-diag-status**

ドライブで現在実行中のセルフ デバイス テストのステータスを取得します。

例

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-3
Server /chassis/storageadapter # scope physical-drive drive-number
Server /chassis/storageadapter/physical-drive # get-diag-status
selftest-type: Background
selftest-status: Self test in progress
selftest-percent-complete:11
Server /chassis/storageadapter/physical-drive # get-diag-status
selftest-type: Background
selftest-status: Self test in progress
selftest-percent-complete:34
```

```
Server /chassis/storageadapter/physical-drive # get-diag-status
selftest-type: Background
selftest-status: Self test completed without error
selftest-percent-complete:100
Server /chassis/storageadapter/physical-drive #
```

次のタスク

テクニカル サポート ユーティリティを使用して、診断結果を表示できます。「診断セルフ テスト レポートの表示 （361 ページ）」を参照してください。

セルフ テスト診断の中止

始める前に

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

手順

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**

ストレージ アダプタ コマンド モードを開始します。

ステップ 3 Server chassis storageadapter# **scope physical-drive**

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# **cancel-diag**

ドライブで現在実行中のセルフ デバイス テストを中止します。

例

この例では、SATA ドライブでのオンデマンド デバイス セルフ テストを中止し、進行中のセルフテストのステータスを表示します。

```
Server /chassis/storageadapter/physical-drive # get-diag-status
  selftest-type: Self test immediate offline
  selftest-status: Self test in progress
  selftest-percent-complete: 20

Server /chassis/storageadapter/physical-drive # cancel-diag
Self test operation on drive: MRAID/10 aborted successfully


Server /chassis/storageadapter/physical-drive # get-diag-status
  selftest-type: Self test immediate offline
```

```
selftest-status: Self test aborted by host
selftest-percent-complete: 0
```

バックグラウンドで診断ドライブ セルフ テストの開始

始める前に

バックグラウンド診断ドライブ セルフテスト ポリシーを設定する前に、次の構成パラメータを確認して設定する必要があります。

- **[bg_diag_enabled]**：この構成パラメータは、システムでバックグラウンド診断を実行するかどうかを指定します。このパラメータは、デフォルトで **False** に設定されます。
- **[bg_diag_frequency_interval]**：この構成パラメータは、ドライブでドライブ診断ジョブが開始される頻度を指定します。

  バックグラウンド診断ドライブのセルフテスト モードを、次の頻度で物理ドライブで実行するようにスケジュールできます。

  - 毎日
  - 毎週
  - 2 週に 1 回
  - 毎月

  デフォルトでは、このパラメータは**毎週**に設定されています。
- **[bg_diag_powersave_override]**：この構成パラメータは、省電力モードの HDD で診断ドライブのセルフテスト ポリシーを設定します。

  このパラメータを有効にすると、省電力モードのドライブがスピンアップされ、ドライブのセルフテストが実行されます。このパラメータを無効にすると、省電力モードのドライブでドライブのセルフテストが開始されません。

  デフォルトでは、このパラメータは **True** に設定されています。

手順

ステップ 1 Server # **scope diag-config**

構成モードを開始します。

ステップ 2 Server diag-config # **scope drive-diag-config**

drive-diag-config モードを開始します。

ステップ 3 Server diag-config/drive-diag-config # **show**

設定済みのバックグラウンド診断セルフテスト パラメータを表示します。

ステップ 4 （任意） Server diag-config/drive-diag-config # **set bg_diag_enabled** {*true*|*false*}

バックグラウンド診断の有効化パラメーターを `true` に設定して、バックグラウンド ドライブのセルフテストを有効にします。

ステップ 5 （任意） Server diag-config/drive-diag-config # **set bg_diag_frequency_interval** {*daily*|*weekly*|*fortnightly*|*monthly*}

バックグラウンド診断の頻度間隔パラメータを、バックグラウンド診断デバイスのセルフテストを物理ドライブで実行する必要がある望ましい頻度に設定します。

（注） 周波数パラメータ値の変更を変更してすぐに有効にするには、`bg_diag_enabled` パラメータを無効にしてから有効にする必要があります。

ステップ 6 （任意） Server diag-config/drive-diag-config # **set bg_diag_powersave_override** {*true*|*false*}

物理ドライブの省電力モードを無効にするには、バックグラウンド診断の省電力パラメータを `false` に設定します。

デフォルトでは、このパラメータは **True** に設定されています。

ステップ 7 Server diag-config/drive-diag-config # **commit**

構成パラメータに加えられた変更をシステム構成にコミットします。

例

この例では、バックグラウンド ドライブのセルフテスト構成パラメータを表示します。

```
Server# scope diag-config
Server /diag-config # scope drive-diag-config
scope /diag-config/drive-diag-config* # set  bg_diag_frequency_interval fortnightly
scope /diag-config/drive-diag-config # set  bg_diag_enabled true
scope /diag-config/drive-diag-config # set  bg_diag_powersave_override false
scope /diag-config/drive-diag-config* # commit
Config parameters committed successfully
scope /diag-config/drive-diag-config* # show
Background DST Enabled Background DST Frequency   Powersave Override
---------------------- -------------------------- ----------------------
True                   fortnightly                      False
```

次のタスク

テクニカル サポート ユーティリティから診断ドライブのセルフテスト レポートを表示できます。

省電力モードの HDD での診断ドライブ セルフテスト ポリシーの設定

コントローラが未構成の正常なホット スペア HDD ドライブを省電力モードにすると、ドライブで診断セルフテストを開始できません。そのため、診断ドライブセルフテストを実行するためにドライブはスピンアップする必要があります。

省電力モードにある HDD で診断ドライブ セルフテスト ポリシーを設定するには、パラメータ **[bg_diag_powersave_override]** を使用できます。

デフォルトでは、**[bg_diag_powersave_override]** パラメータが有効になっています。そのため、省電力モードのドライブはスピンアップして、診断ドライブ セルフテストを開始します。

省電力モードのドライブで診断ドライブ セルフテストを実行しない場合は、**[bg_diag_powersave_override]** パラメータを無効にする必要があります。

手順

ステップ 1 Server # **scope diag-config**

構成モードを開始します。

ステップ 2 Server diag-config # **scope drive-diag-config**

drive-diag-config モードを開始します。

ステップ 3 Server diag-config/drive-diag-config # **show**

ドライブ診断構成パラメータを表示します。

ステップ 4 （任意） Server diag-config/drive-diag-config # **set bg_diag_powersave_override** {*true*|*false*}

[bg_diag_powersave_override] パラメータを `false` に設定して、HDD の省電力モードを無効にします。

（注） デフォルトでは、**[bg_diag_powersave_override]** パラメータが有効になっています。

ステップ 5 Server diag-config/drive-diag-config # **commit**

構成パラメータに加えられた変更をシステム構成にコミットします。

例

この例では、ドライブ診断構成パラメータと、`[bg_diag_powersave_override]` パラメータを無効にする方法を示しています。

```
Server# scope diag-config
Server /diag-config # scope drive-diag-config
scope /diag-config/drive-diag-config # set  bg_diag_powersave_override false
scope /diag-config/drive-diag-config* # commit
Config parameters committed successfully
scope /diag-config/drive-diag-config* # show
```

```
Background DST Enabled Background DST Frequency   Powersave Override
---------------------- -------------------------- ----------------------
True                   weekly                     False
```

診断セルフ テスト レポートの表示

テクニカル サポート ユーティリティを開始し、ドライブ診断セルフテスト レポートの詳細を表示します。

始める前に

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。このテクニカル サポート 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構成情報、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。

（注） 診断セルフテスト レポートで利用可能な情報の詳細については、診断セルフテスト レポートの概要 （363 ページ） を参照してください。

手順

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 tech-support**

テクニカル サポート コマンド モードを開始します。

ステップ 3 サーバ/chassis/tech-support # **set remote-ip** *ip* アドレス

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 /chassis/tech-support # **set remote-path** *path/filename*

リモート サーバーで保存する必要のある診断セルフテスト レポートにファイル名を指定します。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 /chassis/tech-support # **set remote-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 サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバー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 サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。

このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[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 6 Server /chassis/tech-support # **set remote-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 /chassis/tech-support # **set remote-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 /chassis/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 /chassis/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 （任意） Server /chassis/tech-support # **show detail**

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# **tar -xzvf nv/log/storaged/diag/***diagnosic-report.tar.gz*

ファイルパス：`nv/log/storaged/diag/` に移動し、診断レポートにアクセスします。

次のタスク

生成されたレポート ファイルを Cisco TAC に提供します。

診断セルフテスト レポートの概要

このテクニカル サポート 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構成情報、ログ、および診断データの要約が含まれるセルフテストレポートを作成します。

セルフテスト レポートは、`.txt` および `.bin` フォーマットで生成されます。

次のリストは、診断セルフテスト レポートで使用できる構成情報とログの詳細を示しています。

- ドライブ スロット ID
- ドライブ セルフテスト結果
- ベンダー名
- 製造部分番号
- シリアル番号
- ファームウェア リビジョン
- 製造日
- 作成日
- セルフモニタリング、分析、およびレポーティング テクノロジー（SMART）モニタリング システムの値
- 温度の読み取り値
- 電源投入時間
- 検証エラー
- 非中程度のエラー
- プロトコル エラー
- 電源遷移
- バックグラウンド メディア スキャン
- 読み取り/書き込みエラー回復

（注）
- セルフテスト レポートの値は、16 進数形式です。値を 10 進数形式に変換する必要があります。
- セルフテスト レポートの最後にある **[診断の要約（Diagnostic Summary）]** セクションで、ID、ベンダーなどのドライブ固有の詳細を表示できます。

診断ファイル レポート形式のサンプル

以下のサンプルは、SATA ドライブのサンプル診断ファイル レポートの形式を示しています。

```
-----------------------------------------------
            DRIVE DIAGNOSTIC REPORT
-----------------------------------------------
    DIAG TIME STAMP := Thu Feb 24 04:43:01 2022

------------------------------------------------------------------------
  READ IDENTIFY DEVICE :0xec : 512 Bytes
------------------------------------------------------------------------
Vendor  Id         :  ATA
Product Id         :  INTEL SSDSC2KG960G8K
Firmware revision  :  XCV1CS04
Unit serial number :  BTYG817308KB960CGN
------------------------------------------------------------------------
  READ SMART ATTRIBUTES :0xd0 : 512 Bytes
------------------------------------------------------------------------
Self test status                        : 0 ( Self test completed without error )
Short self test rec poll time           : 1 (mins)
Extended self test rec poll time        : 2 (mins)
Conveyance self test rec poll time      : 2 (mins)
Offline data collection capability      : 121
                       Abort/restart offline by host not supported
                      Offline read scanning supported
                      Short and extended self-test supported
                      Conveyance self-test supported
                      Selective self-test supported

Offline data collection status          : 2 ( Offline data collection activity was
completed without error )
Total time Offline data collection      : 2 (secs)
Smart capability                      : 3 ( Smart save enabled, Smart attribute autosave
 enabled )
Error log capability                    : 1 ( Error logging supported )
------------------------------------------------------------------------
  READ SMART THRESHOLDS :0xd1 : 512 Bytes
------------------------------------------------------------------------
------------------------------------------------------------------------
                    SMART ATTRIBUTES SUMMARY
------------------------------------------------------------------------
ID#              ATTRIBUTE_NAME                FLAGS   VALUE    WORST  THRESH  RAW_VALUE
-------------------------------------------------------------------------------------------
5         Reallocate Sector Count               0x32    100      100    0       0
9         Power On Hours                        0x32    100      100    0       4318
12        Power Cycle Count                     0x32    100      100    0       1756
171       Program Fail Count                    0x32    100      100    0       0
172       Erase Fail Count                      0x32    100      100    0       0
184       End To End Data Path Error Count      0x33    100      100    90      0
187       Uncorrectable Error Count             0x32    100      100    0       0
194       Operating Temperature                 0x22    100      100    0       36
```

```
199       CRC Error Count                         0x3e    100       100     0       0
232       Reserved Capacity Consumed              0x33    100       100     10      0
233       Percentage Life Left                    0x32    98        98      0       98
233       Wear Status In Days                     0x32    98        98      0       1764
-----------------------------------------------------
                DIAGNOSTIC SUMMARY
-----------------------------------------------------
 Date of drive diag test  : Thu Feb 24 04:43:01 2022

 DST result (PASS/FAIL)   : PASS: Self test completed without error
 Drive slot id            : 102
 Drive Interface type     : SATA
 Drive Media type         : SSD
 Vendor                   : ATA
 Mfg Part Number          : INTEL SSDSC2KG960G8K
 Serial Number            : BTYG817308KB960CGN
 Firmware revision        : XCV1CS04
-----------------------------------------------------
```

以下のサンプルは、SAS ドライブのサンプル診断ファイル レポートの形式を示しています。

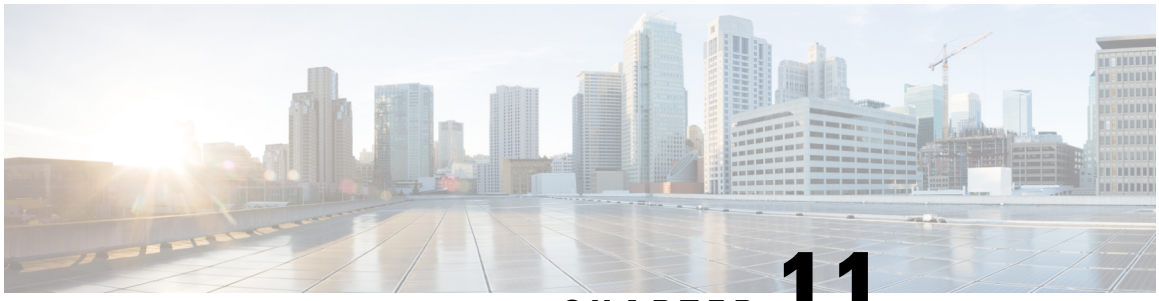
```
-------------------------------------------------
            DRIVE DIAGNOSTIC REPORT
-------------------------------------------------
    DIAG TIME STAMP := Tue Apr 12 14:43:54 2022

-------------------------------------------------
  INQUIRY EPVD0 PAGE:0x0 ( EVPD0 PAGE:0h) : 96 Bytes
-------------------------------------------------
Vendor  Id         : TOSHIBA
Product Id         : AL14SXB60EN
Firmware revision  : 5703
Unit serial number : X060A05HFJVF
-------------------------------------------------
 INQUIRY EPVD1 PAGE:0x0 ( SUPPORTED EPVD1 PAGES ) : 19 Bytes
-------------------------------------------------
Page 0x0
Page 0x80
Page 0x83
Page 0x86
Page 0x8a
Page 0x90
Page 0x91
Page 0xb1
-------------------------------------------------
  INQUIRY EPVD1 PAGE:0x83 : 76 Bytes
-------------------------------------------------
LUN(World Wide ID)                          := 0x5000039a780a1fad
Target Port Identifier(World Wide ID)       := 0x5000039a780a1fae
Relative Port Identifier                    := 0x1
Target Device Name(World Wide ID)           := 0x5000039a780a1fac
Target Device Name(World Wide ID) in ASCII := 5000039A780A1FAC
-------------------------------------------------
  INQUIRY EPVD1 PAGE:0x8a : 18 Bytes
-------------------------------------------------
Standby Z                         := 0x1
Standby Y                         := 0x1
Idle    A                         := 0x1
Idle    B                         := 0x1
Idle    C                         := 0x1
Stopped condition recovery time   := 0x3a98
Standby Z condition recovery time := 0x3a98
Standby Y condition recovery time := 0xfa0
Idle A condition recovery time    := 0x64
Idle B condition recovery time    := 0x4b0
```

```
Idle C condition recovery time    := 0xfa0
-------------------------------------------------
  INQUIRY EPVD1 PAGE:0xb1 : 64 Bytes
-------------------------------------------------
Medium rotation rate := 0x3a98
Nominal form factor  := 0x3
-----------------------------------------------------
  LOG SENSE PAGE:0x0 ( SUPPORTED PAGES) : 18 Bytes
-----------------------------------------------------
Page 0x0
Page 0x1
Page 0x2
Page 0x3
Page 0x5
Page 0x6
Page 0xd
Page 0xe
Page 0xf
Page 0x10
Page 0x15
Page 0x18
Page 0x1a
Page 0x2f
-----------------------------------------------------
 LOG SENSE PAGE:0x10 ( SELF TEST RESULTS ) : 404 Bytes
-----------------------------------------------------
Parameter code             : 0x1
General parameter data     : 0x3
Parameter len              : 0x10
Self test result           : 0x0 : Self test completed without error
Function code              : 0x1
Extended segment number    : 0x0 : No extended segment failures
First failure LBA          : 0xffffffffffffffff
Sense key                  : 0x0
Add Sense Code             : 0x0
Add Sense Code Qual        : 0x0
Vendor data                : 0x0
Timestamp( Power on hours) : 0x123e
-----------------------------------------------------------
  LOG SENSE PAGE:0x2f ( SMART STATUS ) : 12 Bytes
-----------------------------------------------------------
SMART sense code byte             := 0x0
SMART sense qualifier             := 0x0
Most recent temperature reading   := 0x1f
Vendor HDA temperature trip point := 0x0
-------------------------------------------------------
  LOG SENSE PAGE:0x2 ( WRITE ERROR COUNTERS ) : 88 Bytes
-------------------------------------------------------
errs_recovered_without_delay  := 0x10004
errs_recovered_with_delay     := 0x2000400000000
total_errors_recovered        := 0x1c8cbeba000006
times_recovery_invoked        := 0x0
total_bytes_written           := 0x0
count_hard_errors             := 0x0
-------------------------------------------------------
  LOG SENSE PAGE:0x3 ( READ ERROR COUNTERS ) : 88 Bytes
-------------------------------------------------------
errs_recovered_without_delay  := 0x10004
errs_recovered_with_delay     := 0x2000400000000
total_errors_recovered        := 0x6f0de26344000006
times_recovery_invoked        := 0x0
total_bytes_read              := 0x0
count_hard_errors             := 0x0
-------------------------------------------------------
```

```
  LOG SENSE PAGE:0x5 ( VERIFY ERROR COUNTERS ) : 88 Bytes
-------------------------------------------------------
errs_recovered_without_delay  := 0x10004
errs_recovered_with_delay     := 0x2000400000000
total_errors_recovered        := 0x6
times_recovery_invoked        := 0x0
total_bytes_verified          := 0x0
count_hard_errors             := 0x0
-------------------------------------------------------------
  LOG SENSE PAGE:0x6 ( NON-MEDIUM ERROR COUNTERS ) : 16 Bytes
-------------------------------------------------------------
error_count        := 0x4000000000
-------------------------------------------------
  LOG SENSE PAGE:0xd ( TEMPERATURE INFO ) : 16 Bytes
-------------------------------------------------
Temperature(celsius)     := 0x1f
Ref Temperature(celsius) := 0x41
-------------------------------------------------
  LOG SENSE PAGE:0xe ( START STOP CYCLE INFO  ) : 56 Bytes
-------------------------------------------------
Year of Manufacture                              := 2020
Week of Manufacture                              := 41
Accounting date year                             :=
Accounting date week                             :=
Specified cycle count over device lifetime       := c350
Accumulated start stop cycles                    := 46
Specified load unload count over device lifetime := 927c0
Accumulated load unload cycles                   := a84
-------------------------------------------------
  LOG SENSE PAGE:0x1a ( POWER TRANSITION INFO ) : 52 Bytes
-------------------------------------------------
Accumulated transitions to active state    := 5a83
Accumulated transitions to idle A          := 5a47
Accumulated transitions to idle B          := a3e
Accumulated transitions to idle C          := 0
Accumulated transitions to standby Z       := 0
Accumulated transitions to standby Y       := 0
-------------------------------------------------
  LOG SENSE PAGE:0x15 ( BMS TEST RESULTS ) : 503 Bytes
-------------------------------------------------
 Power on mins                     := 0x446a3
 BMS status                       := 8 (BMS suspended until BMS interval timer expires)

 BMS num_bg_scans_performed        := 203
 BMS medium_scan_progress          := 0
 BMS num_bg_medium_scans_performed := 0

-----------------------------------------------------------
  MODE SENSE PAGE:0x0 ( VENDOR UNIQUE PARAMS ) : 14 Bytes
-----------------------------------------------------------
Merge Glist into Plist(MRG)              : 0x0
Report Recovered Non Data Errors(RRNDE)  : 0x0
Veggie mode(VGMDE)                       : 0x0
Command Aging Enable(CAEN)               : 0x0
Format Degraded Disable(FDD)             : 0x0
Overall Command Timer(OCT)               : 0x0
AV ERP Mode(AVERP)                       : 0x0
Ignore Reassigned LBA(IGRA)              : 0x0
First Format Enable(FFMT)                : 0x0
Disable Restore Reassign Target(DRRT)    : 0x0
Format Certification(FCERT)              : 0x0
Overall Command Timer(low byte)          : 0x8
Temperature Threshold                    : 0xdd
Command Aging Limit(Hi byte)             : 0x2f
```

```
Command Aging Limit(Low byte)            : 0xb0
Read reporting threshold                 : 0x0
Write reporting threshold                : 0x0
----------------------------------------------------------------------
  MODE SENSE PAGE:0x1 ( READ/WRITE ERROR RECOVERY PARAMS) : 10 Bytes
----------------------------------------------------------------------
Automatic Write Reallocation Enabled(AWRE)   : 0x0
Automatic Read Reallocation Enabled(ARRE)    : 0x0
Transfer Block (TB)                          : 0x0
Read Continous(RC)                           : 0x0
Enable Early Recovery(EER)                   : 0x0
Post Error(PER)                              : 0x0
Data Teriminate on Error(DTE)                : 0x0
Disable Correction (DCR)                     : 0x0
Read Retry Count                             : 0x10
Write Retry Count                            : 0x45
Read Retry Count                             : 0x10
Recovery Time Limit                          : 0x0
----------------------------------------------------------
  MODE SENSE PAGE:0x3 ( FORMAT DEVICE PARAMS) : 22 Bytes
----------------------------------------------------------
Tracks per Zone                       : 0x1000
Alternate sectors per Zone            : 0x0
Alternate Tracks per Zone             : 0x800
Alternate Tracks per Logical Unit     : 0xdd45
Sectors Per Track                     : 0xb02f
Data Bytes per Physical Sector        : 0x0
Interleave                            : 0x2
Track Skew Factor                     : 0x1683
Cylinder Skew Factor                  : 0xdc00
Support Soft Sector Formatting(SSEC)  : 0x0
Removable Fixed Disk(RMB)             : 0x0
Hard Sector Formatting(HSEC)          : 0x0
SURF                                  : 0x0
----------------------------------------------------------------------
  MODE SENSE PAGE:0x7 ( VERIFY ERROR RECOVERY PARAMS) : 10 Bytes
----------------------------------------------------------------------
Early Error Recovery    (EER)  : 0x0
Data Terminate on Error (DTE)  : 0x0
PER                            : 0x0
DCR                            : 0x0
Verify Retry Count             : 0x10
Verify Recovery Time Limit     : 0x0
----------------------------------------------------------
  MODE SENSE PAGE:0x8 ( CACHING PARAMS ) : 18 Bytes
----------------------------------------------------------
Initiator Control (IC)                  : 0x0
Abort Pre-fetch(ABPF)                   : 0x0
Caching Analysis Permitted(CAP)         : 0x0
Discontinuity(DISC)                     : 0x0
Size Enable(SIZE)                       : 0x0
Write Cache Enable(WCE)                 : 0x0
Multiplication Factor(MF)               : 0x0
Read Cache Disable(RCD)                 : 0x0
Disable Read Ahead(DRA)                 : 0x0
Force Sequential Write(FSW)             : 0x0
Logical Block Cache Segment Size(LBCSS) : 0x0
Write Retention Priority                : 0x0
Demand Read Retention Priority          : 0x1
Disable Prefetch Transfer Len           : 0x0
Minimum Pre-fetch                       : 0x800
Maximum Pre-fetch                       : 0xdd45
Maximum Pre-fetch Celing                : 0xb02f
Number of Cache Segments                : 0x0
```

```
Cache Segment Size                      : 0x2
Non Cache Segment Size                  : 0x12
-----------------------------------------------------------------------
  MODE SENSE PAGE:0xa ( CONTROL MODE PAGE PARAMS ) : 10 Bytes
-----------------------------------------------------------------------
Descriptor Sense Data (D_SENSE)           := 0x0
Disable Protection Info Check (DPICZ)     := 0x0
Queue Error Management(QERR)              := 0x0
Disable Queuing(DQUE)                     := 0x0
Application Tag Owner(ATO)                := 0x0
Application Tag Mode Page Enabled(ATMPE)  := 0x0
Reject Write Without Protection(RWWP)     := 0x0
Queue Algorithm Modifier                  := 0x1
Busy Timeout Period                       := 0xdd45
Extended Self Test Completion time        := 0x0
-------------------------------------------------------------
  MODE SENSE PAGE:0x1a ( POWER CONTROL ) : 38 Bytes
-------------------------------------------------------------
Standby_Y                  : 0x0
Standby_Z                  : 0x0
Idle_A                     : 0x0
Idle_B                     : 0x0
Idle_C                     : 0x0
Idle A Condition Timer     : 0x8000000
Idle B Condition Timer     : 0x20000
Idle C Condition Timer     : 0x640269a
Standy Y Condition Timer   : 0x14000000
Standy Z Condition Timer   : 0xb02fdd45
PM BG Predence             : 0x0
-----------------------------------------------------------------------
  MODE SENSE PAGE:0x1c ( INFORMATIONAL EXCEPTIONS CONTROL ) : 10 Bytes
-----------------------------------------------------------------------
Performance(PERF)                  : 0x0
Enable Background Function(EBF)    : 0x0
Enable Warning ASC(EWASC)          : 0x0
Disable Exception Control(DEXCPT)  : 0x0
TEST                               : 0x0
Enable Background Error(EBACKERR)  : 0x0
Log Errors(LOGERR)                 : 0x0
Method of Reporting                : 0x0
Interval Timer                     : 0x8000000
Report Count                       : 0xdd45
-----------------------------------------------------------------------
                     SMART ATTRIBUTES SUMMARY
-----------------------------------------------------------------------
-------------------------------------------------------
                DIAGNOSTIC SUMMARY
-------------------------------------------------------
 Date of drive diag test  : Tue Apr 12 14:43:54 2022

 DST result (PASS/FAIL)   : PASS: Self test completed without error
 Drive slot id            : 1
 Drive Interface type     : SAS
 Drive Media type         : HDD
 Vendor                   : TOSHIBA
 Mfg Part Number          : AL14SXB60EN
 Serial Number            : X060A05HFJVF
 Firmware revision        : 5703
 Build date               :
 Mfg date                 : 2020/10
-------------------------------------------------------
```



CHAPTER 11

コミュニケーション サービスの設定

この章は、次の内容で構成されています。

TLS v1.2 の有効化または無効化

リリース 4.2 (2a) 以降、Cisco IMC は TLS v1.2 の無効化と、v1.2 と v1.3 の両方の暗号値のカスタマイズをサポートしています。

始める前に

[セキュリティの設定（Security Configuration）]の**[CC]**（コモンクライテリア）が有効になっている場合、TLS v1.2 を無効にすることはできません。TLS v1.2 を無効にする前に、**[CC]** が無効になっていることを確認してください。

TLS v1.2 を有効または無効にすると、vKVM、Web サーバー、XML API、および Redfish API セッションが再起動します。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	
ステップ 2	Server# **scope tls-config**	TLS 構成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/tls-config # **set tlsv2Enabled** *yes*|*no*	確認のために **y** を入力します。 TLS v1.2 を有効または無効にします。
ステップ 4	Server/tls-config* # **Commit**	変更を保存します。
ステップ 5	Server/tls-config # **set tlsv2CipherMode** *Custom*|*High*|*Low*|*Medium*	**[高（High）]**、**[低（Low）]**、または **[中（Medium）]** を選択すると、プリセットの暗号値が自動的に提供されます。
ステップ 6	（任意） Server/tls-config # **set tlsv2CipherMode Custom** *Cipher_Value*	**[カスタム（Custom）]** 暗号モードの有効な暗号値を入力します。 （注） カスタム暗号で提供される特定の暗号用の OpenSSL 同等の暗号名については https://www.openssl.org/docs/man1.0.2/man1/ciphers.html を参照してください。 入力された暗号値が無効またはサポートされていない場合、構成の保存中に、Cisco IMC は自動的に **[TLS v1.2 暗号モード（TLS v1.2 Cipher Mode）]** の値を **[高（High）]** に変更し、構成を保存します。次のステータスが表示される場合があります。 `TLS v1.2 Custom Cipher Status: Error: Configuring an invalid or unsupported TLS v1.2 Cipher List-'Cipher_Name'. Setting TLS v1.2 Cipher Mode to High.`
ステップ 7	Server/tls-config* # **Commit**	変更を保存します。

例

次の例は、TLS v1.2 を有効にし、暗号モードを高に設定する方法を示しています。

```
Server# scope cimc
Server /cimc # scope tls-config
Server /cimc/tls-config # set tlsv2Enabled yes
Server /cimc/tls-config* # commit
Server /cimc/tls-config # set tlsv2CipherMode high
Server /cimc/tls-config* # commit
```

次の例は、TLS v1.2 を有効にし、暗号モードをカスタムに設定する方法を示しています。

```
server# scope cimc
server /cimc # scope tls-config
server /cimc/tls-config # set tlsv2CipherMode Custom
server /cimc/tls-config *# set tlsv2CipherList ECDHE-RSA-AES256-GCM-SHA384
server /cimc/tls-config *# commit
```

TLS 静的キー暗号の有効化

この手順を実行して、Cisco UCS サーバーの TLS 静的キー暗号を有効にします。TLS 静的キー暗号は、デフォルトでは無効です。

（注） この機能は、Cisco IMC CLI インターフェイスを介してのみ有効にできます。

[TLS v1.2 暗号モード（TLS v1.2 Cipher Mode）] が **[高（High）]** または **[カスタム（Custom）]** に設定されている場合、静的キー暗号オプションは適用されません。

静的キー暗号が有効になっている場合、**[TLS v1.2 暗号モード（TLS v1.2 Cipher Mode）]** が **[中（Medium）] / [低（Low）]** から **[高（High）] / [カスタム（Custom）]** に変更されると、自動的に NA に切り替わります。

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 /chassis # **scope tls-config**	TLS 構成モードを開始します。
ステップ 3	Server /chassis/tls-config # **show detail**	**[TLS 静的暗号の有効化（TLS Static Cipher Enabled）]** ステータスを表示します。 `TLS 構成：TLS 静的暗号の有効化：いいえ`
ステップ 4	Server /chassis/tls-config # **set static-cipher-enabled yes**	TLS 暗号を有効にします。
ステップ 5	Server /chassis/tls-config # **commit**	次の警告メッセージが表示されます。 `警告：これにより、TLS で静的暗号が有効になります。KVM、Web サーバー、XMLAPI、および Redfish セッションは切断されます。続行しますか? [[Y]es/[N]o]`

	コマンドまたはアクション	目的
ステップ 6	**[y]** を入力して、**[Enter]** を押します。	トランザクションをシステムの設定にコミットします。

例

次の例は、TLS 静的キー暗号を有効にする方法を示しています。

```
Server# scope cimc
Server /cimc # scope tls-config
Server /cimc/tls-config # show detail
TLS Configuration :
    TLS Static Cipher Enabled: no
Server /cimc/tls-config #
Server /cimc/tls-config # set static-cipher-enabled yes
Server /cimc/tls-config *# commit
Warning: This will enable static ciphers in TLS.
         KVM, Webserver, XMLAPI and Redfish sessions will be disconnected.
Do you wish to continue? [[Y]es/[N]o] y
Server /cimc/tls-config # show detail
TLS Configuration :
    TLS Static Cipher Enabled: yes
```

HTTP の設定

リリース 4.1(2b) 以降、Cisco IMC は個別の HTTPS および HTTP 通信サービスをサポートします。この機能を使用して無効にできるのは HTTP サービスのみです。

この機能は、次のサーバーでのみサポートされています。

- Cisco UCS C220 M5
- Cisco UCS C240 M5
- Cisco UCS C480 M5
- Cisco UCS C480 ML M5
- Cisco UCS C240 SD M5
- Cisco UCS C125 M5
- Cisco UCS S3260 M4/M5

（注） 4.1(2b) より以前のリリースで**[HTTP を HTTPS にリダイレクトすることを有効化する（Redirect HTTP to HTTPS Enabled）]** が無効になっている場合、4.1(2b) 以降のリリースにアップグレードすると、システムによって **[HTTP 有効化（HTTP Enabled）]** の値が **[無効（Disabled）]** に設定されます。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope http**	HTTP コマンド モードを開始します。
ステップ 2	Server /http # **set https-enabled** {**yes** | **no**}	Cisco IMC で HTTPS サービスを有効にするか、または HTTPS と HTTP サービスの両方を無効にします。
ステップ 3	Server /http # **set http-enabled** {**yes** | **no**}	Cisco IMC で HTTP サービスを有効または無効にします。
ステップ 4	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 5	Server /http # **set https-port** *number*	HTTPS 通信に使用するポートを設定します。デフォルトは 443 です。
ステップ 6	Server /http # **set http-redirect** {**yes** | **no**}	（注） このオプションは、HTTP が有効になっている場合にのみ適用されます。 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 7	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 8	Server /http # **commit**	トランザクションをシステムの設定にコミットします。

例

この例では、Cisco IMC の HTTP を構成します。

```
Server# scope http
Server /http # set https-enabled yes
Server /http # set http-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 HTTPS Enabled HTTP Redirected  HT
                                          TP Enabled
---------- ---------- -------- --------------- ------- ---------------- --------
                                             --------
80         443        1800     0               yes     yes              yes
Server /http #
```

SSH の設定

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ssh**	SSH コマンド モードを開始します。
ステップ 2	Server /ssh # **set enabled** {**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 # **set ssh-port** *number*	セキュア シェル アクセスに使用するポートを設定します。デフォルトは 22 です。
ステップ 4	Server /ssh # **set timeout** *seconds*	SSH 要求がタイム アウトしたものとシステムが判断するまで待機する秒数を設定します。 60 ～ 10,800 の範囲の整数を入力します。デフォルトは 300 秒です。
ステップ 5	Server /ssh # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 6	Server /ssh # **show** [**detail**]	（任意）SSH の設定を表示します。

例

次に、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 サーバー用の 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

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope xmlapi**	XML API コマンド モードを開始します。
ステップ 2	Server /xmlapi # **set enabled** {**yes** | **no**}	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。

例

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 #
```

Redfish のイネーブル化

始める前に

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

手順

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

例

この例では、Cisco IMC の redfish 制御をイネーブルにします。

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

Server /redfish #
```

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。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ipmi**	IPMI コマンド モードを開始します。
ステップ 2	Server /ipmi # **set enabled** {**yes** | **no**}	このサーバーで IPMI アクセスをイネーブルまたはディセーブルにします。
ステップ 3	Server /ipmi # **set privilege-level** {**readonly** | **user** | **admin**}	このサーバーで IPMI セッションに割り当て可能な最高特権レベルを指定します。ここに表示される値は次のとおりです。 • **readonly** ：IPMI ユーザ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

	コマンドまたはアクション	目的
		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」ユーザー ロールを持つ IPMI ユーザーは、管理者、ユーザー、および読み取り専用セッションをこのサーバーで作成できます。
ステップ 4	Server /ipmi # **set encryption-key** *key*	IPMI 通信に使用する IPMI 暗号キーを設定します。キーの値は、40 個の 16 進数であることが必要です。
ステップ 5	Server /ipmi # **commit**	トランザクションをシステムの設定にコミットします。
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。

例

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 サポートされている Management Information Base（MIB）ファイルの詳細については、次の URL にある『*MIB Quick Reference for Cisco UCS*』を参照してください。http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/mib/b-series/b_UCS_MIBRef.html

リリース 4.1（3b） 以降、Cisco IMC では SNMP v3 バージョンの拡張認証プロトコルが導入されています。

SNMP プロパティの設定

この手順は、Cisco UCS C シリーズ M6 以前のサーバーに適用されます。Cisco UCS C シリーズ M7 以降のサーバーの SNMP ユーザーを構成するには、Cisco USC C シリーズ M7 および以降のサーバー向けローカル ユーザーの構成 （123 ページ） を参照してください。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope snmp**	SNMP コマンド モードを開始します。
ステップ 2	Server /snmp # **set enabled** {**yes** | **no**}	SNMP をイネーブルまたはディセーブルにします。 （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 # **set enable-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 # **set snmp-port** ポート番号	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 # **set community-str** コミュニティ	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 # **set community-access**	[Disabled]、[Limited]、または [Full] のいずれかになります。
ステップ 8	Server /snmp # **set trap-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 # **set sys-contact** 連絡先	SNMP の実装を担当する、システムの連絡先を指定します。連絡先情報には、電子メール アドレス、名前と電話番号などを最大 254 文字で指定できます。スペースが含まれている値を入力するには、エントリを引用符で囲む必要があります。
ステップ 10	Server /snmp # **set sys-location** 場所	SNMP エージェント（サーバー）が実行されるホストの場所を指定します。ロケーション情報には最大 254 文字を使用できます。スペースが含まれている値を入力するには、エントリを引用符で囲む必要があります。

	コマンドまたはアクション	目的
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。

例

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

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

次のタスク

「SNMP トラップ設定の指定 （383 ページ）」の説明に従って SNMP トラップ設定を設定します。

SNMP トラップ設定の指定

始める前に

- このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。
- トラップの設定を実行する前に、SNMP をイネーブルにして保存する必要があります。

手順

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

	コマンドまたはアクション	目的
ステップ 2	Server /snmp # **scope trap-destinations** *number*	指定した宛先に対して SNMP トラップ宛先コマンドモードを開始します。4つの SNMP トラップ宛先を使用できます。宛先の *number* は、1 ～ 15 の範囲の整数です。
ステップ 3	Server /snmp/trap-destinations # **set enabled** {**yes** | **no**}	SNMP トラップ宛先をイネーブルまたはディセーブルにします。
ステップ 4	Server /snmp/trap-destinations # **set version** { | **2** | **3**}	必要なトラップ メッセージの SNMP バージョンを指定します。 （注） SNMPv3 トラップは SNMPv3 ユーザーおよびキー値が正しく設定されている場所だけに配信されます。
ステップ 5	Server /snmp/trap-destinations # **set type** {**trap** | **inform**}	SNMP 通知メッセージを単純なトラップとして送信するのか、レシーバによる確認応答が必要なインフォーム要求として送信するかを指定します。 （注） 通知オプションは V2 ユーザーに対してのみ選択できます。
ステップ 6	Server /snmp/trap-destinations # **set user** *user*	（注） SNMP v3 バージョンの構成中、暗号化方式が **[DES]** に設定されている SNMP ユーザーを使用することはできません。
ステップ 7	Server /snmp/trap-destination # **set trap-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。

	コマンドまたはアクション	目的
		（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 # **set trap-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。

例

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

```
Server# scope snmp
Server /snmp # Scope trap-destinations 1
Server /snmp/trap-destination *# set enabled yes
Server /snmp/trap-destination *#  set version 2
Server /snmp/trap-destination *# set type inform
Server /snmp/trap-destination *# set user user1
Server /snmp/trap-destination *# set trap-addr 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

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope snmp**	SNMP コマンド モードを開始します。
ステップ 2	Server /snmp # **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。

例

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

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

SNMPv3 ユーザーの設定

始める前に

- このタスクを実行するには、admin 権限を持つユーザ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。

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

	コマンドまたはアクション	目的
		（注） v3 バージョンでは、authnopriv および authpriv セキュリティ レベルのみが使用可能です。
ステップ 6	Server /snmp/v3users # **set v3proto** {**MD5** | **SHA**}	（注） v3 バージョンでは、SHA 認証方式のみを使用できます。 このユーザーの認証プロトコルを選択します。
ステップ 7	Server /snmp/v3users # **set v3auth-key** *auth-key*	このユーザーの許可パスワードを入力します。
ステップ 8	Server /snmp/v3users # **set v3priv-proto** {**DES** |**AES**}	（注） v3 バージョンでは、AES オプションのみを使用できます。 このユーザーの暗号化プロトコルを選択します。
ステップ 9	Server /snmp/v3users # **set v3priv-auth-key** *priv-auth-key*	このユーザーの秘密暗号キー（プライバシー パスワード）を入力します。
ステップ 10	Server /snmp/v3users # **commit**	トランザクションをシステムの設定にコミットします。

例

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

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

```
User 2:
    Add User: yes
    Security Name: ucsSNMPV3user
    Security Level: authpriv
    Auth Type: SHA
    Auth Key: ******
    Encryption: AES
    Private Key: ******

Server /snmp/v3users #
```

SMTP を使用して電子メール アラートを送信するようにサーバーを設定する

Cisco IMC は、SNMP に依存せずに受信者に対する電子メール ベースのサーバー障害の通知をサポートします。システムは Simple Mail Transfer Protocol（SMTP）を使用して、設定された SMTP サーバーに電子メール アラートとしてサーバー障害を送信します。

最大 4 人の受信者がサポートされます。

電子メール アラートを受信するように SMTP サーバを設定

始める前に

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

手順

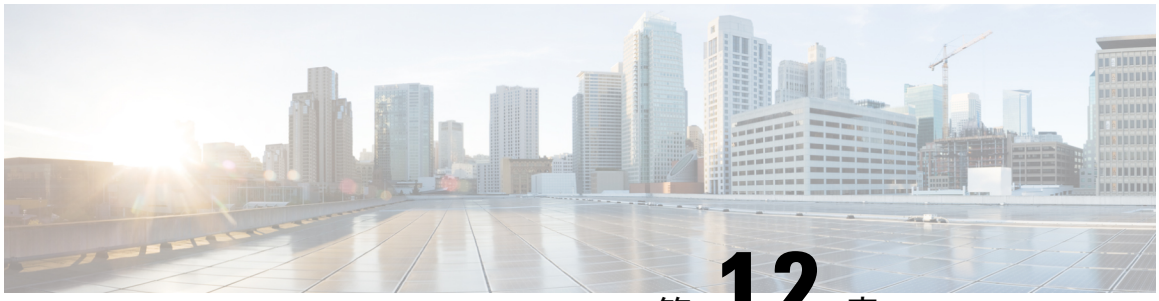
	コマンドまたはアクション	目的
ステップ 1	Server# **scope smtp**	SMTP コマンド モードを開始します。
ステップ 2	Server /smtp # **set enabled** {**yes** | **no**}	SMTP 機能をイネーブルまたはディセーブルにします。
ステップ 3	Server /smtp * # **set server-addr** *IP_Address*	SMTP サーバの IP アドレスを割り当てます。
ステップ 4	Server /smtp * # **set port** *port_number*	SMTP サーバに使用するポート番号を指定します。
ステップ 5	Server /smtp # **set-mail-addr** *email_address recipient_minimum_severity informational | warning | minor | major | critical*	受信者の E メール アドレスを最小のシビラティ（重大度）レベルで設定します。
ステップ 6	Server /smtp * # **commit**	トランザクションをシステムの設定にコミットします。

	コマンドまたはアクション	目的
ステップ 7	Server /smtp # **send-test-mail recipient1**	選択した受信者に割り当てられたメール アドレスにテスト メール アラートを送信します。

例

この例では、メール アラートを受信するための SMTP を設定する方法を示します。

```
Server # scope smtp
Server /smtp # set enabled yes
Server /smtp *# set server-addr 10.10.10.10
Server /smtp *# set port 25
Server /smtp *# set-mail-addr recipient4 user@cisco.com critical
This operation will add the recipient4
Continue?[y|N]y
Server /smtp *#
Server /smtp *# commit
Server /smtp #
```



第 12 章

証明書とサーバー セキュリティの管理

この章は、次の内容で構成されています。

サーバー証明書の管理

サーバー証明書の管理

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ー証明書と交換することができます。サーバー証明書は、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。ホスト名の変更および事自己署名証明書の自動生成の詳細は、「**共通プロパティの設定**」セクション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。

始める前に

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope certificate**	証明書コマンド モードを開始します。
ステップ 2	Server /certificate # **generate-csr**	証明書署名要求（CSR）の生成に関するダイアログを起動します。

証明書署名要求に関して、次の情報の入力を求めるプロンプトが表示されます。

名前	説明
[コモンネーム（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しても、CNはそのままの状態で保持されます。
[組織名（Organization Name）]フィールド	証明書を要求している組織。
[組織単位（Organization Unit）] フィールド	組織ユニット
[地域（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。

名前	説明
[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。
[電子メール（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。

例

次に、証明書署名要求を生成する例を示します。

```
Server# scope certificate
Server /certificate # generate-csr
Common Name (CN): test.example.com
Organization Name (O): Example, Inc.
Organization Unit (OU): Test Department
Locality (L): San Jose
StateName (S): CA
Country Code (CC): US
Email: user@example.com
Continue to generate CSR?[y|N]y


-----BEGIN CERTIFICATE REQUEST-----
MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
ZgAMivyCsKgb/6CjQtsofvzxmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
-----END CERTIFICATE REQUEST-----

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

次のタスク

次のいずれかの作業を実行します。

- 公共の認証局から証明書を取得せず、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ーを運用している場合は、「-----BEGIN ...」から「END CERTIFICATE REQUEST-----」までのコマンド出力をコピーして、csr.txt というファイルに貼り付けます。CSR ファイルを証明書サーバーに入力して、自己署名証明書を生成します。
- 公共の認証局から証明書を取得する場合は、「-----BEGIN ...」から「END CERTIFICATE REQUEST-----」までのコマンド出力をコピーして、csr.txt というファイルに貼り付けます。CSR ファイルを認証局に提出して、署名付き証明書を取得します。
- 証明書のタイプが [サーバ（Server）] で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。

信頼されていない CA 署名付き証明書の作成

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 証明書サーバーを使用して CA を作成するコマンドおよびサーバー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 サーバーで入力します。

始める前に

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

	コマンドまたはアクション	目的
ステップ 1	**openssl genrsa -out** *CA_keyfilename keysize* 例： `# openssl genrsa -out ca.key 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。
ステップ 2	**openssl req -new -x509 -days** *numdays* **-key** *CA_keyfilename* **-out** *CA_certfilename* 例： `# openssl req -new -x509 -days 365 -key ca.key -out ca.crt`	このコマンドは、指定されたキーを使用して、CA の自己署名証明書を新規に作成します。証明書は指定された期間有効になります。このコマンドは、ユーザに証明書の追加情報を求めるプロンプトを表示します。 証明書サーバーは、アクティブな CA です。
ステップ 3	**echo "nsCertType = server" > openssl.conf** 例： `# echo "nsCertType = server" > openssl.conf`	このコマンドは、証明書がサーバー限定の証明書であることを指定する行を OpenSSL 設定ファイルに追加します。この指定により、認証されたクライアントがサーバになりすます man-in-the-middle 攻撃を防御できます。 OpenSSL 設定ファイル openssl.conf には、"nsCertType = server" という文が含まれています。
ステップ 4	**openssl x509 -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ー証明書を生成するように指示します。 サーバー証明書は、出力ファイルに含まれています。

	コマンドまたはアクション	目的
ステップ 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 [サーバー（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] サーバーの値が [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。
ステップ 6	（任意） 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、ステップ 1 ～ 5 を繰り返して証明書を再生成します。	正しい有効期限が設定された証明書が作成されます。

例

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

```
# /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 #
```

次のタスク

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

始める前に

- 証明書をアップロードするには、admin 権限を持つユーザーとしてログインする必要があります。
- アップロードする証明書は、読み取り可能テキストとして使用できる必要があります。アップロード手順で、証明書テキストをコピーして CLI に貼り付けます。
- 生成された証明書のタイプが [サーバ（Server）] であることを確認します。
- 次の証明書形式がサポートされています。
  - .crt
  - .cer
  - .pem

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

手順

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

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

例

次に、新しい証明書をサーバーにアップロードする例を示します。

```
Server# scope certificate
Server /certificate # upload
Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
ZgAMivyCsKgb/6CjQtsofvzxmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
-----END CERTIFICATE-----
<CTRL+D>
```

外部証明書の管理

外部証明書のアップロード

始める前に

- 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ファイルは、ローカルにアクセスできるファイル システムに配置されている必要があります。
- 次の証明書形式がサポートされています。
  - .crt
  - .cer
  - .pem

手順

ステップ 1 Server# **scope certificate**

Cisco IMC 証明書コマンドモードを開始します。

ステップ 2 Server /certificate # **upload-remote-external-certificate** *remote-protocol server_address path certificate_filename*

リモート サーバー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） FTP、SCP または SFTP としてプロトコルを選択した場合は、ユーザー名とパスワードの入力が求められます。

外部 証明書をアップロードする場所からファイルパス、およびリモート プロトコルを入力します。リモート サーバーのユーザー名とパスワードを検証した後、リモート サーバーから外部証明書をアップロードします。

ステップ 3 （オプション）Server /certificate #**upload-paste-external-certificate**

これは、外部証明書をアップロードするための追加オプションです。

プロンプトされたら、証明書の内容を貼り付け、`Ctrl+D` を押します。

例

- この例では、リモート サーバーから外部証明書をアップロードします。

```
Server # scope certificate
Server /certificate # upload-remote-external-certificate scp 10.10.10.10
/home/user-xyz/ext-certif.cert
Server (RSA) key fingerprint is dd:b5:2b:07:ad:c0:30:b2:d5:6a:6a:78:80:85:93:b0
Do you wish to continue? [y/N]y
Username: user-xyz
Password:
External Certificate uploaded successfully
Server /certificate #
```

- この例では、貼り付けオプションを使用して外部証明書をアップロードします。

```
Server # scope certificate
Server /certificate # upload-paste-external-certificate
Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIID8zCCAtugAwIBAgIBBDANBgkqhkiG9w0BAQwFADCBsDELMAkGA1UEBhMCSU4x
EjAQBgNVBAgMCUthcm5hdGFrYTESMBAGA1UEBwwJQmFuZ2Fsb3JlMSQwIgYDVQQK
DBtDaXNjbyBTeXN0ZW1zIEluZGlhIFB2dCBMdGQxGDAWBgNVBAsMD1VDUy1SYWNr
LVNlcnZlcjEWMBQGA1UEAwwNQ2lzY28gU3lzdGVtczEhMB8GCSqGSIb3DQEJARYS
c3JpdmF0c3NAY2lzY28uY29tMB4XDTIwMDExMzA4MTM1NVoXDTIxMDExMjA4MTM1
NVowgbExCzAJBgNVBAYTAklOMRIwEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcT
CUJlbmdhbHVydTEkMCIGA1UEChMbQ2lzY28gU3lzdGVtcyBJbmRpYSBQdnQgTHRk
MRgwFgYDVQQLEw9VQ1MtUmFjay1TZXJ2ZXIxFjAUBgNVBAMTDUNpc2NvIFN5YXRl
bXMxIjAgBgkqhkiG9w0BCQEWE3NyaXZhdHNzQGNpc2NvLmNvbm0wggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQC6fcG9QISg6t1fi6U3+czmek2LvfhAxSGd
r2g7uMssgdTrBh59TEgZl5azal5zWaZm/1iO69D6/iabyoli8+MiQAtANnKxqWM3
STeih+3U2jOf39lIlZrAMpd4Ag/OtK5OcUtwUHM52ixm/UU61geVPZ5mJpPkzq3T
JNcv6TR90K8v0nEILm1lgoA96y64I9YN3ufSE4gm9VOS/sFughmAyYErsgvgoJpn
SQZUYxwdueBm4XV48QY7Mc7neUVYCNo7TcfBX7DC/N0BHv3hlKhGCCQ+5if63uOh
ja8ahdBoIPJqI0h70a92yBK5lv4dxSHexccw2D40kar4CzfVSqx9AgMBAAGjFTAT
MBEGCWCGSAGG+EIBAQQEAwIGQDANBgkqhkiG9w0BAQwFAAOCAQEAXdVTJevqNyI9
```

```
DEVibfjGXiKnJ2gEuYr8MdhpDeff/WrsLk7lxhOomVrDZ3iyCX99tNoCIvtOMgNs
jOu9OEjNtBulOlgwdQ9ugwp/JToohbD+2JHRK/MgrFpZmewH1oKKDNpOdayR6u9m
SNfvMNBgvxg+cMcbkif0pJU3XHlniPF6UVgj/LJDyBSGrULpnyDwTOq2UEF6g9Dc
6gOgRGYNHn7MRzigPJtyjbJsbxgPQ9C46I3Me9N2sJNaSLSVQhOxW7KonPI6USRs
e2iEAYaaCvThGE4HTwOMF9dJ24inU+SKTci1AFq2+V4I3P9v+aH5ao1H9T/p/AUP
ho6MuZ+wWg==
-----END CERTIFICATE-----
External Certificate pasted successfully.
Server /certificate #
```

次のタスク

外部秘密キーをアップロードしてから、外部証明書をアクティブにする必要があります。

外部秘密キーのアップロード

始める前に

- 外部秘密キー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。

（注）
- Cisco IMC は、Cisco UCS C シリーズ M4 サーバで、2048ビットおよび4096ビットの外部秘密キー サイズをサポートしています。
- Cisco IMC は、Cisco UCS C シリーズ M5 サーバで 2048ビット、4096ビット、および8192ビットの外部秘密キー サイズをサポートしています。

手順

ステップ 1 Server# **scope certificate**

Cisco IMC 証明書コマンドモードを開始します。

ステップ 2 Server /certificate # **upload-remote-external-private-key** *remote-protocol server_address path key_filename*

リモート サーバーに接続するためのプロトコルを指定します。次のいずれかを指定できます。

- SFTP
- SCP

秘密キーをアップロードする場所からファイルパス、およびリモート プロトコルを入力します。リモート サーバーのユーザー名とパスワードを検証した後、リモート サーバーから秘密キーをアップロードします。

ステップ 3 （オプション）Server /certificate #**upload-paste-external-private-key**

これは、秘密キーをアップロードするための追加オプションです。

プロンプトで、秘密キーの内容を貼り付け、Ctrl+D を押します。

（注） アップロード用にサポートされるファイルの最大サイズは次のとおりです。

- Cisco UCS C シリーズ M5 サーバで最大 8 KB
- Cisco UCS C シリーズ M4 サーバで最大 4 KB

例

- この例では、リモート サーバーから外部秘密キーをアップロードします。

```
Server # scope certificate
Server /certificate # upload-remote-external-private-key scp 10.10.10.10
/home/user-xyz/ext-pvt-key.pem
Server (RSA) key fingerprint is dd:b5:2b:07:ad:c0:30:b2:d5:6a:6a:78:80:85:93:b0
Do you wish to continue? [y/N]y
Username: user-xyz
Password:
External Private Key uploaded successfully
Server /certificate #
```

- この例では、貼り付けオプションを使用して外部秘密キーをアップロードします。

```
Server # scope certificate
Server /certificate # upload-paste-external-private-key
Please paste your private key here, when finished, press CTRL+D.
-----BEGIN RSA PRIVATE KEY-----
MIIEoQIBAAKCAQEAun3BvUCEoOrdX4ulN/nM5npNi734QMUhna9oO7jLLIHU6wYe
fUxIGZeWs2pec1mmZv9YjuvQ+v4mm8qJYvPjIkALQDZysaljN0k3ooft1Nozn9/Z
SJWawDKXeAIPzrSuTnFLcFBzOdosZv1FOtYHlT2eZiaT5M6t0yTXL+k0fdCvL9Jx
CC5tZYKAPesuuCPWDd7n0hOIJvVTkv7BboIZgMmBK7IL4KCaZ0kGVGMcHbngZuF1
ePEGOzHO53lFWAjaO03HwV+wwvzdAR794ZSoRggkPuYn+t7joY2vGoXQaCDyaiNI
e9GvdsgSuZb+HcUh3sXHMNg+NJGq+As31UqsfQIDAQABAoH/MSv3aW8ZiVRkCk1H
wvqajCqzR6VPT8SqmGknkpem+pVBDrcOUvtKB3Vwxt3FCaUZuw6YyxZig8t/YpSE
pRKpUN6SGNxCYZXIE0u635/3lafy9LSRFhJcO1EbnwjsIhSB4Sz+Nx7/QsHD82PU
XS8R0MfufACv/iSAsKuGEZvru0BWexD1ycojGTDRhGqWZGzsN6ncsbhQ0kItC0Pv
Ycx+9NeKfGwO+P9NwyWwaKW9M4nOyx3/MviMx9QRbNjgxjrdTj+A0aBUEzgdeZOf
WCJ/LlSbHmJ46HYZOILL4KDBbow/c7a1c2JcFWn01m33qNCRWdkb5H+1UZA+el7g
XnxDAoGBALzBdW26GGIZjj42Ayr9PAXFsO8n0MonqVHRlRTvxeuLOvHYdD9HzgkH
CFXA0IGmNk/1RuwEArx6U6ezSP6z7za9B63MskE7t3Vs28/OJg14KptRftGKUIbZ
NRf1o3J7VUf9mYk9u3pc/PJ8oVweFoml/SwRTDvZyUn5WRLq7zJ3AoGBAPztx24M
qj0Gcbqa7U5pUM+9bD9eGPxrGranFlDp79eobG+9kva286clp0Yr5XrNsQpx42Q6
RJLBVEwrB03D7X9UIOaAgyiaDbDMbIeAcRqOC9qpLDUXrpMVrdvVhtcPrKS8VAp4
hOle6zYKMShMXDExhH3EHaQ7aVOQRpt5GoGrAoGBAKBX1uE3TK9I9kRyrY4/QFXG
8d62++4+ct9GIlZ+uKq2w4PeVCHNZYDVsIboHDeGcmzJ901WutxRLe8vpbp4L6VY
PsWtNV+k0tu1daS5gim/ArKeMBTgYjerHCcWS5pcmr1k+KBVCIWRqG504L3X8V1M
3BwrNY9CGnP0lW40lK1RAoGASikuIIZ2JA6Pqjdi/WrD1yWjZ7EfgmOlIYk8cd0m
BgXMRbdAMDbUml3f/iNA1hEZqAZctjafhKhLH0o+if641GzGeM+VpYIGIaDO8awn
fbHIqASSgb6/4UCqCZtCPizKYkMWITvVPNgn/2BdqYM6RPJP9tBaIJ2K9IWJLm0D
6KECgYB9rmj/8YW7Rz1Isfg7JhK32p7LC+5xSSbpxQc8s/3PftZ5uQnsXXHoZJ0H
cfA4mbj4nttyFwX+kuUpQdG/ZhoJ/SDqE5lvzVM4stMRKFEJq8ksld+KGGzLFEkj
OotvpQor5dHHU46IIu9tv5ctrJImMjSM7wro26kW2EE3UzZMYw==
-----END RSA PRIVATE KEY-----
External Private Key pasted successfully.
Server /certificate #
```

次のタスク

外部証明書をアクティベートする必要があります。

外部証明書の有効化

- 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。
- 証明書と秘密キーがアップロードされた後にのみ、外部証明書をアクティブ化できます。
- 外部証明書をアクティブにすると、既存の証明書が置き換えられ、すべてのアクティブな HTTPS セッションと SSH セッションが切断されます。

手順

ステップ 1 Server# **scope certificate**

Cisco IMC 証明書コマンドモードを開始します。

ステップ 2 Server /certificate # **activate-external-certificate**

アップロードされた外部証明書をアクティブにします。

例

この例ではアップロードされた証明書をアクティブにします。

```
Server # scope certificate
Server /certificate # activate-external-certificate
This operation will overwrite the current certificate with the uploaded external
certificate.
All HTTPS and SSH sessions will be disconnected.
Continue?[y|N]y
A system reboot has been initiated.
Server /certificate #
```

SPDM セキュリティ：MCTP SPDM

SPDM セキュリティ

Cisco M6 サーバーには、デバイス自体に対する攻撃のベクトルを提供したり、デバイスを使用してシステム内の別のデバイスを攻撃したりする可能性のある可変コンポーネントが含まれている場合があります。これらの攻撃から防御するために、SPDM（セキュリティ プロトコルおよびデータ モデル）の仕様は、さまざまなトランスポートおよび物理メディアを介してデバイス間でメッセージ交換を実行するためのメッセージ、データ オブジェクト、およびシーケンス

を定義します。これは、管理コンポーネントトランスポートプロトコル（MCTP）を介した管理コントローラとエンドポイント デバイス間のメッセージ交換を調整します。

メッセージ交換には、コントローラにアクセスするハードウェア ID の認証が含まれます。SPDMは、デバイス認証および証明書管理の管理レベルを指定することにより、低レベルのセキュリティ機能と操作へのアクセスを可能にします。この機能は、Cisco IMC リリース 4.2（1a）で Cisco UCS C220 および 240 M6 サーバーでサポートされています。

エンドポイント証明書と認証局（ルート CA）証明書は、サーバーのすべてのユーザー インターフェイスにリスト表示されます。1 つ以上の外部デバイス証明書のコンテンツを Cisco IMC にアップロードすることもできます。SPDM ポリシーを使用すると、必要に応じて外部ルート CA 証明書または設定を変更または削除できます。不要になったルート CA 証明書を削除または置き換えることもできます。

SPDM セキュリティ ポリシーでは、次にリストするように、3 つのセキュリティ レベル設定のいずれかを指定できます。

- フル セキュリティ：

  これは、最高の MCTP セキュリティ設定です。この設定を選択した場合、エンドポイントの認証が失敗すると、障害が生成されます。また、エンドポイントのいずれかでエンドポイント認証がサポートされていない場合も、障害が発生します。

- 部分的なセキュリティ：

  この設定を選択した場合、エンドポイントの認証が失敗すると、障害が生成されます。エンドポイントのいずれかでエンドポイント認証がサポートされていない場合には、障害が生成されません。これはデフォルト設定として選択されています。

- No Security

  この設定を選択した場合（エンドポイント測定が失敗しても）障害は発生しません。

MCTP SPDM 障害アラート設定の構成と表示

MCTP SPDM 障害アラート設定を構成できます。

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 mctp**	MCTP SPDM セキュリティ コマンドモードを開始します。
ステップ 3	Server /chassis/mctp# **set fault-alert-setting** *Partial* | *Full* | *Disabled*	選択した値で MCTP SPDM **[fault-alert-setting]** を設定します。 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
		• **[Full]**：このオプションを選択した場合、エンドポイントの認証が失敗すると、障害が生成されます。 このオプションを選択した場合、エンドポイントがエンドポイント認証をサポートしていないときに障害が生成されます。 • **[一部（Partial）]**：デフォルトのオプション。このオプションを選択した場合、エンドポイントの認証が失敗すると、障害が生成されます。 このオプションを選択した場合、エンドポイントがエンドポイント認証をサポートしていなくても障害は生成されません。 • **[無効（Disabled）]**：このオプションを選択した場合、エンドポイント認証の失敗に対して障害は生成されません。
ステップ 4	Server /chassis/mctp# **show detail**	構成済みの MCTP SPDM 障害アラート設定を表示します。
ステップ 5	（オプション）Server /chassis/mctp# **exit**	シャーシ コマンド モードに戻ります。
ステップ 6	（オプション）Server /chassis# **exit**	サーバー コマンド モードに戻ります。
ステップ 7	（オプション）Server# **scope fault**	障害コマンド モードを開始します。
ステップ 8	（オプション）Server /chassis/fault# **show fault-entries**	すべての障害のログを表示します。 （注） デバイスの構成証明が失敗すると、障害が生成されます。手順 5 ～ 8 を実行して、関連する障害を表示します。

例

この例では、**[fault-alert-setting]** を **[full]** に構成します。

```
Server# scope chassis
Server /chassis # scope mctp
```

```
Server /chassis/mctp # set fault-alert-setting full
Server /chassis/mctp # show detail
Fault Alert Setting: Full
```

SPDM ルート CA 証明書のアップロード

ルート CA 証明書をサーバーにリモートでアップロードすることにより、SPDM ルート CA 証明書をアップロードできます。必要に応じて、証明書の詳細を貼り付けてアップロードすることもできます（.pem フォーマットのみ）。

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 mctp**	MCTP SPDM セキュリティ コマンドモードを開始します。
ステップ 3	Server /chassis/mctp# **upload-remote-external-certificate** *protocol server_address path/certificate_filename*	リモート サーバー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） FTP、SCP または SFTP としてプロトコルを選択した場合は、ユーザー名とパスワードの入力が求められます。 SPDM ルート CA 証明書をアップロードする場所からファイルパス、およびリモートプロトコルを入力します。リモート サーバーのユーザー名とパスワードを検証した後、リモート サーバーから SPDM ルート CA 証明書をアップロードします。
ステップ 4	（オプション）Server /chassis/mctp# **show status**	証明書のアップロードステータスが表示されます。

	コマンドまたはアクション	目的
ステップ 5	（オプション）Server /chassis/mctp# **upload-paste-external-certificate**	これは、SPDM ルート CA 証明書をアップロードするための追加オプションです（.pem フォーマットのみ）。 プロンプトされたら、証明書の内容を貼り付け、Ctrl+D を押します。

例

- この例では、リモート サーバーから SPDM ルート CA 証明書をアップロードします。

```
Server# scope chassis
Server /chassis # scope mctp
Server /chassis/mctp# upload-remote-external-certificate scp 10.10.10.10
/home/user-xyz/ext-certif.cert
Server (RSA) key fingerprint is dd:b5:2b:07:ad:c0:30:b2:d5:6a:6a:78:80:85:93:b0
Do you wish to continue? [y/N]y
Username: user-xyz
Password:
External Certificate uploaded successfully
Server /chassis/mctp #
```

- この例では、貼り付けオプション（.pem フォーマットのみ）を使用して SPDM ルート証明書をアップロードします。

```
Server# scope chassis
Server /chassis # scope mctp
Server /chassis/mctp# upload-paste-external-certificate
Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIIDfDCCAmSgAwIBAgIQGKy1av1pthU6Y2yv2vrEoTANBgkqhkiG9w0BAQUFADBY
MQswCQYDVQQGEwJVUzEWMBQGA1UEChMNR2VvVHJ1c3QgSW5jLjExMC8GA1UEAxMo
R2VvVHJ1c3QgUHJpbWFyeSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAeFw0wNjEx
MjcwMDAwMDBaFw0zNjA3MTYyMzU5NTlaMFgxCzAJBgNVBAYTAlVTMRYwFAYDVQQK
Ew1HZW9UcnVzdCBJbmMuMTEwLwYDVQQDEyhHZW9UcnVzdCBQcmltYXJ5IENlcnRp
ZmljYXRpb24gQXV0aG9yaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
mO9Y+pyEtzavwt+s0vQQBnBxNQIDAQABo0IwQDAPBgNVHRMBAf8EBTADAQH/MA4G
A1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQULNVQQZcVi/CPNmFbSvtr2ZnJM5IwDQYJ
6CePbJC/kRYkRj5KTs4rFtULUh38H2eiAkUxT87z+gOneZ1TatnaYzr4gNfTmeGl
4b7UVXGYNTq+k+qurUKykG/g/CFNNWMziUnWm07Kx+dOCQD32sfvmWKZd7aVIl6K
oKv0uHiYyjgZmclynnjNS6yvGaBzEi38wkG6gZHaFloxt/m0cYASSJlyc1pZU8Fj
UjPtp8nSOQJw+uCxQmYpqptR7TBUIhRf2asdweSU8Pj1K/fqynhG1riR/aYNKxoU
AT6A8EKglQdebc3MS6RFjasS6LPeWuWgfOgPIh1a6Vk=
-----END CERTIFICATE-----
External Certificate pasted successfully.
Server /chassis/mctp#
```

- この例は、証明書のアップロードの進行状況とステータスを示しています。

```
Server# /chassis/mctp # show status
MCTP External Certificate Upload Status: NONE
MCTP External Certificate Upload Progress: 0
```

SPDM 認証ステータスおよび SPDM 証明書チェーンの表示

特定のスロットの SPDM 認証ステータスと SPDM 証明書チェーンを表示できます。

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 mctp**	MCTP SPDM セキュリティ コマンドモードを開始します。
ステップ 3	Server /chassis/mctp# **spdm-status**	SPDM ステータスを表示します。
ステップ 4	Server /chassis/mctp# **spdm-cert-chain** *Slot-ID*	特定のスロットの SPDM 証明書チェーンを表示します。

例

この例では、進行中および正常終了時の SPDM ステータスを表示します。

```
Server# scope chassis
Server /chassis # scope mctp
Server /chassis/mctp # spdm-status
Overall SPDM Status : in progress
Server /chassis/mctp # spdm-cert-chain MRAID
Certificate Chain Information
Error :  Failed to get cert chain due to on-going handshake ( Please try after some time)
Server /chassis/mctp # spdm-status
Overall SPDM Status : success
Slot ID         Status                    Name
------------------------------------------------------------------
MRAID           success                   N/A
Server /chassis/mctp # spdm-cert-chain MRAID
Certificate Chain Information
Slot ID                         :  MRAID
---------------------------------------
Depth                           :  0
Subject Country Code (C)        :  US
Subject State (ST)              :  Colorado
Subject City (L)                :  Colorado Springs
Subject Organization (O)        :  Broadcom Inc.
Subject Organization Unit(OU)   :  NA
Subject Common Name (CN)        :  Aero Device
Issuer Country Code (C)         :  US
Issuer State (ST)               :  Colorado
Issuer City (L)                 :  NA
Issuer Organization (O)         :  Broadcom Inc.
Issuer Organization Unit(OU)    :  DCSG
Issuer Common Name (CN)         :  Aero Model
Valid From                      :  Oct 23 01:01:28 2019 GMT
Valid To                        :  Mar 10 01:01:28 2047 GMT
---------------------------------------------------------
Depth                           :  1
```

```
Subject Country Code (C)      :  US
Subject State (ST)            :  Colorado
Subject City (L)              :  Colorado Springs
Subject Organization (O)      :  Broadcom Inc.
Subject Organization Unit(OU) :  NA
Subject Common Name (CN)      :  Aero Model
Issuer Country Code (C)       :  US
Issuer State (ST)             :  Colorado
Issuer City (L)               :  Colorado Springs
Issuer Organization (O)       :  Broadcom Inc.
Issuer Organization Unit(OU)  :  NA
Issuer Common Name (CN)       :  NA
Valid From                    :  Oct 23 00:36:24 2019 GMT
Valid To                      :  Aug  3 00:36:24 2126 GMT
-------------------------------------------------------
```

証明書および証明書の詳細のリストを表示する

アップロードされた SPDM ルート CA 証明書のリストを表示できます。

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 mctp**	MCTP SPDM セキュリティ コマンドモードを開始します。
ステップ 3	Server /chassis/mctp# **cert-list**	すべての証明書をリストします。
ステップ 4	Server /chassis/mctp# **cert-details** *Certificate-ID*	証明書 ID **[1]** の SPDM ルート CA 証明書の詳細をリストします。

次の例は、2 つの Broadcom 証明書の証明書 ID、共通名、発行者の組織、および有効性を示しています。

例

次の例では、すべての SDPM ルート CA 証明書をリストしています。

```
Server# scope chassis
Server /chassis # scope mctp
Server /chassis/mctp# cert-list

Certificate ID          Common Name              Issuer Organization (O)          Valid
 To
---------------  ------------------------------ ------------------------------
------------------------
1101                    Broadcom                        Broadcom              Apr 8
10:36:14 2021 GMT
```

```
1109                    Broadcom1                       Broadcom                Apr 8
10:36:15 2021 GMT
```

以下の例は、証明書 ID **[1]** の SPDM ルート CA 証明書のすべての詳細をリストしています。

```
Server# scope chassis
Server /chassis # scope mctp
Server /chassis/mctp# cert-details 1


Certificate Information
Subject Country Code (C)      :  US
Subject State (ST)            :  Colorado
Subject City (L)              :  Colorado Springs
Subject Organization (O)      :  Broadcom Inc.
Subject Organization Unit(OU) :  NA
Subject Common Name (CN)      :  NA
Issuer Country Code (C)       :  US
Issuer State (ST)             :  Colorado
Issuer City (L)               :  Colorado Springs
Issuer Organization (O)       :  Broadcom Inc.
Issuer Organization Unit(OU)  :  NA
Issuer Common Name (CN)       :  NA
Valid From                    :  Oct 23 00:25:13 2019 GMT
Valid To                      :  Apr 29 00:25:13 2129 GMT
```

証明書の削除

アップロードした任意の証明書を削除できます。

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 mctp**	MCTP SPDM セキュリティ コマンドモードを開始します。
ステップ 3	Server /chassis/mctp# **delete-certificate** *Certificate-id*	アップロードされた SPDM ルート CA 証明書を証明書 ID **[1]** で正常に削除します。 証明書 ID が内部証明書に対応している場合、次のメッセージが表示されます。 `証明書 ID は内部証明書に対応します。内部証明書を削除することはできません。`

例

この例では、選択したアップロードされた証明書のいずれかを削除します。

```
Server# scope chassis
Server /chassis # scope mctp
Server /chassis/mctp # delete-certificate
Please provide Certificate ID to delete certificate
Server /chassis/mctp # delete-certificate 1
Successfully deleted the user uploaded MCTP Certificate
Server /chassis/mctp # delete-certificate 11
The Certificate ID corresponds to Internal certificate. Can’t delete Internal certificates.
```

キー管理相互運用性プロトコル

キー管理相互運用性プロトコル（KMIP）は、主要な管理サーバーでキーまたは機密データを処理するためのメッセージ形式を定義する通信プロトコルです。KMIP はオープン スタンダードで、複数のベンダーによってサポートされています。キー管理には、複数の相互運用可能な実装が伴うため、KMIP クライアントは KMIP サーバーと効率的に連動します。

自己暗号化ドライブ（SED）には、リアルタイムで着信データを暗号化し、発信データを復号するハードウェアが含まれています。ドライブまたはメディア暗号化キーは、この機能を制御します。しかし、セキュリティを維持するために、ドライブはロックされている必要があります。セキュリティ キー ID とセキュリティ キー（キー暗号キー）を使用すると、この目的を達成できます。キー ID では、ドライブに一意の ID が提供されます。

異なるキーには異なる使用要件があります。現在、ローカル キーの管理および追跡の責任は主にユーザーにあるため、人的ミスが生じる可能性があります。ユーザーはさまざまなキーとそれらの機能を覚えている必要があり、それが困難な場合があります。KMIP は、この懸念領域に対処し、人的関与なしでキーを効率的に管理します。

KMIP の有効化または無効化

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope kmip**	KMIP コマンド モードを開始します。
ステップ 2	Server/kmip# **set enabled** {**yes** | **no**}	KMIP 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/kmip*# **commit**	トランザクションをシステムの設定にコミットします。
ステップ 4	（任意） Server/kmip # **show detail**	KMIP ステータスを表示します。

例

次に KMIP を有効にする例を示します。

```
Server # scope kmip
Server /kmip # set enabled yes
Server /kmip *# commit
Server /kmip # show detail
  Enabled: yes
Server /kmip #
```

KMIP 設定のクライアント秘密キーおよびクライアント証明書の作成

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 証明書サーバーを使用して CA を作成するコマンドおよびサーバー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 サーバーで入力します。

始める前に

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

	コマンドまたはアクション	目的
ステップ 1	**openssl genrsa -out** *Client_Privatekeyfilename keysize* 例： `# openssl genrsa -out client_private.pem 2048`	このコマンドは、クライアント証明書の生成に使用されるクライアント秘密キーを生成します。 指定されたファイル名には、指定されたサイズの RSA キーが含まれています。
ステップ 2	**openssl req -new -x509 -days** *numdays* **-key** *Client_Privatekeyfilename* **-out** *Client_certfilename* 例： `# openssl req -new -x509 -key client_private.pem -out client.pem -days 365`	このコマンドは、前の手順で入手したクライアント秘密キーを使用して、新しい自己署名クライアント証明書を生成します。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、ユーザーに証明

	コマンドまたはアクション	目的
		書の追加情報を求めるプロンプトを表示します。 新しい自己署名クライアント証明書が作成されます。
ステップ 3	KMIP サーバーから KMIP ルート CA 証明書を取得します。	ルート CA 証明書の取得については、KMIP のベンダーマニュアルを参照してください。

次のタスク

新しい証明書を Cisco IMC にアップロードします。

KMIP クライアント証明書のダウンロード

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope kmip**	KMIP コマンド モードを開始します。
ステップ 2	Server/kmip # **set enabled yes**	KMIP を有効にします。
ステップ 3	Server/kmip*# **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/kmip # **scope kmip-client-certificate**	KMIP クライアント証明書コマンドモードを開始します。
ステップ 5	Server /kmip/kmip-client-certificate # **download-client-certificate** *remote-protocol IP アドレス KMIP クライアント証明書ファイル*	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

	コマンドまたはアクション	目的
		（注） Cisco UCS C シリーズ サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバー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 サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[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 6	確認プロンプトで、**y** と入力します。	これにより KMIP クライアント証明書のダウンロードが開始されます。
ステップ 7	（任意） Server /kmip/kmip-client-certificate # **paste-client-certificate**	プロンプトで、署名付き証明書の内容を貼り付け、**Ctrl+D** を押します。 （注） 前の手順のリモート サーバ メソッドを使用するか、貼り付けオプションを使用して、クライアント証明書をダウンロードできます。

例

この例は、KMIP クライアント証明書をダウンロードします。

```
Server # scope kmip
Server /kmip # set enabled yes
Server /kmip *# commit
Server /kmip # scope kmip-client-certificate
Server /kmip/kmip-client-certificate # show detail
    KMIP client certificate Available: 1
    Download client certificate Status: COMPLETED
    Export client certificate Status: NONE
Server /kmip/kmip-client-certificate #  download-client-certificate tftp 10.10.10.10
KmipCertificates/
svbu-xx-blr-dn1-13_ClientCert.pem
  You are going to overwrite the KMIP client certificate.
  Are you sure you want to proceed and overwrite the KMIP client certificate? [y|N]y
KMIP client certificate downloaded successfully

You can  either use the remote server method from the previous steps or use the paste
option to download the client certificate.

Server /kmip/kmip-client-certificate # paste-client-certificate
Please paste your certificate here, when finished, press CTRL+D.
----BEGIN CERTIFICATE-----
MIIDTzCCAjegAwIBAgIQXuWPdBbyTb5M7/FT8aAjZTANBgkqhkiG9w0BAQUFADA6
MRMwEQYKCZImiZPyLGQBGRYDY29tMRMwEQYKCZImiZPyLGQBGRYDbmV3MQ4wDAYD
VQQDEwVuZXdDQTAeFw0xNTAzMTIxMTM5MTZaFw0yMDAzMTIxMTQ5MTVaMDoxEzAR
BgoJkiaJk/IsZAEZFgNjb20xEzARBgoJkiaJk/IsZAEZFgNuZXcxDjAMBgNVBAMT
BW5ld0NBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuPSAwHtk0IbM
Cd5tYdCa498bfX5Nfdgnq5zE+cGIOqv0dAkucofC/Y0+m7hne9H12aQ9SqTOK1+L
5IT3PVCczhasI7L7jAa+Oe5AOYw7Nsugw5Bd23n42BTVMMp7xsgr1mVfFoHXbBkQ
wiT9DieyImSyGiq5n0/8Iooc0iN5WPMVcHO2ysz76jR8p07xRqgYNC16cbKAhWfZ
oYIwjhpZv0+SXEs8sEJZKDUhWIfOIpnDL7MoZYgl/kymgs/0hsW4L338jy303c7T
TwnG2/7BOMK0YFkEhqcjlkamGP7MKB2T9e/Cug6VkvFSkkim8M1eHx1gEnQxRtAG
YGp1n55iHQIDAQABo1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAd
BgNVHQ4EFgQUl2F3U7cggzCuvRWliZWg91n5lccwEAYJKwYBBAGCNxUBBAMCAQAw
DQYJKoZIhvcNAQEFBQADggEBAJXoJJDDB3QH0q8VY8G/oC1SkAwyOE1dH0NdxFES
tNqQMTaRB2Sb2L/ZzAtfIaZ0Xab9Ig4MqNIMBbHDCwlzhD5gX42GPYWhA/GjRj3O
Q5KcRaEFomxp+twRrJ25ScVSczKJaRonWqKDVL9TwoSuDar3ObiS9ZC0KuBBf0vu
dzrJEYY/1zz7WVPZVyevhba3VSt4LW75URTqOKBSuKO+fvGyyNHWvMPFEIEnJAKt
7QmhO2fiWhD8CxaPFIByqkvrJ96no6oBxdEcjm9n1MttF/UJcpypSPH+46mRn5Az
SzgCBftYNjBPLcwbZGJkF/GpPwjd0TclMM08UOdqiTxR7Ts=
-----END CERTIFICATE-----
  You are going to overwrite the KMIP Client Certificate.
  Are you sure you want to proceed and overwrite the KMIP Client Certificate? [y|N]
y
Server /kmip/kmip-client-certificate #
```

KMIP クライアント証明書のエクスポート

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。
- KMIP クライアント証明書をエクスポートするには、証明書がダウンロード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 kmip**	KMIP コマンド モードを開始します。
ステップ 2	Server /kmip # **scope kmip-client-certificate**	KMIP クライアント証明書コマンドモードを開始します。
ステップ 3	Server /kmip/kmip-client-certificate # **export-client-certificate** *remote-protocol IP アドレス KMIP ルート CA 証明書ファイル*	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 サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバー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 サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[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
		証明書のエクスポートを開始します。
ステップ 4	（任意） Server /kmip/kmip-client-certificate # **show detail**	証明書のエクスポートのステータスを表示します。

例

この例は、KMIP クライアント証明書をエクスポートします。

```
Server # scope kmip
Server /kmip # scope kmip-client-certificate
Server /kmip/kmip-client-certificate #  export-client-certificate ftp 10.10.10.10
/TFTP_DIR/KmipCertificates
/svbu-xx-blr-dn1-13_ClientCert.pem_exported_ftp
Username: username
Password:
KMIP Client Certificate exported successfully
Server /kmip/kmip-client-certificate # show detail
    KMIP Client Certificate Available: 1
    Download KMIP Client Certificate Status: COMPLETED
    Export KMIP Client Certificate Status: COMPLETED
Server /kmip/kmip-client-certificate #
```

KMIP クライアント証明書の削除

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope kmip**	KMIP コマンド モードを開始します。
ステップ 2	Server# /kmip **scope kmip-client-certificate**	KMIP クライアント証明書バインド コマンド モードを開始します。
ステップ 3	Server /kmip/kmip-client-certificate # **delete-client-certificate**	確認のプロンプトが表示されます。
ステップ 4	確認プロンプトで、**y** と入力します。	これでKMIP クライアント証明書が削除されます。

例

この例は、KMIP クライアント証明書を削除します。

```
Server # scope kmip
Server /kmip # scope kmip-client-certificate
Server /kmip/kmip-client-certificate # delete-client-certificate
  You are going to delete the KMIP Client Certificate.
  Are you sure you want to proceed and delete the KMIP Client Certificate? [y|N]y
 KMIP Client Certificate deleted successfully.
```

KMIP ルート CA 証明書のダウンロード

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope kmip**	KMIP コマンド モードを開始します。
ステップ 2	Server/kmip # **set enabled yes**	KMIP を有効にします。
ステップ 3	Server/kmip * # **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 /kmip # **scope kmip-root-ca-certificate**	KMIP ルート CA 証明書のコマンド モードを開始します。
ステップ 5	Server /kmip/kmip-root-ca-certificate # **download-root-ca-certificate** *remote-protocol IP アドレス KMIP CA 証明書ファイル*	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

	コマンドまたはアクション	目的
		（注） Cisco UCS C シリーズ サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバー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 サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[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 6	確認プロンプトで、**y** と入力します。	これにより KMIP ルート CA 証明書のダウンロードが開始されます。
ステップ 7	（任意） Server /kmip/kmip-root-ca-certificate # **paste-root-ca-certificate**	プロンプトで、ルート CA 証明書の内容を貼り付け、**Ctrl+D** を押します。 （注） 前の手順のリモート サーバ メソッドを使用するか、貼り付けオプションを使用して、ルート CA 証明書をダウンロードできます。

例

この例は、KMIP ルート CA 証明書をダウンロードします。

```
Server # scope kmip
Server /kmip # set enabled yes
Server /kmip *# commit
Server /kmip # scope kmip-root-ca-certificate
Server /kmip/kmip-root-ca-certificate # show detail
    KMIP Root CA Certificate Available: 1
    Download Root CA Certificate Status: COMPLETED
    Export Root CA Certificate Status: NONE
Server /kmip/kmip-root-ca-certificate # download-root-ca-certificate tftp 10.10.10.10
KmipCertificates/
svbu-xx-blr-dn1-13_ServerCert.pem
  You are going to overwrite the KMIP Root CA Certificate.
  Are you sure you want to proceed and overwrite the KMIP Root CA Certificate? [y|N]y
KMIP Root CA Certificate downloaded successfully

You can  either use the remote server method from the previous steps or use the paste
option to download the client certificate.

Server /kmip/kmip-root-ca-certificate # paste-root-ca-certificate
Please paste your certificate here, when finished, press CTRL+D.
----BEGIN CERTIFICATE-----
MIIDTzCCAjegAwIBAgIQXuWPdBbyTb5M7/FT8aAjZTANBgkqhkiG9w0BAQUFADA6
MRMwEQYKCZImiZPyLGQBGRYDY29tMRMwEQYKCZImiZPyLGQBGRYDbmV3MQ4wDAYD
VQQDEwVuZXdDQTAeFw0xNTAzMTIxMTM5MTZaFw0yMDAzMTIxMTQ5MTVaMDoxEzAR
BgoJkiaJk/IsZAEZFgNjb20xEzARBgoJkiaJk/IsZAEZFgNuZXcxDjAMBgNVBAMT
BW5ld0NBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuPSAwHtk0IbM
Cd5tYdCa498bfX5Nfdgnq5zE+cGIOqv0dAkucofC/Y0+m7hne9H12aQ9SqTOK1+L
5IT3PVCczhasI7L7jAa+Oe5AOYw7Nsugw5Bd23n42BTVMMp7xsgr1mVfFoHXbBkQ
wiT9DieyImSyGiq5n0/8Iooc0iN5WPMVcHO2ysz76jR8p07xRqgYNCl6cbKAhWfZ
oYIwjhpZv0+SXEs8sEJZKDUhWIfOIpnDL7MoZYgl/kymgs/0hsW4L338jy303c7T
TwnG2/7BOMK0YFkEhqcjlkamGP7MKB2T9e/Cug6VkvFSkkim8M1eHx1gEnQxRtAG
YGp1n55iHQIDAQABo1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAd
BgNVHQ4EFgQUl2F3U7cggzCuvRWliZWg91n5lccwEAYJKwYBBAGCNxUBBAMCAQAw
DQYJKoZIhvcNAQEFBQADggEBAJXoJJDDB3QH0q8VY8G/oC1SkAwyOE1dH0NdxFES
tNqQMTaRB2Sb2L/ZzAtfIaZ0Xab9Ig4MqNIMBbHDCwlzhD5gX42GPYWhA/GjRj3O
Q5KcRaEFomxp+twRrJ25ScVSczKJaRonWqKDVL9TwoSuDar3ObiS9ZC0KuBBf0vu
dzrJEYY/1zz7WVPZVyevhba3VSt4LW75URTqOKBSuKO+fvGyyNHWvMPFEIEnJAKt
7QmhO2fiWhD8CxaPFIByqkvrJ96no6oBxdEcjm9n1MttF/UJcpypSPH+46mRn5Az
SzgCBftYNjBPLcwbZGJkF/GpPwjd0TclMM08UOdqiTxR7Ts=
-----END CERTIFICATE-----
  You are going to overwrite the KMIP Root CA Certificate.
  Are you sure you want to proceed and overwrite the KMIP Root CA Certificate? [y|N]
y
Server /kmip/kmip-root-ca-certificate #
```

KMIP ルート CA 証明書のエクスポート

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。
- KMIP ルート CA 証明書をエクスポートするには、証明書がダウンロード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 kmip**	KMIP コマンド モードを開始します。
ステップ 2	Server /kmip # **scope kmip-root-ca-certificate**	KMIP ルート CA 証明書のコマンド モードを開始します。
ステップ 3	Server /kmip/kmip-root-ca-certificate # **export-root-ca-certificate** *remote-protocol IP アドレス KMIP ルート CA 証明書ファイル*	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 サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバー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 サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[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
		証明書のエクスポートを開始します。
ステップ 4	（任意） Server /kmip/kmip-root-ca-certificate # **show detail**	証明書のエクスポートのステータスを表示します。

例

この例は、KMIP ルート CA 証明書をエクスポートします。

```
Server # scope kmip
Server /kmip # scope kmip-root-ca-certificate
Server /kmip/kmip-root-ca-certificate #  export-root-ca-certificate tftp 10.10.10.10
KmipCertificates/
svbu-xx-blr-dn1-13_ServerCert.pem_exported_tftp
KMIP Root CA Certificate exported successfully
Server /kmip/kmip-root-ca-certificate # show detail
    KMIP Root CA Certificate Available: 1
    Download Root CA Certificate Status: COMPLETED
    Export Root CA Certificate Status: COMPLETED
Server /kmip/kmip-root-ca-certificate #
```

KMIP ルート CA 証明書の削除

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope kmip**	KMIP コマンド モードを開始します。
ステップ 2	Server# /kmip **scope kmip-root-ca-certificate**	KMIP ルート CA 証明書バインド コマンド モードを開始します。
ステップ 3	Server /kmip/kmip-root-ca-certificate # **delete-root-ca-certificate**	確認のプロンプトが表示されます。
ステップ 4	確認プロンプトで、**y** と入力します。	これで KMIP ルート CA 証明書が削除されます。

例

この例は、KMIP ルート CA 証明書を削除します。

```
Server # scope kmip
Server /kmip # scope kmip-root-ca-certificate
Server /kmip/kmip-root-ca-certificate # delete-root-ca-certificate
```

```
 You are going to delete the KMIP root CA certificate.
 Are you sure you want to proceed and delete the KMIP root CA certificate? [y|N]y
KMIP root CA certificate deleted successfully.
```

KMIP クライアント秘密キーのダウンロード

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope kmip**	KMIP コマンド モードを開始します。
ステップ 2	Server/kmip# **set enabled yes**	KMIP を有効にします。
ステップ 3	Server/kmip*# **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/kmip # **scope kmip-client-private-key**	KMIP クライアント秘密キー コマンド モードを開始します。
ステップ 5	Server /kmip/kmip-client-private-key # **download-client-pvt-key** *remote-protocol IP アドレス KMIP クライアント秘密キー ファイル*	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

	コマンドまたはアクション	目的
		（注） Cisco UCS C シリーズ サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバー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 サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[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 6	確認プロンプトで、**y** と入力します。	これにより KMIP クライアント秘密キーのダウンロードが開始されます。
ステップ 7	（任意） Server /kmip/kmip-client-private-key # **paste-client-pvt-key**	プロンプトで、秘密キーの内容を貼り付け、**Ctrl+D** を押します。 （注） 前の手順のリモート サーバ メソッドを使用するか、貼り付けオプションを使用して、クライアント秘密キーをダウンロードできます。

例

この例は、KMIP クライアント秘密キーをダウンロードします。

```
Server # scope kmip
Server /kmip # set enabled yes
Server /kmip *# commit
Server /kmip # scope kmip-client-private-key
Server /kmip/kmip-client-private-key # show detail
    KMIP Client Private Key Available: 1
    Download Client Private Key Status: COMPLETED
    Export Client Private Key Status: NONE
Server /kmip/kmip-client-private-key #  download-client-pvt-key tftp 10.10.10.10
KmipCertificates/
svbu-xx-blr-dn1-13_ClientPvtKey.pem
  You are going to overwrite the KMIP Client Private Key.
  Are you sure you want to proceed and overwrite the KMIP Client Private Key? [y|N]y
KMIP Client Private Key downloaded successfully

You can  either use the remote server method from the previous steps or use the paste
option to download the client certificate.

Server /kmip/kmip-client-private-key # paste-client-pvt-key
Please paste your client private here, when finished, press CTRL+D.
----BEGIN CERTIFICATE-----
MIIDTzCCAjegAwIBAgIQXuWPdBbyTb5M7/FT8aAjZTANBgkqhkiG9w0BAQUFADA6
MRMwEQYKCZImiZPyLGQBGRYDY29tMRMwEQYKCZImiZPyLGQBGRYDbmV3MQ4wDAYD
VQQDEwVuZXdDQTAeFw0xNTAzMTIxMTM5MTZaFw0yMDAzMTIxMTQ5MTVaMDoxEzAR
BgoJkiaJk/IsZAEZFgNjb20xEzARBgoJkiaJk/IsZAEZFgNuZXcxDjAMBgNVBAMT
BW5ld0NBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuPSAwHtk0IbM
Cd5tYdCa498bfX5Nfdgnq5zE+cGIOqv0dAkucofC/Y0+m7hne9H12aQ9SqTOK1+L
5IT3PVCczhasI7L7jAa+Oe5AOYw7Nsugw5Bd23n42BTVMMp7xsgr1mVfFoHXbBkQ
wiT9DieyImSyGiq5n0/8Iooc0iN5WPMVcHO2ysz76jR8p07xRqgYNC16cbKAhWfZ
oYIwjhpZv0+SXEs8sEJZKDUhWIfOIpnDL7MoZYgl/kymgs/0hsW4L338jy303c7T
TwnG2/7BOMK0YFkEhqcjlkamGP7MKB2T9e/Cug6VkvFSkkim8M1eHx1gEnQxRtAG
YGp1n55iHQIDAQABo1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAd
BgNVHQ4EFgQUl2F3U7cggzCuvRWliZWg91n5lccwEAYJKwYBBAGCNxUBBAMCAQAw
DQYJKoZIhvcNAQEFBQADggEBAJXoJJDDB3QH0q8VY8G/oC1SkAwyOE1dH0NdxFES
tNqQMTaRB2Sb2L/ZzAtfIaZ0Xab9Ig4MqNIMBbHDCwlzhD5gX42GPYWhA/GjRj3O
Q5KcRaEFomxp+twRrJ25ScVSczKJaRonWqKDVL9TwoSuDar3ObiS9ZC0KuBBf0vu
dzrJEYY/1zz7WVPZVyevhba3VSt4LW75URTqOKBSuKO+fvGyyNHWvMPFEIEnJAKt
7QmhO2fiWhD8CxaPFIByqkvrJ96no6oBxdEcjm9n1MttF/UJcpypSPH+46mRn5Az
SzgCBftYNjBPLcwbZGJkF/GpPwjd0TclMM08UOdqiTxR7Ts=
-----END CERTIFICATE-----
  You are going to overwrite the KMIP client private key.
  Are you sure you want to proceed and overwrite the KMIP Client Private Key? [y|N]
y
Server /kmip/kmip-client-private-key #
```

KMIP クライアント秘密キーのエクスポート

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。
- KMIP クライアントの秘密キーをエクスポートするには、秘密キーがダウンロード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 kmip**	KMIP コマンド モードを開始します。
ステップ 2	Server /kmip # **scope kmip-client-private-key**	KMIP クライアント秘密キー コマンド モードを開始します。
ステップ 3	Server /kmip/kmip-client-private-key # **export-client-pvt-key** *remote-protocol IP* アドレス *KMIP* ルート *CA* 証明書ファイル	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 サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバー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 サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[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
		証明書のエクスポートを開始します。
ステップ 4	（任意） Server /kmip/kmip-client-private-key # **show detail**	証明書のエクスポートのステータスを表示します。

例

この例は、KMIP クライアントの秘密キーをエクスポートします。

```
Server # scope kmip
Server /kmip # scope kmip-client-private-key
Server /kmip/kmip-client-private-key #  export-client-pvt-key tftp 10.10.10.10
KmipCertificates
/svbu-xx-blr-dn1-13_ClientPvtKey.pem_exported_tftp
KMIP Client Private Key exported successfully
Server /kmip/kmip-client-private-key # show detail
    KMIP Client Private Key Available: 1
    Download Client Private Key Status: COMPLETED
    Export Client Private Key Status: COMPLETED
Server /kmip/kmip-client-private-key #
```

KMIP クライアント秘密キーの削除

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope kmip**	KMIP コマンド モードを開始します。
ステップ 2	Server# /kmip **scope kmip-client-private-key**	KMIP クライアント秘密キー バインド コマンド モードを開始します。
ステップ 3	Server /kmip/kmip-client-private-key # **delete-client-pvt-key**	確認のプロンプトが表示されます。
ステップ 4	確認プロンプトで、**y** と入力します。	これでKMIPクライアントの秘密キーが削除されます。

例

この例は、KMIP クライアントの秘密キーを削除します。

```
Server # scope kmip
Server /kmip # scope kmip-client-private-key
Server /kmip/kmip-client-private-key # delete-client-pvt-key
```

```
 You are going to delete the KMIP client private key.
 Are you sure you want to proceed and delete the KMIP client private key? [y|N]y
KMIP client private key deleted successfully.
```

KMIP サーバ ログインの資格情報の構成

この手順では、KMIP サーバのログイン資格情報を設定し、KMIP サーバのログイン資格情報をメッセージ認証に必須にする方法を示しています。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope kmip**	KMIP コマンド モードを開始します。
ステップ 2	Server /kmip # **scope kmip-login**	KMIP ログイン コマンド モードを開始します。
ステップ 3	Server/kmip/kmip-login # **set login** *username*	KMIP サーバのユーザ名を設定します。
ステップ 4	Server/kmip/kmip-login * # **set password**	プロンプトでパスワードを入力し、パスワードの確認プロンプトで再度同じパスワードを入力します。これで KMIP サーバのパスワードが設定されます。
ステップ 5	Server/kmip/kmip-login * # **set use-kmip-cred** {**yes** | **no**}	KMIP サーバのログイン資格情報をメッセージ認証に必須にするかどうかを決定します。
ステップ 6	Server/kmip/kmip-login * # **commit**	トランザクションをシステム設定にコミットします。
ステップ 7	（任意） Server/kmip/kmip-login # **restore**	KMIP の設定をデフォルトに戻します。

例

次に、KMIP サーバの資格情報を設定する例を示します。

```
Server /kmip # scope kmip-login
Server /kmip/kmip-login # set login username
Server /kmip/kmip-login *# set password
Please enter password:
Please confirm password:
Server /kmip/kmip-login *# set use-kmip-cred yes
Server /kmip/kmip-login *# commit
Server /kmip/kmip-login # show detail
```

```
    Use KMIP Login: yes
    Login name to KMIP server: username
    Password to KMIP server: ******

You can restore the KMIP server credentials to default settings by preforming the following
 step:

Server /kmip/kmip-login # restore
Are you sure you want to restore KMIP settings to defaults?
Please enter 'yes' to confirm: yes
Restored factory-default configuration.
Server /kmip/kmip-login # show detail
    Use KMIP Login: no
    Login name to KMIP server:
    Password to KMIP server: ******
Server /kmip/kmip-login #
```

KMIP サーバ プロパティの構成

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope kmip**	KMIP コマンド モードを開始します。
ステップ 2	Server /kmip # **scope kmip-server** サーバ *ID*	選択した KMIP サーバのコマンド モードを開始します。
ステップ 3	Server /kmip/kmip-server # **set** *kmip-port*	KMIP ポートを設定します。
ステップ 4	Server /kmip/kmip-server *# **set** *kmip-server*	KMIP サーバ ID を設定します。
ステップ 5	Server /kmip/kmip-server # **set** *kmip-timeout*	KMIP サーバのタイムアウトを設定します。
ステップ 6	Server /kmip/kmip-server # **commit**	トランザクションをシステム設定にコミットします。
ステップ 7	（任意） Server /kmip/kmip-server # **show detail**	KMIP サーバの詳細を表示します。

例

次に、KMIP サーバの接続をテストする例を示します。

```
Server # scope kmip
Server /kmip # scope kmip-server 1
Server /kmip/kmip-server # set kmip-port  5696
Server /kmip/kmip-server * # set kmip-server  kmipserver.com
```

```
Server /kmip/kmip-server * # set kmip-timeout  10
Server /kmip/kmip-server * # commit
Server /kmip/kmip-server # show detail
Server number 1:
    Server domain name or IP address: kmipserver.com
    Port: 5696
    Timeout: 10
Server /kmip/kmip-server #
```

Cisco IMC での FIPS 140-2 の準拠

Federal Information Processing Standard（FIPS）パブリケーション 140-2 は、暗号モジュールの認定に使用される米国政府のコンピュータ セキュリティ標準です3.1(3) リリースでは、ラック Cisco IMC は NIST ガイドラインに従った FIPS 対応ではありません。これは FIPS 140-2 で承認された暗号化アルゴリズムとモジュールに従っていません。このリリースで、すべての CIMC サービスは、Cisco FIPS オブジェクト モジュール（FOM）を使用します。これにより、FIPS 140-2 に準拠した暗号化モジュールが提供されます。

Cisco FIPS オブジェクト モジュールは、Cisco の広範なネットワー キング製品およびコラボレーション製品に暗号化サービスを提供するソフトウェア ライブラリです。モジュールは、IPSec（IKE）、SRTP、SSH、TLS、SNMP などのサービスに対して、FIPS 140 の検証済みの暗号化アルゴリズムと KDF 機能を提供します。

セキュリティ設定の有効化

始める前に

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

手順

	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 security-configuration**	セキュリティの設定コマンド モードを開始します。
ステップ 3	Server /chassis/security-configuration # **set fips enabled**または**disabled**	有効になっている場合は、FIPS を有効にします。
ステップ 4	Server /chassis/security-configuration* # **commit**	FIPS を有効にして、システムにトランザクションをコミットする警告プロンプトで **y** を入力します。

	コマンドまたはアクション	目的
		（注） FIPS モードを切り替えると、SSH、KVM、SNMP、web サーバ、XMLAPI、および redfish サービスが再起動されます。

	コマンドまたはアクション	目的
		（注）

	コマンドまたはアクション	目的
		FIPS、または FIPS と CC の両方を有効にすると、次の SNMP 設定の変更が発生します。 • SNMPv2 プロトコル向けのコミュニティ文字列の設定、および [noAuthNoPriv] または [authNoPriv] が指定された SNMPv3 ユーザーのセキュリティ レベル オプションが無効になります。 • [NoAuthNoPriv] のセキュリティ レベル オプションが指定された SNMPv2 または SNMPv3 ユーザー向けに設定されたトラップが無効になります。 • [MD5] および [DES] 認証タイプおよびプライバシー タイプが無効になります。 （注） DES プライバシー タイプは、リリース 4.1（3b） 以降には適用されません。ただし、DES をリリース 4.1（3b） 以降にアップグレードする前に以前のリリースで構成されていた場合は、DES

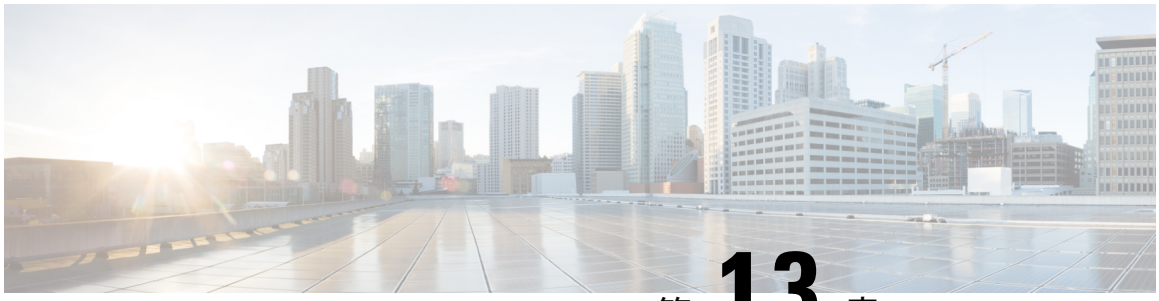
	コマンドまたはアクション	目的
		プライバシー タイプが表示される場合がありますが、FIPS が有効になっている場合は無効になります。 （注） **[MD5]** および **[DES]** 認証タイプとプライバシー タイプは、Cisco UCS M6 C シリーズ サーバーではサポートされていません。 • また、SSH、Webサーバ、KVM 接続で FIPS 準拠の暗号方式のみが使用されるようになります。
ステップ 5	Server /chassis/security-configuration # **set cc enabled**または**disabled**	（注） FIPS は、CC を有効にする有効な状態である必要があります。 有効にすることを選択すると、CC が有効になります。
ステップ 6	Server /chassis/security-configuration* # **commit**	FIPS を有効にして、システムにトランザクションをコミットする警告プロンプトで **y** を入力します。

	コマンドまたはアクション	目的
		（注） FIPS モードを切り替えると、SSH、KVM、SNMP、web サーバ、XMLAPI、および redfish サービスが再起動されます。 （注） FIPS、または FIPS と CC の両方を有効にすると、次の SNMP 設定の変更が発生します。 • SNMPv2 プロトコル向けのコミュニティ文字列の設定、および [noAuthNoPriv] または [authNoPriv] が指定された SNMPv3 ユーザーのセキュリティ レベル オプションが無効になります。 • [NoAuthNoPriv] のセキュリティ レベル オプションが指定された SNMPv2 または SNMPv3 ユーザー向けに設定されたトラップが無効になります。 • [MD5] および [DES] 認証タイプおよびプライバシー タイプが無効になります。 • また、SSH、Webサーバー、KVM 接続で FIPS 準拠の暗号方式のみが使用されるようになります。

例

この例は、コントローラ情報を表示する方法を示します。

```
Server# scope cimc
Server /cimc # scope security-configuration
Server /cimc/security-configuration # set fips enabled
Enabling FIPS would
1. Disables support for SNMP V2 and V3 with No 'Auth/Priv' security level.
2. Disables support for 'MD5/DES' crypto algorithms in SNMP 'Auth/Priv' keys.
3. Ensures use of only FIPS-compliant ciphers in SSH, webserver and KVM connections.
Server /cimc/security-configuration* # commit
Server/cimc/security-configuration # set cc enabled
Enabling Common Criteria
Server /cimc/security-configuration* # commit
Warning: changing "fips" or "CC" will restart SSH, KVM, SNMP, webserver, XMLAPI and
redfish services.
Do you wish to continue? [y/N] y
Server /cimc/security-configuration #
```



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、次の内容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
7	メモリ緊急アサート フィルタ

プラットフォーム イベント フィルタの設定

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope fault**	障害コマンド モードを開始します。
ステップ 2	Server /fault # **scope pef** *id*	指定したイベントに対してプラットフォーム イベント フィルタ コマンド モードを開始します。 イベント ID 番号に対応するプラットフォーム イベント フィルタの表を参照してください。
ステップ 3	Server /fault/pef # **set action** {**none** | **reboot** | **power-cycle** | **power-off**}	このイベントが発生した場合に必要なシステムの処理を選択します。次のいずれかの処理を選択できます。 • **none** ：システム アクションは実行されません。 • **reboot** ：サーバーがリブートされます。 • **power-cycle** ：サーバーに電源が再投入されます。 • **power-off** ：サーバーの電源がオフになります。
ステップ 4	Server /fault/pef # **commit**	トランザクションをシステムの設定にコミットします。

例

次に、イベントに対するプラットフォーム イベント アラートを設定します。

```
Server# scope fault
Server /fault # scope pef 5
Server /fault/pef # set action reboot
Server /fault/pef *# commit
Server /fault/pef # show
Platform Event Filter Event                       Action
-------------------- --------------------------- -----------
5                    Processor 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

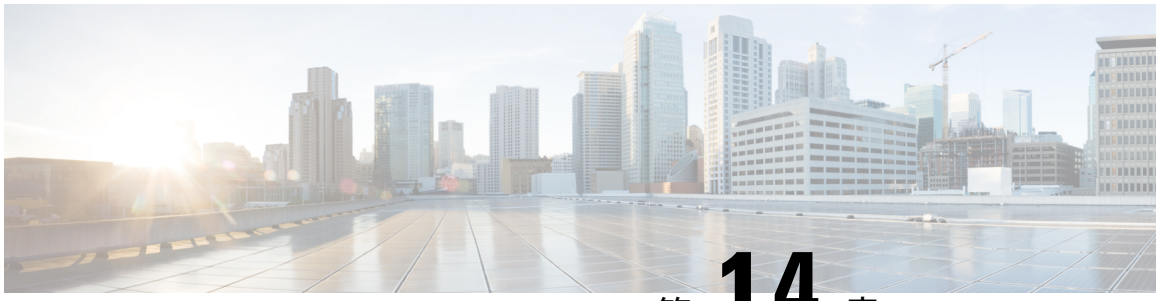
手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope fault**	障害コマンド モードを開始します。
ステップ 2	Server /fault # **set platform-event-enabled yes**	プラットフォーム イベント アラートをイネーブルにします。
ステップ 3	Server /fault # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 4	Server /fault # **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 # **show pef**	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。

例

次に、プラットフォーム イベント アラートをイネーブルにする例を示します。

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

Server /fault # 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、次の内容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 リリースに付属の 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 UtilityISO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。

Cisco Host Upgrade Utilityを含むこの ISO ファイルを使用して、Cisco IMC とサーバーの 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付属の 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。

リリース 3.0 以降、BIOS および Cisco IMC ファームウェア ファイルは、単独の .zip ファイルとして HUU 内に組み込まれなくなりました。現在、BIOS と Cisco IMC ファームウェアを抽出するには、HUU の GETFW フォルダにある **getfw** ユーティリティを使用する必要があります。BIOS または Cisco IMC ファームウェア ファイルを抽出するには、次の手順を実行します。

（注） この手順を実行するには：

- Openssl をターゲット システムにインストールする必要があります。
- Squashfs カーネル モジュールをターゲット システムにロードする必要があります。

```
Viewing the GETFW help menu:
[root@RHEL65-***** tmp]# cd GETFW/
[root@RHEL65-***** GETFW]# ./getfw -h
Help:
  Usage: getfw {-b -c -C -H -S -V -h} [-s SRC] [-d DEST]
    -b      : Get BIOS Firmware
    -c      : Get CIMC Firmware
    -C      : Get CMC Firmware
    -H      : Get HDD Firmware
    -S      : Get SAS Firmware
    -V      : Get VIC Firmware
    -h      : Display Help
    -s SRC  : Source of HUU ISO image
    -d DEST : Destination to keep Firmware/s
  Note : Default BIOS & CIMC get extracted

Extracting the BIOS firmware:

[root@RHEL65-***** GETFW]# ./getfw -s /root/Desktop/HUU/ucs-c2xxx-huu-3.0.1c.iso -d
/tmp/HUU
FW/s available at '/tmp/HUUucs-c2xxx-huu-3.0.1c'
[root@RHEL65-***** GETFW]# cd /tmp/HUU/
[root@RHEL65-***** HUU]# cd ucs-c2xxx-huu-3.0.1c/
[root@RHEL65-***** ucs-c2xxx-huu-3.0.1c]# ls
bios  cimc
[root@RHEL65-***** ucs-c2xxx-huu-3.0.1c]# cd bios/
[root@RHEL65-***** bios]# ls
bios.cap
[root@RHEL65-***** bios]#

Extracting the CIMC firmware:

[root@RHEL65-***** GETFW]# ./getfw -s /root/Desktop/HUU/ucs-c2xxx-huu-3.0.1c.iso -d
/tmp/HUU
FW/s available at '/tmp/HUUucs-c2xxx-huu-3.0.1c'
[root@RHEL65-***** GETFW]# cd /tmp/HUU/
[root@RHEL65-***** HUU]# cd ucs-c2xxx-huu-3.0.1c/
[root@RHEL65-***** ucs-c2xxx-huu-3.0.1c]# ls
bios  cimc
[root@RHEL65-***** ucs-c2xxx-huu-3.0.1c]# cd cimc/
[root@RHEL65-***** cimc]# ls
cimc.cap
[root@RHEL65-***** cimc]#
```

ステップ 12 （任意）リモート サーバー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 サーバーに 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 サーバーは次のいずれかになります。

- TFTP
- FTP

- SFTP
- SCP
- HTTP

サーバーにはリモート サーバー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際に、サーバのフィンガープリント確認がサポートされます。このオプションは、リモート サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。

このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[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。

次のタスク

Cisco Host Upgrade Utility 使用してサーバー上のすべてのファームウェアをアップグレードするか、手動でサーバーに 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	目的の Cisco IMC バージョン	可能性
2.0(x)	1.5(1) よりも前	可能性なし

Cisco IMC バージョンから	目的の Cisco IMC バージョン	可能性
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 「一部の Cisco IMC ファームウェア コンポーネントが正しくインストールされていません。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

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。

Cisco IMC ファームウェアのインストール

- フロント パネルの USB デバイスを介して Cisco IMC ファームウェアを更新する場合は、スマート アクセス USB オプションが有効であることを確認します。
- 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。

始める前に

- 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 UtilityISO ファイルを入手し、シスコからのファームウェアの取得 （443 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。

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** プロトコル *IP* アドレス パス	プロトコル、リモート サーバーの IP アドレス、サーバー上のファームウェア ファイルへのファイル パスを指定します。プロトコルは次のいずれかになります。 • TFTP • FTP • SFTP • SCP • HTTP

	コマンドまたはアクション	目的
		（注） Cisco UCS C シリーズ サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバー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 サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[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 usb** パスとファームウェア ファイル名	接続されている USB から Cisco IMC ファームウェアを更新します。
ステップ 5	（任意） server /cimc /firmware # **update-secure** プロトコル *IP* アドレス パス	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 6	（任意） server /cimc /firmware # **show detail**	ファームウェア アップデートの進捗状況を表示します。

例

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 ファームウェアを更新する例を示します。

次のタスク

新しいファームウェアをアクティブにします。

インストールした CIMC ファームウェアのアクティブ化

始める前に

CIMC ファームウェアをサーバにインストールします。

重要 アクティブ化の進行中は、次のことを行わないでください。

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

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。
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	（任意） 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。	

例

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
```

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 で入手可能な *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

始める前に

- 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 （452 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）
- 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。
- フロントパネルのUSBデバイスを介してBIOSファームウェアを更新する場合は、スマート アクセス USB オプションが有効であることを確認します。

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。

	コマンドまたはアクション	目的
ステップ 3	Server /cimc/firmware # **show detail**	使用可能なファームウェア イメージおよびステータスを表示します。
ステップ 4	[現在のファームウェア バージョン（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（452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** プロトコル *IP* アドレス パス	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。

	コマンドまたはアクション	目的
		（注） Cisco UCS C シリーズ サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバー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 サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[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。
ステップ 8	Server /bios # **update usb** パスとファームウェア ファイル名	接続されている USB から BIOS ファームウェアを更新します。

例

次に、BIOS ファームウェアをアップデートする例を示します。

```
Server# scope bios
Server /bios# show detail
BIOS:
    BIOS Version: CxxMx.2.0.3.0.080720142114
    Backup BIOS Version: CxxMx.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 10.10.10.10 //upgrade_bios_files/Cxx-BIOS-1-4-3j-0.CAP
 <CR>  Press Enter key
Firmware update has started.
Please check the status using "show detail"

For updating the BIOS using the front panel USB:

Server /bios # update usb CxxMx-BIOS-3-1-0-289.cap
 User Options:USB Path[Cxxmx-BIOS-3-1-0-289.cap]
<CR> Press Enter key
Firmware update has started.
Please check the status using "show detail"
Server /bios # show detail
BIOS:
BIOS Version: CxxMx.3.1.0.289.0530172308
Boot Order: (none)
FW Update Status: None, OK
UEFI Secure Boot: disabled
Configured Boot Mode: Legacy
Actual Boot Mode: Legacy
Last Configured Boot Order Source: BIOS
One time boot device: (none)
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）

- リリース 4.0(1) から、サーバがオンの場合に BIOS をアクティベートすることができます。サーバがオンのときに、ファームウェアをアクティブにすると、アクティベーションが保留状態で、ファームウェアは次のサーバが再起動した後にアクティベーションされます。
- [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。

始める前に

- 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 IMCCisco 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。	

例

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
 Server /bios #
```

```
Server# scope bios
Server /bios # show detail
BIOS:
    BIOS Version: Cxxx.4.0.0.19.0528180450
    Backup BIOS Version: Cxxx.4.0.0.23.0612180433
    Boot Order: (none)
    FW Update Status: Done, OK
    UEFI Secure Boot: disabled
    Actual Boot Mode: Uefi
    Last Configured Boot Order Source: BIOS
    One time boot device: (none)
Server /bios # activateSystem is powered-on. This operation will activate backup BIOS
version
"C125.4.0.0.23.0612180433" during next boot.
Continue?[y|N]y
Server# scope bios
Server /bios # show detail
BIOS:
    BIOS Version: Cxx.4.0.0.19.0528180450
    Backup BIOS Version: Cxxx.4.0.0.23.0612180433
    Boot Order: (none)
    FW Update Status: Done, Activation pending
    UEFI Secure Boot: disabled
    Actual Boot Mode: Uefi
    Last Configured Boot Order Source: BIOS
    One time boot device: (none)
Server /bios #
```

保留中の BIOS アクティベーションのキャンセル

始める前に

BIOS ファームウェアが保留状態になければなりません。

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。

	コマンドまたはアクション	目的
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 # **cancel-activate**	（注） BIOS ファームウェアが保留状態でなければなりません。 保留中の BIOS のアクティブ化をキャンセルします。
ステップ 4	プロンプトで、**y**を入力してアクティブ化をキャンセルします。	

例

この例では、保留中の BIOSファームウェアのアクティブ化をキャンセルします。

```
Server# scope bios
Server /bios # show detail
 BIOS:
    BIOS Version: Cxxx.4.0.0.19.0528180450
    Backup BIOS Version: Cxxx.4.0.0.23.0612180433
    Boot Order: (none)
    FW Update Status: Done, Activation pending
    UEFI Secure Boot: disabled
    Actual Boot Mode: Uefi
    Last Configured Boot Order Source: BIOS
    One time boot device: (none)
Server /bios # cancel-activate
This will cancel Pending BIOS activation[y|N]y
Server /bios # show detail
BIOS:
    BIOS Version: Cxxx.4.0.0.19.0528180450
    Backup BIOS Version: Cxxx.4.0.0.23.0612180433
    Boot Order: (none)
    FW Update Status: None, OK
    UEFI Secure Boot: disabled
    Actual Boot Mode: Uefi
    Last Configured Boot Order Source: BIOS
    One time boot device: (none)
Server /bios #
```

VIC ファームウェアのインストール

始める前に

- 管理者権限を持つユーザとしてログインします。

- フロント パネルの USB デバイスから VIC ファームウェアを更新する場合は、スマート USB オプションが有効で、有効な VIC ファームウェアが USB デバイスで利用可能であることを確認します。
- アップデートがすでに処理中であるときに新た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 # **update-adapter-fw** ｐ プロトコル リモート サーバ アドレス 画像ファイル パス**activate|no-activate***PCI* スロット番号	VIC ファームウェアは、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。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

	コマンドまたはアクション	目的
		（注） Cisco UCS C シリーズ サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバー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 サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[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 3	server/chassis # **update-adapter-fw usb** イメージファイル パス **activate|no-activate** *PCI* スロット番号	USB デバイスのイメージ ファイルのパス、VIC PCI スロット番号を指定します。
ステップ 4	（任意） server /cimc # **show adapter detail**	ファームウェア アップデートの進捗状況を表示します。

例

次に、VIC ファームウェアを更新する例を示します。

```
Server# scope chassis
Server /chassis # update-adapter-fw update ftp 10.10.10.10 cruzfw_new.bin activate MLOM
Adapter firmware update has started.
Please check the status using "show adapter detail".
You have chosen to automatically activate the new firmware
image.  Please restart your host after the update finish.
```

```
Server /chassis # show adapter detail
PCI Slot MLOM:
    Product Name: UCS VIC 1387
    Serial Number: FCH2102J8SU
    Product ID: UCSC-MLOM-C40Q-03
    Adapter Hardware Revision: 3
    Current FW Version: 4.1(3.143)
    VNTAG: Disabled
    FIP: Enabled
    LLDP: Enabled
    Configuration Pending: no
    Cisco IMC Management Enabled: yes
    VID: V03
    Vendor: Cisco Systems Inc
    Description:
    Bootloader Version: 4.1(2d)
    FW Image 1 Version: 4.1(3.143)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: N/A
    FW Image 2 State: N/A
    FW Update Status: Update in progress
    FW Update Error: No error
    FW Update Stage: Erasing (12%)
    FW Update Overall Progress: 19%
Server /chassis #
```

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

始める前に

- 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 UtilityISO ファイルを入手し、シスコからのファームウェアの取得 （443 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。

	コマンドまたはアクション	目的
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** プロトコル *IP* アドレス パス	プロトコル、リモート サーバーの IP アドレス、サーバー上のファームウェア ファイルへのファイル パスを指定します。プロトコルは次のいずれかになります。 • TFTP • FTP • SFTP • SCP • HTTP （注） Cisco UCS C シリーズ サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバー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 サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[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	（任意） server /chassis/cmc # **show detail**	ファームウェア アップデートの進捗状況を表示します。

例

次に、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 #
```

次のタスク

新しいファームウェアをアクティブにします。

インストールした 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。

始める前に

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 IMCCisco 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。

例

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
```

リモート サーバからの SAS エクスパンダ ファームウェアのインストール

始める前に

- このアクションを実行するには、admin としてログオンする必要があります。
- 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 # **scope sas-expander {1 | 2}**	SAS エクスパンダ コマンド モードを開始します。
ステップ 3	Server /chassis/sas-expander # **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 /chassis/sas-expander # **update** *protocol IP_Address path*	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。

	コマンドまたはアクション	目的
		（注） Cisco UCS C シリーズ サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバー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 サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[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 SAS エクスパンダ ファームウェア ファイルへのファイル パス。

例

次に、SAS エクスパンダ ファームウェアをアップデートする例を示します。

```
Server# scope chassis
Server /chassis # scope sas-expander 1
Server /chassis/sas-expander # show detail
Firmware Image Information:
    ID: 1
    Name: SASEXP1
    Update Stage: NONE
    Update Progress: 0
    Current FW Version: 65103900
    FW Image 1 Version: 65103900
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 65103900
    FW Image 2 State: BACKUP INACTIVATED
Server /chassis/sas-expander # update ftp 192.0.20.34
//upgrade_sas_expander_files/sas-expander-2-0-12a.fw
 <CR>  Press Enter key
Firmware update has started.
Please check the status using "show detail"
Server /chassis/sas-expander #
```

インストール済みSASエクスパンダ ファームウェアの有効化

始める前に

- このアクションを実行するには、admin としてログオンする必要があります。
- ファームウェアをエクスパンダにインストールします。
- ホストの電源をオンにする必要があります。

手順

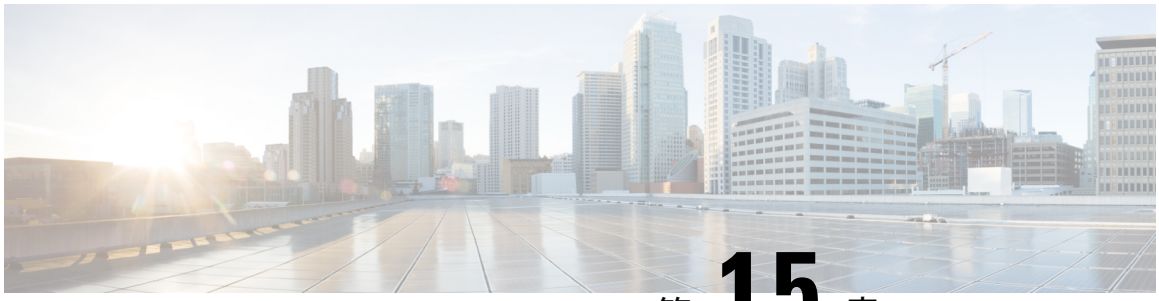
	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope sas-expander {1 | 2}**	SAS エクスパンダ コマンド モードを開始します。
ステップ 3	Server /chassis/sas-expander # **activate**	現在非アクティブになっているイメージをアクティブにします。

	コマンドまたはアクション	目的
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。	

例

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 chassis
Server /chassis # scope sas-expander 1
Server /chassis/sas-expander # show detail
 ID: 1
    Name: SASEXP1
    Update Stage: NONE
    Update Progress: 0
    Current FW Version: 65103900
    FW Image 1 Version: 65103900
    FW Image 1 State: RUNNING INACTIVATED
    FW Image 2 Version: 65103900
    FW Image 2 State: BACKUP INACTIVATED

Server /chassis/sas-expander # activate
This operation will activate "65103900" after next host power off
Continue?[y|N] y

Server /chassis/sas-expander # show detail
ID: 1
    Name: SASEXP1
    Update Stage: NONE
    Update Progress: 0
    Current FW Version: 65103900
    FW Image 1 Version: 65103900
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 65103900
    FW Image 2 State: BACKUP INACTIVATED
Server /chassis/sas-expander #
```



第 15 章

障害およびログの表示

この章は、次の内容で構成されています。

障害のサマリー

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 # **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-entries**	すべての障害のログを表示します。

例

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。

例

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# **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。

	コマンドまたはアクション	目的
ステップ 3	Server /cimc/log # **show entries** [**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。

例

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# **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 # **clear**	Cisco IMC ログをクリアします。

例

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 # **set local-syslog-severity** *level*	シビラティ（重大度）の *level* には、次のいずれかを指定できます。順にシビラティ（重大度）が下がります。 • emergency • alert • critical • error • warning

	コマンドまたはアクション	目的
		• notice • informational • debug （注） Cisco IMC では、選択したシビラティ（重大度）よりも低いシビラティ（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 ログにはシビラティ（重大度）が Emergency、Alert、Critical、または Error のすべてのメッセージが含まれます。Warning、Notice、Informational、または Debug のメッセージは表示されません。
ステップ 4	Server /cimc/log # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 5	（任意） Server /cimc/log # **show local-syslog-severity**	設定されたシビラティ（重大度）レベルを表示します。

例

次に、最小シビラティ（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。

始める前に

- 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	（任意） Server /cimc/log # **set remote-syslog-severity** *level*	シビラティ（重大度）の *level* には、次のいずれかを指定できます。順にシビラティ（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、選択したシビラティ（重大度）よりも低いシビラティ（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 サーバはシビラティ（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 エントリの送信を有効にします。
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。

例

次に、リモート syslog サーバ プロファイルを設定し、シビラティ（重大度）レベル Warning 以上の Cisco IMC ログ エントリの送信を有効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

始める前に

- 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。

例

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 #
```

無効なユーザー名のロギングを有効にする

ロギングの試行が失敗した場合に無効なユーザー名のロギングを有効にするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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 log-username-on-auth-fail enabled**	無効なユーザー名のロギングを有効にします。
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。

例

この例は、無効なユーザー名のロギングを有効にする方法を示しています。

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # set log-username-on-auth-fail enabled
Server /cimc/log* #commit
Server /cimc/log
```

リモート Syslog 証明書のアップロード

始める前に

- 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ファイルは、ローカルにアクセスできるファイルシステムに配置されている必要があります。

- 次の証明書形式がサポートされています。
  - .crt
  - .cer
  - .pem

リリース 4.2 (2a) 以降、リモート Syslog 証明書を Cisco UCS C シリーズ サーバーにアップロードできます。証明書を 1 つまたは 2 つの Cisco UCS C シリーズ サーバーにアップロードできます。

手順

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 # **scope server{1|2}**

2 つのリモート Syslog サーバー プロファイルのいずれかを選択し、コマンドモードを開始して、リモート Syslog 証明書をアップロードし、選択したサーバーでセキュアなリモート Syslog を有効にします。

ステップ 4 Server /cimc/log/server # **upload-certificate** *remote-protocol server_address path certificate_filename*

リモート サーバー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） FTP、SCP または SFTP としてプロトコルを選択した場合は、ユーザー名とパスワードの入力が求められます。

リモート Syslog 証明書をアップロードする場所からファイルパス、およびリモート プロトコルを入力します。リモート サーバーのユーザー名とパスワードを検証した後、リモート サーバーからリモート Syslog 証明書をアップロードします。

ステップ 5 （オプション）Server /cimc/log/server # **paste-certificate**

これは、リモート Syslog 証明書をアップロードするための追加オプションです。

プロンプトされたら、証明書の内容を貼り付け、Ctrl+D を押します。

ステップ 6 Server /cimc/log/server # **setsecure-enabledyes**

サーバーでセキュアなリモート Syslog を有効にします。

ステップ 7 Server /cimc/log/server # **commit**

トランザクションをシステムの設定にコミットします。

例

- この例では、リモート サーバーからリモート Syslog 証明書をアップロードし、選択したサーバーでセキュアなリモート Syslog を有効にします。

```
Server # scope cimc
Server /cimc # scope log
Server /cimc/log # scope server
Server /cimc/log/server # upload-certificate scp 10.10.10.10
/home/user-xyz/rem-sys-log-certif.cert
Server (RSA) key fingerprint is dd:b5:2b:07:ad:c0:30:b2:d5:6a:6a:78:80:85:93:b0
Do you wish to continue? [y/N]y
Username: user-xyz
Password:
Syslog Certificate uploaded successfully
Server /cimc/log/server # set secure-enabled yes
Server /cimc/log/server # commit
Server /cimc/log/server #
```

- この例では、貼り付けオプションを使用してリモート Syslog 証明書をアップロードします。

```
Server # scope cimc
Server /cimc # scope log
Server /cimc/log # scope server
Server /cimc/log/server # paste-certificate
Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIIFUDCCBDigAwIBAgIKYRF49gAAAAAAAjANBgkqhkiG9w0BAQUFADBLMRMwEQYK
CZImiZPyLGQBGRYDY29tMRMwEQYKCZImiZPyLGQBGRYDbmV3MR8wHQYDVQQDExZu
ZXctV0lOLU9WQlNBNElFU0NBLUNBMB4XDTE3MDczMDIxNTA1NVoXDTE5MDczMDIy
MDA1NVowSzETMBEGCgmSJomT8ixkARkWA2NvbTETMBEGCgmSJomT8ixkARkWA25l
dzEfMB0GA1UEAxMWbmV3LVdJTi1PVkJTQTRJRUJDQS1DQTCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBALd8c+hhJddfUH6XKqBvllZVtIAiHfCx+l7z9o7F
bELOWu0LDVSC9pC1zpJ9wykr6VqUsVhZTkqQan23+84X4lYBsd92shQp9bri2gKj
MGntmnXE6qP3b6Trw94j6JVyWXKImYEda/SFtx722orLap8Sdliurue62JGNfq56
vxXBT1SNUHOmgOdfTOeNjVyeh51jceOCdKTppBij4wuq+jJfkndhW7KKE7ubmyRv
xpRSkiVaqNypf8jv7uG8Kwx1Q8jbCr0wG4nAbPndwhkyJpgyA5zuCdMRU2cN47om
u0VfMzJeVu+HuAif25BqKn4cjwHGOnrWKZcfHtnpKEbbmv0CAwEAAaOCAjQwggIw
MBAGCSsGAQQBgjcVAQQDAgEAMB0GA1UdDgQWBBR2+YJQuCmHKCkBkqVim0/kvfzB
bTAZBgkrBgEEAYI3FAIEDB4KAFMAdQBiAEMAQTAOBgNVHQ8BAf8EBAMCAYYwDwYD
VR0TAQH/BAUwAwEB/zAfBgNVHSMEGDAWgBRo6OQnLNNVa71VtllYAVRPmw8LQjCB
2AYDVR0fBIHQMIHNMIHKoIHHoIHEhoHBbGRhcDovLy9DTj1uZXctV0lOLU9WQlNB
NElFU0NBLUNBLENOPVdJTi1PVkJTQTRJRVNDQSxDTj1DRFAsQ049UHVibGljJTIw
S2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz1u
ZXcsREM9Y29tP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RD
bGFzcz1jUkxEaXN0cmlidXRpb25Qb2ludDCBxAYIKwYBBQUHAQEEgbcwgbQwgbEG
CCsGAQUFBzAChoGkbGRhcDovLy9DTj1uZXctV0lOLU9WQlNBNElFU0NBLUNBLENO
```

```
PUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1D
b25maWd1cmF0aW9uLERDPW5ldyxEQz1jb20/Y0FDZXJ0aWZpY2F0ZT9iYXNlP29i
amVjdENsYXNzPWNlcnRpZmljYXRpb25BdXRob3JpdHkwDQYJKoZIhvcNAQEFBQAD
ggEBAE8IWaRFEqrrwMHNaJunoomON2rdBWRNAMlJhKdIzi49J/9Yy9IlOGF+l0wR
Q5TeKFYIcWxBj5ltlYVWVdB+9YtTKsoEoq7/MeSg/c5KuprJhugqN3OU6zCqU4vq
rS1UHNnYkOJiSdOjkOdNeT9EG2YUqiDPr6CqIUcdU4+e36LdtQZW0TlIko+0z/be
bwIgtmxzkhlyDU711SuKmyz3uRrKq1CWhiIhSaOq4yYFQ0iw6TmFFKJGZ1KnjOrA
AwHhf8QvBBJhPMOwncWGL6DLFb7md2lE2YBu+zcVPGLdXYm0Xgk8lXsE22bRJYJU
gyHqA2enmHAmJequlUFoSH9apKU=
-----END CERTIFICATE-----
Syslog Certificate pasted successfully.
Server /cimc/log/server #
```

- この例では、リモート Syslog 証明書がサーバーに存在し、セキュアなリモート sylog がサーバーで有効になっていることが表示されます。

```
Server # scope cimc
Server /cimc # scope log
Server /cimc/log # scope server
Server /cimc/log/server # show detail
    Syslog Server 1:
    Syslog Server Address: 10.10.10.10
    Syslog Server Port: 514
    Enabled: yes
    Secure Enabled: yes
    Syslog Server protocol: udp
    Certificate Exists: yes
Server /cimc/log/server #
```

リモート Syslog 証明書の削除

始める前に

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 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 # **scope server{1|2}**

2つのリモート Syslog サーバープロファイルのいずれかを選択し、選択したサーバーのリモート Syslog 証明書を削除するためのコマンド モードを開始します。

ステップ 4 Server /cimc/log/server # **show detail**

サーバーの詳細を表示し、選択したサーバーにリモート Syslog 証明書が存在することを確認します。

ステップ 5 Server /cimc/log/server # **delete-client-certificate**

確認プロンプトで y と入力して、選択したサーバーからリモート Syslog 証明書を削除します。

ステップ 6 Server /cimc/log/server # **show detail**

サーバーの詳細を表示し、選択したサーバーでリモート Syslog 証明書が使用できないことを確認します。

例

- この例では、サーバー上にリモート Syslog 証明書が存在することが表示されます。

```
Server # scope cimc
Server /cimc # scope log
Server /cimc/log # scope server
Server /cimc/log/server # show detail
Server /cimc/log/server # commit
    Syslog Server 1:
    Syslog Server Address: 10.10.10.10
    Syslog Server Port: 514
    Enabled: yes
    Secure Enabled: yes
    Syslog Server protocol: udp
    Certificate Exists: yes
Server /cimc/log/server #
```

- この例では、サーバー上のリモート Syslog 証明書を削除します。

```
Server # scope cimc
Server /cimc # scope log
Server /cimc/log # scope server
Server /cimc/log/server # show detail
    Syslog Server 1:
    Syslog Server Address: 10.10.10.10
    Syslog Server Port: 514
    Enabled: yes
    Secure Enabled: yes
    Syslog Server protocol: udp
    Certificate Exists: yes
Server /cimc/log/server # delete-client-certificate
You are going to delete the Syslog Certificate.
Are you sure you want to proceed and delete the Syslog Certificate? [y|N]y
Syslog Certificate deleted successfully
Server /cimc/log/server #
```

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、イベントのシビラティ（重大度）、およびイベントの説明を表示します。 **detail** キーワードを指定すると、表形式ではなくリスト形式で情報が表示されます。

例

次に、システム イベント ログを表示する例を示します。

```
Server# scope sel
Server /sel # show entries
Time                 Severity      Description
-------------------- ------------- ----------------------------------------
[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

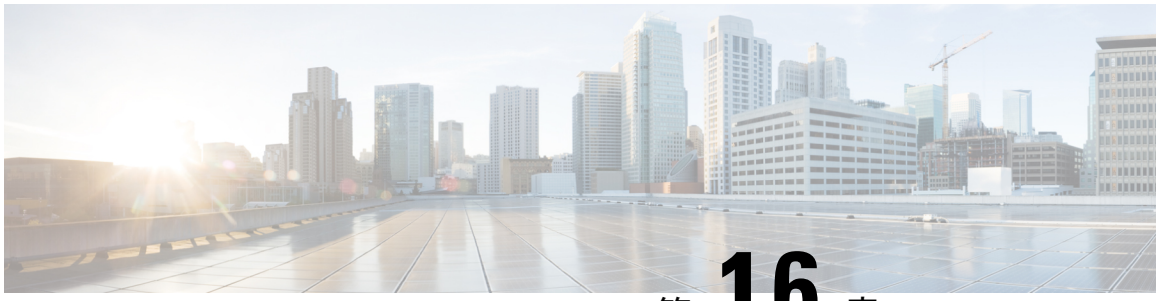
手順

	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。

例

次に、システム イベント ログをクリアする例を示します。

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



第 16 章

サーバー ユーティリティ

この章は、次の内容で構成されています。

スマート アクセス USB の有効化または無効化

スマート アクセス USB 機能を有効にすると、フロント パネルの USB デバイスはホスト オペレーティング システムから切断され、Cisco IMC に接続します。スマート アクセス USB 機能を有効にした後は、フロント パネルの USB デバイスを使用して、テクニカル サポート データをエクスポート、Cisco IMC 構成をインポートまたはエクスポート、あるいは Cisco IMC、BIOS および VIC のファームウェアを更新できます。

スマート アクセス USB でサポートされるファイル システムは次のとおりです。

- EXT2

- EXT3
- EXT4
- FAT 32
- FAT 16
- DoS

（注） 巨大ファイル サポートは BMC ではサポートされません。EXT4 ファイルシステムの場合、巨大ファイルのサポートをオフにする必要があります。

始める前に

このタスクを実行するには、admin 権限でログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope smart-access-usb**	スマート アクセス USB コマンド モードを開始します。
ステップ 3	Server /cimc/smart-access-usb # **set enabled** { *yes* | *no* }	**[set enabled yes]** は、スマート アクセス USB を有効にします。**[set enabled no]** は、スマート アクセス USB を無効にします。 スマート アクセス USB 機能を有効にすると、フロント パネルの USB デバイスはホスト オペレーティング システムから切断されます。スマート アクセス USB 機能を無効にすると、フロント パネルの USB デバイスは CIMC から切断されます。
ステップ 4	Server /cimc/smart-access-usb *# **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 /cimc/smart-access-usb # **show detail**	スマート アクセス USB のプロパティが表示されます。

例

次に、スマート アクセス USB を有効にする例を示します。

```
Server# scope cimc
Server /cimc # scope smart-access-usb
Server /cimc/smart-access-usb # set enabled yes
Enabling smart-access-usb feature will
disconnect front panel USB devices from
host operating system.
Do you wish to continue? [y/N] y
Server /cimc/smart-access-usb *# commit
Server /cimc/smart-access-usb # show detail
   Enabled: yes
   Storage Device attached: no
Server /cimc/smart-access-usb #
```

次に、スマート アクセス USB を無効にする例を示します。

```
Server# scope cimc
Server /cimc # scope smart-access-usb
Server /cimc/smart-access-usb # set enabled no
Disabling smart-access-usb feature will
disconnect front panel USB devices from CIMC.
Do you wish to continue? [y/N] y
Server /cimc/smart-access-usb *# commit
Server /cimc/smart-access-usb # show detail
   Enabled: no
   Storage Device attached: no
Server /cimc/smart-access-usb #
```

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 # **scope tech-support**	テクニカル サポート コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	Server /cimc/tech-support # **set remote-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 # **set remote-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 # **set remote-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

	コマンドまたはアクション	目的
		（注） Cisco UCS C シリーズ サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバー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、リモートサーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモートサーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[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 6	Server /cimc/tech-support # **set remote-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 # **set remote-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。

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

例

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 #
```

次のタスク

生成されたレポート ファイルを Cisco TAC に提供します。

フロント パネルの USB デバイスへのテクニカル サポート データのエクスポート

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

重要

- スマート USB オプションが有効であり、フロント パネルに USB デバイスが接続されていることを確認します。
- 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 # **scope tech-support**	テクニカル サポート コマンド モードを開始します。
ステップ 3	Server /cimc/tech-support # **scope fp-usb**	USB モードを開始します。
ステップ 4	Server /cimc/tech-support /fp-usb # **start** *filename*	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 USB デバイスに転送します。ファイル名を指定しない場合は、デフォルトのファイル名が使用されます。

例

この例は、テクニカル サポート データ ファイルを作成し、フロント パネルに接続されている USB デバイスにそのファイルを転送します。

```
Server# scope cimc
Server /cimc # scope tech-support
Server /cimc/tech-support # scope fp-usb
Server /cimc/tech-support/fp-usb # start techsupportUSB.tar.gz
Tech Support collection started.

Server /cimc/tech-support/fp-usb # show detail

Tech Support:
  Path(on USB device): techsupportUSB.tar.gz
  Progress(%): 6
  Status: COLLECTING

Server /cimc/tech-support/fp-usb #
```

次のタスク

生成されたレポート ファイルを Cisco TAC に提供します。

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# **scope cimc**	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 が再起動します。

例

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

手順

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

例

次に、BIOS CMOS メモリをクリアする例を示します。

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

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

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。
- サーバー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（お使いのサーバーモデルでサポートされている場合）。手順については、お使いのサーバーモデルに対応した『Cisco UCS Server Installation and Service Guide』を参照してください。

始める前に

- 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ーの電源が再投入されるため、サーバーのダウンタイムをスケジュール設定します。

手順

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

例

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
```

次のタスク

電源を再投入するか、サーバーをリセットします。

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、ユーザーが設定可能なすべての設定がリセットされます。

この手順は、通常のサーバー メンテナンスには含まれません。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 モードに設定され、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# **scope cimc**	Cisco IMC 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 /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 が有効になっている。Telnet はディセーブルになります。
- Cisco IMC GUI へのアクセス用に、SSH が有効になっている。
- 単一のユーザ アカウントが存在している（ユーザ名は **admin** 、パスワードは **password** です）。
- 管理ポートで DHCP がイネーブルになっている。
- 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。

例

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]y
Server /cimc #
```

出荷時の初期状態へのリセット

工場出荷時のデフォルトにリセットしても、KMIP 関連情報はリセットされません。KMIP 設定をリセットするにはさまざまなKMIPスコープから個別の復元コマンドを実行する必要があります。

重要 VICアダプタを他の世代のCシリーズサーバ（たとえばM4）からM5世代のCシリーズサーバまたはM5サーバから他の世代のサーバに移動する際は、アダプタを出荷時のデフォルトにリセットする必要があります。

始める前に

このタスクを実行するには、admin 権限でログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **factory-default** {**all** | **bmc** | **storage** | **vic** }	工場出荷時のデフォルトにリセットすることを選択したコンポーネントによっては、そのコンポーネントの設定パラメータが工場出荷時のデフォルトに復元されます。次のいずれかのコンポーネントを選択できます。 • **all**：ストレージ コントローラ、VIC、および BMC の設定を工場出荷時のデフォルトにリセットします。 • **bmc**：BMC の設定を工場出荷時のデフォルトにリセットします。 • **storage**：ストレージ コントローラの設定を工場出荷時のデフォルトにリセットします。 • **vic**：VIC の設定を工場出荷時のデフォルトにリセットします。 確認プロンプトで **y** を入力して選択したコンポーネントをデフォルトにリセットします。
ステップ 3	（任意） Server /chassis # **show factory-reset-status**	工場出荷時の状態が表示されます。

例

次に、工場出荷時のデフォルトにリセットする例を示します。

```
Server# scope chassis
Server /chassis # factory-default vic
his factory-default operation does the following on these components without any back-up:
VIC - all user configured data will deleted and controller properties reset to default
values
(Host power-cycle is required for it to be effective)
Storage - all user configured data (including OS VD/drive if any) will be deleted,
```

```
controller properties and zoning settings reset to default values (Host power-cycle is
required for it to be effective)
BMC -  all Server BMC configuration reset to factory default values
CMC - all user configured data (including admin password) will be deleted and CMC settings
 reset to default values
Continue?[y|N]y
factory-default for ' vic' started. Please check the status using "show
factory-reset-status".
Server /chassis # show factory-reset-status
Storage                           VIC                               BMC
--------------------------------- --------------------------------- ----------
NA                                Pending                           NA
C240-FCH1828V0PN /chassis #
Server /chassis #
```

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 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）
- 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 の設定をエクスポートしないでください。
- Cisco IMC 構成をフロント パネルの USB デバイスにエクスポートする場合は、スマート アクセス USB オプションが有効であることを確認します。
- セキュリティ上の理由から、この操作でユーザー アカウントやサーバー証明書をエクスポートしないでください。

始める前に

バックアップ リモート サーバーの 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**	コンフィギュレーション ファイルは、前面パネルの USB デバイスに指定され

	コマンドまたはアクション	目的
		たパスおよびファイル名でエクスポートされます。
ステップ 3	Server /cimc/import-export # **export-config** *protocol ip-address path-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。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 サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバー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 サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[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 /cimc/import-export # **export-config usb** *path-and-filename*	構成データを接続している USB にエクスポートします。
ステップ 5	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。

例

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。
- Cisco IMC 設定をフロント パネルの USB デバイス経由でインポートする場合は、スマート アクセス USB オプションが有効であることを確認します。

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。

	コマンドまたはアクション	目的
ステップ 2	Server /cimc # **scope import-export**	import-export コマンドモードを開始します。
ステップ 3	Server /cimc/import-export # **import-config** *protocol ip-address path-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。リモートサーバー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 サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバー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 サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[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 /cimc/import-export # **import-config usb** *path and filename*	設定ファイルは、前面パネルの USB デバイスに指定されたパスおよびファイル名でインポートされます。
ステップ 5	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。

例

次に、Cisco IMC 設定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 #
```

VIC アダプタ設定のエクスポート

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、VIC アダプタ設定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 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 # **export-all-adapters** *protocol ip-address path-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

	コマンドまたはアクション	目的
		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。リモートサーバー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 サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバー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 サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[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。

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

例

次に、VIC アダプタ設定をエクスポートする例を示します。

```
Server# scope chassis
Server /chassis # export-all-adapters tftp 10.10.10.10 /ucs/backups/cfdes.xml
Do you wish to continue? [y/N]y
Username: draf
Password:
Export config for all Adapters is triggered. Please check status using show
adapter-ie-status detail.
Server /chassis # show adapter-ie-status detail
All VIC Import Export:
    Operation: ALL-VIC-EXPORT
    Status: COMPLETED
    Error Code: 100 (No Error)
    Diagnostic Message: NONE
Server /chassis #
```

VIC 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、VIC アダプタ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# **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 # **import-all-adapters** *protocol ip-address path-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 サーバー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 サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバー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 サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[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 3	ユーザ名とパスワードを入力します。	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。

例

次に、VIC 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 # import-all-adapters tftp 10.10.10.10 /ucs/backups/cfdes.xml
Do you wish to continue? [y/N]y
Username: gdts
Password:
Import config for all Adapters is triggered. Please check status using show
adapter-ie-status detail.
Server /chassis # show adapter-ie-status detail
All VIC Import Export:
    Operation: ALL-VIC-IMPORT
```

```
    Status: COMPLETED
    Error Code: 100 (No Error)
    Diagnostic Message: NONE
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 # **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 # **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	（任意） Server /chassis # **show-banner**	追加したバナーが表示されます。

例

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 # **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 # **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	（任意） Server /chassis # **show-banner**	追加したバナーが表示されます。

例

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 #
```

セキュアなアダプタ更新の有効化

始める前に

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# **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 adapter-secure-update**	セキュアなアダプタ更新コマンド モードを開始します。
ステップ 3	Server /cimc/adapter-secure-update # **enable-security-version-check** {**yes** | **no**}	プロンプトで **yes** と入力します。 （注） プロンプトで、**no** を入力した場合は、セキュリティで保護されたアダプタの更新は無効になります。
ステップ 4	（任意） Server /cimc/adapter-secure-update # **enable-security-version-check status**	セキュア更新のステータスを表示します。

例

次に、アダプタのセキュア更新をイネーブルにする例を示します。

```
Server# scope cimc
Server /cimc # scope adapter-secure-update
Server /cimc/adapter-secure-update # enable-security-version-check yes
Server /cimc/adapter-secure-update # enable-security-version-check status
enable-security-version-check: Enabled
Server /cimc/adapter-secure-update #
```

インベントリの詳細のダウンロードと表示

Web UI から次のインベントリの詳細を取得し、ファイルに保存できます。

- システムのプロパティ
- CPU 情報
- 電源装置インベントリ
- PCI アダプタ カード
- メモリの詳細
- トラステッド プラットフォーム モジュール情報
- ディスク情報
- ネットワーク インターフェイス カード
- ストレージ アダプタ カード
- 仮想インターフェイス カード
- ファン ステータス
- Flex フラッシュ カード
- BBU ステータス

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 # **inventory-refresh**	データ収集アクティビティを開始し、ファイルにデータを保存します。
ステップ 3	Server /chassis # **inventory-all**	インベントリ情報を表示します。

例

次に、インベントリの詳細とインベントリ コレクションの状態を表示する例を示します。

```
Server# scope chassis
Server /chassis #inventory-refresh

Inventory data collection started.

Server /chassis #inventory-all

Hardware Inventory Information:
Status: IN-PROGRESS
Progress(%): 5
...
Progress(%): 50
sysProductName: UCS C240 M3S
sysProductID: UCSC-C240-M3S
sysSerialNum: FCH1925V21U
...
CPU
id: 1
SocketDesignation: CPU1
ProcessorManufacturer: Intel(R) Corporation
ProcessorFamily: Xeon
ThreadCount: 4
Server /chassis #
```

デバイス コネクタ ファームウェアの更新とアクティベート

この機能は、いくつかの C シリーズ サーバのみで使用可能です。

始める前に

このアクションを実行するには、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 cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope device-connector**	デバイス コネクタ コマンド モードを開始します。
ステップ 3	Server /cimc/device-connector # **update-and-activate** *protocol IP Address path*	プロトコル、リモート サーバーの IP アドレス、サーバー上のファームウェア

	コマンドまたはアクション	目的
		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 サーバーでは、リモート サーバーからファームウェアを更新したときの、サーバー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 サーバのタイプとして SCP または SFTP を選択している場合のみ利用できます。 このアクションを実行する際にリモート サーバのタイプとして SCP または SFTP を選択すると、メッセージ「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」が表示されます。サーバのフィンガープリントの真偽に応じて、[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	（任意） Server /cimc/device-connector # **show detail**	アップデートのステータスを表示します。

例

この例では、デバイス コネクタのファームウェアをアップグレードし、アクティブにする方法を示します。

```
Server # scope cimc
Server /cimc # scope device-connector
Server /cimc/device-connector # update-and-activate tftp 10.10.10.10
c240-m5-cimc.4.0.1.227-cloud-connector.bin
Device connector firmware update initialized.
Please check the status using "show detail".
Server /cimc/device-connector # show detail
Device Connector Information:
    Update Stage: DOWNLOAD
    Update Progress: 5
    DC FW Version: 1.0.9-343
Server /cimc/device-connector # show detail
Device Connector Information:
    Update Stage: INSTALL
    Update Progress: 90
    DC FW Version:
Server /cimc/device-connector # show detail
Device Connector Information:
    Update Stage: NONE
    Update Progress: 100
Server /cimc/device-connector #
```

PCIe スイッチの回復

スイッチ上のファームウェアが破損した場合、このオプションを使用してスイッチを回復できます。

始める前に

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

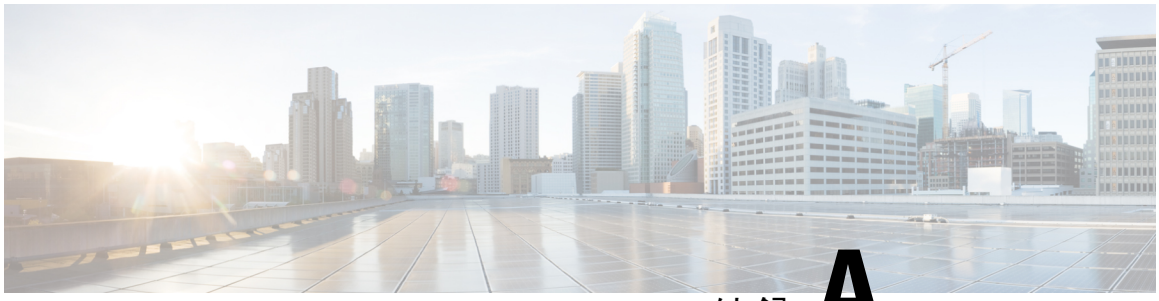
手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope 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 nvmeadapter**	NVMe アダプタおよび PCIe スイッチの名前を表示します。
ステップ 3	Server /chassis # **recover-pcie-switch** *PCIe Switch Name*	ホストの再起動プロンプトで **y** と入力します。選択された PCIe スイッチを回復します。

例

この例では、PCIe スイッチを回復する方法を示します。

```
Server # scope chassis
Server /chassis # show nvmeadapter
PCI Slot
----------------------------
PCIe-Switch
Server /chassis/persistent-memory # recover-pcie-switch PCIe-Switch
Host will be powered on for this operation.
Continue?[y|N]y
Server /chassis #
```



付録 A

サーバー モデル別 BIOS パラメータ

C220 M7 および C240 M7 サーバー

I/O Tab

Note BIOS parameters listed in this tab may vary depending on the server.

Table 3: BIOS Parameters in I/O Tab

Name	Description
Reboot Host Immediately check box	If the Reboot Host Immediately check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise the changes are saved until the server is manually rebooted.

サーバー モデル別 BIOS パラメータ

Name	Description
MLOM OptionROM drop-down list **set PcieSlotMLOMOptionROM**	This options allows you to control the Option ROM execution of the PCIe adapter connected to the MLOM slot. This can be one of the following: • **Disabled**—Does not execute Option ROM of the PCIe adapter connected to the MLOM slot. • **Enabled**—Executes Option ROM of the PCIe adapter connected to the MLOM slot.
MLOM Link Speed drop-down list **set PcieSlotMLOMLinkSpeed**	This option allows you to restrict the maximum speed of an adapter card installed in PCIe MLOM slot. This can be one of the following: • **Disabled**—The maximum speed is not restricted. • **Auto**—System selects the maximum speed allowed. • **GEN1**—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **GEN2**—5GT/s is the maximum speed allowed. • **GEN3**—8GT/s is the maximum speed allowed. • **GEN4**—16GT/s is the maximum speed allowed.
PCIe Slot*n* OptionROM drop-down list **set PcieSlot*n*OptionROM**	Whether the server can use the Option ROMs present in the PCIe card slot designated by *n*. This can be one of the following: • **Disabled**—Option ROM for slot *n* is not available. • **Enabled**—Option ROM for slot *n* is available.

Name	Description
PCIe Slot*n* Link Speed drop-down list **set PcieSlot*n*LinkSpeed**	System IO Controller *n* (SIOCn) add-on slot (designated by *n*) link speed. This can be one of the following: • **Disabled**—Slot is disabled, and the card is not enumerated. • **Auto**— The default link speed. Link speed is automatically assigned. • **GEN1**—Link speed can reach up to first generation. • **GEN2**—Link speed can reach up to second generation. • **GEN3**—Link speed can reach up to third generation.
MRAID OptionROM drop-down list **set PcieSlotMRAIDOptionROM**	This options allows you to control the Option ROM execution of the MRAID PCIe adapter connected. This can be one of the following: • **Disabled**—Does not execute Option ROM of the MRAID PCIe adapter. • **Enabled**—Executes Option ROM of the MRAID PCIe adapter.
MRAID Link Speed drop-down list **set PcieSlotMRAIDLinkSpeed**	This option allows you to restrict the maximum speed of an MRAID adapter card installed. This can be one of the following: • **Disabled**—The maximum speed is not restricted. • **Auto**—System selects the maximum speed allowed. • **GEN1**—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **GEN2**—5GT/s is the maximum speed allowed. • **GEN3**—8GT/s is the maximum speed allowed. • **GEN4**—16GT/s is the maximum speed allowed.

サーバー モデル別 BIOS パラメータ

Name	Description
Front NVME-*n* OptionROM drop-down list **set PcieSlotFrontNvme*n*OptionROM**	This options allows you to control the Option ROM execution of the PCIe adapter connected to the SSD:NVMe slot *n*. This can be one of the following: • **Disabled**—Does not execute Option ROM of the PCIe adapter connected to the SSD:NVMe1 slot. • **Enabled**—Executes Option ROM of the PCIe adapter connected to the SSD:NVMe1 slot
Front NVME-*n* Link Speed drop-down list **set PcieSlotFrontNvme*n*LinkSpeed**	Link speed for NVMe front slot designated by slot *n*. This can be one of the following: • **Disabled**—Slot is disabled, and the card is not enumerated. • **Auto**—The default link speed. Link speed is automatically assigned. • **GEN1**—Link speed can reach up to first generation. • **GEN2**—Link speed can reach up to second generation. • **GEN3**—Link speed can reach up to third generation. • **GEN4**—Link speed can reach up to fourth generation.
PCIe Slot MSTOR RAID OptionROM drop-down list **set PcieSlotMSTORRAIDOptionROM**	Whether the server can use the Option ROMs present in the PCIe MSTOR RAID. This can be one of the following: • **Disabled**—Option ROM is not available. • **Enabled**—Option ROM is available.
Intel VTD Coherency Support drop-down list **set CoherencySupport**	Whether the processor supports Intel VT-d Coherency. This can be one of the following: • **Disabled**—The processor does not support coherency. • **Enabled**—The processor uses VT-d Coherency as required.

Name	Description
Intel VT for Directed IO drop-down list **set IntelVTD**	Whether the processor uses Intel Virtualization Technology (VT), which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following: • **Disabled**—The processor does not permit virtualization. • **Enabled**—The processor allows multiple operating systems in independent partitions. **Note** If you change this option, you must power cycle the server before the setting takes effect.
VMD Enable drop-down list **set VMDenable**	Intel Volume Management Device (VMD) is for PCIe NVMe SSDs that provides hardware logic to manage and aggregate NVMe SSDs. This can be one the following: • **Enabled**— Enables benefits like robust surprise hot-plug, status LED management. • **Disabled**— Disables the feature. Default value: **Disabled**. Refer Intel® Virtual RAID on CPU User Guide to configure VMD. **Note** VROC is not supported with Cisco UCS C-Series M7 servers.
PCIe RAS Support drop-down list **set PCIeRASSupport**	Whether PCIe RAS Support is available on the PCIe slot. This can be one of the following: • **Disabled**—PCIe RAS is not available on the slot. • **Enabled**—PCIe RAS is available on port.
USB Port Rear drop-down list **set UsbPortRear**	Whether the rear panel USB devices are enabled or disabled. This can be one of the following • **Disabled**— Disables the rear panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled**— Enables the rear panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.

サーバー モデル別 BIOS パラメータ

Name	Description
VGA Priority drop-down list **set VgaPriority**	Allows you to set the priority for VGA graphics devices if multiple VGA devices are found in the system. This can be one of the following: • **OnBoard**—Priority is given to the onboard VGA device. BIOS post screen and OS boot are driven through the onboard VGA port. • **OffBoard**—Priority is given to the PCIE Graphics adapter. BIOS post screen and OS boot are driven through the external graphics adapter port. • **OnBoardDisabled**—Priority is given to the PCIe Graphics adapter, and the onboard VGA device is disabled. The vKVM does not function when the onboard VGA is disabled.
IPV6 PXE Support drop-down list **set IPV6PXE**	Enables or disables IPv6 support for PXE. This can be one of the following • **disabled**—IPv6 PXE support is not available. • **enabled**—IPv6 PXE support is always available.
PCIe PLL SSC drop-down list **set PciePllSsc**	Enable this feature to reduce EMI interference by down spreading clock 0.5%. Disable this feature to centralize the clock without spreading. This can be one of the following: • **auto**—EMI interference is auto adjusted. **Disabled**—EMI interference is auto adjusted. • **ZeroPointFive**—EMI interference is reduced by down spreading the clock 0.5%.
Network Stack drop-down list **set NetworkStack**	This option allows you to monitor IPv6 and IPv4. This can be one of the following • **disabled**—Network Stack support is not available. **Note** When disabled, the value set for **IPV4 PXE Support** does not impact the system. • **enabled**—Network Stack support is always available.

Name	Description
IPV4 PXE Support drop-down list **set IPV4PXE**	Enables or disables IPv4 support for PXE. This can be one of the following • **disabled**—IPv4 PXE support is not available. • **enabled**—IPv4 PXE support is always available.
External SSC enable drop-down list **set EnableClockSpreadSpec**	This option allows you to reduce the EMI of your motherboard by modulating the signals it generates so that the spikes are reduced to flatter curves. This can be one of the following: • **Disabled**—Clock Spread Spectrum support is not available. • **Enabled**—Clock Spread Spectrum support is always available.
IPV4 HTTP Support drop-down list **set IPV4HTTP**	Enables or disables IPv4 support for HTTP. This can be one of the following: • **disabled**—IPv4 HTTP support is not available. • **enabled**—IPv4 HTTP support is always available.
IIO eDPC Support drop-down list **set EdpEn**	eDPC allows a downstream link to be disabled after an uncorrectable error, making recovery possible in a controlled and robust manner. This can be one of the following: • Disabled—eDPC support is disabled. • On Fatal Error—eDPC is enabled only for fatal errors. • On Fatal and Non-Fatal Errors—eDPC is enabled for both fatal and non-fatal errors.
IPV6 HTTP Support drop-down list **set IPV6HTTP**	Enables or disables IPv6 support for HTTP. This can be one of the following: • **disabled**—IPv6 HTTP support is not available. • **enabled**—IPv6 HTTP support is always available.

[Server Management] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *4 : [*サーバ管理（***Server Management***）*]* タブの ***BIOS*** パラメータ

名前	説明
[ホストを即座リブート（**Reboot Host Immediately**）**]** チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバー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、変更内容はサーバーが手動でリブートされるまで保存されます。
[OS ブート ウォッチドッグ タイマー ポリシー（OS Boot Watchdog Timer Policy）] ドロップダウン リスト **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。 • [電源オフ（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、サーバーはリセットされます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にする場合にのみ適用されます。
[FRB 2 タイマー（FRB 2 Timer）] ドロップダウン リスト **set FRB-2**	POST 中にシステムがハングした場合に、システムを回復するために Cisco IMC によって FRB2 タイマーが使用されるかどうか。次のいずれかになります。 • [無効（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 ウォッチドッグ タイマー（OS Watchdog Timer）] ドロップダウン リスト **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]：サーバーのブートにかかる時間をトラッキングするためにウォッチドッグ タイマーは使用されません。 • [有効（enabled）]：サーバーがブートにかかる時間をウォッチドッグ タイマーで追跡します。サーバーのブートが [OS ブート ウォッチドッグ タイマー タイムアウト（OS Boot Watchdog Timer Timeout）] フィールドで指定された時間内に完了しない場合は、Cisco IMC によってエラーがログに記録され、[OS ブート ウォッチドッグ ポリシー（OS Boot Watchdog Policy）] フィールドで指定されたアクションが実行されます。
[OS ブート ウォッチドッグ タイマー タイムアウト（OS Watchdog Timer Timeout）] ドロップダウン リスト **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 分（5 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [10 分（10 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [15 分（15 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [20 分（20 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にした場合にのみ適用されます。

名前	説明
[ボー レート（Baud Rate）] ドロップダウン リスト **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。[コンソール リダイレクション（Console Redirection）] を無効にした場合、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]：9,600 ボー レートが使用されます。 • [19.2k]：19,200 ボー レートが使用されます。 • [38.4k]：38,400 ボー レートが使用されます。 • [57.6k]：57,600 ボー レートが使用されます。 • [115.2k]：115,200 ボー レートが使用されます。 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。
[フロー制御（Flow Control）] ドロップダウン リスト **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を設定します。送信要求/クリア ツー センド（RTS/CTS）を使用すると、隠れた端末の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。 • [なし（None）]：フロー制御は使用されません。 • [RTS/CTS]：RTS/CTS がフロー制御に使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。

名前	説明
[コンソール リダイレクション（Console Redirection）] ドロップダウン リスト **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 リダイレクションで使用できるようにします。OS起動後は、コンソールのリダイレクトが関係なくなります。次のいずれかになります。 • **[COM 0]**：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有効にします。 • **[COM 1]**：POST 中にシリアル ポート B でコンソール リダイレクションを有効にします。 • [Disabled]：POST 中にコンソール リダイレクションは発生しません。
[ターミナル タイプ（Terminal Type）] ドロップダウン リスト **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。
[PCIe Slots CDN コントロール（PCIe Slots CDN Control）] ドロップダウンリスト **set PcieSlotsCdnEnable**	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。 • [無効（Disabled）]：VIC カードに対する CDN サポートは無効です。 • [有効（Enabled）]：VIC カードの CDN サポートが有効になります。

名前	説明
[CDN コントロール（CDN Control）] ドロップダウン リスト **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。 • [無効（Disabled）]：VIC カードに対する CDN サポートは無効です。 • [有効（Enabled）]：VIC カードの CDN サポートが有効になります。
[OptionROM起動最適化（OptionROM Launch Optimization）]	このオプションが [有効（Enabled）] の場合、ブート順序のポリシーに存在するコントローラにのみ OptionROMs が起動されます。 （注） オンボードストレージコントローラ、Emulex FC アダプタおよび GPU コントローラなどのいくつかのコントローラについて、ブート順序のポリシーに含まれていなくても、OptionROM が起動されます。 このオプションが [無効（Disabled）] の場合、すべての OptionROMs が起動されます。 デフォルト値：[有効（Enabled）]

名前	説明
適応型メモリ トレーニング	このオプションを[有効（Enabled）]にすると、次のようになります。 メモリ トレーニングは毎回のブートでは実行されず、BIOSは、保存されたメモリ トレーニングの結果を毎回のリブートで使用します。 毎回のブートでメモリ トレーニングが実行されるいくつかの例外には、次のものがあります。 BIOS の更新、CMOS のリセット、CPU やメモリの設定変更、SPD または実行時の修正不可能なエラー、または、前回のブートから 24 時間以上経過している場合。 このオプションが [無効（Disabled）] の場合、毎回のブートでメモリ トレーニングが行われます。 デフォルト値：[有効（Enabled）]。 （注） [高速ブート（Fast Boot）] オプションを無効にするには、エンドユーザーは次のトークンを下記の説明のとおりに設定する必要があります。 [適応型メモリ トレーニング（Adaptive Memory Training）]を [無効（Disabled）] に [BIOS Techlogレベル（BIOS Techlog level）] を [標準（Normal）] に [OptionROM起動最適化（OptionROM Launch Optimization）] を [無効（Disabled）] に

名前	説明
[BIOS Techlogレベル（BIOS Techlog Level）]	このオプションは、**BIOS tech ログファイル**のメッセージのタイプを示します。 ログファイルには、次のタイプのいずれかを指定できます。 • [最小（Minimum）]：重要なメッセージがログファイルに表示されます。 • [標準（Normal）]：警告およびロードメッセージがログファイルに表示されます。 • [最大（Maximum）]：標準に加え、情報関連のメッセージがログファイルに表示されます。 デフォルト値：[最小（Minimum）] （注） このオプションは、主に、内部のデバッグを目としています。

[セキュリティ（Security）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *5*：*[*セキュリティ管理（*Security Management*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバー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、変更内容はサーバーが手動でリブートされるまで保存されます。

名前	説明
[トラステッド プラットフォーム モジュール状態（Trusted Platform Module State）] ドロップダウン リスト **set TPMControl**	信頼されたプラットフォーム モジュール（TPM）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。次のいずれかになります。 • [Disabled]：サーバーは TPM を使用しません。 • [有効（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ください。
セキュリティ デバイス サポート（Security Device Support）] ドロップダウン リスト **set TpmSupport**	セキュリティ デバイスのサポートを有効にするには、TPM サポートを有効にする必要があります。次のいずれかになります。 • **[無効（Disabled）]**：機能は無効です。 • **[有効（Enabled）]**：TPM が有効な場合、機能が有効になります。
[SHA-256 PCR バンク（SHA-256 PCR Bank）] ドロップダウン リスト **set SHA256PCRBank**	BIOS が測定を実行しているときに OS で使用可能な PCR バンクです。 • **[無効（Disabled）]**：SHA256 PCR バンクは BIOS で使用できません。 • **[有効（Enabled）]**：SHA256 PCR バンクは BIOS で使用できます。
[SHA-1 PCR バンク（SHA-1 PCR Bank）] ドロップダウン リスト **set SHA1PCRBank**	BIOS が測定を実行しているときに OS で使用可能な PCR バンクです。 • **[無効（Disabled）]**：SHA-1 PCR バンクは BIOS で使用できません。 • **[有効（Enabled）]**：SHA-1 PCR バンクは BIOS で使用できます。

サーバー モデル別 BIOS パラメータ

名前	説明
[TPM の最小限の物理的存在（TPM Minimal Physical Presence）] ドロップダウン リスト	このトークンを使用すると、TPM に推奨される Microsoft のデフォルト設定を適用できます。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[TPM 保留中の操作（TPM Pending Operation）] ドロップダウン リスト **set TPMPendingOperation**	トラステッド プラットフォーム モジュール（TPM）Pending Operation オプションを使用すると、保留中の操作のステータスを制御できます。次のいずれかになります。 • [None]：アクションなし。 • TpmClear：保留中の操作をクリアします。
[電源オン パスワード（Power On Password）] ドロップダウン リスト **set PowerOnPassword**	このトークンでは、F2 BIOS 設定を使用する前にBIOSパスワードを設定する必要があります。有効にすると、BIOS関数（IO設定、BIOSセットアップ、BIOSを使用したオペレーティング システムへのブート）にアクセスする前にパスワードの検証が必要になります。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[Intel Trusted Execution Technology サポート（Intel Trusted Execution Technology Support）] ドロップダウン リスト **set TXTSupport**	信頼されたプラットフォームモジュール(TPM)が 有効 である場合にのみ 有効 に設定できます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

名前	説明
[マルチキー トータル メモリ暗号化（Multikey Total Memory Encryption、MK-TME） ドロップダウン リスト **set EnableMktme**	MK-TME を使用すると、独自のキーを持つ 1 つの暗号化ドメインを複数持つことができます。異なるメモリ ページを異なるキーで暗号化できます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[トータル メモリ暗号化（Total Memory Encryption、TME）] ドロップダウン リスト **set EnableTme**	システムの物理メモリ全体を暗号化する機能を提供します。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SGX 工場出荷時リセット（SGX Factory Reset）] ドロップダウン リスト **set SgxFactoryReset**	その後の起動時にシステムが SGX の工場出荷時リセットを実行できるようにします。これにより、すべての登録データが削除されます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SWガード拡張（SW Guard Extensions、SGX）] ドロップダウン リスト **set EnableSgx**	ソフトウェア ガード拡張（SGX）機能を有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

名前	説明
[SGX QoS] ドロップダウン リスト **set SgxQoS**	SGX QoS を有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SGX パッケージ情報インバンド アクセス（SGX Pkg info In-Band Access）] ドロップダウン リスト **set SgxPackageInfoInBandAccess**	SGX パッケージ情報インバンドアクセスを有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SGX 書き込み有効（SGX Write Enable）] ドロップダウン リスト **set SgxLeWr**	SGX 書き込み機能を有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[所有者 EPOCH入力タイプ選択（Select Owner EPOCH input type）] ドロップダウン リスト **set EpochUpdate**	作成され、ロックされたメモリ領域に使用されるセキュリティ キーのシードを変更できます。次のいずれかになります。 • **SGX 所有者 EPOCH 有効化（SGX Owner EPOCH activated）]**：現在の入力タイプを変更しません。 • **[新しいランダム所有者 EPOCH に変更（Change to New Random Owner EPOCHs）]**：EPOCH をシステムが生成したランダムな数値に変更します。 • **[手動ユーザー定義所有者 EPOCH（Manual User Defined Owner EPOCHs）]**：EPOCH シードをユーザーが入力した 16 進値に変更します。

名前	説明
[SProcessor Epoch*n*] フィールド **set SgxEpoch0**	*n* で指定された EPOCH 番号の SGX EPOCH 所有者値を定義できます。
[SGX 自動 MP レジストレーション エージェント（SGX Auto MP Registration Agent）] ドロップダウン リスト **set SgxAutoRegistrationAgent**	レジストレーション エージェント サービスがプラットフォーム キーを保存できるようにします。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SGX PUBKEY HASH*n*] フィールド **set SgxLePubKeyHash*n***	ソフトウェア ガード拡張（SGX）の値を設定できます。この値の設定範囲は、以下のとおりです。 • SGX PUBKEY HASH0 — 7 ～ 0 の間 • SGX PUBKEY HASH1 — 15 ～ 8 の間 • SGX PUBKEY HASH2 — 23 ～ 16 の間 • SGX PUBKEY HASH3 — 31 ～ 24 の間
[CPU PA を 46 ビットに制限（LIMIT CPU PA to 46 Bits）] ドロップダウン リスト **set CpuPaLimit**	Intel ® VT-d でこのオプションを有効にして、2019 OS でブートできるようにします。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[DMA 制御オプトイン フラグ（DMA Control Opt-In Flag）] ドロップダウン リスト	DMA 制御オプトイン フラグ：このトークンを有効にすると、オペレーティング システムは入出力メモリ管理ユニット（IOMMU）を有効にして、悪意のあるデバイスからの DMA 攻撃を防ぐことができます。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

メモリ タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *6 : [*メモリ（***Memory***）*]* タブの ***BIOS*** パラメータ

名前	説明
[ホストを即座リブート（**Reboot Host Immediately**）**]** チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバー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、変更内容はサーバーが手動でリブートされるまで保存されます。

名前	説明
[メモリ RAS 構成の選択（Select Memory RAS configuration）] ドロップダウン リスト **set SelectMemoryRAS**	サーバーに対するメモリの信頼性、可用性、およびサービス性（RAS）の設定方法。次のいずれかになります。 • [最大パフォーマンス（Maximum Performance）]：システムのパフォーマンスが最適化されます。 • **ADDDC のスペアリング**: 適応可能な仮想ロックステップは、ADDDC モードをサポートするためにハードウェアおよびファームウェアで実装されるアルゴリズムです。選択すると、アルゴリズムがアクティブになるまでシステムのパフォーマンスが最適化されます。このアルゴリズムは、DRAM デバイスで障害が発生した場合にアクティブになります。アルゴリズムがアクティブになると、仮想ロックステップ リージョンがアクティブになり、実行時に障害が発生したリージョンが動的にマッピングされ、パフォーマンスへの影響はリージョン レベルで制限されます。 • [ミラー モード 1LM（Mirror Mode 1LM）]：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。 • **部分的なミラー モード 1LM**: 部分的な DIMM ミラーリングによって完全なミラーコピーを保持するのではなく、メモリ セルの特定の領域のミラーコピーが作成されます。部分的なミラーリングでは、部分的なミラー コピーの属性を使用して、メモリ マップにミラー領域が作成されます。最大 4 個の部分的なミラーを使用して、合計メモリ容量の最大 50% をミラーリングできます。

サーバー モデル別 BIOS パラメータ

名前	説明
[NUMA] ドロップダウン リスト **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]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[部分的なキャッシュ行の節約（Partial Cache Line Sparing）] ドロップダウンリスト **set PartialCacheLineSparing**	パーシャル キャッシュ ライン スペアリング (PCLS) は、メモリ コントローラーのエラー防止メカニズムです。PCLS は、メモリ アクセス中に置換できるように、ビットの欠陥のあるニブルの場所を、対応するデータ コンテンツとともにスペア ディレクトリに静的にエンコードします。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[ディスク タイプの選択 (Select Disk Type)] ドロップダウン リスト **set SelectPprType**	Cisco IMC は、指定された障害のある行から指定されたスペア行へのアクセスを永続的に再マッピングする、**ハード PPR**をサポートしています。 次のいずれかになります。 • **[ハード PPR (Hard PPR)]**: サポートは有効になっています。 （注） ハード PPR は、**[メモリ RAS 設定 (Memory RAS Configuration)]**が **[ADDDC スペア (ADDDC Sparing)]**に設定されている場合にのみ使用できます。他の RA の選択では、この設定を **Disabled** に設定する必要があります。 • **[無効 (Disabled)]**：サポートは無効になっています。

名前	説明
[BME DMA 移行 (BME DMA Mitigation)] ドロップダウン リスト **set BmeDmaMitigation**	不正な外部 DMA からの脅威を緩和する PCI BME ビットを無効にできます。次のいずれかになります。 • **[無効 (disabled)]**: PCI BME ビットは BIOS で無効になっています。 • **[有効 (Enabled)**: PCI BME ビットは BIOS で有効になっています。
[4 G 以上の復号化（Above 4G Decoding）] ドロップダウン リスト **set MemoryMappedIOAbove4GB**	4 GB 以上の MMIO を有効または無効にします。次のいずれかになります。 • [Disabled]：サーバーでは 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。 • [有効（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。
[Partial Memory Mirror Mode (部分メモリ ミラー モード)]ドロップダウン リスト **set PartialMirrorModeConfig**	部分的なメモリ サイズは、パーセンテージまたは GB 単位のいずれかです。次のいずれかになります。 • **割合**: 部分的なメモリのミラーはパーセンテージで定義されます。 • **値 (GB)**: 部分的なメモリ ミラーは GB で定義されます。 • **無効**: 部分的なメモリ ミラーが無効になります。

名前	説明
[DCPMM Firmware Downgrade (DCPMM ファームウェアのダウングレード)] ドロップダウン リスト **set DCPMMFirmwareDowngrade**	BIOS が DCPMM ファームウェアのダウングレードをサポートしているかどうか。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[部分ミラー *n* サイズ（GB）（Partial Mirror n Size in GB）] フィールド **set PartialMirrorValue1**	最初の部分メモリ ミラーのサイズ（GB）。 n = 1、2、または 3 0 ～ 65535 の整数を入力します。 （注） すべての部分的なミラーの合計メモリ サイズは、物理メモリ サイズの 50% を超えないようにする必要があります。
[部分的なミラー パーセンテージ (Partial Mirror percentage)] フィールド **set PartialMirrorPercent**	4GB を超えてミラーリングするメモリの割合。 0 ～ 60 の整数を入力します。
[メモリ サイズ制限 (GB) (Memory Size Limit in GB)] フィールド **set MemorySizeLimit**	このオプションを使用して、物理メモリの上限のサイズを GB 単位で減らします。 0 ～ 65535 の整数を入力します。
[NVM パフォーマンス設定 (NVM Performance Setting)] ドロップダウンリスト **set NvmdimmPerformConfig**	ワークロードの動作に応じて、NVM ベースラインのパフォーマンス設定を設定できます。 • **BW 最適化** • **遅延の最適化** • **バランス プロファイル**
[CR QoS] ドロップダウンリスト **set CRQoS**	CR QoS 調整を選択できます。 次のいずれかになります。 • **[モード 1（Mode 1）]**： • **[モード 2（Mode 2）]**： • **[モード 0（Mode 0）]**：**[CR QoS]** 機能は無効です。

名前	説明
[AD の Snoopy モード (Snoopy mode for AD)] ドロップダウン リスト **set SnoopyModeForAD**	新しい AD 固有の機能を有効にして、NUMA に最適化されていないワークロードからDDRT メモリへのディレクトリ更新を回避します。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[CR Fastgo Config] ドロップダウンリスト **set CrfastgoConfig**	CR QoS 設定プロファイルを選択できるようにします。 次のいずれかになります。 • **[最適化の有効化（Enable Optimization）]** • **[最適化の無効化（Disable Optimization）]** • **Auto**
[メモリ リフレッシュ レート（Memory Refresh Rate）] ドロップダウンリスト **set MemoryRefreshRate**	メモリのリフレッシュ レートを増減できます。DRAM のリフレッシュ レートを上げると、次のリフレッシュの前に発生する可能性のあるアクティブ化（ハンマー）の最大数が減少します。 次のいずれかになります。 • **[1X リフレッシュ（1X Refresh）]**：リフレッシュ レートは最小です。 • **[2X リフレッシュ（2X Refresh）]**：リフレッシュは 2 倍高速です。
[2LM の Snoopy モード (Snoopy mode for 2LM)] ドロップダウン リスト **set SnoopyModeFor2LM**	NUMA に最適化されていないワークロードから far メモリへのディレクトリ更新を回避できます。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

サーバー モデル別 BIOS パラメータ

名前	説明
[メモリ サーマル スロットリング モード（Memory Thermal Throttling Mode）] ドロップダウンリスト **set MemoryThermalThrottling**	この関数は、メモリ温度の調整に使用されます。この機能を有効にした後、メモリ温度が極端に高くなると、メモリアクセスレートが低下し、Baseboard Management Controller（BMC）がファンを調整してメモリを冷却し、DIMM の損傷を防ぎます。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • **PECI を使用した CLTT**：プラットフォーム環境制御インターフェイスを使用してクローズドループ サーマル スロットリングを有効にします。
[パニックと高水準点（Panic and High Watermark）] ドロップダウンリスト **set PanicHighWatermark**	低に設定した場合、**[メモリ更新レート（Memory Refresh Rate）]** が **[1X リフレッシュ（1X Refresh）]** に設定されている間、メモリコントローラは更新を延期しません。 次のいずれかになります。 • **[低（Low）]**：リフレッシュ レートは低に設定します。 • **[高（High）]**：リフレッシュ レートは高に設定します。
[UMA] ドロップダウンリスト **set UmaBasedClustering**	UMA 設定を設定できます。次のいずれかになります。 • Disable(All2All) • Hemisphere(2-clusters)

名前	説明
[拡張メモリ テスト（Enhanced Memory Test）] ドロップダウンリスト **set AdvancedMemTest**	（注） この機能は、Samsung、Hynix、および Micron DIMM にのみ適用されます。 この機能を使用して、BIOS POST 中に高度な DIMM テストを有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[eADR サポート（eADR Support）] ドロップダウンリスト **set EadrSupport**	拡張非同期 DRAM リフレッシュ（eADR）のサポートにより、CPU キャッシュに格納されているデータを永続メモリに移動するためのキャッシュ フラッシュ コマンドの待機期間を回避できます。これによりパフォーマンスが向上します。次のいずれかになります。 • **Disabled** • **有効化** • **Auto**
[揮発性メモリ モード（Volatile Memory Mode）] ドロップダウンリスト **set VolMemoryMode**	揮発性メモリ モードの設定は、BIOS が Intel® Optane™ PMem をサポートしている場合に表示されます。次のいずれかになります。 • **[1LM]**：このオプションは、Intel® Optane™ PMem を App-Direct モードで設定するために使用できます。 • **[2LM]**：このオプションにより、2LM は DDR4 メモリをキャッシュとして動作させることができます。

サーバー モデル別 BIOS パラメータ

名前	説明
[アダプティブ リフレッシュ管理レベル（Adaptive Refresh Management Level）] ドロップダウン リスト **set AdaptiveRefreshMgmtLevel**	リフレッシュ管理設定は読み取り専用です。現用系 RFM により、コントローラは RFM レベルと呼ばれる追加の RFM しきい値設定を柔軟に選択できます。RFM レベルにより、コントローラが発行した RFM コマンドと、これらのコマンドの DRAM 内管理との調整が可能になります。 次のいずれかになります。 • **デフォルト (Default)** • **[レベル A（Level A）]** • **[レベル B（Level B）]** • **[レベル C（Level C）]**
[メモリ帯域幅ブースト（Memory Bandwidth Boost）] ドロップダウンリスト **set MemoryBandwidthBoost**	Intel® メモリ帯域幅ブーストは、Intel® Optane™ パーシステント メモリの機能であり、サーマル ヘッドルームが利用可能な場合に、ダイナミック レンジの電力と帯域幅を提供します。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[エラー チェック スクラブ（Error Check Scrub）] ドロップダウン リスト **set ErrorCheckScrub**	結果収集の有無にかかわらず、メモリ チェックを有効にすることができます。次のいずれかになります。 • **Disabled** • **[結果収集なしで有効化（Enabled without Result Collection）]** • **[結果収集ありで有効化（Enabled with Result Collection）]**

名前	説明
[ランク マージン ツール（Rank Margin Tool）] ドロップダウン リスト **set EnableRMT**	ランク マージン ツールが使用されているかどうか、およびマージン テスト（メモリ シーケンスと電圧信号をテストするもの）が実行されているかどうかを示します。次のいずれかになります。 • **Disabled** • **有効化**

[電源/パフォーマンス（Power/Performance）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *7 : [*電源/パフォーマンス（*Power/Performance*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバー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、変更内容はサーバーが手動でリブートされるまで保存されます。
[隣接キャッシュ ライン プリフェッチャ（Adjacent Cache Line Prefetcher）] ドロップダウン リスト **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。

名前	説明
[ハードウェア プリフェッチャ（Hardware Prefetcher）] ドロップダウン リスト **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。
[DCU IP プリフェッチャ（DCU IP Prefetcher）] ドロップダウン リスト **set DcuIpPrefetch**	プロセッサで DCU IP プリフェッチ 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 プリフェッチャ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。
[DCU ストリーマ プリフェッチ（DCU Streamer Prefetch）] ドロップダウン リスト **set DcuStreamerPrefetch**	プロセッサで DCU IP プリフェッチ 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。

名前	説明
[仮想 Numa（Virtual Numa）] ドロップダウン リスト **set VirtualNuma**	仮想 NUMA（仮想非均一メモリ アクセス）は、VMware 仮想マシン（VM）のメモリ アクセス最適化方法であり、メモリ帯域幅のボトルネックを防ぐのに役立ちます。 次のいずれかになります。 • **[無効（Disabled）]**：機能は無効です。 • **[有効（Enabled）]**：機能は有効です。
[CPU パフォーマンス（CPU Performance）] ドロップダウン リスト **set CPUPerformance**	上記のオプションに対し CPU パフォーマンス プロファイルを設定します。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。 • [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。 • [高スループット（Hight Throughput）]：DCU IP Prefetcher のみが有効です。残りのオプションは無効になります。 • [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、[ハードウェア プリフェッチャ（Hardware Prefetcher）] オプションと [隣接キャッシュ ライン プリフェッチャ（Adjacent Cache Line Prefetcher）] オプションも同様に設定できます。

サーバー モデル別 BIOS パラメータ

名前	説明
[LLC デッドライン（LLC Dead Line）] ドロップダウンリスト **set LLCALLoc**	CPU の非包括的キャッシュ スキームでは、MLC から削除された内容が LLC に書き込まれます。行を MLC から削除する際、コアはそれらに **[デッド（dead）]** としてフラグを立てることがあります（再度読み取られる可能性が小さい場合）。LLC には、デッドラインを削除し、LLC に書き込まないオプションがあります。 この機能が無効の場合、デッド ラインは常に削除されます。LLC に書き込まれることはありません。 この機能が有効の場合、使用可能な空きスペースがある場合にデッドラインを LLC に書き込むことを LLC に許可します。 次のいずれかになります。 • **[無効（Disabled）]**：機能は無効です。 • **[有効（Enabled）]**：機能は有効です。 • **[自動（Auto）]**：CPU が LLC のデッドラインの割り当てを決定します。
[XPT リモート プリフェッチ（XPT Remote Prefetch） ドロップダウンリスト **set XPTRemotePrefetch**	この機能は、LLC 要求を複製し、最近の LLC 履歴に基づいてリモート マシンの適切なメモリ コントローラに送信して、待ち時間を減らします。 次のいずれかになります。 • **[無効（Disabled）]**：機能は無効です。 • **[有効（Enabled）]**：機能は有効です。 • **[自動（Auto）]**：CPU が機能を決定します。
[UPI リンク有効化（UPI Link Enablement）] ドロップダウンリスト **set UPILinkEnablement**	プロセッサが必要とする最小数の UPI リンクを有効にします。 次のいずれかになります。 • **1** • **2** • **Auto**

名前	説明
[強化 CPU パフォーマンス（Enhanced CPU Performance）] ドロップダウンリスト **set EnhancedCPUPerformance**	（注） この機能を有効にすると、**[電源特性の有効化（Enable Power Characterization）]** および **[パワーキャッピング（Power Capping）]** を有効にすることはできません。 サーバー設定を自動的に調整することにより、CPU パフォーマンスを向上させます。 （注） この機能を有効にすると、消費電力が増加する可能性があります。 この機能を使用するには、サーバーが次の要件を満たしている必要があります。 • サーバーが、Barlow Pass DIMM を使用していないこと • Cisco UCS C220 M6 サーバーの DIMM モジュール サイズは 64 GB 未満であり、Cisco UCS C240 M6 サーバーでは 256 GB 未満であること • サーバーに GPU カードが搭載されていないこと。 次のいずれかになります。 • **[無効（Disabled）]**：プロセッサでこの機能を使用しません。 • **[自動（Auto）]**：Cisco IMC がサーバー設定を調整して、パフォーマンスを向上させることができます。
[C1 自動降格（C1 Auto Demotion）] ドロップダウンリスト **set C1AutoDemotion**	有効にすると、CPU は非コア自動降格情報に基づいて C1 状態に自動的に降格します。 • **[無効（Disabled）]**：プロセッサでこの機能を使用しません。 • **[有効（Enabled）]**：機能は有効です。

名前	説明
[UPI 電力管理（UPI Power Manangement）] ドロップダウンリスト **set UPIPowerManagement**	UPI 電力管理は、サーバーの電力を節約するために使用されます。 次のいずれかになります。 • **[無効（Disabled）]**：プロセッサでこの機能を使用しません。 • **[自動（Auto）]**：機能は有効です。
[C1 自動降格解除（C1 Auto UnDemotion）] ドロップダウンリスト **set C1AutoUnDemotion**	プロセッサが C1 降格状態から自動的に解除できるようにするかどうかを選択します。 • **[無効（Disabled）]**：プロセッサでこの機能を使用しません。 • **[有効（Enabled）]**：機能は有効です。

[プロセッサ（Processor）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *8 : [プロセッサ（Processor）] タブの BIOS パラメータ*

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバー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、変更内容はサーバーが手動でリブートされるまで保存されます。
[拡張 APIC（Extended APIC）] ドロップダウンリスト **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。 • 有効：APIC サポートを有効にします • [無効（Disabled）]：APIC サポートを無効にします。

名前	説明
[Intel Virtualization Technology] ドロップダウン リスト **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。 • [有効（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。
[プロセッサ C6 レポート（Processor C6 Report）] ドロップダウン リスト **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 [カスタム（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。 （注） このオプションを使用できるのは一部の C シリーズ サーバーだけです。

サーバー モデル別 BIOS パラメータ

名前	説明
[プロセッサ C1E（Processor C1E）] ドロップダウン リスト **set ProcessorC1E**	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。 • [無効（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。 • [有効（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） このオプションを使用できるのは一部の C シリーズ サーバーだけです。
[EIST PSD 関数（EIST PSD Function）] ドロップダウンリスト **set ExecuteDisable**	EIST は、電圧と周波数のペア（P 状態）の変更に固有の遅延を短縮するため、これらの遷移がより頻繁に発生するようになります。これにより、より詳細なデマンドベースのスイッチングが可能になり、アプリケーションの要求に基づいて電力とパフォーマンスのバランスを最適化できます。次のいずれかになります。 • **[HW ALL]**：プロセッサは、論理プロセッサの依存関係間の P 状態を調整します。OS は、すべての論理プロセッサで P-state 要求を最新の状態に保ちます。 • **[SW ALL]**：OS Power Manager によって、依存関係にある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します。

名前	説明
[ターボ モード（Turbo Mode）] ドロップダウンリスト **set IntelTurboBoostTech**	プロセッサでインテル ターボ ブースト テクノロジーを使用するかどうか。このテクノロジーでは、仕様よりも低い電力、温度、または電圧でプロセッサが動作していると、自動的にそのプロセッサの周波数が上がります。次のいずれかになります。 • [Disabled]：プロセッサの周波数は自動的には上がりません。 • [Enabled]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。 （注） [CPUPowerManagement] を [カスタム（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。
[非コア周波数スケーリング (Uncore Frequency Scaling)] ドロップダウンリスト **set UFSDisable**	この機能を使用すると、プロセッサのコア以外の周波数のスケーリングを設定できます。次のいずれかになります。 • **[enabled]**：プロセッサの非コア部分の周波数を、負荷に応じて上下します。 • **[無効 (disabled)]**: プロセッサのコア以外の周波数を固定します。 『Intel® Dear Customer Letter (DCL)』には、固定されていない場合の **[非コア周波数スケーリング (Uncore Frequency Scaling)]** の固定の上限値と下限値が記されています。
[ブート パフォーマンス モード（Boot Performance Mode）] ドロップダウン リスト **set BootPerformanceMode**	オペレーティング システムのハンドオフ前に設定される BIOS パフォーマンス状態を選択できます。次のいずれかになります。 • [Max Performance]：プロセッサの P-state 率は最大です • **[最大効率（Max Efficient）]**：プロセッサの P-state の比率が最小です。 • **[Intel NM による設定（Set by Intel NM）]**：値は自動的に設定されます。

サーバー モデル別 BIOS パラメータ

名前	説明
[TDP の設定（Config TDP）]ドロップダウンリスト **set ConfigTDPLevel**	**[TDP の設定（Config TDP）]**機能により、プロセッサの温度設計の電力値を調整できます。プロセッサの動作とパフォーマンス レベルを変更することにより、プロセッサの消費電力と TDP を同時に調整できます。したがって、プロセッサは、使用可能な冷却容量と望ましい消費電力に応じて、パフォーマンス レベルが高いまたは低い方で動作します。次のいずれかになります。 • **[標準 (Normal)]** • **[レベル 1 (Level 1)]** • **[レベル 2 (Level 2)]** TDP レベルの値については、『Intell® Dear Customer Letter (DCL)』を参照してください。
[SpeedStep（Pstates）] ドロップダウンリスト **set EnhancedIntelSpeedStep**	プロセッサで拡張版 Intel SpeedStep テクノロジーを使用するかどうか設定します。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。 • [有効（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 [カスタム（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 CMCI] ドロップダウン リスト **set ProcessorCMCI**	CPU が corrected machine check events で割り込みをトリガーできるようにします。corrected machine check interrupt（CMCI）により、従来のポーリング タイマーよりも反応速度を向上できます。次のいずれかになります。 • [無効（Disabled）] : CMCI が無効になります。 • [有効（有効）] : CMCI が有効になります。これはデフォルト値です。
[HyperThreading [All]] ドロップダウン リスト **set IntelHyperThread**	プロセッサでインテル ハイパースレッディング テクノロジーを使用するかどうか。このテクノロジーでは、マルチスレッド ソフトウェア アプリケーションのスレッドを各プロセッサ内で並列に実行できます。次のいずれかになります。 • [Disabled] : プロセッサでのハイパースレッディングを禁止します。 • [有効（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。
[Workload Configuration] ドロップダウン リスト **set WorkLdConfig**	この機能を使用すると、ワークロードを最適化できます。オプションは [Balanced] と [I/O Sensitive] です。 • **[バランス（Balanced）]** • **[I/O 重視（IO Sensitive）]**

サーバー モデル別 BIOS パラメータ

名前	説明
[コアは有効化されました（Cores Enabled）] ドロップダウン リスト **set CoreMultiProcessing**	サーバー上の 1 つ以上の物理コアを無効にできます。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] ～ [48]**：サーバー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。 （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ください。
[UPI リンク周波数選択 (UPI Link Frequency Select)] ドロップダウン リスト **set QpiLinkSpeed**	（注） **[UPI リンク周波数選択 (UPI Link Frequency Select)]** トークンは、単一ソケット構成には適用されません。 この機能を使用すると、複数のソケット間の Intel Ultra Path Interconnect (UPI) リンク速度を設定できます。次のいずれかになります。 • **[自動 (Auto)]**]: このオプションは、最適なリンク速度を自動的に設定します。 • **[9.6 GT/s]**: このオプションは、最適なリンク速度として 9.6GT/s を使用します。 • **[10.4 GT/s]**—このオプションは、最適なリンク速度として 10.4GT/s を使用します。

名前	説明
[UPI プリフェッチ（UPI Prefetch）] ドロップダウン リスト **set KTIPrefetch**	UPI プリフェッチは、DDR バス上でメモリ読み込みが早期に開始されるようにするメカニズムです。これは次のいずれかになります。 • [無効（disabled）][無効（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。 • [有効（enabled）][有効（Enabled）]：UPI プリフェッチャ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。 • **[自動（Auto）]**：CPU が UPI プリフェッチ モードを決定します。
[Sub NUMA Clustering] ドロップダウンリスト **set SNC**	CPUがサブNUMAクラスタリングをサポートするかどうか。そのクラスタリングでは、タグディレクトリとメモリ チャネルは常に同じ領域にあります。次のいずれかになります。 • [disabled][Disabled]：サブNUMAクラスタリングは発生しません。 • [enabled][Enabled]：サブ NUMAクラスタリングが発生します。
[電力パフォーマンスの調整（Power Performance Tuning）] ドロップダウン リスト **set PwrPerfTuning**	BIOS またはOS によってエネルギー パフォーマンスのバイアス調整をオンにできるかどうかを指定します。オプションは [BIOS] と [OS] です。 • **[BIOS]**：エネルギー効率の調整のためにBIOS を選択します。 • **[OS]**：エネルギーパフォーマンスの調整にOSを選択します。 • **[PECI]**：エネルギー パフォーマンス チューニング用のプラットフォーム環境制御インターフェースを選択します。

名前	説明
[XPT Prefetch] ドロップダウン リスト **set XPTPrefetch**	XPT プリフェッチを使用して、最後のレベルのキャッシュに読み取り要求を送信できるようにして、その要求のコピーをメモリ コントローラのプリフェッチャに発行するかどうか。次のいずれかになります。 • [disabled][Disabled]：CPU はXPT Prefetch オプションを使用しません。 • [enabled][Enabled]：CPU はXPT プリフェッチ オプションを有効にします。

名前	説明
[パッケージのCステート（Package C State）] ドロップダウン リスト **set PackageCstateLimit**	アイドル時にサーバー 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。 • [no-limit][制限なし（No Limit）]：サーバーは、使用可能な任意の Cステートに入ることがあります。 • [自動（auto）][自動（Auto）]：物理的な高度を CPUが決定します。 • [C0 C1 ステート（C0 C1 State）]：サーバーはすべてのサーバーコンポーネントに常にフル パワーを提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • [C2]：CPU のアイドル時に、システムの電力消費をC1 オプションよりもさらに低減します。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、サーバーがハイ 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 保持なし（C6 Non Retention）]：CPU のアイドル時に、C3 オプションよりもさらに電力消費が低減されます。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、サーバー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。 • [C6 保持（C6 Retention）]：CPUのアイドル時に、C3 オプションよりもさらに電力消費が低減されます。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、サーバー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。

サーバー モデル別 BIOS パラメータ

名前	説明
[エネルギー パフォーマンスのバイアス構成（Energy/Performance Bias Config）] ドロップダウン リスト **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ー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。 • —サーバではすべてのサーバ コンポーネントにフルパワーを常時提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • —サーバはすべてのサーバ コンポーネントに、パフォーマンスとパワーのバランスを保つのに十分な電力を提供します。 • [バランス電力（Balanced Power）]：サーバーは、すべてのサーバーコンポーネントに、パフォーマンスと電力のバランスを保つのに十分な電力を提供します。 • [電力（Power）]：サーバーは、すべてのサーバーコンポーネントに、消費電力の低減を維持するのに最大の電力を提供します。
[ハードウェア P ステート（Hardware P-States）] ドロップダウン リスト **set CpuHWPM**	プロセッサ ハードウェアの P ステートを有効にします。次のいずれかになります。 • [disabled][Disabled]：HWPM がディセーブルになります。 • [hwpm-native-mode][HWPM Native Mode]：HWPM ネイティブモードがイネーブルになります。 • [hwpm-oob-mode][HWPM OOB Mode]：HWPM アウトオブボックスモードがイネーブルになります。 • [Native Mode with no Legacy]（GUI のみ）

名前	説明
[LLC Prefetch] ドロップダウン リスト **set LLCPrefetch**	プロセッサがLLCプリフェッチ メカニズムを使用して日付を LLC にフェッチするかどうか。次のいずれかになります。 • [disabled][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][Enabled]：LLC 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。
[自律コア C 状態（Autonomous Core C-state）] ドロップダウン リスト **set AutoCCState**	HALT 命令を MWAIT 命令に変換する CPU Autonomous C-State を有効にします。次のいずれかになります。 • [Disabled]：CPU Autonomous C-state が無効です。 • [有効（Enabled）]：CPU 自律 C-state が有効になります。
[エネルギー効率ターボ（Energy Efficient Turbo）] ドロップダウンリスト **set EnergyEfficientTurbo**	エネルギー効率の高いターボが有効になっている場合、CPUの最適なターボ周波数は、CPU使用率に基づいてダイナミックになります。パワー/パフォーマンスのバイアス設定も、エネルギー効率の高いターボに影響します。次のいずれかになります。 • **[無効（Disabled）]**：エネルギー効率ターボが無効です。 • **[有効（Enabled）]**：エネルギー効率ターボが有効です。

名前	説明
[パトロール スクラブ（Patrol Scrub）] ドロップダウンリスト **set PatrolScrub**	システムにサーバーのメモリ（未使用部分も含む）における単一ビット メモリ エラーを検出させて修復させることが可能です。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。 • [有効（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、システムは修復を試みます。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。 • **[POST の最後に有効化する（Enable at End of POST）]**：システムは、BIOS POST 後にメモリ ECC エラーをチェックします。
[プロセッサ EPP プロファイル（Processor EPP Profile）] ドロップダウンリスト **set EPPProfile**	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ー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。 • Performance • Balanced Performance • Balanced Power • 電源

名前	説明
[Intel ダイナミック速度選択（Intel Dynamic Speed Select）] ドロップダウンリスト **set IntelDynamicSpeedSelect**	**[Intel ダイナミック速度選択（Intel Dynamic Speed Select）]** モードでは、ユーザーは自動モードで異なる速度とコアを使用して CPU を動作させることができます。次のいずれかになります。 • **[無効（Disabled）]** : **[Intel ダイナミック速度選択（Intel Dynamic Speed Select）]** が無効になっています。 • **[有効（Enabled）]** : **[Intel ダイナミック速度選択（Intel Dynamic Speed Select）]** が有効になっています。
[Intel Speed Select (Intel の速度選択)] ドロップダウン リスト **set IntelSpeedSelect**	**[Intel の速度選択（Intel Speed Select）]** モードでは、ユーザーは異なる速度とコアを使用して CPU を実行できます。 次のいずれかになります。 • **基本**): ユーザーは最大コアおよび熱設計電力 (TDP) 比率にアクセスすることができます。 • **設定 3** ユーザーは **基本**より小さいコアと TDP 比率にアクセスできます。 • **[構成 4（Config 4）]** : ユーザーは **[構成 3（Config 3）]** より小さいコアと TDP 比率にアクセスできます。 デフォルト値: **基本**。

C220 M6 および C240 M6 サーバー

I/O Tab

Note BIOS parameters listed in this tab may vary depending on the server.

サーバー モデル別 BIOS パラメータ

Table 9: BIOS Parameters in I/O Tab

Name	Description
Reboot Host Immediately check box	If the Reboot Host Immediately check box is checked, the server is rebooted immediately and the new BIOS settings go into effect. Otherwise the changes are saved until the server is manually rebooted.
MLOM OptionROM drop-down list **set PcieSlotMLOMOptionROM**	This options allows you to control the Option ROM execution of the PCIe adapter connected to the MLOM slot. This can be one of the following: • **Disabled**—Does not execute Option ROM of the PCIe adapter connected to the MLOM slot. • **Enabled**—Executes Option ROM of the PCIe adapter connected to the MLOM slot.
MLOM Link Speed drop-down list **set PcieSlotMLOMLinkSpeed**	This option allows you to restrict the maximum speed of an adapter card installed in PCIe MLOM slot. This can be one of the following: • **Disabled**—The maximum speed is not restricted. • **Auto**—System selects the maximum speed allowed. • **GEN1**—2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **GEN2**—5GT/s is the maximum speed allowed. • **GEN3**—8GT/s is the maximum speed allowed. • **GEN4**—16GT/s is the maximum speed allowed.
PCIe Slot*n* OptionROM drop-down list **set PcieSlot*n*OptionROM**	Whether the server can use the Option ROMs present in the PCIe card slot designated by *n*. This can be one of the following: • **Disabled**—Option ROM for slot *n* is not available. • **Enabled**—Option ROM for slot *n* is available.

Name	Description
PCIe Slot*n* Link Speed drop-down list **set PcieSlot*n*LinkSpeed**	System IO Controller *n* (SIOCn) add-on slot (designated by *n*) link speed. This can be one of the following: • **Disabled**—Slot is disabled, and the card is not enumerated. • **Auto**— The default link speed. Link speed is automatically assigned. • **GEN1**—Link speed can reach up to first generation. • **GEN2**—Link speed can reach up to second generation. • **GEN3**—Link speed can reach up to third generation.
Front NVME-*n* OptionROM drop-down list **set PcieSlotFrontNvme*n*OptionROM**	This options allows you to control the Option ROM execution of the PCIe adapter connected to the SSD:NVMe slot *n*. This can be one of the following: • **Disabled**—Does not execute Option ROM of the PCIe adapter connected to the SSD:NVMe1 slot. • **Enabled**—Executes Option ROM of the PCIe adapter connected to the SSD:NVMe1 slot
Front NVME-*n* Link Speed drop-down list **set PcieSlotFrontNvme*n*LinkSpeed**	Link speed for NVMe front slot designated by slot *n*. This can be one of the following: • **Disabled**—Slot is disabled, and the card is not enumerated. • **Auto**—The default link speed. Link speed is automatically assigned. • **GEN1**—Link speed can reach up to first generation. • **GEN2**—Link speed can reach up to second generation. • **GEN3**—Link speed can reach up to third generation. • **GEN4**—Link speed can reach up to fourth generation.

サーバー モデル別 BIOS パラメータ

Name	Description
Rear NVME-*n* OptionROM drop-down list **set PcieSlotRearNvme*n*OptionROM**	This options allows you to control the Option ROM execution of the PCIe adapter connected to the rear SSD:NVMe slot *n*. This can be one of the following: • **Disabled**—Does not execute Option ROM of the PCIe adapter connected to the SSD:NVMe1 slot. • **Enabled**—Executes Option ROM of the PCIe adapter connected to the SSD:NVMe1 slot
Rear NVME-*n* Link Speed drop-down list **set PcieSlotRearNvme*n*LinkSpeed**	Link speed for NVMe rear slot designated by slot *n*. This can be one of the following: • **Disabled**—Slot is disabled, and the card is not enumerated. • **Auto**—The default link speed. Link speed is automatically assigned. • **GEN1**—Link speed can reach up to first generation. • **GEN2**—Link speed can reach up to second generation. • **GEN3**—Link speed can reach up to third generation. • **GEN4**—Link speed can reach up to fourth generation.
Legacy USB Support drop-down list **set UsbLegacySupport**	Whether the system supports legacy USB devices. This can be one of the following: • **Disabled**—USB devices are only available to EFI applications. • **Enabled**—Legacy USB support is always available. • **Auto**—Feature is is automatically assigned.
PCIe Slot MSTOR RAID OptionROM drop-down list **set PcieSlotMSTORRAIDOptionROM**	Whether the server can use the Option ROMs present in the PCIe MSTOR RAID. This can be one of the following: • **Disabled**—Option ROM is not available. • **Enabled**—Option ROM is available.

Name	Description
Intel VTD Coherency Support drop-down list **set CoherencySupport**	Whether the processor supports Intel VT-d Coherency. This can be one of the following: • **Disabled**—The processor does not support coherency. • **Enabled**—The processor uses VT-d Coherency as required.
Intel VT for Directed IO drop-down list **set IntelVTD**	Whether the processor uses Intel Virtualization Technology (VT), which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following: • **Disabled**—The processor does not permit virtualization. • **Enabled**—The processor allows multiple operating systems in independent partitions. **Note** If you change this option, you must power cycle the server before the setting takes effect.
VMD Enable drop-down list **set VMDenable**	Intel Volume Management Device (VMD) is for PCIe NVMe SSDs that provides hardware logic to manage and aggregate NVMe SSDs. This can be one the following: • **Enabled**— Enables benefits like robust surprise hot-plug, status LED management. • **Disabled**— Disables benefits like robust surprise hot-plug, status LED management. Default value: **Disabled**. Refer Intel® Virtual RAID on CPU User Guide and Intel® Virtual RAID on CPU (Intel® VROC) to configure VMD.

サーバー モデル別 BIOS パラメータ

Name	Description
	Details of VMD supported and unsupported ports for Cisco UCS C480 M5 servers: Cisco UCS C480 NVMe SKU (32 drive NVME System) • DMI connected ports 7, 8, and 23 do not support VMD. • All other twenty nine ports support VMD. Cisco UCS C480 Non-NVMe SKU • DMI connected ports 1, 2, and 18 do not support VMD. • Ports 7, 8, 9, 10, 15, 16, 17, 23, 24 support VMD.
Intel VTD ATS support drop-down list **set ATS**	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following: • **Disabled**—The processor does not support ATS. • **Enabled**—The processor uses VT-d ATS as required.
LOM Port *n* OptionROM drop-down list **set LomOpromControlPort0**	Whether Option ROM is available on the LOM port slot *n*. This can be one of the following: • **Disabled**—Option ROM is not available on LOM port 1. • **Enabled**—Option ROM is available on LOM port 1.
PCIe RAS Support drop-down list **set PCIeRASSupport**	Whether PCIe RAS Support is available on the PCIe slot. This can be one of the following: • **Disabled**—PCIe RAS is not available on the slot. • **Enabled**—PCIe RAS is available on port.
All Onboard LOM Ports drop-down list **set AllLomPortControl**	Whether Option ROM is available on all LOM ports. This can be one of the following: • **Disabled**—Option ROM is disabled on all the ports. • **Enabled**—Option ROM is enabled on all the ports.

Name	Description
USB Port Rear drop-down list **set UsbPortRear**	Whether the rear panel USB devices are enabled or disabled. This can be one of the following • **Disabled**— Disables the rear panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled**— Enables the rear panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.
VGA Priority drop-down list **set VgaPriority**	Allows you to set the priority for VGA graphics devices if multiple VGA devices are found in the system. This can be one of the following: • **OnBoard**—Priority is given to the onboard VGA device. BIOS post screen and OS boot are driven through the onboard VGA port. • **OffBoard**—Priority is given to the PCIE Graphics adapter. BIOS post screen and OS boot are driven through the external graphics adapter port. • **OnBoardDisabled**—Priority is given to the PCIe Graphics adapter, and the onboard VGA device is disabled. The vKVM does not function when the onboard VGA is disabled.
IPV6 PXE Support drop-down list **set IPV6PXE**	Enables or disables IPv6 support for PXE. This can be one of the following • **disabled**—IPv6 PXE support is not available. • **enabled**—IPv6 PXE support is always available.
USB Port Internal drop-down list **set UsbPortInt**	Whether the internal USB devices are enabled or disabled. This can be one of the following • **Disabled**— Disables the internal USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • **Enabled**— Enables the internal USB ports. Devices connected to these ports are detected by the BIOS and operating system.

サーバー モデル別 BIOS パラメータ

Name	Description
PCIe PLL SSC drop-down list **set PciePllSsc**	Enable this feature to reduce EMI interference by down spreading clock 0.5%. Disable this feature to centralize the clock without spreading. This can be one of the following: • **auto**—EMI interference is auto adjusted. **Disabled**—EMI interference is auto adjusted. • **ZeroPointFive**—EMI interference is reduced by down spreading the clock 0.5%.
Network Stack drop-down list **set NetworkStack**	This option allows you to monitor IPv6 and IPv4. This can be one of the following • **disabled**—Network Stack support is not available. **Note** When disabled, the value set for **IPV4 PXE Support** does not impact the system. • **enabled**—Network Stack support is always available.
IPV4 PXE Support drop-down list **set IPV4PXE**	Enables or disables IPv4 support for PXE. This can be one of the following • **disabled**—IPv4 PXE support is not available. • **enabled**—IPv4 PXE support is always available.
External SSC enable drop-down list **set EnableClockSpreadSpec**	This option allows you to reduce the EMI of your motherboard by modulating the signals it generates so that the spikes are reduced to flatter curves. This can be one of the following: • **Disabled**—Clock Spread Spectrum support is not available. • **Enabled**—Clock Spread Spectrum support is always available.
IPV4 HTTP Support drop-down list **set IPV4HTTP**	Enables or disables IPv4 support for HTTP. This can be one of the following: • **disabled**—IPv4 HTTP support is not available. • **enabled**—IPv4 HTTP support is always available.

Name	Description
IIO eDPC Support drop-down list **set EdpEn**	eDPC allows a downstream link to be disabled after an uncorrectable error, making recovery possible in a controlled and robust manner. This can be one of the following: • Disabled—eDPC support is disabled. • On Fatal Error—eDPC is enabled only for fatal errors. • On Fatal and Non-Fatal Errors—eDPC is enabled for both fatal and non-fatal errors.
IPV6 HTTP Support drop-down list **set IPV6HTTP**	Enables or disables IPv6 support for HTTP. This can be one of the following: • **disabled**—IPv6 HTTP support is not available. • **enabled**—IPv6 HTTP support is always available.

[Server Management] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *10 : [*サーバ管理（***Server Management***）*]* タブの ***BIOS*** パラメータ

名前	説明
[ホストを即座リブート（**Reboot Host Immediately**）**]** チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバー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、変更内容はサーバーが手動でリブートされるまで保存されます。

サーバー モデル別 BIOS パラメータ

名前	説明
[OS ブート ウォッチドッグ タイマー ポリシー（OS Boot Watchdog Timer Policy）] ドロップダウン リスト **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。 • [電源オフ（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、サーバーはリセットされます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にする場合にのみ適用されます。
[FRB 2 タイマー（FRB 2 Timer）] ドロップダウン リスト **set FRB-2**	POST 中にシステムがハングした場合に、システムを回復するために Cisco IMC によって FRB2 タイマーが使用されるかどうか。次のいずれかになります。 • [無効（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 ウォッチドッグ タイマー（OS Watchdog Timer）] ドロップダウン リスト **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]：サーバーのブートにかかる時間をトラッキングするためにウォッチドッグ タイマーは使用されません。 • [有効（enabled）]：サーバーがブートにかかる時間をウォッチドッグ タイマーで追跡します。サーバーのブートが [OS ブート ウォッチドッグ タイマー タイムアウト（OS Boot Watchdog Timer Timeout）] フィールドで指定された時間内に完了しない場合は、Cisco IMC によってエラーがログに記録され、[OS ブート ウォッチドッグ ポリシー（OS Boot Watchdog Policy）] フィールドで指定されたアクションが実行されます。
[OS ブート ウォッチドッグ タイマー タイムアウト（OS Watchdog Timer Timeout）] ドロップダウン リスト **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 分（5 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [10 分（10 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [15 分（15 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [20 分（20 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にした場合にのみ適用されます。

サーバー モデル別 BIOS パラメータ

名前	説明
[ボー レート（Baud Rate）] ドロップダウン リスト **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。[コンソール リダイレクション（Console Redirection）] を無効にした場合、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]：9,600 ボー レートが使用されます。 • [19.2k]：19,200 ボー レートが使用されます。 • [38.4k]：38,400 ボー レートが使用されます。 • [57.6k]：57,600 ボー レートが使用されます。 • [115.2k]：115,200 ボー レートが使用されます。 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。
[フロー制御（Flow Control）] ドロップダウン リスト **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を設定します。送信要求/クリア ツー センド（RTS/CTS）を使用すると、隠れた端末の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。 • [なし（None）]：フロー制御は使用されません。 • [RTS/CTS]：RTS/CTS がフロー制御に使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。

名前	説明
[コンソール リダイレクション（Console Redirection）] ドロップダウン リスト **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 リダイレクションで使用できるようにします。OS 起動後は、コンソールのリダイレクトが関係なくなります。次のいずれかになります。 • **[COM 0]**：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有効にします。 • **[COM 1]**：POST 中にシリアル ポート B でコンソール リダイレクションを有効にします。 • [Disabled]：POST 中にコンソール リダイレクションは発生しません。
[ターミナル タイプ（Terminal Type）] ドロップダウン リスト **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。

名前	説明
[PCIe Slots CDN コントロール（PCIe Slots CDN Control）] ドロップダウンリスト **set PcieSlotsCdnEnable**	（注） このオプションは、スロット 2 または 5 に Mellanox カードを搭載した Cisco UCS C240 M6 サーバーでのみ使用できます。 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。 • [無効（Disabled）]：VIC カードに対する CDN サポートは無効です。 • [有効（Enabled）]：VIC カードの CDN サポートが有効になります。
[CDN コントロール（CDN Control）] ドロップダウン リスト **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。 • [無効（Disabled）]：VIC カードに対する CDN サポートは無効です。 • [有効（Enabled）]：VIC カードの CDN サポートが有効になります。
[OptionROM起動最適化（OptionROM Launch Optimization）]	このオプションが [有効（Enabled）] の場合、ブート順序のポリシーに存在するコントローラにのみ OptionROMs が起動されます。 （注） オンボードストレージコントローラ、Emulex FC アダプタおよび GPU コントローラなどのいくつかのコントローラについて、ブート順序のポリシーに含まれていなくても、OptionROM が起動されます。 このオプションが [無効（Disabled）] の場合、すべての OptionROMs が起動されます。 デフォルト値：[有効（Enabled）]

名前	説明
適応型メモリ トレーニング	このオプションを[有効（Enabled）]にすると、次のようになります。 メモリ トレーニングは毎回のブートでは実行されず、BIOSは、保存されたメモリ トレーニングの結果を毎回のリブートで使用します。 毎回のブートでメモリ トレーニングが実行されるいくつかの例外には、次のものがあります。 BIOS の更新、CMOS のリセット、CPU やメモリの設定変更、SPD または実行時の修正不可能なエラー、または、前回のブートから 24 時間以上経過している場合。 このオプションが [無効（Disabled）] の場合、毎回のブートでメモリ トレーニングが行われます。 デフォルト値：[有効（Enabled）]。 （注） [高速ブート（Fast Boot）] オプションを無効にするには、エンドユーザーは次のトークンを下記の説明のとおりに設定する必要があります。 [適応型メモリ トレーニング（Adaptive Memory Training）]を [無効（Disabled）] に [BIOS Techlogレベル（BIOS Techlog level）] を [標準（Normal）] に [OptionROM起動最適化（OptionROM Launch Optimization）] を [無効（Disabled）] に

名前	説明
[BIOS Techlogレベル（BIOS Techlog Level）]	このオプションは、**BIOS tech ログファイル**のメッセージのタイプを示します。 ログファイルには、次のタイプのいずれかを指定できます。 • [最小（Minimum）]：重要なメッセージがログファイルに表示されます。 • [標準（Normal）]：警告およびロードメッセージがログファイルに表示されます。 • [最大（Maximum）]：標準に加え、情報関連のメッセージがログファイルに表示されます。 デフォルト値：[最小（Minimum）] （注） このオプションは、主に、内部のデバッグを目としています。

[セキュリティ（Security）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *11 : [*セキュリティ管理（*Security Management*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバー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、変更内容はサーバーが手動でリブートされるまで保存されます。
[SHA-1 PCR バンク（SHA-1 PCR Bank）] ドロップダウンリスト **set SHA1PCRBank**	BIOS が測定を実行しているときに OS で使用可能な PCR バンクです。 • **[無効（Disabled）]**：SHA-1 PCR バンクは BIOS で使用できません。 • **[有効（Enabled）]**：SHA-1 PCR バンクは BIOS で使用できます。

名前	説明
[トラステッド プラットフォーム モジュール状態（Trusted Platform Module State）] ドロップダウンリスト **set TPMControl**	信頼されたプラットフォーム モジュール（TPM）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。次のいずれかになります。 • [Disabled]：サーバーはTPMを使用しません。 • [有効（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ください。
[DMA 制御オプトイン フラグ（DMA Control Opt-In Flag）] ドロップダウンリスト	DMA 制御オプトイン フラグ：このトークンを有効にすると、オペレーティング システムは入出力メモリ管理ユニット（IOMMU）を有効にして、悪意のあるデバイスからの DMA 攻撃を防ぐことができます。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[TPM 保留中の操作（TPM Pending Operation）] ドロップダウンリスト **set TPMPendingOperation**	トラステッド プラットフォーム モジュール（TPM）Pending Operation オプションを使用すると、保留中の操作のステータスを制御できます。次のいずれかになります。 • [None]：アクションなし。 • TpmClear：保留中の操作をクリアします。

名前	説明
[SHA-256 PCR バンク（SHA-256 PCR Bank）] ドロップダウンリスト **set SHA256PCRBank**	BIOS が測定を実行しているときに OS で使用可能な PCR バンクです。 • **[無効（Disabled）]**：SHA256 PCR バンクは BIOS で使用できません。 • **[有効（Enabled）]**：SHA256 PCR バンクは BIOS で使用できます。
[電源オン パスワード（Power On Password）] ドロップダウン リスト **set PowerOnPassword**	このトークンでは、F2 BIOS 設定を使用する前に BIOS パスワードを設定する必要があります。有効にすると、BIOS 関数（IO 設定、BIOS セットアップ、BIOS を使用したオペレーティング システムへのブート）にアクセスする前にパスワードの検証が必要になります。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[TPM の最小限の物理的存在（TPM Minimal Physical Presence）] ドロップダウンリスト	このトークンを使用すると、TPM に推奨される Microsoft のデフォルト設定を適用できます。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[Intel Trusted Execution Technology サポート（Intel Trusted Execution Technology Support）] ドロップダウン リスト **set TXTSupport**	信頼されたプラットフォームモジュール(TPM)が 有効 である場合にのみ 有効 に設定できます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

名前	説明
[マルチキー トータル メモリ暗号化（Multikey Total Memory Encryption、MK-TME） ドロップダウンリスト **set EnableMktme**	MK-TME を使用すると、独自のキーを持つ 1 つの暗号化ドメインを複数持つことができます。異なるメモリ ページを異なるキーで暗号化できます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[トータル メモリ暗号化（Total Memory Encryption、TME）] ドロップダウンリスト **set EnableTme**	システムの物理メモリ全体を暗号化する機能を提供します。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SGX 工場出荷時リセット（SGX Factory Reset）] ドロップダウンリスト **set SgxFactoryReset**	その後の起動時にシステムが SGX の工場出荷時リセットを実行できるようにします。これにより、すべての登録データが削除されます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SWガード拡張（SW Guard Extensions、SGX）] ドロップダウンリスト **set EnableSgx**	ソフトウェア ガード拡張（SGX）機能を有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

名前	説明
[SGX QoS] ドロップダウンリスト **set SgxQoS**	SGX QoS を有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SGX パッケージ情報インバンド アクセス（SGX Pkg info In-Band Access）] ドロップダウンリスト **set SgxPackageInfoInBandAccess**	SGX パッケージ情報インバンドアクセスを有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SGX 書き込み有効（SGX Write Enable）] ドロップダウンリスト **set SgxLeWr**	SGX 書き込み機能を有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[所有者 EPOCH入力タイプ選択（Select Owner EPOCH input type）] ドロップダウンリスト **set EpochUpdate**	作成され、ロックされたメモリ領域に使用されるセキュリティ キーのシードを変更できます。次のいずれかになります。 • **SGX 所有者 EPOCH 有効化（SGX Owner EPOCH activated）]**：現在の入力タイプを変更しません。 • **[新しいランダム所有者 EPOCH に変更（Change to New Random Owner EPOCHs）]**：EPOCH をシステムが生成したランダムな数値に変更します。 • **[手動ユーザー定義所有者 EPOCH（Manual User Defined Owner EPOCHs）]**：EPOCH シードをユーザーが入力した 16 進値に変更します。

名前	説明
[SProcessor Epoch*n*] フィールド **set SgxEpoch0**	*n* で指定された EPOCH 番号の SGX EPOCH 所有者値を定義できます。
[SGX 自動 MP レジストレーション エージェント（SGX Auto MP Registration Agent）] ドロップダウンリスト **set SgxAutoRegistrationAgent**	レジストレーション エージェント サービスがプラットフォーム キーを保存できるようにします。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[SGX PUBKEY HASH*n*] フィールド **set SgxLePubKeyHash*n***	ソフトウェア ガード拡張（SGX）の値を設定できます。この値の設定範囲は、以下のとおりです。 • SGX PUBKEY HASH0 — 7 ～ 0 の間 • SGX PUBKEY HASH1 — 15 ～ 8 の間 • SGX PUBKEY HASH2 — 23 ～ 16 の間 • SGX PUBKEY HASH3 — 31 ～ 24 の間
[CPU PA を 46 ビットに制限（LIMIT CPU PA to 46 Bits）] ドロップダウンリスト **set CpuPaLimit**	Intel ® VT-d でこのオプションを有効にして、2019 OS でブートできるようにします。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

メモリ タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

サーバー モデル別 BIOS パラメータ

表 *12 : [*メモリ（*Memory*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（**Reboot Host Immediately**）**]** チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバー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、変更内容はサーバーが手動でリブートされるまで保存されます。

名前	説明
[メモリ RAS 構成の選択（Select Memory RAS configuration）] ドロップダウン リスト **set SelectMemoryRAS**	サーバーに対するメモリの信頼性、可用性、およびサービス性（RAS）の設定方法。次のいずれかになります。 • [最大パフォーマンス（Maximum Performance）]：システムのパフォーマンスが最適化されます。 • **ADDDC のスペアリング**: 適応可能な仮想ロックステップは、ADDDC モードをサポートするためにハードウェアおよびファームウェアで実装されるアルゴリズムです。選択すると、アルゴリズムがアクティブになるまでシステムのパフォーマンスが最適化されます。このアルゴリズムは、DRAM デバイスで障害が発生した場合にアクティブになります。アルゴリズムがアクティブになると、仮想ロックステップ リージョンがアクティブになり、実行時に障害が発生したリージョンが動的にマッピングされ、パフォーマンスへの影響はリージョン レベルで制限されます。 • [ミラー モード 1LM（Mirror Mode 1LM）]：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。 • **部分的なミラー モード 1LM**: 部分的な DIMM ミラーリングによって完全なミラーコピーを保持するのではなく、メモリ セルの特定の領域のミラーコピーが作成されます。部分的なミラーリングでは、部分的なミラー コピーの属性を使用して、メモリ マップにミラー領域が作成されます。最大 4 個の部分的なミラーを使用して、合計メモリ容量の最大 50% をミラーリングできます。

サーバー モデル別 BIOS パラメータ

名前	説明
[NUMA] ドロップダウン リスト **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]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[パーシャル キャッシュ ライン スペアリング（Partial Cache Line Sparing）] ドロップダウン リスト **set PartialCacheLineSparing**	パーシャル キャッシュ ライン スペアリング (PCLS) は、メモリ コントローラーのエラー防止メカニズムです。PCLS は、メモリ アクセス中に置換できるように、ビットの欠陥のあるニブルの場所を、対応するデータ コンテンツとともにスペア ディレクトリに静的にエンコードします。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[ディスク タイプの選択 (Select Disk Type)] ドロップダウン リスト **set SelectPprType**	Cisco IMC は、指定された障害のある行から指定されたスペア行へのアクセスを永続的に再マッピングする、**ハード PPR**をサポートしています。 次のいずれかになります。 • **[ハード PPR (Hard PPR)]**: サポートは有効になっています。 （注） ハード PPR は、**[メモリ RAS 設定 (Memory RAS Configuration)]**が **[ADDDC スペア (ADDDC Sparing)]**に設定されている場合にのみ使用できます。他の RA の選択では、この設定を **Disabled** に設定する必要があります。 • **[無効 (Disabled)]**：サポートは無効になっています。

名前	説明
[BME DMA 移行 (BME DMA Mitigation)] ドロップダウン リスト **set BmeDmaMitigation**	不正な外部 DMA からの脅威を緩和する PCI BME ビットを無効にできます。次のいずれかになります。 • **[無効 (disabled)]**: PCI BME ビットは BIOS で無効になっています。 • **[有効 (Enabled)**: PCI BME ビットは BIOS で有効になっています。
[4 G 以上の復号化（Above 4G Decoding）] ドロップダウン リスト **set MemoryMappedIOAbove4GB**	4 GB 以上の MMIO を有効または無効にします。次のいずれかになります。 • [Disabled]：サーバーでは 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。 • [有効（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。
[Partial Memory Mirror Mode (部分メモリ ミラー モード)]ドロップダウン リスト **set PartialMirrorModeConfig**	部分的なメモリ サイズは、パーセンテージまたは GB 単位のいずれかです。次のいずれかになります。 • **割合**: 部分的なメモリのミラーはパーセンテージで定義されます。 • **値 (GB)**: 部分的なメモリ ミラーは GB で定義されます。 • **無効**: 部分的なメモリ ミラーが無効になります。

サーバー モデル別 BIOS パラメータ

名前	説明
[DCPMM Firmware Downgrade (DCPMM ファームウェアのダウングレード)] ドロップダウン リスト **set DCPMMFirmwareDowngrade**	BIOS が DCPMM ファームウェアのダウングレードをサポートしているかどうか。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[部分ミラー *n* サイズ（GB）（Partial Mirror n Size in GB）] フィールド **set PartialMirrorValue1**	最初の部分 *nth* メモリ ミラーのサイズ（GB）。 n = 1、2、または 3 0 ～ 65535 の整数を入力します。 （注） すべての部分的なミラーの合計メモリ サイズは、物理メモリ サイズの 50% を超えないようにする必要があります。
[部分的なミラー パーセンテージ (Partial Mirror percentage)] フィールド **set PartialMirrorPercent**	4GB を超えてミラーリングするメモリの割合。 0 ～ 60 の整数を入力します。
[メモリ サイズ制限 (GB) (Memory Size Limit in GB)] フィールド **set MemorySizeLimit**	このオプションを使用して、物理メモリの上限のサイズを GB 単位で減らします。 0 ～ 65535 の整数を入力します。
[NVM パフォーマンス設定 (NVM Performance Setting)] ドロップダウンリスト **set NvmdimmPerformConfig**	ワークロードの動作に応じて、NVM ベースラインのパフォーマンス設定を設定できます。 • **BW 最適化** • **遅延の最適化** • **バランス プロファイル**
[CR QoS] ドロップダウンリスト **set CRQoS**	CR QoS 調整を選択できます。 次のいずれかになります。 • **[モード 1（Mode 1）]**： • **[モード 2（Mode 2）]**： • **[モード 0（Mode 0）]**：**[CR QoS]** 機能は無効です。

名前	説明
[AD の Snoopy モード (Snoopy mode for AD)] ドロップダウン リスト **set SnoopyModeForAD**	新しい AD 固有の機能を有効にして、NUMA に最適化されていないワークロードからDDRT メモリへのディレクトリ更新を回避します。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[CR Fastgo Config] ドロップダウンリスト **set CrfastgoConfig**	CR QoS 設定プロファイルを選択できるようにします。 次のいずれかになります。 • **[最適化の有効化（Enable Optimization）]** • **[最適化の無効化（Disable Optimization）]** • **Auto**
[メモリ リフレッシュ レート（Memory Refresh Rate）] ドロップダウンリスト **set MemoryRefreshRate**	メモリのリフレッシュ レートを増減できます。DRAM のリフレッシュ レートを上げると、次のリフレッシュの前に発生する可能性のあるアクティブ化（ハンマー）の最大数が減少します。 次のいずれかになります。 • **[1X リフレッシュ（1X Refresh）]**：リフレッシュ レートは最小です。 • **[2X リフレッシュ（2X Refresh）]**：リフレッシュは 2 倍高速です。
[2LM の Snoopy モード (Snoopy mode for 2LM)] ドロップダウン リスト **set SnoopyModeFor2LM**	NUMA に最適化されていないワークロードから far メモリへのディレクトリ更新を回避できます。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

サーバー モデル別 BIOS パラメータ

名前	説明
[メモリ サーマル スロットリング モード（Memory Thermal Throttling Mode）] ドロップダウンリスト **set MemoryThermalThrottling**	この関数は、メモリ温度の調整に使用されます。この機能を有効にした後、メモリ温度が極端に高くなると、メモリアクセスレートが低下し、Baseboard Management Controller（BMC）がファンを調整してメモリを冷却し、DIMM の損傷を防ぎます。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • **PECI を使用した CLTT**：プラットフォーム環境制御インターフェイスを使用してクローズドループ サーマル スロットリングを有効にします。
[パニックと高水準点（Panic and High Watermark）] ドロップダウン リスト **set PanicHighWatermark**	低に設定した場合、**[メモリ更新レート（Memory Refresh Rate）]** が **[1X リフレッシュ（1X Refresh）]** に設定されている間、メモリコントローラは更新を延期しません。 次のいずれかになります。 • **[低（Low）]**：リフレッシュ レートは低に設定します。 • **[高（High）]**：リフレッシュ レートは高に設定します。
[UMA] ドロップダウン リスト **set UmaBasedClustering**	UMA 設定を設定できます。次のいずれかになります。 • Disable(All2All) • Hemisphere(2-clusters)

名前	説明
[高度なメモリ テスト（Advanced Memory Test）] ドロップダウン リスト **set AdvancedMemTest**	（注） この機能は、Samsung、Hynix、および Micron DIMM にのみ適用されます。 この機能を使用して、BIOS POST 中に高度な DIMM テストを有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[eADR サポート（eADR Support）] ドロップダウン リスト **set EadrSupport**	拡張非同期 DRAM リフレッシュ（eADR）のサポートにより、CPU キャッシュに格納されているデータを永続メモリに移動するためのキャッシュ フラッシュ コマンドの待機期間を回避できます。これによりパフォーマンスが向上します。次のいずれかになります。 • **Disabled** • **有効化** • **Auto**
[揮発性メモリ モード（Volatile Memory Mode）] ドロップダウン リスト **set VolMemoryMode**	揮発性メモリ モードの設定は、BIOS が Intel® Optane™ PMem をサポートしている場合に表示されます。次のいずれかになります。 • **[1LM]**：このオプションは、Intel® Optane™ PMem を App-Direct モードで設定するために使用できます。 • **[2LM]**：このオプションにより、2LM は DDR4 メモリをキャッシュとして動作させることができます。

名前	説明
[メモリ帯域幅ブースト（Memory Bandwidth Boost）] ドロップダウン リスト **set MemoryBandwidthBoost**	Intel® メモリ帯域幅ブーストは、Intel® Optane™ パーシステント メモリの機能であり、サーマル ヘッドルームが利用可能な場合に、ダイナミック レンジの電力と帯域幅を提供します。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

[電源/パフォーマンス（Power/Performance）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *13 : [*電源/パフォーマンス（*Power/Performance*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバー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、変更内容はサーバーが手動でリブートされるまで保存されます。
[隣接キャッシュ ライン プリフェッチャ（Adjacent Cache Line Prefetcher）] ドロップダウン リスト **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。

名前	説明
[ハードウェア プリフェッチャ（Hardware Prefetcher）] ドロップダウン リスト **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。
[DCU IP プリフェッチャ（DCU IP Prefetcher）] ドロップダウン リスト **set DcuIpPrefetch**	プロセッサで DCU IP プリフェッチ 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 プリフェッチャ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。
[DCU ストリーマ プリフェッチ（DCU Streamer Prefetch）] ドロップダウン リスト **set DcuStreamerPrefetch**	プロセッサで DCU IP プリフェッチ 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。

名前	説明
[仮想 Numa（Virtual Numa）] ドロップダウン リスト **set VirtualNuma**	仮想 NUMA（仮想非均一メモリ アクセス）は、VMware 仮想マシン（VM）のメモリ アクセス最適化方法であり、メモリ帯域幅のボトルネックを防ぐのに役立ちます。 次のいずれかになります。 • **[無効（Disabled）]** — 機能は無効です。 • **[有効（Enabled）]** — 機能は有効です。
[CPU パフォーマンス（CPU Performance）] ドロップダウン リスト **set CPUPerformance**	上記のオプションに対し CPU パフォーマンス プロファイルを設定します。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。 • [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。 • [高スループット（Hight Throughput）]：DCU IP Prefetcher のみが有効です。残りのオプションは無効になります。 • [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、[ハードウェア プリフェッチャ（Hardware Prefetcher）] オプションと [隣接キャッシュ ライン プリフェッチャ（Adjacent Cache Line Prefetcher）] オプションも同様に設定できます。

名前	説明
[LLC デッド ライン（LLC Dead Line）] ドロップダウン リスト **set LLCALLoc**	CPU の非包括的キャッシュ スキームでは、MLC から削除された内容が LLC に書き込まれます。行を MLC から削除する際、コアはそれらに **[デッド（dead）]** としてフラグを立てることがあります（再度読み取られる可能性が小さい場合）。LLC には、デッド ラインを削除し、LLC に書き込まないオプションがあります。 この機能が無効の場合、デッド ラインは常に削除されます。LLC に書き込まれることはありません。 この機能が有効の場合、使用可能な空きスペースがある場合にデッドラインを LLC に書き込むことを LLC に許可します。 次のいずれかになります。 • **[無効（Disabled）]** — 機能は無効です。 • **[有効（Enabled）]** — 機能は有効です。 • **[自動（Auto）]** — CPU が LLC のデッド ラインの割り当てを決定します。
[XPT リモート プリフェッチ（XPT Remote Prefetch） ドロップダウン リスト **set XPTRemotePrefetch**	この機能は、LLC 要求を複製し、最近の LLC 履歴に基づいてリモート マシンの適切なメモリ コントローラに送信して、待ち時間を減らします。 次のいずれかになります。 • **[無効（Disabled）]** — 機能は無効です。 • **[有効（Enabled）]** — 機能は有効です。 • **[自動（Auto）]** — CPU が機能を決定します。
[UPI リンク有効化（UPI Link Enablement）] ドロップダウン リスト **set UPILinkEnablement**	プロセッサが必要とする最小数の UPI リンクを有効にします。 次のいずれかになります。 • **1** • **2** • **Auto**

名前	説明
[強化 CPU パフォーマンス（Enhanced CPU Performance）] ドロップダウン リスト **set EnhancedCPUPerformance**	（注） この機能を有効にすると、**[電源特性の有効化（Enable Power Characterization）]**および**[パワーキャッピング（Power Capping）]**を有効にすることはできません。 サーバー設定を自動的に調整することにより、CPU パフォーマンスを向上させます。 （注） この機能を有効にすると、消費電力が増加する可能性があります。 この機能を使用するには、サーバーが次の要件を満たしている必要があります。 • サーバーが、Barlow Pass DIMM を使用していないこと • Cisco UCS C220 M6 サーバーの DIMM モジュール サイズは 64 GB 未満であり、Cisco UCS C240 M6 サーバーでは 256 GB 未満であること • サーバーにGPUカードが搭載されていないこと。 次のいずれかになります。 • **[無効（Disabled）]** — プロセッサでこの機能を使用しません。 • **[自動（Auto）]** — Cisco IMC がサーバー設定を調整して、パフォーマンスを向上させることができます。
[C1 自動降格（C1 Auto Demotion）] ドロップダウン リスト **set C1AutoDemotion**	有効にすると、CPU は非コア自動降格情報に基づいて C1 状態に自動的に降格します。 • **[無効（Disabled）]**：プロセッサでこの機能を使用しません。 • **[有効（Enabled）]**：機能は有効です。

名前	説明
[UPI 電力管理（UPI Power Manangement）] ドロップダウン リスト **set UPIPowerManagement**	UPI 電力管理は、サーバーの電力を節約するために使用されます。 次のいずれかになります。 • **[無効（Disabled）]** — プロセッサでこの機能を使用しません。 • **[自動（Auto）]** — 機能は有効です。
[C1 自動降格解除（C1 Auto UnDemotion）] ドロップダウン リスト **set C1AutoUnDemotion**	プロセッサが C1 降格状態から自動的に解除できるようにするかどうかを選択します。 • **[無効（Disabled）]** — プロセッサでこの機能を使用しません。 • **[有効（Enabled）]** — 機能は有効です。

[プロセッサ（Processor）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *14 : [プロセッサ（Processor）] タブの BIOS パラメータ*

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバー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、変更内容はサーバーが手動でリブートされるまで保存されます。
[拡張 APIC（Extended APIC）] ドロップダウンリスト **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。 • 有効：APIC サポートを有効にします • [無効（Disabled）]：APIC サポートを無効にします。

サーバー モデル別 BIOS パラメータ

名前	説明
[Intel Virtualization Technology] ドロップダウン リスト **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。 • [有効（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。
[プロセッサ C6 レポート（Processor C6 Report）] ドロップダウン リスト **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 [カスタム（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。 （注） このオプションを使用できるのは一部の C シリーズ サーバーだけです。

名前	説明
[プロセッサ C1E（Processor C1E）] ドロップダウン リスト **set ProcessorC1E**	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。 • [無効（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。 • [有効（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） このオプションを使用できるのは一部の C シリーズ サーバーだけです。
[EIST PSD 関数（EIST PSD Function）] ドロップダウンリスト **set ExecuteDisable**	EIST は、電圧と周波数のペア（P 状態）の変更に固有の遅延を短縮するため、これらの遷移がより頻繁に発生するようになります。これにより、より詳細なデマンドベースのスイッチングが可能になり、アプリケーションの要求に基づいて電力とパフォーマンスのバランスを最適化できます。次のいずれかになります。 • **[HW ALL]**：プロセッサは、論理プロセッサの依存関係間の P 状態を調整します。OS は、すべての論理プロセッサで P-state 要求を最新の状態に保ちます。 • **[SW ALL]**：OS Power Manager によって、依存関係にある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します。

サーバー モデル別 BIOS パラメータ

名前	説明
[ターボ モード（Turbo Mode）] ドロップダウンリスト **set IntelTurboBoostTech**	プロセッサでインテル ターボ ブーストテクノロジーを使用するかどうか。このテクノロジーでは、仕様よりも低い電力、温度、または電圧でプロセッサが動作していると、自動的にそのプロセッサの周波数が上がります。次のいずれかになります。 • [Disabled]：プロセッサの周波数は自動的には上がりません。 • [Enabled]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。 （注） [CPUPowerManagement] を [カスタム（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。
[非コア周波数スケーリング (Uncore Frequency Scaling)] ドロップダウンリスト **set UFSDisable**	この機能を使用すると、プロセッサのコア以外の周波数のスケーリングを設定できます。次のいずれかになります。 • **[enabled]**：プロセッサの非コア部分の周波数を、負荷に応じて上下します。 • **[無効 (disabled)]**: プロセッサのコア以外の周波数を固定します。 『Intel® Dear Customer Letter (DCL)』には、固定されていない場合の **[非コア周波数スケーリング (Uncore Frequency Scaling)]** の固定の上限値と下限値が記されています。
[ブート パフォーマンス モード（Boot Performance Mode）] ドロップダウン リスト **set BootPerformanceMode**	オペレーティング システムのハンドオフ前に設定される BIOS パフォーマンス状態を選択できます。次のいずれかになります。 • [Max Performance]：プロセッサの P-state 率は最大です • **[最大効率（Max Efficient）]**：プロセッサの P-state の比率が最小です。 • **[Intel NM による設定（Set by Intel NM）]**：値は自動的に設定されます。

名前	説明
[TDP の設定（Config TDP）]ドロップダウンリスト **set ConfigTDPLevel**	**[TDP の設定（Config TDP）]**機能により、プロセッサの温度設計の電力値を調整できます。プロセッサの動作とパフォーマンス レベルを変更することにより、プロセッサの消費電力と TDP を同時に調整できます。したがって、プロセッサは、使用可能な冷却容量と望ましい消費電力に応じて、パフォーマンス レベルが高いまたは低い方で動作します。次のいずれかになります。 • **[標準 (Normal)]** • **[レベル 1 (Level 1)]** • **[レベル 2 (Level 2)]** TDP レベルの値については、『Intell® Dear Customer Letter (DCL)』を参照してください。
[SpeedStep（Pstates）]ドロップダウンリスト **set EnhancedIntelSpeedStep**	プロセッサで拡張版 Intel SpeedStep テクノロジーを使用するかどうか設定します。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。 • [有効（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 [カスタム（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。

サーバー モデル別 BIOS パラメータ

名前	説明
[Processor CMCI] ドロップダウン リスト **set ProcessorCMCI**	CPU が corrected machine check events で割り込みをトリガーできるようにします。corrected machine check interrupt（CMCI）により、従来のポーリング タイマーよりも反応速度を向上できます。次のいずれかになります。 • [無効（Disabled）]：CMCI が無効になります。 • [有効（有効）]：CMCI が有効になります。これはデフォルト値です。
[HyperThreading [All]] ドロップダウン リスト **set IntelHyperThread**	プロセッサでインテル ハイパースレッディング テクノロジーを使用するかどうか。このテクノロジーでは、マルチスレッド ソフトウェア アプリケーションのスレッドを各プロセッサ内で並列に実行できます。次のいずれかになります。 • [Disabled]：プロセッサでのハイパースレッディングを禁止します。 • [有効（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。
[Workload Configuration] ドロップダウン リスト **set WorkLdConfig**	この機能を使用すると、ワークロードを最適化できます。オプションは [Balanced] と [I/O Sensitive] です。 • **[バランス（Balanced）]** • **[I/O 重視（IO Sensitive）]**

名前	説明
[コアは有効化されました（Cores Enabled）] ドロップダウン リスト **set CoreMultiProcessing**	サーバー上の 1 つ以上の物理コアを無効にできます。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] ～ [48]**：サーバー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。 （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ください。
[UPI リンク周波数選択 (UPI Link Frequency Select)] ドロップダウン リスト **set QpiLinkSpeed**	（注） **[UPI リンク周波数選択 (UPI Link Frequency Select)]** トークンは、単一ソケット構成には適用されません。 この機能を使用すると、複数のソケット間の Intel Ultra Path Interconnect (UPI) リンク速度を設定できます。次のいずれかになります。 • **[自動 (Auto)]**]: このオプションは、最適なリンク速度を自動的に設定します。 • **[9.6 GT/s]**: このオプションは、最適なリンク速度として 9.6GT/s を使用します。 • **[10.4 GT/s]**—このオプションは、最適なリンク速度として 10.4GT/s を使用します。

サーバー モデル別 BIOS パラメータ

名前	説明
[UPI プリフェッチ（UPI Prefetch）] ドロップダウン リスト **set KTIPrefetch**	UPI プリフェッチは、DDR バス上でメモリ読み込みが早期に開始されるようにするメカニズムです。これは次のいずれかになります。 • [無効（disabled）][無効（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。 • [有効（enabled）][有効（Enabled）]：UPI プリフェッチャ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。 • **[自動（Auto）]**：CPU が UPI プリフェッチ モードを決定します。
[Sub NUMA Clustering] ドロップダウンリスト **set SNC**	CPUがサブNUMA クラスタリングをサポートするかどうか。そのクラスタリングでは、タグディレクトリとメモリ チャネルは常に同じ領域にあります。次のいずれかになります。 • [disabled][Disabled]：サブ NUMAクラスタリングは発生しません。 • [enabled][Enabled]：サブ NUMAクラスタリングが発生します。
[電力パフォーマンスの調整（Power Performance Tuning）] ドロップダウン リスト **set PwrPerfTuning**	BIOS またはOS によってエネルギー パフォーマンスのバイアス調整をオンにできるかどうかを指定します。オプションは[BIOS] と [OS] です。 • **[BIOS]**：エネルギー効率の調整のためにBIOS を選択します。 • **[OS]**：エネルギーパフォーマンスの調整にOSを選択します。 • **[PECI]**：エネルギー パフォーマンス チューニング用のプラットフォーム環境制御インターフェースを選択します。

名前	説明
[XPT Prefetch] ドロップダウン リスト **set XPTPrefetch**	XPT プリフェッチを使用して、最後のレベルのキャッシュに読み取り要求を送信できるようにして、その要求のコピーをメモリ コントローラのプリフェッチャに発行するかどうか。次のいずれかになります。 • [disabled][Disabled]：CPU はXPT Prefetch オプションを使用しません。 • [enabled][Enabled]：CPU はXPT プリフェッチ オプションを有効にします。

サーバー モデル別 BIOS パラメータ

名前	説明
[パッケージのCステート（Package C State）] ドロップダウン リスト **set PackageCstateLimit**	アイドル時にサーバー 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。 • [no-limit][制限なし（No Limit）]：サーバーは、使用可能な任意の Cステートに入ることがあります。 • [自動（auto）][自動（Auto）]：物理的な高度を CPUが決定します。 • [C0 C1 ステート（C0 C1 State）]：サーバーはすべてのサーバーコンポーネントに常にフル パワーを提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • [C2]：CPU のアイドル時に、システムの電力消費をC1 オプションよりもさらに低減します。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、サーバーがハイ 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 保持なし（C6 Non Retention）]：CPU のアイドル時に、C3 オプションよりもさらに電力消費が低減されます。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、サーバー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。 • [C6 保持（C6 Retention）]：CPUのアイドル時に、C3 オプションよりもさらに電力消費が低減されます。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、サーバー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。

名前	説明
[エネルギー パフォーマンスのバイアス構成（Energy/Performance Bias Config）] ドロップダウン リスト **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ー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。 • ―サーバではすべてのサーバ コンポーネントにフルパワーを常時提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • ―サーバはすべてのサーバ コンポーネントに、パフォーマンスとパワーのバランスを保つのに十分な電力を提供します。 • [バランス電力（Balanced Power）]：サーバーは、すべてのサーバーコンポーネントに、パフォーマンスと電力のバランスを保つのに十分な電力を提供します。 • [電力（Power）]：サーバーは、すべてのサーバーコンポーネントに、消費電力の低減を維持するのに最大の電力を提供します。
[ハードウェア P ステート（Hardware P-States）] ドロップダウン リスト **set CpuHWPM**	プロセッサ ハードウェアの P ステートを有効にします。次のいずれかになります。 • [disabled][Disabled]：HWPM がディセーブルになります。 • [hwpm-native-mode][HWPM Native Mode]：HWPM ネイティブモードがイネーブルになります。 • [hwpm-oob-mode][HWPM OOB Mode]：HWPM アウトオブボックスモードがイネーブルになります。 • [Native Mode with no Legacy]（GUI のみ）

サーバー モデル別 BIOS パラメータ

名前	説明
[LLC Prefetch] ドロップダウン リスト **set LLCPrefetch**	プロセッサがLLCプリフェッチメカニズムを使用して日付を LLC にフェッチするかどうか。次のいずれかになります。 • [disabled][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][Enabled]：LLC 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。
[自律コア C 状態（Autonomous Core C-state）] ドロップダウン リスト **set AutoCCState**	HALT 命令を MWAIT 命令に変換する CPU Autonomous C-State を有効にします。次のいずれかになります。 • [Disabled]：CPU Autonomous C-state が無効です。 • [有効（Enabled）]：CPU 自律 C-state が有効になります。
[エネルギー効率ターボ（Energy Efficient Turbo）] ドロップダウンリスト **set EnergyEfficientTurbo**	エネルギー効率の高いターボが有効になっている場合、CPUの最適なターボ周波数は、CPU使用率に基づいてダイナミックになります。パワー/パフォーマンスのバイアス設定も、エネルギー効率の高いターボに影響します。次のいずれかになります。 • **[無効（Disabled）]**：エネルギー効率ターボが無効です。 • **[有効（Enabled）]**：エネルギー効率ターボが有効です。

名前	説明
[パトロール スクラブ（Patrol Scrub）] ドロップダウンリスト **set PatrolScrub**	システムにサーバーのメモリ（未使用部分も含む）における単一ビット メモリ エラーを検出させて修復させることが可能です。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。 • [有効（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、システムは修復を試みます。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。 • **[POST の最後に有効化する（Enable at End of POST）]**：システムは、BIOS POST 後にメモリ ECC エラーをチェックします。
[プロセッサ EPP プロファイル（Processor EPP Profile）] ドロップダウンリスト **set EPPProfile**	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ー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。 • Performance • Balanced Performance • Balanced Power • 電源

名前	説明
[Intel ダイナミック速度選択（Intel Dynamic Speed Select）] ドロップダウンリスト **set IntelDynamicSpeedSelect**	**[Intel ダイナミック速度選択（Intel Dynamic Speed Select）]** モードでは、ユーザーは自動モードで異なる速度とコアを使用して CPU を動作させることができます。次のいずれかになります。 • **[無効（Disabled）]** : **[Intel ダイナミック速度選択（Intel Dynamic Speed Select）]** が無効になっています。 • **[有効（Enabled）]** : **[Intel ダイナミック速度選択（Intel Dynamic Speed Select）]** が有効になっています。
[Intel Speed Select (Intel の速度選択)] ドロップダウン リスト **set IntelSpeedSelect**	**[Intel の速度選択（Intel Speed Select）]** モードでは、ユーザーは異なる速度とコアを使用して CPU を実行できます。 次のいずれかになります。 • **基本)**: ユーザーは最大コアおよび熱設計電力 (TDP) 比率にアクセスすることができます。 • **設定 3** ユーザーは **基本**より小さいコアと TDP 比率にアクセスできます。 • **[構成 4（Config 4）]** : ユーザーは **[構成 3（Config 3）]** より小さいコアと TDP 比率にアクセスできます。 デフォルト値: **基本**。

C225 M6 および C245 M6 サーバー

[I/O] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *15 : [I/O]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバー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、変更内容はサーバーが手動でリブートされるまで保存されます。
[MLOM OptionROM] ドロップダウン リスト **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。 • [無効（Disabled）] : MLOM スロットに接続されている PCIe アダプタのオプション ROM を実行しません。 • [有効（Enabled）] : MLOM スロットに接続されている PCIe アダプタのオプション ROM を実行します。
[MLOM リンク速度（MLOM Link Speed）] ドロップダウン リスト **set PcieSlotMLOMLinkSpeed**	このオプションを使用すると、PCIe MLOM 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。 • [無効（Disabled）] : 最大スピードは制限されていません。 • [自動（Auto）] : システムは許可される最大速度を選択します。 • [GEN1] : 最大 2.5 GT/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 5 GT/s までの速度が許可されます。 • [GEN3] : 最大 8 GT/s までの速度が許可されます。 • **[GEN3]** : 最大 16GT/s までの速度が許可されます。

名前	説明
[PCIe Slot*n* OptionROM] ドロップダウン リスト **set PcieSlot*n*OptionROM**	サーバーが *n* で指定した PCIe カード スロットにあるオプション ROM を使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：スロット *n* のオプションの ROM は使用できません。 • [有効（Enabled）]：スロット *n* のオプション ROM は使用可能です。
[PCIe スロット *n* リンク速度（PCIe Slot n Link Speed）] ドロップダウン リスト **set PcieSlot*n*LinkSpeed**	システム IO コントローラ *n*（SIOCn）アドオン スロット（*n* によって示される）のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効となり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：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。 • **[GEN4]**：リンク速度は第 4 世代まで到達可能です。
MRAID OptionROM **set PcieSlotMRAID*n*OptionROM**	サーバーが *n* で指定された PCIe カード スロット内の RAID オプションの ROM を使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：スロット *n* のオプションの ROM は使用できません。 • [有効（Enabled）]：スロット *n* のオプション ROM は使用可能です。

名前	説明
[MRAID リンク速度（MRAID Link Speed）] ドロップダウン リスト **set PcieSlotMRAID*n*LinkSpeed**	RAID IO コントローラ *n*（SIOCn）アドオン スロット（*n*によって指定）のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効となり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：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。 • **[GEN4]**：リンク速度は第 4 世代まで到達可能です。
[前面 NVME-*n* OptionROM（Front NVME-n OptionROM）] ドロップダウン リスト **set PcieSlotFrontNvme*n*OptionROM**	このオプションでは、SSD:NVMe スロット*n*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。 • [無効（Disabled）]：SSD:NVMe1 スロットに接続されている PCIe アダプタのオプションの ROM を実行しません。 • [有効（Enabled）]：SSD:NVMe1 スロットに接続されている PCIe アダプタのオプション ROM を実行します

名前	説明
[前面 NVME *n*リンク速度（Front NVME n Link Speed）] [ドロップダウン リスト（drop-down list）] **set PcieSlotFrontNvme*n*LinkSpeed**	スロット *n* で指定された NVMe 前面スロットのリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効となり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：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。 • **[GEN4]**：リンク速度は第 4 世代まで到達可能です。
[背面 NVME-*n* OptionROM（Rear NVME-n OptionROM）] ドロップダウンリスト **set PcieSlotRearNvme*n*OptionROM**	（注） このオプションは、Cisco UCS C245 M6 サーバーにのみ適用されます。 このオプションでは、SSD:NVMe スロット*n*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。 • [無効（Disabled）]：SSD:NVMe1 スロットに接続されている PCIe アダプタのオプションの ROM を実行しません。 • [有効（Enabled）]：SSD:NVMe1 スロットに接続されている PCIe アダプタのオプション ROM を実行します

名前	説明
Rear NVME *n* Link Speed [ドロップダウンリスト（drop-down list）] **set PcieSlotRearNvme*n*LinkSpeed**	（注） このオプションは、Cisco UCS C245 M6 サーバーにのみ適用されます。 スロット *n* で指定された NVMe 前面スロットのリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効となり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：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。 • **[GEN4]**：リンク速度は第 4 世代まで到達可能です。
[PCIe スロット MSTOR RAID OptionROM (PCIe Slot MSTOR RAID OptionROM)] ドロップダウン リスト **set PcieSlotMSTORRAIDOptionROM**	サーバが PCIe MSTOR RAID のオプション ROM を使用するかどうか。次のいずれかになります。 • Disabled：オプション ROM は使用できません。 • [Enabled]—オプション ROM は使用できます。

名前	説明
[PCIe Slot MSTOR リンク速度（PCIe Slot MSTOR Link Speed）] ドロップダウンリスト **set PcieSlotMSTORRAIDLinkSpeed**	スロット *n* で指定された PCIe 前面スロットのリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効となり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：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。 • **[GEN4]**：リンク速度は第 4 世代まで到達可能です。
[IPV6 PXE サポート（IPV6 PXE Support）] ドロップダウン リスト **set IPV6PXE**	PXE の IPv6 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 • **[無効 (disabled)]** : PV6 PXE のサポートは利用できません。 • **[enabled (有効)]**:IPV6 PXE のサポートを常に利用できます。
[IPV4 PXE サポート (IPV4 PXE Support)] ドロップダウン リスト **set IPV4PXE**	PXE の IPv4 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 • **[無効 (disabled)]**: IPV4 PXE のサポートは利用できません。 • **[enabled (有効)]**: IPV4 PXE のサポートを常に利用できます。

名前	説明
[PCIe ARI サポート (PCIe ARI Support)] ドロップダウン リスト **set PcieARISupport**	Windows での PCI 代替ルーティング ID 解釈（ARI）サポートが有効になっているかどうか。次のいずれかになります。 • **[自動（auto）]**：ARI サポートは、システムによって自動制御されるように設定されます。 • **[無効（disabled）]**：ARI サポートは使用できません。 • **[有効（enabled）]**：ARI サポートを常に使用できます。
[SR-IOVサポート（SR-IOV Support）] ドロップダウン リスト **set SrIov**	SR-IOV 機能により、PCIe デバイスは複数の個別の物理 PCIe デバイスのように見えます。次のいずれかになります。 • **[無効（Disabled）]**：SR-IOV 機能は無効です。 • **[有効（Enabled）]**：SR-IOV 機能は有効です。
[IPv6 HTTP サポート（IPv6 HTTP Support）] ドロップダウン リスト **set IPV6HTTP**	HTTP の IPv6 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。 • **[無効（disabled）]**：IPv6 HTTP サポートは使用できません。 • **[有効（enabled）]**：IPv6 HTTP サポートを常に使用できます。
[IPV4 HTTP サポート（IPV4 HTTP Support）] ドロップダウン リスト **set IPV4HTTP**	HTTP の IPv4 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。 • **[無効（disabled）]**：IPv4 HTTP サポートは使用できません。 • **[有効（enabled）]**：IPv4 HTTP サポートを常に使用できます。

名前	説明
[Network Stack (ネットワーク スタック)] ドロップダウン リスト **set NetworkStack**	このオプションでは、IPv6 と IPv4 をモニタできます。次のいずれかになります • **[無効 (disabled)]**: ネットワーク スタックのサポートは使用できません。 （注） 無効にすると、**IPV4 PXE サポート**に設定された値はシステムに影響しません。 • **[enabled (有効)]**: ネットワーク スタックのサポートを常に利用できます。

[Server Management] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *16 : [*サーバ管理（*Server Management*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバー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、変更内容はサーバーが手動でリブートされるまで保存されます。
[OS ブート ウォッチドッグ タイマー ポリシー（OS Boot Watchdog Timer Policy）] ドロップダウン リスト **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。 • [電源オフ（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、サーバーはリセットされます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にする場合にのみ適用されます。

名前	説明
[FRB 2 タイマー（FRB 2 Timer）] ドロップダウン リスト **set FRB-2**	POST 中にシステムがハングした場合に、システムを回復するために Cisco IMC によって FRB2 タイマーが使用されるかどうか。次のいずれかになります。 • [無効（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 ウォッチドッグ タイマー（OS Watchdog Timer）] ドロップダウン リスト **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]：サーバーのブートにかかる時間をトラッキングするためにウォッチドッグ タイマーは使用されません。 • [有効（enabled）]：サーバーがブートにかかる時間をウォッチドッグ タイマーで追跡します。サーバーのブートが [OS ブート ウォッチドッグ タイマー タイムアウト（OS Boot Watchdog Timer Timeout）] フィールドで指定された時間内に完了しない場合は、Cisco IMC によってエラーがログに記録され、[OS ブート ウォッチドッグ ポリシー（OS Boot Watchdog Policy）] フィールドで指定されたアクションが実行されます。

名前	説明
[OS ブート ウォッチドッグ タイマー タイムアウト（OS Watchdog Timer Timeout）] ドロップダウン リスト **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 分（5 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [10 分（10 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [15 分（15 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [20 分（20 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にした場合にのみ適用されます。

名前	説明
[ボー レート（Baud Rate）] ドロップダウン リスト **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。[コンソール リダイレクション（Console Redirection）] を無効にした場合、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]：9,600 ボー レートが使用されます。 • [19.2k]：19,200 ボー レートが使用されます。 • [38.4k]：38,400 ボー レートが使用されます。 • [57.6k]：57,600 ボー レートが使用されます。 • [115.2k]：115,200 ボー レートが使用されます。 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。
[フロー制御（Flow Control）] ドロップダウン リスト **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を設定します。送信要求/クリア ツー セント（RTS/CTS）を使用すると、隠れた端末の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。 • [なし（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。

サーバー モデル別 BIOS パラメータ

名前	説明
[コンソール リダイレクション（Console Redirection）] ドロップダウン リスト **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 リダイレクションで使用できるようにします。OS 起動後は、コンソールのリダイレクトが関係なくなります。次のいずれかになります。 • **[COM 0]**：POST 中に COM 1 でコンソール リダイレクションを有効にします。 • **[COM 1]**：POST 中に COM 1 でコンソール リダイレクションを有効にします。 • [Disabled]：POST 中にコンソール リダイレクションは発生しません。
[ターミナル タイプ（Terminal Type）] ドロップダウン リスト **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。

名前	説明
[PCIe Slots CDN コントロール（PCIe Slots CDN Control）] ドロップダウンリスト **set PcieSlotsCdnEnable**	（注） このオプションは、スロット 2 または 5 に Mellanox カードを搭載した Cisco UCS C245 M6 サーバーでのみ使用できます。 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。 • [無効（Disabled）]：VIC カードに対する CDN サポートは無効です。 • [有効（Enabled）]：VIC カードの CDN サポートが有効になります。
[CDN コントロール（CDN Control）] ドロップダウン リスト **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。 • [無効（Disabled）]：VIC カードに対する CDN サポートは無効です。 • [有効（Enabled）]：VIC カードの CDN サポートが有効になります。
[OptionROM起動最適化（OptionROM Launch Optimization）] **set CiscoOpromLaunchOptimization**	このオプションが [有効（Enabled）] の場合、ブート順序のポリシーに存在するコントローラにのみ OptionROMs が起動されます。 （注） オンボードストレージコントローラ、Emulex FC アダプタおよび GPU コントローラなどのいくつかのコントローラについて、ブート順序のポリシーに含まれていなくても、OptionROM が起動されます。 このオプションが [無効（Disabled）] の場合、すべての OptionROMs が起動されます。

名前	説明
[BIOS Techlogレベル（BIOS Techlog Level）] **set CiscoDebugLevel**	このオプションは、**BIOS tech ログファイル**のメッセージのタイプを示します。 ログファイルには、次のタイプのいずれかを指定できます。 • [最小（Minimum）]：重要なメッセージがログファイルに表示されます。 • [標準（Normal）]：警告およびロードメッセージがログファイルに表示されます。 • [最大（Maximum）]：標準に加え、情報関連のメッセージがログファイルに表示されます。 デフォルト値：[最小（Minimum）] （注） このオプションは、主に、内部のデバッグを目としています。

[セキュリティ（Security）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *17 : [*セキュリティ管理（*Security Management*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバー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、変更内容はサーバーが手動でリブートされるまで保存されます。

名前	説明
[トラステッド プラットフォーム モジュール状態（Trusted Platform Module State）] ドロップダウンリスト **set TPMControl**	信頼されたプラットフォーム モジュール（TPM）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。次のいずれかになります。 • [Disabled]：サーバーはTPM を使用しません。 • [有効（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ください。
[SHA-1 PCR バンク（SHA-1 PCR Bank）] ドロップダウンリスト **set SHA1PCRBank**	SHA-1 PCR バンクを有効または無効にします。次のいずれかになります。 • **[無効（Disabled）]**：サーバーはこの機能を使用しません。 • **[有効（Enabled）]**：サーバーはこの機能を使用します。
[SHA-256 PCR バンク（SHA-256 PCR Bank）] ドロップダウンリスト **set SHA256PCRBank**	SHA256 PCR バンクを有効または無効にします。次のいずれかになります。 • **[無効（Disabled）]**：サーバーはこの機能を使用しません。 • **[有効（Enabled）]**：サーバーはこの機能を使用します。

名前	説明
[電源オン パスワード（Power On Password）] ドロップダウン リスト **set PowerOnPassword**	このトークンでは、F2 BIOS 設定を使用する前にBIOSパスワードを設定する必要があります。有効にすると、BIOS関数（IO設定、BIOSセットアップ、BIOSを使用したオペレーティング システムへのブート）にアクセスする前にパスワードの検証が必要になります。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

メモリ タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *18 : [*メモリ（*Memory*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（**Reboot Host Immediately**）**]** チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバー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、変更内容はサーバーが手動でリブートされるまで保存されます。

名前	説明
[ソケットごとのNUMAノード（NUMA Nodes per Socket）] ドロップダウンリスト **set CbsDfCmnDramNps**	ソケットごとにメモリNUMAドメインを構成できます。次のいずれかになります。 • **[自動（Auto）]**：チャネル数を自動に設定します。 • **[NPS0]**：システムごとのNUMAノード数を1にします。 • **[NPS1]**：ソケットごとのNUMAノード数を1にします。 • **[NPS2]**：ソケットごとのNUMAノード数を2にし、SoCの左半分と右半分に1つずつにします。 • **[NPS4]**：ソケットごとのNUMAノード数を4にし、クワドラントごとに1つにします。
[4 G以上の復号化（Above 4G Decoding）] ドロップダウン リスト **set MemoryMappedIOAbove4GB**	4 GB以上のMMIOを有効または無効にします。次のいずれかになります。 • [Disabled]：サーバーでは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。 • [有効（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。

サーバー モデル別 BIOS パラメータ

名前	説明
[Chipselect Interleaving] ドロップダウンリスト **set CbsCmnMemMapBankInterleaveDdr4**	ノード 0 に選択する DRAM チップ経由でメモリブロックがインターリーブされるかどうか。次のいずれかになります。 • **[無効（Disabled）]**：チップの選択は、メモリ コントローラ内でインターリーブされません。 • **[自動（Auto）]**：CPU でチップ セレクトのインタリーブの方法を自動的に決定します。
[メモリ インターリービング サイズ（Memory Interleaving Size）] ドロップダウンリスト **set CbsDfCmnMemIntlvSize**	インターリーブされるメモリ ブロックのサイズを決定します。また、インターリーブの開始アドレス（ビット 8、9、10、11）も指定します。次のいずれかになります。 • **Auto** • **256 バイト** • **512 バイト** • **1 KB** • **2 KB** • **4 KB**
[IOMMU] ドロップダウンリスト **set CbsCmnGnbNbIOMMU**	出入力メモリ管理ユニット（IOMMU） により、AMDプロセッサが物理アドレスへ仮想アドレスをマッピングすることが可能です。次のいずれかになります。 • **[自動（Auto）]**：これらのアドレスのマッピング方法を CPU で決定します。 • **[無効（Disabled）]**：IOMMU は使用されません。 • **[有効（Enabled）]**：IOMMU によりアドレスマッピングを行います。

名前	説明
BankGroupSwap **set CbsCmnMemCtrlBankGroupSwapDdr4**	物理アドレスをアプリケーションに割り当てる方法を決定します。次のいずれかになります。 • **[自動（Auto）]**：アプリケーションへの物理アドレスの割り当て方法を CPU で自動的に決定します。 • **[無効（Disabled）]**：バンク グループ スワップは使用されません。 • **[有効（Enabled）]**：バンク グループ スワップによりアプリケーションのパフォーマンスを向上させます。
[TSME] ドロップダウンリスト **set TSME**	透過的セキュア メモリ暗号化（TSME）を有効にすることができます。次のいずれかになります。 • **[自動（Auto）]**：機能の使用は自動に設定されます。 • **[無効（Disabled）]**：プロセッサで TSME 機能を使用しません。 • **[有効（Enabled）]**：プロセッサで TSME 機能を使用します。
[SMEE] ドロップダウンリスト **set CbsCmnCpuSmee**	プロセッサで、メモリの暗号化サポートを実現する Secure Memory Encryption Enable（SMEE）機能を使用するかどうかを指定します。次のいずれかになります。 • **[自動（Auto）]**：これらのアドレスのマッピング方法を CPU で決定します。 • **[無効（Disabled）]**：プロセッサで SMEE 機能を使用しません。 • **[有効（Enabled）]**：プロセッサで SMEE 機能を使用します。

名前	説明
[SNP メモリ カバレッジ（SNP Memory Coverage）] ドロップダウンリスト **set CbsDbgCpuSnpMemCover**	SNP メモリ カバレッジを設定できます。次のいずれかになります。 • **[自動（Auto）]**：システムがメモリ カバレッジを決定します。 • **[無効（Disabled）]**：プロセッサはこの機能を使用しません。 • **[有効（Enabled）]**：この機能は有効です。 • **[カスタム（Custom）]**：カスタム サイズは、**[カバーする SNP メモリ サイズ（SNP Memory Size to Cover）]** で定義できます。
[SEV-SNP サポート（SEV-SNP Support）] ドロップダウン リスト **set CbsSevSnpSupport**	セキュア ネスティッド ページング機能を有効にできます。次のいずれかになります。 • **[無効（Disabled）]**：プロセッサで SEV-SNP 機能を使用しません。 • **[有効（Enabled）]**：プロセッサで SEV-SNP 機能を使用します。
[BME DMA 移行 (BME DMA Mitigation)] ドロップダウン リスト **set BmeDmaMitigation**	不正な外部 DMA からの脅威を緩和する PCI BME ビットを無効にできます。次のいずれかになります。 • **[無効 (disabled)]**: PCI BME ビットは BIOS で無効になっています。 • **[有効 (Enabled)**: PCI BME ビットは BIOS で有効になっています。
[カバーされる SNP メモリ サイズ（MB）（SNP Memory Size to Cover in MB）] フィールド **set CbsDbgCpuSnpMemSizeCover**	SNP メモリ サイズを設定できます。
バーストおよび遅延された更新（Burst and Postponed Refresh）] フィールド **set BurstAndPostponedRefresh**	• **[無効（disabled）]**：プロセッサはこの機能を使用しません。 • **[有効（enabled）]**：プロセッサはこの機能を使用します。

名前	説明
[パッケージ修復のポスト（Post Package Repair）] フィールド **set PostPackageRepair**	Cisco IMC は、指定された障害のある行から指定されたスペア行へのアクセスを永続的に再マッピングする、ハード PPRをサポートしています。次のいずれかになります。 • **[ハード PPR (Hard PPR)]**: サポートは有効になっています。 • [Disabled]：サポートはディセーブルになっています。

[電源/パフォーマンス（Power/Performance）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *19 : [*電源/パフォーマンス（*Power/Performance*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（Reboot Host Immediately）] チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバー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、変更内容はサーバーが手動でリブートされるまで保存されます。
[Core Performance Boost] ドロップダウンリスト **set CbsCmnCpuCpb**	AMD プロセッサがアイドル状態（ほとんど使用されていない状態）のときにコアの周波数を上げるかどうかを指定します。次のいずれかになります。 • **[auto]**：パフォーマンスをブーストする方法を CPU で自動的に決定します。 • **[disabled]**：CPU により自動的にブーストパフォーマンスが決定されます。

名前	説明
[Global C-state Control] ドロップダウンリスト **set CbsCmnCpuGlobalCstateCtrl**	AMD プロセッサが IO ベースの C ステートおよびDF Cステートを制御するかどうかに関係なく、これは次のうちいずれかになります。 • **[auto]**：CPU で IO ベースの C ステートの生成方法を自動的に決定します。 • **[disabled]**：グローバル C ステートの制御が無効になります。 • **[enabled]**：グローバル C ステートの制御が有効になります。
[L1 Stream HW Prefetcher] ドロップダウンリスト **set CbsCmnCpuL1StreamHwPrefetcher**	プロセッサで、AMD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、L1 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。 • [auto][Auto]：CPU は、I/Oデバイスからプロセッサ キャッシュにデータを配置する方法を決定します。 • [disabled][Disabled]：ハードウェアプリフェッチャは使用しません。 • [enabled][Enabled]：プロセッサで、キャッシュの問題が検出されたときにハードウェア プリフェッチャを使用します。
[L2 Stream HW Prefetcher] ドロップダウンリスト **set CbsCmnCpuL2StreamHwPrefetcher**	プロセッサで、AMDハードウェアプリフェッチャが必要に応じてメモリからデータおよび命令ストリームを取得し、L2 キャッシュに入れることを許可するかどうかを指定します。次のいずれかになります。 • [auto][Auto]：CPU は、I/Oデバイスからプロセッサ キャッシュにデータを配置する方法を決定します。 • [disabled][Disabled]：ハードウェアプリフェッチャは使用しません。 • [enabled][Enabled]：プロセッサで、キャッシュの問題が検出されたときにハードウェア プリフェッチャを使用します。

名前	説明
[Determinism Slider] ドロップダウンリスト **set CbsCmnDeterminismSlider**	AMDプロセッサにより動作方法を決定できます。次のいずれかになります。 • **[auto]**：CPUはデフォルトの決定論的な電源設定を自動で使用します。 • **[performance]**：プロセッサは、最適なパフォーマンスかつ一貫した方法で動作します。 • **[power]**：プロセッサは、ダイごとに許容される最大のパフォーマンスで動作します。
[CPPC] ドロップダウンリスト **set CbsCmnGnbSMUCPPC**	コラボレーティブ プロセッサ パフォーマンス制御を設定できます。 次のいずれかになります。 • **自動**：CPU はデフォルトの CPPC 設定を自動で使用します。 • **無効**：機能は無効です。 • **有効**：コラボレーティブ プロセッサ パフォーマンスが有効になっています。
[効率モードの有効（Efficiency Mode Enable）] ドロップダウン リスト **set CbsCmnEfficiencyModeEn**	効率に基づいて消費電力を設定できます。 次のいずれかになります。 • **自動**：CPU はデフォルトの設定を自動で使用します。 • **有効**：効率モードは有効です。

[プロセッサ（Processor）] タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

サーバー モデル別 BIOS パラメータ

表 *20 : [*プロセッサ（*Processor*）*]* タブの *BIOS* パラメータ

名前	説明
[ホストを即座リブート（**Reboot Host Immediately**）**]** チェック ボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバー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、変更内容はサーバーが手動でリブートされるまで保存されます。
[SVM Mode] ドロップダウンリスト **set SvmMode**	プロセッサが AMD セキュア仮想マシン テクノロジを使用するかどうか。次のいずれかを選択できます。 • **[disabled]**：プロセッサで SVM テクノロジーを使用しません。 • **[enabled]**：プロセッサで SVM テクノロジーを使用します。
[SMT Mode] ドロップダウンリスト **set CbsCpuSmtCtrl**	プロセッサで AMD Simultaneous MultiThreading テクノロジーを使用するかどうかを指定します。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。 • **[auto]**：プロセッサは、マルチスレッドの並列実行を許可します。 • **[**無効（**disabled**）**]**：プロセッサで SMT モードを使用しません。 • **[**有効（**enabled**）**]**：プロセッサで SMT モードを使用します。

名前	説明
[ダウンコア制御 7xx2（Downcore control 7xx2）] ドロップダウンリスト **set CbsCmnCpuGenDowncoreCtrl**	（注） このトークンは、7xx2 モデルのプロセッサを搭載した Tehama サーバーにのみ適用されます。 1 つ以上のコアの動作を停止する機能を提供します。シリコン回路でサポートされています。OS の制限、またはシステムの電力削減要件により、コア数を減らすことが望ましい場合があります。この項目により、実行中のコアの数を制御できます。この設定では、プロセッサで使用可能なコアの数を減らすことしかできません。次のいずれかになります。 • **[auto]**：有効化する必要のあるコアの数を CPU で判断します。 • TWO（1+1）：片方の CPU コンプレックスで 2 つのコアを有効にします。 • FOUR（2+2）：1 つの CPU コンプレックスで 4 つのコアを有効にします。 • SIX（3+3）：1 つの CPU コンプレックスで 6 つのコアを有効にします。

サーバー モデル別 BIOS パラメータ

名前	説明
[CPU ダウンコア制御 7xx3（CPU Downcore control 7xx3） ドロップダウンリスト **set CbsCpuCoreCtrl**	（注） このトークンは、7xx3 モデルのプロセッサを搭載した Tehama サーバーにのみ適用されます。 1つ以上のコアの動作を停止する機能を提供します。シリコン回路でサポートされています。OS の制限、またはシステムの電力削減要件により、コア数を減らすことが望ましい場合があります。この項目により、実行中のコアの数を制御できます。この設定では、プロセッサで使用可能なコアの数を減らすことしかできません。次のいずれかになります。 • **[auto]**：有効化する必要のあるコアの数を CPU で判断します。 • One（1+0）：1 つの CPU コンプレックスで 1 つのコアを有効にします。 • [TWO（2+0）]：片方の CPU コンプレックスのみで 2 つのコアを有効にします。 • [THREE（3+0）]：片方の CPU コンプレックスのみで 3 つのコアを有効にします。 • [FOUR（4+0）]：片方の CPU コンプレックスのみで 4 つのコアを有効にします。 • Five（5+0）：1 つの CPU コンプレックスで 5 つのコアを有効にします。 • SIX（6+0）：1 つの CPU コンプレックスで 6 つのコアを有効にします。 • SEVEN（7+0）：1 つの CPU コンプレックスで 7 つのコアを有効にします。

名前	説明
[固定 SOC P ステート（Fixed SOC P-State）] ドロップダウンリスト **set CbsCmnFixedSocPstate**	このオプションは、APBDIS が設定されている場合のターゲット PState を定義します。**P*x***：取り付けられているプロセッサの有効な P ステートを指定します。次のいずれかになります。 • P0 • P1 • P2 • P3 • 自動（Auto）
[APBDIS] ドロップダウンリスト **set CbsCmnApbdis**	SMU の APB 無効化の値を選択できます。次のいずれかになります。 • **0**：SMU への ApbDis をクリアします。 • **[1]**：SMU への ApbDis を設定します。 • **[自動（auto）]**：CPU が値を判断します。
[CCD 制御（CCD Control）] ドロップダウンリスト **set CbsCpuCcdCtrlSsp**	システムで有効にしたい CCD の数を指定できます。次のいずれかになります。 • **[自動（Auto）]**：プロセッサによって提供される最大数の CCD が有効になります。 • 2 CCD • 3 CCD • 4 CCD • 6 CCD
[Cisco xGMI 最大速度（Cisco xGMI Max Speed）] ドロップダウンリスト **set CiscoXgmiMaxSpeed**	このオプションは、18 Gbps XGMI リンク速度を有効にします。次のいずれかになります。 • **[無効（Disabled）]**：機能は無効です。 • **[有効（Enabled）]** — 機能は有効です。

名前	説明
[NUMAドメインとしての ACPI SRAT L3 キャッシュ（ACPI SRAT L3 Cache As NUMA Domain）] ドロップダウンリスト **set CbsDfCmnAcpiSratL3Numa**	各 CCX がそのオン ドメインにあると宣言されている物理ドメインの上に仮想ドメインのレイヤーを作成します。次のいずれかになります。 • **[自動（Auto）]**：自動モードに設定します。 • **[無効（Disabled）]**：ドメイン構成に NPS 設定を使用します。 • **[有効（Enabled）]**：各 CCX を独自のドメインにあると宣言します。
[ストリーミング ストア制御（Streaming Stores Control）] ドロップダウンリスト **set CbsCmnCpuStreamingStoresCtrl**	ストリーミング ストア機能を有効にします。次のいずれかになります。 • **[自動（Auto）]**：自動モードに設定します。 • **[無効（Disabled）]**：機能は無効です。 • **[有効（Enabled）]** — 機能は有効です。
[DF C ステート（DF C-States）] ドロップダウンリスト **set CbsCmnGnbSMUDfCstates**	システムで長時間のアイドル状態が予想される場合、この制御により、システムは、システムをさらに低電力状態に設定できる DF C ステートに移行できます。次のいずれかになります。 • **[自動（Auto）]**：自動モードに設定します。 • **[無効（Disabled）]**：長時間のアイドル状態は予想されないため、省電力は実現されません。 • **[有効（Enabled）]**：このオプションはアクティブです。システムがアイドル状態のときに電力を節約します。

C125 サーバの場合

[Server Management] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

表 *21 : [*サーバ管理（*Server Management*）*]* タブの *BIOS* パラメータ

名前	説明
[Reboot Host Immediately] チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバー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、変更内容はサーバーが手動でリブートされるまで保存されます。
[OS ブート ウォッチドッグ タイマー ポリシー（OS Boot Watchdog Timer Policy）] ドロップダウン リスト **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。 • [電源オフ（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、サーバーはリセットされます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にする場合にのみ適用されます。

名前	説明
[OS ウォッチドッグ タイマー（OS Watchdog Timer）] ドロップダウン リスト **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]：サーバーのブートにかかる時間をトラッキングするためにウォッチドッグ タイマーは使用されません。 • [有効（enabled）]：サーバーがブートにかかる時間をウォッチドッグ タイマーで追跡します。サーバーのブートが [OS ブート ウォッチドッグ タイマー タイムアウト（OS Boot Watchdog Timer Timeout）] フィールドで指定された時間内に完了しない場合は、Cisco IMC によってエラーがログに記録され、[OS ブート ウォッチドッグ ポリシー（OS Boot Watchdog Policy）] フィールドで指定されたアクションが実行されます。
[ボー レート（Baud Rate）] ドロップダウン リスト **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。[コンソール リダイレクション（Console Redirection）] を無効にした場合、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]：9,600 ボー レートが使用されます。 • [19.2k]：19,200 ボー レートが使用されます。 • [38.4k]：38,400 ボー レートが使用されます。 • [57.6k]：57,600 ボー レートが使用されます。 • [115.2k]：115,200 ボー レートが使用されます。 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
[コンソール リダイレクション（Console Redirection）] ドロップダウン リスト **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 リダイレクションで使用できるようにします。OS 起動後は、コンソールのリダイレクトが関係なくなります。次のいずれかになります。 • [シリアル ポート 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有効にします。 • [シリアル ポート B（Serial Port B）]：POST 中にシリアル ポート B でコンソール リダイレクションを有効にします。 • [無効（Disabled）]：POST 中にコンソール リダイレクションは発生しません。

サーバー モデル別 BIOS パラメータ

名前	説明
[BIOS Techlogレベル（BIOS Techlog Level）]	このオプションは、**BIOS tech ログファイル**のメッセージのタイプを示します。 ログファイルには、次のタイプのいずれかを指定できます。 • [最小（Minimum）]：重要なメッセージがログファイルに表示されます。 • [標準（Normal）]：警告およびロードメッセージがログファイルに表示されます。 • [最大（Maximum）]：標準に加え、情報関連のメッセージがログファイルに表示されます。 デフォルト値：[最小（Minimum）] （注） このオプションは、主に、内部のデバッグを目としています。 （注） [高速ブート（Fast Boot）] オプションを無効にするには、エンドユーザは次のトークンを下記の説明のとおりに設定する必要があります。 [BIOS Techlogレベル（BIOS Techlog level）] を [標準（Normal）] に [OptionROM起動最適化（OptionROM Launch Optimization）] を [無効（Disabled）] に

名前	説明
[OptionROM起動最適化（OptionROM Launch Optimization）]	このオプションが [有効（Enabled）] の場合、ブート順序のポリシーに存在するコントローラにのみ OptionROMs が起動されます。 （注） ブート順序のポリシーにはリストされていないオンボードストレージコントローラでは、OptionROM が起動されます。 このオプションが [無効（Disabled）] の場合、すべての OptionROMs が起動されます。 デフォルト値：[有効（Enabled）]
[FRB 2 タイマー（FRB 2 Timer）] ドロップダウン リスト **set FRB-2**	POST 中にシステムがハングした場合に、システムを回復するために Cisco IMC によって FRB2 タイマーが使用されるかどうか。次のいずれかになります。 • [無効（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。

サーバー モデル別 BIOS パラメータ

名前	説明
[OS ブート ウォッチドッグ タイマー タイムアウト（OS Watchdog Timer Timeout）] ドロップダウン リスト **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 分（5 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [10 分（10 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [15 分（15 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [20 分（20 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 （注） このオプションは [OS ブート ウォッチドッグ タイマー（OS Boot Watchdog Timer）] を有効にした場合にのみ適用されます。
[フロー制御（Flow Control）] ドロップダウン リスト **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を設定します。送信要求/クリア ツー セント（RTS/CTS）を使用すると、隠れた端末の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。 • [なし（None）]：フロー制御は使用されません。 • [RTS/CTS]：RTS/CTS がフロー制御に使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。

名前	説明
[ターミナル タイプ（Terminal Type）] ドロップダウン リスト **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。
[CDN コントロール（CDN Control）] ドロップダウン リスト **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。 • [無効（Disabled）]：VICカードに対するCDNサポートは無効です。 • [有効（Enabled）]：CDNサポートはVICカードに対して有効です。

[セキュリティ（Security）] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

サーバー モデル別 BIOS パラメータ

表 *22 : [*セキュリティ（*Security*）*]* タブの *BIOS* パラメータ

名前	説明
[Reboot Host Immediately] チェックボックス	**[**ホストを即座にリブート（**Reboot Host Immediately**）**]** チェックボックスがオフの場合、サーバー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、変更内容はサーバーが手動でリブートされるまで保存されます。
[信頼されたプラットフォームモジュールのサポート（Trusted Platform Module Support）] ドロップダウン リスト **set TPMAdminCtrl**	信頼されたプラットフォーム モジュール（TPM）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]：サーバーは TPM を使用しません。 • [有効（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ください。
[電源オン パスワード（Power On Password）] ドロップダウン リスト **set PowerOnPassword**	このトークンでは、F2 BIOS 設定を使用する前に BIOS パスワードを設定する必要があります。有効にすると、BIOS 関数（IO 設定、BIOS セットアップ、BIOS を使用したオペレーティング システムへのブート）にアクセスする前にパスワードの検証が必要になります。次のいずれかを指定できます。 • **[無効（Disabled）]**：サポートは無効になります。 • [Enabled]：サポートはイネーブルになっています。

[Memory] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

表 *23 : [*メモリ（***Memory***）*]* タブの ***BIOS*** パラメータ

名前	説明
[今すぐホストを再起動（Reboot Host Immediately）] チェックボックス	このチェックボックスをオンにすると、直ちにホスト サーバが再起動します。このチェックボックスは、変更を保存してからオンにする必要があります。
[4 G 以上の復号化（Above 4G Decoding）] ドロップダウン リスト **set MemoryMappedIOAbove4GB**	4 GB 以上の MMIO を有効または無効にします。次のいずれかになります。 • [Disabled]：サーバーでは 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。 • [有効（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
[Memory Interleaving]ドロップダウン リスト	物理メモリの更新中に別のメモリにアクセスできるよう、AMD CPU がメモリをインターリーブするかどうかを指定します。このオプションは、ファブリック レベルでメモリのインターリーブを制御します。チャネル、ダイ、ソケットの要件はメモリによって異なるため、選択したオプションがメモリでサポートされない場合これらは無視されます。次のいずれかを選択できます。 • **[auto]**：CPUがメモリのインターリーブの方法を決定します。 • **[channel]**：各チャネルに単一の連続したアドレス空間を配置するのではなく、複数のチャネル全体に物理アドレス空間をインターリーブします。 • **[die]**：各ダイに単一の連続したアドレス空間を配置するのではなく、複数のダイ全体に物理アドレス空間をインターリーブします。 • **[none]**：同一の物理メモリから連続したメモリ ブロックにアクセスします。 • **[socket]**：各ソケットに単一の連続したアドレス空間を配置するのではなく、複数のソケット全体に物理アドレス空間をインターリーブします。 • [Platform Default][platform-default]：BIOSは、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Memory Interleaving] ドロップダウン リスト	インターリーブされるメモリ ブロックのサイズを決定します。また、インターリーブの開始アドレス（ビット 8、9、10、11）も指定します。次のいずれかになります。 • 1 KB • 2 KB • 256 バイト • 512 バイト • **自動**: CPU、メモリ ブロックのサイズを決定します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOS デフォルト値に含まれるこの属性の値を使用します。
[Chipselect Interleaving] ドロップダウンリスト	ノード 0 に選択する DRAM チップ経由でメモリ ブロックがインターリーブされるかどうか。次のいずれかになります。 • **[auto]**：CPU でチップ セレクトのインタリーブの方法を自動的に決定します。 • **[disabled]**：チップの選択は、メモリ コントローラ内でインターリーブされません。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Bank Group Swap] ドロップダウンリスト	物理アドレスをアプリケーションに割り当てる方法を決定します。次のいずれかになります。 • **[auto]**：アプリケーションへの物理アドレスの割り当て方法を CPU で自動的に決定します。 • **[disabled]**：バンク グループ スワップは使用されません。 • **[enabled]**：バンク グループ スワップによりアプリケーションのパフォーマンスを向上させます。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOS デフォルト値に含まれるこの属性の値を使用します。
[IOMMU] ドロップダウンリスト	出入力メモリ管理ユニット（IOMMU） により、AMD プロセッサが物理アドレスへ仮想アドレスをマッピングすることが可能です。次のいずれかになります。 • **[auto]**：これらのアドレスのマッピング方法を CPU で決定します。 • **[disabled]**：IOMMU は使用されません。 • **[enabled]**：IOMMU によりアドレス マッピングを行います。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[SMEE] ドロップダウンリスト	プロセッサで、メモリの暗号化サポートを実現する Secure Memory Encryption Enable（SMEE）機能を使用するかどうかを指定します。次のいずれかになります。 • **[disabled]**：プロセッサで SMEE 機能を使用しません。 • **[enabled]**：プロセッサで SMEE 機能を使用します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOS デフォルト値に含まれるこの属性の値を使用します。
[TSME] ドロップダウンリスト	プロセッサで、メモリの暗号化サポートを実現する透過的セキュアメモリ暗号化（TSME）機能を使用するかどうかを指定します。次のいずれかになります。 • **[無効（disabled）]**：プロセッサは TSME 機能を使用しません。 • **[有効（enabled）]**：プロセッサは TSME 機能を使用します。 • **[自動（auto）]**：BIOS は、サーバー タイプとベンダーに関する BIOS のデフォルト設定に含まれるこの属性の値を使用します。
[SEV] ドロップダウンリスト	VM のコードとデータが分離された、暗号化仮想マシン（VM）の実行を有効にします。次のいずれかになります。 • **[253_ASIDs]**：値は 253 の最小アドレス空間識別子（ASID）に設定されます。 • **[509_ASIDs]**：値は 509 の最小アドレス空間識別子（ASID）に設定されます。 • **[自動（auto）]**：BIOS は、サーバー タイプとベンダーに関する BIOS のデフォルト設定に含まれるこの属性の値を使用します。

名前	説明
[DRAM SW サーマル スロットリング（DRAM SW Thermal Throttling）] ドロップダウンリスト	ソフトウェアが温度制限内で機能することを保証する保護メカニズムを提供します。温度が最大しきい値を超えると、パフォーマンスを低下させ、最小しきい値まで冷却します。次のいずれかになります。 • **[無効（disabled）]**：プロセッサはこの機能を使用しません。 • **[有効（enabled）]**：プロセッサはこの機能を使用します。 • **[自動（auto）]**：BIOS は、サーバー タイプとベンダーに関する BIOS のデフォルト設定に含まれるこの属性の値を使用します。
[バーストおよび遅延リフレッシュ（Burst and Postponed Refresh）] ドロップダウンリスト	• **[無効（disabled）]**：プロセッサはこの機能を使用しません。 • **[有効（enabled）]**：プロセッサはこの機能を使用します。 • **[自動（auto）]**：BIOS は、サーバー タイプとベンダーに関する BIOS のデフォルト設定に含まれるこの属性の値を使用します。

[I/O] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

表 *24 : [I/O]* タブの *BIOS* パラメータ

名前	説明
[今すぐホストを再起動（Reboot Host Immediately）] チェックボックス	このチェックボックスをオンにすると、直ちにホスト サーバが再起動します。このチェックボックスは、変更を保存してからオンにする必要があります。

名前	説明
[PCIe スロット *n* Oprom（Pcie Slot n Oprom）] ドロップダウン リスト **set PcieSlotnOptionROM**	サーバーが *n* で指定した PCIe カード スロットにあるオプション ROM を使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：スロット *n* のオプションの ROM は使用できません。 • [有効（Enabled）]：スロット *n* のオプション ROM は使用可能です。
[PCIe スロット *n* リンク速度（PCIe Slot n Link Speed）] ドロップダウン リスト **set PcieSlotnLinkSpeed**	システム IO コントローラ *n*（SIOCn）アドオン スロット（*n* によって示される）のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効となり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：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。
[IPV6 PXE サポート（IPV6 PXE Support）] ドロップダウン リスト **set IPV6PXE**	PXE の IPv6 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 • [無効（disabled）][無効（Disabled）]：IPV6 PXEのサポートは利用できません。 • [enabled][Enabled]：IPV6 PXEのサポートを常に利用できます。
[IPV4 PXE サポート (IPV4 PXE Support)]ドロップダウン リスト **set IPV4PXE**	PXE の IPv4 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。 • [無効（disabled）][無効（Disabled）]：IPV4 PXEのサポートは利用できません。 • [enabled][Enabled]：IPV4 PXEのサポートを常に利用できます。
[SR-IOV サポート（SR-IOV Support）] ドロップダウン リスト **set SrIov**	サーバー上で SR-IOV（Single Root I/O Virtualization）を有効にするか無効にするか。次のいずれかになります。 • [Disabled]：SR-IOV は無効になります。 • [有効（Enabled）]：SR-IOV はイネーブルになります。

名前	説明
[前面 NVME *n* OptionROM（Front NVME n OptionROM）] ドロップダウンリスト **set PcieSlot *n*OptionROM**	このオプションでは、SSD:NVMe *n* 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。 • **[無効（disabled）]**：SSD:NVMe *n* スロットに接続されている PCIe アダプタのオプションの ROM を実行しません。 • **[有効（enabled）]**：SSD:NVMe *n* スロットに接続されている PCIe アダプタのオプションの ROM を実行します。
[前面 NVME *n* リンク速度（Front NVME n Link Speed）] ドロップダウンリスト **set PcieSlotFrontNvme1LinkSpeed**	NVMe 前面スロット *n* のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効となり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：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。
[PCIe スロット MSTOR RAID OptionROM (PCIe Slot MSTOR RAID OptionROM)] ドロップダウン リスト **set PcieSlotMSTORRAIDOptionROM**	サーバが PCIe MSTOR RAID のオプション ROM を使用するかどうか。次のいずれかになります。 • Disabled：オプション ROM は使用できません。 • [Enabled]—オプション ROM は使用できます。
[PCIe ARI サポート (PCIe ARI Support)] ドロップダウン リスト **set PcieARISupport**	リリース 4.1(2a) 以降、Cisco IMC は PCIe 代替ルーティング ID (ARI) 解釈機能をサポートしています。PCIe 仕様では、8 個以上の機能を有効にする PCIeヘッダーのデバイス番号フィールドを再解釈する ARI の実装を通じて、より多くの仮想機能をサポートしています。次のいずれかになります。 • **無効**：PCIe ARI サポートは使用できません。 • **有効**：PCIe ARIサポートを使用できます。 • **自動**：PCIe ARI サポートは自動モードです。

名前	説明
[IPv6 HTTP サポート（IPv6 HTTP Support）] ドロップダウンリスト **set IPV6HTTP**	HTTP の IPv6 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。 • **[無効（disabled）]**：IPv6 HTTP サポートは使用できません。 • **[有効（enabled）]**：IPv6 HTTP サポートを常に使用できます。
[IPV4 HTTP サポート（IPV4 HTTP Support）] ドロップダウンリスト **set IPV4HTTP**	HTTP の IPv4 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。 • **[無効（disabled）]**：IPv4 HTTP サポートは使用できません。 • **[有効（enabled）]**：IPv4 HTTP サポートを常に使用できます。

[電源/パフォーマンス（Power/Performance）] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

表 *25 : [*電源/パフォーマンス（*Power/Performance*）*] タブの BIOS* パラメータ

名前	説明
[今すぐホストを再起動（Reboot Host Immediately）] チェックボックス	このチェックボックスをオンにすると、直ちにホスト サーバが再起動します。このチェックボックスは、変更を保存してからオンにする必要があります。
[Core Performance Boost] ドロップダウンリスト	AMDプロセッサがアイドル状態（ほとんど使用されていない状態）のときにコアの周波数を上げるかどうかを指定します。次のいずれかになります。 • **[auto]**：パフォーマンスをブーストする方法を CPU で自動的に決定します。 • **[disabled]**：CPUにより自動的にブースト パフォーマンスが決定されます。 • [Platform Default][platform-default]：BIOSは、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

サーバー モデル別 BIOS パラメータ

名前	説明
[Global C-state Control] ドロップダウンリスト	AMD プロセッサが IO ベースの C ステートおよび DF C ステートを制御するかどうかに関係なく、これは次のうちいずれかになります。 • **[auto]**：CPU で IO ベースの C ステートの生成方法を自動的に決定します。 • **[disabled]**：グローバル C ステートの制御が無効になります。 • **[enabled]**：グローバル C ステートの制御が有効になります。 • [Platform Default][platform-default]：BIOSは、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[L1 Stream HW Prefetcher] ドロップダウンリスト	プロセッサで、AMD 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、L1 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。 • [auto][Auto]：CPUは、I/Oデバイスからプロセッサ キャッシュにデータを配置する方法を決定します。 • [disabled][Disabled]：ハードウェアプリフェッチャは使用しません。 • [enabled][Enabled]：プロセッサで、キャッシュの問題が検出されたときにハードウェア プリフェッチャを使用します。 • [Platform Default][platform-default]：BIOSは、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[L2 Stream HW Prefetcher] ドロップダウンリスト	プロセッサで、AMD ハードウェア プリフェッチャが必要に応じてメモリからデータおよび命令ストリームを取得し、L2 キャッシュに入れることを許可するかどうかを指定します。次のいずれかになります。 • [auto][Auto]：CPU は、I/Oデバイスからプロセッサ キャッシュにデータを配置する方法を決定します。 • [disabled][Disabled]：ハードウェアプリフェッチャは使用しません。 • [enabled][Enabled]：プロセッサで、キャッシュの問題が検出されたときにハードウェア プリフェッチャを使用します。 • [Platform Default][platform-default]：BIOSは、サーバー タイプとベンダーを決める際に、BIOS デフォルト値に含まれるこの属性の値を使用します。
[Determinism Slider] ドロップダウンリスト	AMD プロセッサにより動作方法を決定できます。次のいずれかになります。 • **[auto]**：CPU はデフォルトの決定論的な電源設定を自動で使用します。 • **[performance]**：プロセッサは、最適なパフォーマンスかつ一貫した方法で動作します。 • **[power]**：プロセッサは、ダイごとに許容される最大のパフォーマンスで動作します。 • [Platform Default][platform-default]：BIOSは、サーバー タイプとベンダーを決める際に、BIOS デフォルト値に含まれるこの属性の値を使用します。

[Processor] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

表 *26 : [*プロセッサ（*Processor*）*]* タブの *BIOS* パラメータ

名前	説明
[Reboot Host Immediately] チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバー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、変更内容はサーバーが手動でリブートされるまで保存されます。
[SMT Mode] ドロップダウンリスト	プロセッサで AMD Simultaneous MultiThreading テクノロジーを使用するかどうかを指定します。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。 • **[auto]**：プロセッサは、マルチスレッドの並列実行を許可します。 • **[off]**：プロセッサでマルチスレッディングを禁止します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOS デフォルト値に含まれるこの属性の値を使用します。
[SVM Mode] ドロップダウンリスト	プロセッサが AMD セキュア仮想マシン テクノロジを使用するかどうか。次のいずれかを選択できます。 • **[disabled]**：プロセッサで SVM テクノロジーを使用しません。 • **[enabled]**：プロセッサで SVM テクノロジーを使用します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Downcore control] ドロップダウンリスト	AMDプロセッサ コアを無効にしているため、有効にするコアの数を選択できます。次のいずれかになります。 • [FOUR（2+2）]：各 CPU コンプレックスで 2 つのコアを有効にします。 • [FOUR（4+0）]：片方の CPU コンプレックスのみで 4 つのコアを有効にします。 • [SIX（3+3）]：各 CPU コンプレックスで 3 つのコアを有効にします。 • [THREE（3+0）]：片方の CPU コンプレックスのみで 3 つのコアを有効にします。 • [TWO（1+1）]：各 CPU コンプレックスで 1 つのコアを有効にします。 • [TWO（2+0）]：片方の CPU コンプレックスのみで 2 つのコアを有効にします。 • **[auto]**：有効化する必要のあるコアの数を CPU で判断します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOS デフォルト値に含まれるこの属性の値を使用します。

C220 M5、C240 M5、C240 SD M5、および C480 M5 サーバ

I/O タブ

（注） このタブに記載されている BIOS のパラメータは、サーバによって異なります。

サーバー モデル別 BIOS パラメータ

表 *27 : [I/O]* タブの *BIOS* のパラメータ

名前	説明
[Reboot Host Immediately] チェックボックス	オンにすると、ホスト サーバが直ちに再起動されます。このチェックボックスは、変更を保存してからオンにする必要があります。
[レガシー USB サポート（Legacy USB Support）] ドロップダウン リスト **set UsbLegacySupport**	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。
[ダイレクト IO への Intel VT（Intel VT for directed IO）] ドロップダウン リスト **set IntelVTD**	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 VTD coherency サポート（Intel VTD coherency support）] ドロップダウン リスト **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 VTD ATS サポート（Intel VTD ATS support）] ドロップダウン リスト **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
[VMD Enable (VMD の有効化)] ドロップダウン リスト	Intel Volume Management Device (VMD) は、NVMe SSD を管理および集約するためのハードウェア ロジックを提供する PCIe NVMe SSD 向けです。 これは次のいずれかになります。 • **有効**: 堅牢で安定したホットプラグ、ステータス LED 管理などの利点を有効にします。 • **無効**: 堅牢で安定したホットプラグ、ステータス LED 管理などの利点を無効にします。 デフォルト値：**無効**。 VMD を設定するには、『CPU ユーザー ガイドの Intel® 仮想 RAID』と『CPU の Intel® 仮想 RAID』を参照してください。
	Cisco UCS C480 M5 サーバでサポートされている VMD およびサポートされていないポートの詳細は次のとおりです。 Cisco UCS C480 NVMe SKU (32 ドライブ NVME システム) • DMI 接続ポート7、8、および 23 は、VMD をサポートしていません。 • その他の 29 個のポートはすべて、VMD をサポートしています。 Cisco UCS C480 非 NVMe SKU • DMI 接続ポート 1、2、および 18 は、VMD をサポートしていません。 • ポート7、8、9、10、15、16、17、23、24 は、VMD をサポートします。
[すべてのオンボード LOM Oprom（All Onboard LOM Oprom）] ドロップダウン リスト **set AllLomPortControl**	オプション ROM がすべての LOM ポートで使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：すべてのポートでオプション ROM を無効にします。 • [有効（Enabled）]：すべてのポートでオプション ROM を有効にします。

名前	説明
[オンボードLOMポート0 Oprom（Onboard LOM Port0 Oprom）] ドロップダウン リスト **set LomOpromControlPort0**	オプション ROM が LOM ポート 0 で使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：LOM ポート 0 でオプション ROM を 使用できません。 • [有効（Enabled）]：LOM ポート 0 でオプション ROM を使用できます。
[オンボードLOMポート1 Oprom（Onboard LOM Port1 Oprom）] ドロップダウン リスト **set LomOpromControlPort1**	オプション ROM が LOM ポート 1 で使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：LOM ポート 1 でオプション ROM を 使用できません。 • [有効（Enabled）]：LOM ポート 1 でオプション ROM を使用できます。
[PCIe スロット *n* Oprom（Pcie Slot n Oprom）] ドロップダウン リスト **set PcieSlotnOptionROM**	サーバが *n* で指定した PCIe カード スロットにあるオプション ROM を使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：スロット *n* のオプション ROM は使用できません。 • [有効（Enabled）]：スロット *n* のオプション ROM は使用可能です。
[MLOM Oprom] ドロップダウン リスト **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。 • [無効（Disabled）]：MLOM スロットに接続されている PCIe アダプタのオプション ROM を実行しません。 • [有効（Enabled）]：MLOM スロットに接続されている PCIe アダプタのオプション ROM を実行します。
[HBA Oprom] ドロップダウン リスト **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。 • [無効（Disabled）]：HBA スロットに接続されている PCIe アダプタのオプション ROM を実行しません。 • [有効（Enabled）]：HBA スロットに接続されている PCIe アダプタのオプション ROM を実行します。

名前	説明
[フロント NVME1 Oprom（Front NVME1 Oprom）] ドロップダウン リスト **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。 • [無効（Disabled）]：SSD:NVMe1 スロットに接続されている PCIe アダプタのオプション ROM を実行しません。 • [有効（Enabled）]：SSD:NVMe1 スロットに接続されている PCIe アダプタのオプション ROM を実行します
[フロント NVME2 Oprom（Front NVME2 Oprom）] ドロップダウン リスト **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。 • [無効（Disabled）]：SSD:NVMe2 スロットに接続されている PCIe アダプタのオプション ROM を実行しません。 • [有効（Enabled）]：SSD:NVMe2 スロットに接続されている PCIe アダプタのオプション ROM を実行します
[HBA リンク速度（HBA Link Speed）] ドロップダウン リスト **set PcieSlotHBALinkSpeed**	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。 • [無効（Disabled）]：最大速度は制限されません。 • [自動（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 5 GT/s までの速度が許可されます。 • [GEN3]：最大 8 GT/s までの速度が許可されます。
[MLOM リンク速度（MLOM Link Speed）] ドロップダウン リスト **set PcieSlotMLOMLinkSpeed**	このオプションを使用すると、PCIe MLOM 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。 • [無効（Disabled）]：最大速度は制限されません。 • [自動（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 5 GT/s までの速度が許可されます。 • [GEN3]：最大 8 GT/s までの速度が許可されます。

名前	説明
[PCIe スロット *n* リンク速度（PCIe Slot n Link Speed）] ドロップダウン リスト **set PcieSlotnLinkSpeed**	システム IO コントローラ *n*（SIOCn）アドオン スロット（*n* によって示される）のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効であり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：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。
[フロントNVME1リンク速度（Front NVME1 Link Speed）] ドロップダウン リスト **set PcieSlotFrontNvme1LinkSpeed**	NVMeフロントスロット1のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効であり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：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。
[フロントNVME2リンク速度（Front NVME2 Link Speed）] ドロップダウン リスト **set PcieSlotFrontNvme2LinkSpeed**	NVMeフロントスロット2のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効であり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：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。

名前	説明
[リア NVME1 リンク速度（Rear NVME1 Link Speed）] ドロップダウン リスト **set PcieSlotRearNvme1LinkSpeed**	NVMe 背面のスロット 1 のリンク速度。次のいずれかになります。 • [無効（Disabled）] : スロットは無効であり、カードは列挙されません。 • [自動（Auto）] : デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1] : リンク速度は第 1 世代まで到達可能です。 • [GEN2] : 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。
[リア NVME2 リンク速度（Rear NVME2 Link Speed）] ドロップダウン リスト **set PcieSlotRearNvme2LinkSpeed**	NVMe 背面のスロット 2 のリンク速度。次のいずれかになります。 • [無効（Disabled）] : スロットは無効であり、カードは列挙されません。 • [自動（Auto）] : デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1] : リンク速度は第 1 世代まで到達可能です。 • [GEN2] : 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。
[VGA 優先順位（VGA Priority）] ドロップダウン リスト **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 デバイスの優先順位を設定できます。次のいずれかになります。 • [オンボード（OnBoard）] : オンボード VGA デバイスが優先されます。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。 • [オフボード（OffBoard）] : PCIE グラフィックス アダプタが優先されます。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。 • [オンボードを無効（OnBoardDisabled）] : PCIE グラフィックス アダプタが優先され、オンボード VGA デバイスは無効になります。オンボード VGA が無効の場合、vKVM は機能しません。

サーバー モデル別 BIOS パラメータ

名前	説明
[P-SATA OptionROM] ドロップダウン リスト **set pSATA**	PCH SATA オプション ROM モードを選択できます。次のいずれかになります。 • [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。 • [無効（Disabled）]：SATA コントローラと sSATA コントローラを無効にします。
[M2.SATA OptionROM] ドロップダウン リスト **set SataModeSelect**	Serial Advanced Technology Attachment（SATA）ソリッド ステート ドライブ（SSD）の動作モード。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。 • [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。 • [無効（Disabled）]：SATA コントローラと sSATA コントローラを無効にします。
[リア USB ポート（USB Port Rear）] ドロップダウン リスト **set UsbPortRear**	背面パネルの USB デバイスが有効か無効か。次のいずれかになります。 • [無効（Disabled）]：背面パネルの USB ポートを無効にします。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。 • [有効（Enabled）]：背面パネルの USB ポートを有効にします。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。
[フロント USB ポート（USB Port Front）] ドロップダウン リスト **set UsbPortFront**	前面パネルの USB デバイスが有効か無効か。次のいずれかになります。 • [無効（Disabled）]：前面パネルの USB ポートを無効にします。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。 • [有効（Enabled）]：前面パネルの USB ポートを有効にします。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
[内部 USB ポート（USB Port Internal）] ドロップダウン リスト **set UsbPortInt**	内部 USB デバイスが有効か無効か。次のいずれかになります。 • [無効（Disabled）] : 内部の USB ポートを無効にします。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。 • [有効（Enabled）] : 内部の USB ポートを有効にします。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。
[KVM USB ポート（USB Port KVM）] ドロップダウン リスト **set UsbPortKVM**	vKVM ポートが有効になっているか、無効になっているか。次のいずれかになります • **[無効（Disabled）]**—vKVM キーボードとマウス デバイスを無効にします。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。 • **[有効 (Enabled)]**—vKVM キーボードとマウス デバイスを有効にします。
[SD カード USB ポート（USB Port SD Card）] ドロップダウン リスト **set UsbPortSdCard**	SD カードが有効か無効か。次のいずれかになります。 • [無効（Disabled）] : SD カードのポートを無効にします。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。 • [有効（Enabled）] : SD カードのポートを有効にします。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。
[IPV6 PXE サポート（IPV6 PXE Support）] ドロップダウン リスト **set IPV6PXE**	PXE の IPv6 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 • **[無効 (disabled)]** : PV6 PXE のサポートは利用できません。 • **[enabled (有効)]**:IPV6 PXE のサポートを常に利用できます。
PCIe PLL SSC ドロップダウン リスト **set PciePllSsc**	この機能を有効にすると、クロックを 0.5% 下方に拡散することにより、EMI 干渉が軽減されます。この機能を無効にすると、拡散せずにクロックを集中管理できます。 これは次のいずれかになります。 • **[自動 (auto)]**—EMI 干渉は自動調整されます。 **[無効 (Disabled)]**—EMI 干渉は自動調整されます。 • **[ZeroPointFive]**—クロックを 0.5% 下方に拡散することにより、EMI 干渉を軽減します。

名前	説明
[IPV4 PXE サポート (IPV4 PXE Support)] ドロップダウン リスト **set IPV4PXE**	PXE の IPv4 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 • **[無効 (disabled)]**: IPV4 PXE のサポートは利用できません。 • **[enabled (有効)]**: IPV4 PXE のサポートを常に利用できます。
[Network Stack (ネットワーク スタック)] ドロップダウン リスト **set NetworkStack**	このオプションでは、IPv6 と IPv4 をモニタできます。次のいずれかになります • **[無効 (disabled)]**: ネットワーク スタックのサポートは使用できません。 （注） 無効にすると、 **IPV4 PXE サポート**に設定された値はシステムに影響しません。 • **[enabled (有効)]**: ネットワーク スタックのサポートを常に利用できます。
[外部データベース（External Database）] ドロップダウン リスト **set EnableClockSpreadSpec**	このオプションを使用すると、マザーボードからの EMI を、マザーボードが発生する信号に変調をかけ、スパイクがより平坦な曲線になるようにして、軽減します。 次のいずれかになります。 • **[無効 (Disabled)]**—クロック拡散スペクトルのサポートは使用できません。 • **[Enabled (有効)]**—クロック拡散スペクトルのサポートは常に使用できます。
[PCIe スロット MSTOR RAID OptionROM (PCIe Slot MSTOR RAID OptionROM)] ドロップダウン リスト **set PcieSlotMSTORRAIDOptionROM**	サーバが PCIe MSTOR RAID のオプション ROM を使用するかどうか。次のいずれかになります。 • Disabled：オプション ROM は使用できません。 • [Enabled]—オプション ROM は使用できます。

[Server Management] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

表 *28 : [*サーバ管理（*Server Management*）*]* タブの *BIOS* パラメータ

名前	説明
[Reboot Host Immediately] チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバー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、変更内容はサーバーが手動でリブートされるまで保存されます。
[OS ブート ウォッチドッグ タイマー ポリシー（OS Boot Watchdog Timer Policy）] ドロップダウン リスト **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。 • [電源オフ（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、サーバーはリセットされます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にする場合にのみ適用されます。
[OS ウォッチドッグ タイマー（OS Watchdog Timer）] ドロップダウン リスト **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]：サーバーのブートにかかる時間をトラッキングするためにウォッチドッグ タイマーは使用されません。 • [有効（enabled）]：サーバーがブートにかかる時間をウォッチドッグ タイマーで追跡します。サーバーのブートが [OS ブート ウォッチドッグ タイマー タイムアウト（OS Boot Watchdog Timer Timeout）] フィールドで指定された時間内に完了しない場合は、Cisco IMC によってエラーがログに記録され、[OS ブート ウォッチドッグ ポリシー（OS Boot Watchdog Policy）] フィールドで指定されたアクションが実行されます。

サーバー モデル別 BIOS パラメータ

名前	説明
[OS ブート ウォッチドッグ タイマー タイムアウト（OS Watchdog Timer Timeout）] ドロップダウン リスト **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 分（5 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [10 分（10 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [15 分（15 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 • [20 分（20 Minutes）]：OS ウォッチドッグ タイマーの有効期限は起動し始めてから 5 分で切れます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にした場合にのみ適用されます。
[ボー レート（Baud Rate）] ドロップダウン リスト **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。[コンソール リダイレクション（Console Redirection）] を無効にした場合、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]：9,600 ボー レートが使用されます。 • [19.2k]：19,200 ボー レートが使用されます。 • [38.4k]：38,400 ボー レートが使用されます。 • [57.6k]：57,600 ボー レートが使用されます。 • [115.2k]：115,200 ボー レートが使用されます。 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
[コンソール リダイレクション（Console Redirection）] ドロップダウン リスト **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 リダイレクションで使用できるようにします。OS 起動後は、コンソールのリダイレクトが関係なくなります。次のいずれかになります。 • [シリアル ポート 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有効にします。 • [シリアル ポート B（Serial Port B）]：POST 中にシリアル ポート B でコンソール リダイレクションを有効にします。 • [無効（Disabled）]：POST 中にコンソール リダイレクションは発生しません。

サーバー モデル別 BIOS パラメータ

名前	説明
適応型メモリ トレーニング	このオプションを[有効（Enabled）]にすると、次のようになります。 メモリ トレーニングは毎回のブートでは実行されず、BIOSは、保存されたメモリ トレーニングの結果を毎回のリブートで使用します。 毎回のブートでメモリ トレーニングが実行されるいくつかの例外には、次のものがあります。 BIOS の更新、CMOS のリセット、CPU やメモリの設定変更、SPD または実行時の修正不可能なエラー、または、前回のブートから 24 時間以上経過している場合。 このオプションが [無効（Disabled）] の場合、毎回のブートでメモリ トレーニングが行われます。 デフォルト値：[有効（Enabled）]。 （注） [高速ブート（Fast Boot）] オプションを無効にするには、エンドユーザーは次のトークンを下記の説明のとおりに設定する必要があります。 [適応型メモリ トレーニング（Adaptive Memory Training）]を [無効（Disabled）] に [BIOS Techlogレベル（BIOS Techlog level）] を [標準（Normal）] に [OptionROM起動最適化（OptionROM Launch Optimization）] を [無効（Disabled）] に

名前	説明
[BIOS Techlogレベル（BIOS Techlog Level）]	このオプションは、 **BIOS tech ログファイル** のメッセージのタイプを示します。 ログファイルには、次のタイプのいずれかを指定できます。 • [最小（Minimum）]：重要なメッセージがログファイルに表示されます。 • [標準（Normal）]：警告およびロードメッセージがログファイルに表示されます。 • [最大（Maximum）]：標準に加え、情報関連のメッセージがログファイルに表示されます。 デフォルト値：[最小（Minimum）] （注） このオプションは、主に、内部のデバッグを目としています。
[OptionROM起動最適化（OptionROM Launch Optimization）]	このオプションが [有効（Enabled）] の場合、ブート順序のポリシーに存在するコントローラにのみ OptionROMs が起動されます。 （注） オンボードストレージコントローラ、Emulex FC アダプタおよびGPUコントローラなどのいくつかのコントローラについて、ブート順序のポリシーに含まれていなくても、OptionROM が起動されます。 このオプションが [無効（Disabled）] の場合、すべての OptionROMs が起動されます。 デフォルト値：[有効（Enabled）]
[CDN コントロール（CDN Control）] ドロップダウン リスト **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。 • [無効（Disabled）]：VIC カードに対する CDN サポートは無効です。 • [有効（Enabled）]：CDNサポートはVICカードに対して有効です。

サーバー モデル別 BIOS パラメータ

名前	説明
[FRB 2 タイマー（FRB 2 Timer）] ドロップダウン リスト **set FRB-2**	POST 中にシステムがハングした場合に、システムを回復するために Cisco IMC によって FRB2 タイマーが使用されるかどうか。次のいずれかになります。 • [無効（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。
[フロー制御（Flow Control）] ドロップダウン リスト **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を設定します。送信要求/クリア ツー センド（RTS/CTS）を使用すると、隠れた端末の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。 • [なし（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。
[ターミナル タイプ（Terminal Type）] ドロップダウン リスト **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。

名前	説明
[PCIe Slots CDN コントロール（PCIe Slots CDN Control）] ドロップダウンリスト **set PcieSlotsCdnEnable**	（注） このオプションは、スロット 2 または 5 に Qlogic カードを搭載した Cisco UCS C240 M5 サーバーでのみ使用できます。 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。 • [無効（Disabled）]：VIC カードに対する CDN サポートは無効です。 • [Enabled]：VIC カードの CDN サポートが有効になります。

[セキュリティ（Security）] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

表 *29 : [*セキュリティ（*Security*）*]* タブの *BIOS* パラメータ

名前	説明
[Reboot Host Immediately] チェックボックス	**[**ホストを即座にリブート（**Reboot Host Immediately**）**]** チェックボックスがオフの場合、サーバー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、変更内容はサーバーが手動でリブートされるまで保存されます。
[トラステッド プラットフォーム モジュール状態（**Trusted Platform Module State**）**]** ドロップダウンリスト **set TPMAdminCtrl**	信頼されたプラットフォーム モジュール（TPM）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]：サーバーは TPM を使用しません。 • [有効（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ください。
SHA-1 PCRバンク	SHA-1 PCR バンクを有効または無効にします。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
SHA256 PCRバンク	SHA256 PCR バンクを有効または無効にします。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

名前	説明
[Reboot Host Immediately] チェックボックス	**[ホストを即座にリブート（Reboot Host Immediately）]** チェックボックスがオフの場合、サーバー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、変更内容はサーバーが手動でリブートされるまで保存されます。
[Intel Trusted Execution Technology のサポート（Intel Trusted Execution Technology Support）]	信頼されたプラットフォームモジュール(TPM)が 有効 である場合にのみ 有効 に設定できます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[電源オン パスワード（Power On Password）] ドロップダウンリスト **set PowerOnPassword**	このトークンでは、F2 BIOS 設定を使用する前に BIOS パスワードを設定する必要があります。有効にすると、BIOS 関数（IO 設定、BIOS セットアップ、BIOS を使用したオペレーティング システムへのブート）にアクセスする前にパスワードの検証が必要になります。次のいずれかを指定できます。 • **[無効（Disabled）]**：サポートは無効になります。 • [Enabled]：サポートはイネーブルになっています。

[Processor] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

サーバー モデル別 BIOS パラメータ

表 *30 : [*プロセッサ（*Processor*）*]* タブの *BIOS* パラメータ

名前	説明
[Intel Virtualization Technology] ドロップダウン リスト **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。 • [有効（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。
[拡張 APIC（Extended APIC）] ドロップダウンリスト **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。 • [有効（Enabled）]：APIC サポートを有効にします • [無効（Disabled）]：APIC サポートを無効にします。
[プロセッサ C1E（Processor C1E）] ドロップダウン リスト **set ProcessorC1E**	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。 • [無効（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。 • [有効（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） このオプションを使用できるのは一部の C シリーズ サーバーだけです。

サーバー モデル別 BIOS パラメータ

名前	説明
[プロセッサ C6 レポート（Processor C6 Report）] ドロップダウン リスト **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 [カスタム（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。 （注） このオプションを使用できるのは一部の C シリーズ サーバーだけです。
[XD ビット（Execute Disable Bit）] ドロップダウンリスト **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、サーバーのメモリ領域を分類します。この分類の結果、悪意のあるワームがバッファにコードを挿入しようとした場合、プロセッサでコードの実行を無効化します。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。 • [有効（Enabled）]：プロセッサでメモリ領域を分類します。 （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ください。

サーバー モデル別 BIOS パラメータ

名前	説明
[ターボ モード（Turbo Mode）] ドロップダウンリスト **set IntelTurboBoostTech**	プロセッサでインテル ターボ ブーストテクノロジーを使用するかどうか。このテクノロジーでは、仕様よりも低い電力、温度、または電圧でプロセッサが動作していると、自動的にそのプロセッサの周波数が上がります。次のいずれかになります。 • [Disabled]：プロセッサの周波数は自動的には上がりません。 • [Enabled]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。 （注） [CPUPowerManagement] を [カスタム（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。
[EIST PSD 関数（EIST PSD Function）] ドロップダウンリスト	EIST は、電圧と周波数のペア（P 状態）の変更に固有の遅延を短縮するため、これらの遷移がより頻繁に発生するようになります。これにより、より詳細なデマンドベースのスイッチングが可能になり、アプリケーションの要求に基づいて電力とパフォーマンスのバランスを最適化できます。次のいずれかになります。 • HW ALL：プロセッサは、論理プロセッサの依存関係間の P 状態を調整します。OS は、すべての論理プロセッサで P-state 要求を最新の状態に保ちます。 • SW ALL：OS Power Manager によって、依存関係にある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します。

名前	説明
[SpeedStep（Pstates）] ドロップダウンリスト **set EnhancedIntelSpeedStep**	プロセッサで拡張版 Intel SpeedStep テクノロジーを使用するかどうか設定します。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。 • [有効（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 [カスタム（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。
[HyperThreading [All]] ドロップダウンリスト **set IntelHyperThread**	プロセッサでインテル ハイパースレッディング テクノロジーを使用するかどうか。このテクノロジーでは、マルチスレッド ソフトウェア アプリケーションのスレッドを各プロセッサ内で並列に実行できます。次のいずれかになります。 • [Disabled]：プロセッサでのハイパースレッディングを禁止します。 • [有効（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。

サーバー モデル別 BIOS パラメータ

名前	説明
[コアは有効化されました（Cores Enabled）] ドロップダウンリスト **set CoreMultiProcessing**	サーバー上の 1 つ以上の物理コアを無効にできます。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] ～ [27]**：サーバー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。 （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ください。
[Processor CMCI] ドロップダウン リスト **set ProcessorCMCI**	CPU が corrected machine check events で割り込みをトリガーできるようにします。corrected machine check interrupt（CMCI）により、従来のポーリング タイマーよりも反応速度を向上できます。次のいずれかになります。 • [無効（Disabled）]：CMCI が無効になります。 • [有効（有効）]：CMCI が有効になります。これはデフォルト値です。

名前	説明
[Enhanced Intel SpeedStep Tech] ドロップダウン リスト **set EnhancedIntelSpeedStep**	プロセッサで拡張版 Intel SpeedStep テクノロジーを使用するかどうか設定します。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。 • [有効（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] は、[カスタム（Custom）] に設定する必要があります。設定しな場合、サーバはこのパラメータの設定を無視します。
[Workload Configuration] ドロップダウン リスト **set WorkLdConfig**	この機能を使用すると、ワークロードを最適化できます。オプションは [Balanced] と [I/O Sensitive] です。 • **NUMA** • **UMA**

名前	説明
[Sub NUMA Clustering] ドロップダウンリスト	CPUがサブNUMAクラスタリングをサポートするかどうか。そのクラスタリングでは、タグディレクトリとメモリチャネルは常に同じ領域にあります。次のいずれかになります。 • [disabled][Disabled]：サブNUMAクラスタリングは発生しません。 • [enabled][Enabled]：サブNUMAクラスタリングが発生します。 • [自動（Auto）][自動（auto）]：BIOSかサブNUMAのクラスタ リングされるかが決まります。
エネルギー/パフォーマンスのバイアス構成	エネルギーまたはパフォーマンスのバイアス構成を表示します。 次のいずれかになります。 • Balanced Performance • Performance • Balanced Power • 電源
[XPT Prefetch] ドロップダウン リスト	XPT プリフェッチを使用して、最後のレベルのキャッシュに読み取り要求を送信できるようにして、その要求のコピーをメモリ コントローラのプリフェッチャに発行するかどうか。次のいずれかになります。 • [disabled][Disabled]：CPU はXPT Prefetch オプションを使用しません。 • [enabled][Enabled]：CPUはXPTプリフェッチ オプションを有効にします。

名前	説明
[UPI プリフェッチ（UPI Prefetch）] ドロップダウン リスト	UPI プリフェッチは、DDR バス上でメモリ読み込みが早期に開始されるようにするメカニズムです。これは次のいずれかになります。 • [無効（disabled）][無効（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。 • [有効（enabled）][有効（Enabled）]：UPI プリフェッチャ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。
[エネルギー パフォーマンスのバイアス構成（Energy/Performance Bias Config）] ドロップダウンリスト **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ー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。 • [パフォーマンス（Performance）]：サーバーでは、すべてのサーバーコンポーネントに全電力を常時提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • [バランス パフォーマンス（Balanced Performance）]：サーバーは、すべてのサーバーコンポーネントに、パフォーマンスと電力のバランスを保つのに十分な電力を提供します。 • [バランス電力（Balanced Power）]：サーバーは、すべてのサーバーコンポーネントに、パフォーマンスと電力のバランスを保つのに十分な電力を提供します。 • [電力（Power）]：サーバーは、すべてのサーバーコンポーネントに、消費電力の低減を維持するのに最大の電力を提供します。

名前	説明
[電力パフォーマンスの調整（Power Performance Tuning）] ドロップダウン リスト **set PwrPerfTuning**	BIOS または OS によってエネルギー パフォーマンスのバイアス調整をオンにできるかどうかを指定します。オプションは [BIOS] と [OS] です。 • [bios][BIOS]： エネルギー効率を調整する場合は [BIOS] を選択します。 • [os][OS]： エネルギー効率を調整する場合は [OS] を選択します。
[LLC Prefetch] ドロップダウン リスト	プロセッサが LLC プリフェッチ メカニズムを使用して日付を LLC にフェッチするかどうか。次のいずれかになります。 • [disabled][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][Enabled]：LLC 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
[パッケージのCステート（Package C State）] ドロップダウン リスト **set package-c-state-limit-config package-c-state-limit**	アイドル時にサーバー 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。 • [no-limit][制限なし（No Limit）]：サーバーは、使用可能な任意の Cステートに入ることがあります。 • [自動（auto）][自動（Auto）]：物理的な高度を CPUが決定します。 • [C0 C1 ステート（C0 C1 State）]：サーバーはすべてのサーバーコンポーネントに常にフル パワーを提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • [C2]：CPU のアイドル時に、システムの電力消費をC1 オプションよりもさらに低減します。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、サーバーがハイ 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 保持なし（C6 Non Retention）]：CPU のアイドル時に、C3 オプションよりもさらに電力消費が低減されます。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、サーバー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。 • [C6 保持（C6 Retention）]：CPUのアイドル時に、C3 オプションよりもさらに電力消費が低減されます。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、サーバー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。

サーバー モデル別 BIOS パラメータ

名前	説明
[ハードウェア P ステート（Hardware P-States）] ドロップダウン リスト **set CpuHWPM**	プロセッサ ハードウェアの P ステートを有効にします。次のいずれかになります。 • [disabled][Disabled]：HWPM がディセーブルになります。 • [hwpm-native-mode][HWPM Native Mode]：HWPM ネイティブモードがイネーブルになります。 • [hwpm-oob-mode][HWPM OOB Mode]：HWPM アウトオブボックスモードがイネーブルになります。 • [Native Mode with no Legacy]（GUI のみ）
[Intel Speed Select (Intel の速度選択)] ドロップダウン リスト **set IntelSpeedSelect**	**[Intel Speed Select (Intel の速度選択)]** モードでは、ユーザーは異なる速度とコアを使用して CPU を実行できます。 次のいずれかになります。 • **基本**): ユーザーは最大コアおよび熱設計電力 (TDP) 比率にアクセスすることができます。 • **設定 1** ユーザーは **基本**より小さいコアと TDP 比率にアクセスできます。 • **設定 2** ユーザーは **設定 1** より小さいコアと TDP 比率にアクセスできます。 デフォルト値: **基本**。
[非コア周波数スケーリング (Uncore Frequency Scaling)] ドロップダウンリスト **set UFSDisable**	この機能を使用すると、プロセッサのコア以外の周波数のスケーリングを設定できます。次のいずれかになります。 • **[enabled]**：プロセッサの非コア部分の周波数を、負荷に応じて上下します。 • **[無効 (disabled)]**: プロセッサのコア以外の周波数を固定します。 『Intel® Dear Customer Letter (DCL)』には、固定されていない場合の **[非コア周波数スケーリング (Uncore Frequency Scaling)]**の固定の上限値と下限値が記されています。

名前	説明
[TDP の設定（Config TDP）]ドロップダウンリスト **set ConfigTDPLevel**	**[TDP の設定（Config TDP）]**機能により、プロセッサの温度設計の電力値を調整できます。プロセッサの動作とパフォーマンス レベルを変更することにより、プロセッサの消費電力と TDP を同時に調整できます。したがって、プロセッサは、使用可能な冷却容量と望ましい消費電力に応じて、パフォーマンス レベルが高いまたは低い方で動作します。次のいずれかになります。 • **[標準 (Normal)]** • **[レベル 1 (Level 1)]** • **[レベル 2 (Level 2)]** TDP レベルの値については、『Intell® Dear Customer Letter (DCL)』を参照してください。
[UPI リンク速度（UPIH Link Speed）] ドロップダウンリスト **set QpiLinkSpeed**	（注） **[UPI リンク周波数選択 (UPI Link Frequency Select)]** トークンは、単一ソケット構成には適用されません。 この機能を使用すると、複数のソケット間の Intel Ultra Path Interconnect (UPI) リンク速度を設定できます。次のいずれかになります。 • **[自動 (Auto)]**]: このオプションは、最適なリンク速度を自動的に設定します。 • **[9.6 GT/s]**: このオプションは、最適なリンク速度として 9.6GT/s を使用します。 • **[10.4 GT/s]**—このオプションは、最適なリンク速度として 10.4GT/s を使用します。

名前	説明
[エネルギー効率ターボ（Energy Efficient Turbo）] ドロップダウンリスト **set EnergyEfficientTurbo**	エネルギー効率の高いターボが有効になっている場合、CPUの最適なターボ周波数は、CPU使用率に基づいてダイナミックになります。パワー/パフォーマンスのバイアス設定も、エネルギー効率の高いターボに影響します。次のいずれかになります。 • **[無効（Disabled）]**：エネルギー効率ターボが無効です。 • **[有効（Enabled）]**：エネルギー効率ターボが有効です。
プロセッサEPPの有効化	プロセッサ EPP の有効化で選択した値を表示します。 • **[無効（Dissabled）]**：プロセッサ EPP の有効化が無効です。 • **[有効（Enabled）]**：プロセッサ EPP の有効化が有効です。
[自律コア C 状態（Autonomous Core C-state）] ドロップダウンリスト **set AutoCCState**	HALT 命令を MWAIT 命令に変換する CPU Autonomous C-State を有効にします。次のいずれかになります。 • [Disabled]：CPU Autonomous C-state が無効です。 • [有効（Enabled）]：CPU 自律 C-state が有効になります。

名前	説明
[パトロール スクラブ（Patrol Scrub）] ドロップダウンリスト **set PatrolScrub**	システムにサーバーのメモリ（未使用部分も含む）における単一ビット メモリ エラーを検出させて修復させることが可能です。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。 • [有効（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、システムは修復を試みます。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。 • **[POST の最後に有効化する（Enable at End of POST）]**：システムは、BIOS POST 後にメモリ ECC エラーをチェックします。
[プロセッサ EPP プロファイル（Processor EPP Profile）] ドロップダウンリスト **set EPPProfile**	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ー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。 • Performance • Balanced Performance • Balanced Power • 電源

メモリ タブ

（注） このタブに記載されている BIOS のパラメータは、サーバーによって異なります。

表 *31 : [*メモリ（*Memory*）*]* タブの *BIOS* パラメータ

名前	説明
[今すぐホストを再起動（Reboot Host Immediately）] チェックボックス	このチェックボックスをオンにすると、直ちにホスト サーバが再起動します。このチェックボックスは、変更を保存してからオンにする必要があります。
[メモリ RAS 構成の選択（Select Memory RAS configuration）] ドロップダウン リスト **set SelectMemoryRAS**	サーバーに対するメモリの信頼性、可用性、およびサービス性（RAS）の設定方法。次のいずれかになります。 • [最大パフォーマンス（Maximum Performance）]：システムのパフォーマンスが最適化されます。 • **ADDDC のスペアリング**: 適応可能な仮想ロックステップは、ADDDC モードをサポートするためにハードウェアおよびファームウェアで実装されるアルゴリズムです。選択すると、アルゴリズムがアクティブになるまでシステムのパフォーマンスが最適化されます。このアルゴリズムは、DRAM デバイスで障害が発生した場合にアクティブになります。アルゴリズムがアクティブになると、仮想ロックステップ リージョンがアクティブになり、実行時に障害が発生したリージョンが動的にマッピングされ、パフォーマンスへの影響はリージョン レベルで制限されます。 • [ミラー モード 1LM（Mirror Mode 1LM）]：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。 • **部分的なミラー モード 1LM**: 部分的な DIMM ミラーリングによって完全なミラーコピーを保持するのではなく、メモリ セルの特定の領域のミラーコピーが作成されます。部分的なミラーリングでは、部分的なミラー コピーの属性を使用して、メモリ マップにミラー領域が作成されます。最大 4 個の部分的なミラーを使用して、合計メモリ容量の最大 50% をミラーリングできます。

名前	説明
[4 G 以上の復号化（Above 4G Decoding）] ドロップダウン リスト **set MemoryMappedIOAbove4GB**	4 GB 以上の MMIO を有効または無効にします。次のいずれかになります。 • [Disabled]：サーバーでは 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。 • [有効（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。
[DCPMM Firmware Downgrade (DCPMM ファームウェアのダウングレード)]ドロップダウン リスト **set DCPMMFirmwareDowngrade**	BIOS が DCPMM ファームウェアのダウングレードをサポートしているかどうか。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[Partial Memory Mirror Mode (部分メモリ ミラー モード)]ドロップダウン リスト **set PartialMirrorModeConfig**	部分的なメモリ サイズは、パーセンテージまたは GB 単位のいずれかです。次のいずれかになります。 • **割合**: 部分的なメモリのミラーはパーセンテージで定義されます。 • **値 (GB)**: 部分的なメモリ ミラーは GB で定義されます。 • **無効**: 部分的なメモリ ミラーが無効になります。
[部分的なミラー パーセンテージ (Partial Mirror percentage)] フィールド **set PartialMirrorPercent**	4GBを超えてミラーリングするメモリの割合。 0 ～ 60 の整数を入力します。

名前	説明
[部分ミラー 1 サイズ (GB) (Partial Mirror1 Size in GB)] フィールド **set PartialMirrorValue1**	最初の部分メモリ ミラーのサイズ (GB)。 0 ～ 65535 の整数を入力します。 （注） すべての部分的なミラーの合計メモリ サイズは、物理メモリ サイズの 50% を超えないようにする必要があります。
[部分ミラー 2 サイズ (GB) (Partial Mirror2 Size in GB)] フィールド **set PartialMirrorValue2**	2 番目の部分メモリ ミラーのサイズ (GB 単位)。 0 ～ 65535 の整数を入力します。 （注） すべての部分的なミラーの合計メモリ サイズは、物理メモリ サイズの 50% を超えないようにする必要があります。
[部分ミラー 3 サイズ (GB) (Partial Mirror3 Size in GB)] フィールド **set PartialMirrorValue3**	3 番目の部分メモリ ミラーのサイズ (GB 単位)。 0 ～ 65535 の整数を入力します。 （注） すべての部分的なミラーの合計メモリ サイズは、物理メモリ サイズの 50% を超えないようにする必要があります。
[部分ミラー 4 サイズ (GB) (Partial Mirror4 Size in GB)] フィールド **set PartialMirrorValue4**	4 番目の部分メモリ ミラーのサイズ (GB 単位)。 0 ～ 65535 の整数を入力します。 （注） すべての部分的なミラーの合計メモリ サイズは、物理メモリ サイズの 50% を超えないようにする必要があります。
[メモリ サイズ制限 (GB) (Memory Size Limit in GB)] フィールド **set MemorySizeLimit**	このオプションを使用して、物理メモリの上限のサイズを GB 単位で減らします。 0 ～ 65535 の整数を入力します。

名前	説明
[NUMA] ドロップダウン リスト **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]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[BME DMA 移行 (BME DMA Mitigation)] ドロップダウン リスト **set BmeDmaMitigation**	不正な外部 DMA からの脅威を緩和する PCI BME ビットを無効にできます。次のいずれかになります。 • **[無効 (disabled)]**: PCI BME ビットは BIOS で無効になっています。 • **[有効 (Enabled)**: PCI BME ビットは BIOS で有効になっています。
[ディスク タイプの選択 (Select Disk Type)] ドロップダウン リスト **set SelectPprType**	Cisco IMC は、指定された障害のある行から指定されたスペア行へのアクセスを永続的に再マッピングする、**ハード PPR**をサポートしています。 次のいずれかになります。 • **[ハード PPR (Hard PPR)]**: サポートは有効になっています。 （注） ハード PPR は、**[メモリ RAS 設定 (Memory RAS Configuration)]**が **[ADDDC スペア (ADDDC Sparing)]**に設定されている場合にのみ使用できます。他の RA の選択では、この設定を **Disabled** に設定する必要があります。 • **[無効 (Disabled)]**：サポートは無効になっています。

名前	説明
[CR QoS] ドロップダウンリスト **CRQoS**	CR QoS 調整を選択できます。 次のいずれかになります。 • **[レシピ 1 (Recipe 1)]**: QoS ノブ向けで、アクティブなディレクトリでの2-2-2 メモリ設定に推奨されます。 • **[レシピ 2 (Recipe 2)]**: QoS ノブ向けで、アクティブなディレクトリでの他のメモリ設定に推奨されます。 • **[レシピ 3 (Recipe 3)]**: QoS ノブ向けで、チャネルごとに1つの DIMM を設定することを推奨します。 • **[無効 (Disabled)]**:**CR QoS**機能は無効になります。
[AD の Snoopy モード (Snoopy mode for AD)] ドロップダウン リスト **SnoopyModeForAD**	新しい AD 固有の機能を有効にして、NUMA に最適化されていないワークロードからDDRT メモリへのディレクトリ更新を回避します。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[CR Fastgo Config] ドロップダウンリスト **CrfastgoConfig**	CR QoS 設定プロファイルを選択できるようにします。 次のいずれかになります。 • **デフォルト (Default)** • **オプション 1 (Option 1)** • **オプション 2 (Option 2)** • **オプション 3 (Option 3)** • **オプション 4 (Option 4)** • **オプション 5 (Option 5)** • **自動 (Auto)**

名前	説明
[NVM パフォーマンス設定 (NVM Performance Setting)] ドロップダウンリスト **NvmdimmPerformConfig**	ワークロードの動作に応じて、NVMベースラインのパフォーマンス設定を設定できます。 • **BW 最適化** • **遅延の最適化** • **バランス プロファイル**
[2LM の Snoopy モード (Snoopy mode for 2LM)] ドロップダウン リスト **SnoopyModeFor2LM**	NUMA に最適化されていないワークロードから far メモリへのディレクトリ更新を回避できます。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。
[メモリ サーマル スロットリング モード（Memory Thermal Throttling Mode）] ドロップダウンリスト **MemoryThermalThrottling**	この関数は、メモリ温度の調整に使用されます。この機能を有効にした後、メモリ温度が極端に高くなると、メモリアクセスレートが低下し、Baseboard Management Controller（BMC）がファンを調整してメモリを冷却し、DIMM の損傷を防ぎます。 次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • **PECI を使用した CLTT**：プラットフォーム環境制御インターフェイスを使用してクローズドループ サーマル スロットリングを有効にします。

サーバー モデル別 BIOS パラメータ

名前	説明
[メモリ リフレッシュ レート（Memory Refresh Rate）] ドロップダウンリスト **MemoryRefreshRate**	メモリのリフレッシュ レートを増減できます。DRAM のリフレッシュ レートを上げると、次のリフレッシュの前に発生する可能性のあるアクティブ化（ハンマー）の最大数が減少します。 次のいずれかになります。 • **[1X リフレッシュ（1X Refresh）]**：リフレッシュ レートは最小です。 • **[2X リフレッシュ（2X Refresh）]**：リフレッシュは 2 倍高速です。
[パニックと高水準点（Panic and High Watermark）] ドロップダウンリスト **PanicHighWatermark**	低に設定した場合、**[メモリ更新レート（Memory Refresh Rate）]** が **[1X リフレッシュ（1X Refresh）]** に設定されている間、メモリコントローラは更新を延期しません。 次のいずれかになります。 • **[低（Low）]**：リフレッシュ レートは低に設定します。 • **[高（High）]**：リフレッシュ レートは高に設定します。
[高度なメモリ テスト（Advanced Memory Test）] ドロップダウンリスト **AdvancedMemTest**	（注） この機能は、Samsung、Hynix、および Micron DIMM にのみ適用されます。 この機能を使用して、BIOS POST 中に高度な DIMM テストを有効にすることができます。次のいずれかになります。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

名前	説明
[拡張メモリ テスト（Enhanced Memory Test）] ドロップダウンリスト	次のいずれかになります。 • **[自動（Auto）]**：サポートは自動に設定されています。 • [Disabled]：サポートはディセーブルになっています。 • [Enabled]：サポートはイネーブルになっています。

[電源/パフォーマンス（Power/Performance）] タブ

（注） このタブに表示される BIOS パラメータは、サーバによって異なる可能性があります。

表 *32 : [*電源/パフォーマンス（*Power/Performance*）*] タブの BIOS* パラメータ

名前	説明
[今すぐホストを再起動（Reboot Host Immediately）] チェックボックス	このチェックボックスをオンにすると、直ちにホスト サーバが再起動します。このチェックボックスは、変更を保存してからオンにする必要があります。
[ハードウェアプリフェッチャ（Hardware Prefetcher）] ドロップダウン リスト **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。
[隣接キャッシュ ライン プリフェッチャ（Adjacent Cache Line Prefetcher）] ドロップダウン リスト **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。

名前	説明
[DCU ストリーマ プリフェッチ（DCU Streamer Prefetch）] ドロップダウン リスト **set DcuStreamerPrefetch**	プロセッサで DCU IP プリフェッチ 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 プリフェッチャ（DCU IP Prefetcher）] ドロップダウン リスト **set DcuIpPrefetch**	プロセッサで DCU IP プリフェッチ 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 プリフェッチャ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。
[CPU パフォーマンス（CPU Performance）] ドロップダウン リスト **set CPUPerformance**	上記のオプションに対し CPU パフォーマンス プロファイルを設定します。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。 • [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。 • [高スループット（Hight Throughput）]：DCU IP Prefetcher のみが有効です。残りのオプションは無効になります。 • [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。さらに、[ハードウェア プリフェッチャ（Hardware Prefetcher）] オプションと [隣接キャッシュ：ライン プリフェッチ（Adjacent Cache-Line Prefetch）] オプションも設定できます。

C460 M4 サーバ

C460 M4 サーバの [メイン（Main）] タブ

主要な BIOS パラメータ

名前	説明
[今すぐホストを再起動（Reboot Host Immediately）] チェックボックス	このチェックボックスをオンにすると、直ちにホスト サーバが再起動します。このチェックボックスは、変更を保存してからオンにする必要があります。
[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]：サーバーは TPM を使用しません。 • [有効（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。
[Power ON Password Support] ドロップダウン	このトークンでは、F2 BIOS 設定を使用する前に BIOS パスワードを設定する必要があります。有効にすると、BIOS 関数（IO 設定、BIOS セットアップ、BIOS を使用したオペレーティング システムへのブート）にアクセスする前にパスワードの検証が必要になります。次のいずれかを指定できます。 • **[無効（Disabled）]**：サポートは無効になります。 • **[有効（Enabled）]**：サポートは有効になります。

[Actions] 領域

名前	説明
[**Save**] ボタン	BIOS パラメータの設定を保存して、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、サーバー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、変更内容はサーバーが手動でリブートされるまで保存されます。
[Reset] ボタン	3 つすべてのタブ上の BIOS パラメータの値が、このダイアログボックスを最初に開いた際に有効だった設定にリセットされます。
[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。

C460 M4 サーバの [詳細設定（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、[Save Changes] 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] ドロップダウン リスト **set IntelHyperThread**	プロセッサでインテル ハイパースレッディング テクノロジーを使用するかどうか。このテクノロジーでは、マルチスレッド ソフトウェア アプリケーションのスレッドを各プロセッサ内で並列に実行できます。次のいずれかになります。 • [Disabled]：プロセッサでのハイパースレッディングを禁止します。 • [有効（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。
[有効化されたコア数（Number of Enabled Cores）] ドロップダウン リスト **set CoreMultiProcessing**	サーバー上の 1 つ以上の物理コアを無効にできます。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てください。

サーバー モデル別 BIOS パラメータ

名前	説明
[Execute Disable] ドロップダウン リスト **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、サーバーのメモリ領域を分類します。この分類の結果、悪意のあるワームがバッファにコードを挿入しようとした場合、プロセッサでコードの実行を無効化します。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。 • [有効（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。 • [有効（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ー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(R) 割り込み再マッピング（Intel(R) Interrupt Remapping）] ドロップダウン リスト **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(R) パススルー DMA（Intel(R) Passthrough DMA）] ドロップダウン リスト **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。

サーバー モデル別 BIOS パラメータ

名前	説明
[CPU Performance] **set CPUPerformance**	サーバーの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 • ハードウェア プリフェッチャ • 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。 • [HighThroughput]**[High_Throughput]**：DCU IP 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。
[ハードウェア プリフェッチャ（Hardware Prefetcher）] ドロップダウン リスト **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
[隣接キャッシュラインプリフェッチャ（Adjacent Cache Line Prefetcher）] ドロップダウン リスト **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。 • [有効（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ストリーマープリフェッチ（DCU Streamer Prefetch）] ロップダウン リスト **set DcuStreamerPrefetch**	プロセッサで DCU IP プリフェッチ 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プリフェッチャ（DCU IP Prefetcher）] ドロップダウン リスト **set DcuIpPrefetch**	プロセッサで DCU IP プリフェッチ 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 プリフェッチャ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。
[ダイレクトキャッシュアクセスサポート（Direct Cache Access Support）] ドロップダウン リスト **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。

サーバー モデル別 BIOS パラメータ

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]：サーバーで 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][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] ドロップダウン リスト **set EnhancedIntelSpeedStep**	プロセッサで拡張版 Intel SpeedStep テクノロジーを使用するかどうか設定します。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。 • [有効（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） [Power Technology][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**	プロセッサでインテルターボブーストテクノロジーを使用するかどうか。このテクノロジーでは、仕様よりも低い電力、温度、または電圧でプロセッサが動作していると、自動的にそのプロセッサの周波数が上がります。次のいずれかになります。 • [Disabled]：プロセッサの周波数は自動的には上がりません。 • [Enabled]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。 （注） [Power Technology][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） [Power Technology][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 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） [Power Technology][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。
[プロセッサの電源状態C1拡張（Processor Power State C1 Enhanced）] ドロップダウン リスト **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。 • [無効（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。 • [有効（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。

名前	説明
[P-STATE調整（P-STATE Coordination）] ドロップダウン リスト **set PsdCoordType**	BIOS がオペレーティング システムに P-state サポート モデルを伝達する方法を定義できます。Advanced Configuration and Power Interface（ACPI）仕様では、次の 3 つのモデルが定義されています。 • [HW_ALL]：プロセッサ ハードウェアによって、依存関係に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）によって、依存関係に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）によって、依存関係に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できます。 （注） [Power Technology][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。
[SINGLE_PCTL] ドロップダウン リスト **get SinglePCTLEn**	プロセッサの電源管理を向上させるために単一 PCTL サポートを促進します。次のいずれかになります。 • **[いいえ（No）]** • ○
[TDPの設定（Config TDP）] ドロップダウン リスト **get ConfigTDP**	システムの熱設計電力（TDP）を設定できます。TDP は、過熱イベントを引き起こすことなくアプリケーションを実行できる最大電力量です。次のいずれかになります。 • [無効（Disabled）]：TDP の設定を無効にします。これはデフォルト値です。 • [有効（Enabled）]：TDP の設定を有効にします。

名前	説明
[エネルギーパフォーマンスの調整（Energy Performance Tuning）] ドロップダウン リスト **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]：エネルギーパフォーマンスの調整に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。
[エネルギーパフォーマンス（Energy Performance）] ドロップダウン リスト **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ー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**

名前	説明
[パッケージのCステートの制限（Package C State Limit）] ドロップダウン リスト **set PackageCStateLimit**	アイドル時にサーバー 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]：サーバーはすべてのサーバー 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]**：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、サーバーはすばやくハイ パフォーマンス モードに戻ることができます。 • **[C3_state]**：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、サーバーがハイ 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]**：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、サーバー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]**：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、サーバーがハイ パフォーマンス モードに戻るのに要する時間も最も長くなります。 • **[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。
[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 サポートを有効にします。 • [X2APIC]：APIC を有効にして、Intel VT-d と Interrupt Remapping も有効にします。

名前	説明
[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]：最適化のためにバランスのとれたオプションを選択します。 • [I/O Sensitive]：最適化のために I/O を考慮した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。
[IIO エラーの有効化（IIO Error Enable）] ドロップダウン リスト **get IohErrorEn**	IIO 関連のエラーを生成できます。次のいずれかになります。 • 〇 • **[いいえ（No）]**

[Memory Configuration] のパラメータ

名前	説明
[Select Memory RAS] **set SelectMemoryRAS**	サーバーに対するメモリの信頼性、可用性および機密性（RAS）の設定方法。次のいずれかになります。 • **[Maximum_Performance]**：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することで、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図ることができます。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
[DRAMクロックスロットリング（DRAM Clock Throttling）] ドロップダウン リスト **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 スロットリングを無効化し、追加の電力を使用してメモリ帯域幅を増やします。 • [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。
[低電圧DDRモード（Low Voltage DDR Mode）] ドロップダウン リスト **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。
[クローズドループ サーマル スロッティング（Closed Loop Therm Throt）] ドロップダウン リスト **set closedLoopThermThrotl**	閉ループ サーマル スロットリングのサポートを可能にします。これにより信頼性が向上し、CPU がアイドル状態の間は自動電圧制御により CPU の電力消費が低減します。次のいずれかになります。 • [無効（Disabled）]：閉ループ サーマル スロットリングを無効にします。 • [有効（Enabled）]：閉ループ サーマル スロットリングを有効にします。これがデフォルト値です。

サーバー モデル別 BIOS パラメータ

名前	説明
[チャネルインターリーブ（Channel Interleaving）] ドロップダウン リスト **set ChannelInterLeave**	CPU がメモリ ブロックを分割して、インターリーブされたチャネル間にデータの連続部分を分散し、同時読み取り動作を有効にするかどうか。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。 • [1Way][1_Way]：一部のチャネル インターリーブが使用されます。 • [2Way][2_Way] • [3Way][3_Way] • [4Way][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。 • [1Way][1_Way]：一部のランク インターリーブが使用されます。 • [2Way][2_Way] • [4Way][4_Way] • [8Way][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**	システムがサーバー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。 • [有効（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、システムは修復を試みます。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。
[デマンドスクラブ（Demand Scrub）] ドロップダウン リスト **set DemandScrub**	CPU または I/O から読み取り要求があった時に発生したシングル ビット メモリ エラーを、システムで修正するかどうか。次のいずれかになります。 • [無効（Disabled）]：シングル ビット メモリ エラーは修正されません。 • [Enabled]：シングル 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応じて設定されます。
[高度（Altitude）] ドロップダウン リスト **set Altitude**	物理サーバーがインストールされている地点のおよその海抜（m 単位）。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。 • [300M][300_M]：サーバーは海抜約 300 m の位置にあります。 • [900M][900_M]：サーバーは海抜約 900 m の位置にあります。 • [1500M][1500_M]：サーバーは海抜約 1500 m の位置にあります。 • **[3000_M]**：サーバーは、海抜約 3000 m です。

名前	説明
[パニックと高水準点（Panic and High Watermark）] ドロップダウンリスト **PanicHighWatermark**	低に設定した場合、**[メモリ更新レート（Memory Refresh Rate）]** が **[1X リフレッシュ（1X Refresh）]** に設定されている間、メモリ コントローラは更新を延期しません。 次のいずれかになります。 • **[低（Low）]**：リフレッシュ レートは低に設定します。 • **[高（High）]**：リフレッシュ レートは高に設定します。

[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。 • [無効（Disabled）]：QPI スヌープ モードを無効にします。 • [クラスタ オン ダイ（Cluster on Die）]：クラスタ オン ダイが有効になります。有効化したLLCはそれぞれに独立したキャッシング エージェントで2つのパートに分割されます。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、10個以上のコアを搭載した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。 • [自動（Auto）]：CPU は自動的に早期スヌープ モードとして認識します。これはデフォルト値です。

[USB Configuration] のパラメータ

名前	説明
[レガシーUSBサポート（Legacy USB Support）] ドロップダウン リスト **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。 • [無効（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。 • [有効（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。 • [無効（Disabled）]：60h/64エミュレーションはサポートされません。 • [有効（Enabled）]：60h/64エミュレーションはサポートされます。 サーバーで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。
[すべてのUSBデバイス（All USB Devices）] ドロップダウン リスト **set AllUsbDevices**	すべての物理および仮想USBデバイスを有効にするか無効にするか。次のいずれかになります。 • [Disabled]：すべてのUSBデバイスが無効です。 • [Enabled]：すべてのUSBデバイスが有効になります。
[USB Port: Rear] **set UsbPortRear**	背面パネルのUSBデバイスを有効にするか無効にするか。次のいずれかになります。 • [無効（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。 • [有効（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デバイスを有効にするか無効にするか。次のいずれかになります。 • [無効（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。 • [有効（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**	vKVM ポートが有効か無効か。次のいずれかになります。 • **無効**：vKVM キーボードおよびマウス デバイスを無効にします。キーボードとマウスはvKVM ウィンドウで機能しなくなります。 • **有効**：vKVM キーボードとマウス デバイスを有効にします。
[USB Port: vMedia] **set UsbPortVMedia**	仮想メディア デバイスを有効にするか無効にするか。次のいずれかになります。 • [無効（Disabled）]：vMediaデバイスをディセーブルにします。 • [Enabled]：vMedia デバイスを有効にします。
[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 サポートを無効にします。 • [Enabled]：xHCIコントローラのレガシーサポートを有効にします。

[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]：サーバーでは 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。 • [有効（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。
[SR-IOV サポート（SR-IOV Support）] ドロップダウン リスト **set SrIov**	サーバー上で SR-IOV（Single Root I/O Virtualization）を有効にするか無効にするか。次のいずれかになります。 • [Disabled]：SR-IOV は無効になります。 • [有効（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 緊急管理サービスで使用可能な 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。 • [有効（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
[コンソールリダイレクション（Console redirection）] ドロップダウン リスト **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 リダイレクションで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 リダイレクションの関連性はなくなり、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]：POST中に COM ポート 0 でコンソール リダイレクションを有効にします。 • [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有効にします。
[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] を無効にする場合は、このオプションを使用できません。次のいずれかになります。 • [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
[フロー制御（Flow Control）] ドロップダウン リスト **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を設定します。送信要求/クリア ツーセンド（RTS/CTS）を使用すると、隠れた端末の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 キーによって **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 によって 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 によって **ESC [M** ～ **ESC [X** を生成します。ファンクション キーと Shift キーによって **ESC [Y** ～ **ESC [j** を生成します。Ctrl キーとファンクション キーによって **ESC [k** ～ **ESC [v** を生成します。Shift、Ctrl およびファンクション キーによって **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 キーによって **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 キーはデフォルト モードと同様に動作します。テンキーの最上段のキーによって **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]**：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
[VICに対するCDNサポート（CDN Support for VIC）] ドロップダウン リスト **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。 • [無効（Disabled）]：VICカードに対するCDNサポートは無効です。 • [有効（Enabled）]：CDNサポートはVICカードに対して有効です。 （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 の実行を設定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 SATA Mode] **set SataModeSelect**	このオプションでは、PCH SATA モードを選択できます。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 ポートを有効にするか無効にするか。次のいずれかになります。 • [Disabled]：すべての LOM ポートが無効です。 • [Enabled]：すべての LOM ポートが有効になります。
[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 をサーバー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 をサーバー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。 • **[無効（Disabled）]**：レガシーおよび UEFI の両方のオプション ROM は実行されません。 • **[UEFI のみ（UEFI Only）]**：UEFI オプション ROM のみを実行します。 • [Legacy Only]：レガシー オプション ROM のみを実行します。
[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。 • **[無効（Disabled）]**：レガシーおよび UEFI の両方のオプション ROM は実行されません。 • **[UEFI のみ（UEFI Only）]**：UEFI オプション ROM のみを実行します。 • [Legacy Only]：レガシー オプション ROM のみを実行します。

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。 • **[無効（Disabled）]**：レガシーおよびUEFIの両方のオプションROMは実行されません。 • **[UEFIのみ（UEFI Only）]**：UEFIオプションROMのみを実行します。 • [Legacy Only]：レガシー オプションROMのみを実行します。
[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。 • **[無効（Disabled）]**：レガシーおよびUEFIの両方のオプションROMは実行されません。 • **[UEFIのみ（UEFI Only）]**：UEFIオプションROMのみを実行します。 • [Legacy Only]：レガシー オプションROMのみを実行します。
[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。 • **[無効（Disabled）]**：レガシーおよびUEFIの両方のオプションROMは実行されません。 • **[UEFIのみ（UEFI Only）]**：UEFIオプションROMのみを実行します。 • [Legacy Only]：レガシー オプションROMのみを実行します。

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。 • [自動（Auto）]：システムは許可される最大速度を選択します。 • [GEN1]：最大 2.5 GT/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 5 GT/s までの速度が許可されます。 • [GEN3]：最大 8 GT/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。

C460 M4 サーバの [サーバ管理（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、[Save Changes] 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 中にシステムがハングアップした場合に、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。 • [無効（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 ウォッチドッグ タイマー（OS Watchdog Timer）] ドロップダウン リスト **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]：サーバーのブートにかかる時間をトラッキングするためにウォッチドッグ タイマーは使用されません。 • [Enabled]：サーバーのブートにかかる時間をウォッチドッグ タイマーでトラッキングします。サーバーが **set OSBootWatchdogTimerTimeout** コマンドにより、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。

サーバー モデル別 BIOS パラメータ

名前	説明
[OSウォッチドッグタイマータイムアウト（OS Watchdog Timer Timeout）] ドロップダウン リスト **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ウォッチドッグタイマーポリシー（OS Watchdog Timer Policy）] ドロップダウン リスト **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、サーバー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、サーバーはリセットされます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にする場合にのみ適用されます。

[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。

C220 M4 および C240 M4 サーバ

C220M4 および C240M4 サーバのメイン タブ

主要な BIOS パラメータ

名前	説明
[今すぐホストを再起動（Reboot Host Immediately）] チェックボックス	このチェックボックスをオンにすると、直ちにホスト サーバが再起動します。このチェックボックスは、変更を保存してからオンにする必要があります。

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]：サーバーは TPM を使用しません。 • [有効（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。
[Power ON Password Support] ドロップダウン	このトークンでは、F2 BIOS 設定を使用する前に BIOS パスワードを設定する必要があります。有効にすると、BIOS 関数（IO 設定、BIOS セットアップ、BIOS を使用したオペレーティング システムへのブート）にアクセスする前にパスワードの検証が必要になります。次のいずれかを指定できます。 • **[無効（Disabled）]**：サポートは無効になります。 • **[有効（Enabled）]**：サポートは有効になります。

[Actions] 領域

名前	説明
[**Save**] ボタン	BIOS パラメータの設定を保存して、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、サーバー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、変更内容はサーバーが手動でリブートされるまで保存されます。
[Reset] ボタン	3 つすべてのタブ上の BIOS パラメータの値が、このダイアログボックスを最初に開いた際に有効だった設定にリセットされます。
[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。

C220M4 および C240M4 サーバの [詳細（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、[Save Changes] 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] ドロップダウン リスト **set IntelHyperThread**	プロセッサでインテル ハイパースレッディング テクノロジーを使用するかどうか。このテクノロジーでは、マルチスレッド ソフトウェア アプリケーションのスレッドを各プロセッサ内で並列に実行できます。次のいずれかになります。 • [Disabled]：プロセッサでのハイパースレッディングを禁止します。 • [有効（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。

サーバー モデル別 BIOS パラメータ

名前	説明
[有効化されたコア数（Number of Enabled Cores）] ドロップダウン リスト **set CoreMultiProcessing**	サーバー上の 1 つ以上の物理コアを無効にできます。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てください。
[Execute Disable] ドロップダウン リスト **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、サーバーのメモリ領域を分類します。この分類の結果、悪意のあるワームがバッファにコードを挿入しようとした場合、プロセッサでコードの実行を無効化します。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。 • [有効（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 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。 • [有効（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ー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。
[Intel VTD割り込み再マッピング（Intel VTD interrupt Remapping）] ドロップダウンリスト **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] ドロップダウン リスト **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。

サーバー モデル別 BIOS パラメータ

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**	サーバーの 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 • ハードウェア プリフェッチャ • 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。 • [HighThroughput]**[High_Throughput]**：DCU IP 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
[ハードウェア プリフェッチャ（Hardware Prefetcher）] ドロップダウン リスト **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。
[隣接キャッシュラインプリフェッチャ（Adjacent Cache Line Prefetcher）] ドロップダウン リスト **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。 • [有効（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ストリーマープリフェッチ（DCU Streamer Prefetch）] ロップダウン リスト **set DcuStreamerPrefetch**	プロセッサで DCU IP プリフェッチ 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プリフェッチャ（DCU IP Prefetcher）] ドロップダウン リスト **set DcuIpPrefetch**	プロセッサで DCU IP プリフェッチ 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 プリフェッチャ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。

サーバー モデル別 BIOS パラメータ

名前	説明
[ダイレクトキャッシュアクセスサポート（Direct Cache Access Support）] ドロップダウン リスト **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]：サーバーで 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][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] ドロップダウン リスト **set EnhancedIntelSpeedStep**	プロセッサで拡張版 Intel SpeedStep テクノロジーを使用するかどうか設定します。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。 • [有効（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） [Power Technology][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**	プロセッサでインテル ターボ ブースト テクノロジーを使用するかどうか。このテクノロジーでは、仕様よりも低い電力、温度、または電圧でプロセッサが動作していると、自動的にそのプロセッサの周波数が上がります。次のいずれかになります。 • [Disabled]：プロセッサの周波数は自動的には上がりません。 • [Enabled]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。 （注） [Power Technology][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 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） [Power Technology][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） [Power Technology][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。
[プロセッサの電源状態C1拡張（Processor Power State C1 Enhanced）] ドロップダウン リスト **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。 • [無効（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。 • [有効（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。

名前	説明
[P-STATE調整（P-STATE Coordination）] ドロップダウン リスト **set PsdCoordType**	BIOS がオペレーティング システムに P-state サポート モデルを伝達する方法を定義できます。Advanced Configuration and Power Interface（ACPI）仕様では、次の 3 つのモデルが定義されています。 • [HW_ALL]：プロセッサ ハードウェアによって、依存関係に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）によって、依存関係に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）によって、依存関係に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できます。 （注） [Power Technology][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。
[Boot Performance Mode] ドロップダウン リスト **set BootPerformanceMode**	オペレーティング システムのハンドオフ前に設定される BIOS パフォーマンス状態を選択できます。次のいずれかになります。 • [最大パフォーマンス（Max Performance）]：プロセッサの P-state の比率が最大です。 • [Max Efficient]：プロセッサの P-state 率は最小です
[エネルギーパフォーマンスの調整（Energy Performance Tuning）] ドロップダウン リスト **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]：エネルギーパフォーマンスの調整に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
[エネルギーパフォーマンス（Energy Performance）] ドロップダウン リスト **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ー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**
[パッケージのCステートの制限（Package C State Limit）] ドロップダウン リスト **set PackageCStateLimit**	アイドル時にサーバー 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]：サーバーはすべてのサーバー 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]**：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、サーバーはすばやくハイ パフォーマンス モードに戻ることができます。 • **[C3_state]**：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、サーバーがハイ 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]**：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、サーバー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]**：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、サーバーがハイ パフォーマンス モードに戻るのに要する時間も最も長くなります。 • **[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 サポートを有効にします。 • [X2APIC]：APIC を有効にして、Intel VT-d と Interrupt Remapping も有効にします。
[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]：最適化のためにバランスのとれたオプションを選択します。 • [I/O Sensitive]：最適化のために I/O を考慮した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。
[CPU HWPM] ドロップダウンリスト **set HWPMEnable**	CPU のパフォーマンスやエネルギー効率を引き上げるためのハードウェア電源管理（HWPM）インターフェイスを有効にします。次のいずれかになります。 • [無効（Disabled）]：P-state は前世代のプロセッサと同じ方法で制御されます。 • [ネイティブモード（Native Mode）]：HWPM はソフトウェアインターフェイスを介してオペレーティング システムと連動します。 • [OOBモード（OOB Mode）]：CPU は、オペレーティング システムのエネルギー効率に基づいて周波数を自律的に制御します。
[CPU自律C-state] ドロップダウン リスト **set AutonumousCstateEnable**	HALT 命令を MWAIT 命令に変換する CPU 自律 C-state を有効にします。次のいずれかになります。 • [無効（Disabled）]：CPU 自律 C-state が無効になります。これはデフォルト値です。 • [有効（Enabled）]：CPU 自律 C-state が有効になります。

名前	説明
[プロセッサCMCI（Processor CMCI）] ドロップダウン リスト **set CmciEnable**	CPU が corrected machine check events で割り込みをトリガーできるようにします。corrected machine check interrupt（CMCI）により、従来のポーリング タイマーよりも反応速度を向上できます。次のいずれかになります。 • [無効（Disabled）]：CMCI が無効になります。 • [有効（有効）]：CMCI が有効になります。これはデフォルト値です。

[Memory Configuration] のパラメータ

名前	説明
[Select Memory RAS] **set SelectMemoryRAS**	サーバーに対するメモリの信頼性、可用性および機密性（RAS）の設定方法。次のいずれかになります。 • **[Maximum_Performance]**：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することで、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図ることができます。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] ドロップダウン リスト **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。 • [有効（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。このオプションを有効にする場合は、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 インターリーブを無効にする必要があります。
[チャネルインターリーブ（Channel Interleaving）] ドロップダウン リスト **set ChannelInterLeave**	CPU がメモリ ブロックを分割して、インターリーブされたチャネル間にデータの連続部分を分散し、同時読み取り動作を有効にするかどうか。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。 • [1Way][1_Way]：一部のチャネル インターリーブが使用されます。 • [2Way][2_Way] • [3Way][3_Way] • [4Way][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。 • [1Way][1_Way]：一部のランク インターリーブが使用されます。 • [2Way][2_Way] • [4Way][4_Way] • [8Way][8_Way]：最大量のランク インターリーブが使用されます。

サーバー モデル別 BIOS パラメータ

名前	説明
[Patrol Scrub] **set PatrolScrub**	システムがサーバー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。 • [有効（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、システムは修復を試みます。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。
[デマンドスクラブ（Demand Scrub）] ドロップダウン リスト **set DemandScrub**	CPU または I/O から読み取り要求があった時に発生したシングル ビット メモリ エラーを、システムで修正するかどうか。次のいずれかになります。 • [無効（Disabled）]：シングル ビット メモリ エラーは修正されません。 • [Enabled]：シングル 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応じて設定されます。
[高度（Altitude）] ドロップダウン リスト **set Altitude**	物理サーバーがインストールされている地点のおよその海抜（m 単位）。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。 • [300M][300_M]：サーバーは海抜約 300 m の位置にあります。 • [900M][900_M]：サーバーは海抜約 900 m の位置にあります。 • [1500M][1500_M]：サーバーは海抜約 1500 m の位置にあります。 • **[3000_M]**：サーバーは、海抜約 3000 m です。

名前	説明
[パニックと高水準点（Panic and High Watermark）] ドロップダウンリスト **PanicHighWatermark**	低に設定した場合、**[メモリ更新レート（Memory Refresh Rate）]** が **[1X リフレッシュ（1X Refresh）]** に設定されている間、メモリ コントローラは更新を延期しません。 次のいずれかになります。 • **[低（Low）]**：リフレッシュ レートは低に設定します。 • **[高（High）]**：リフレッシュ レートは高に設定します。

[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**

名前	説明
[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。 • [早期スヌープ（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。 • [ホーム スヌープ（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もローカル遅延が高くなりますが、多数の未処理トランザクションに追加のリソースを提供します。 • [Home Directory Snoop]：ホーム ディレクトリはオプションで使用できる機能で、プロセッサ内の HA ロジックと iMC ロジックの両方に実装されています。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、および 2S と 4S の設定内のリモートソケット、およびノード コントローラへスヌープを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。 • [クラスタ オン ダイ（Cluster on Die）]：クラスタ オン ダイが有効になります。有効化した LLC はそれぞれに独立したキャッシング エージェントで 2 つのパートに分割されます。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、10 個以上のコアを搭載した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。

[USB Configuration] のパラメータ

名前	説明
[レガシーUSBサポート（Legacy USB Support）] ドロップダウン リスト **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。 • [無効（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。 • [有効（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。 • [無効（Disabled）]：60h/64エミュレーションはサポートされません。 • [有効（Enabled）]：60h/64エミュレーションはサポートされます。 サーバーで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を無効にします。 • [Enabled]：xHCIコントローラのレガシーサポートを有効にします。
[xHCI Legacy Support] ドロップダウン リスト **set UsbXhciSupport**	システム上でのレガシーxHCIコントローラのサポートを有効/無効にします。次のいずれかになります。 • [無効（Disabled）]：xHCIレガシーサポートを無効にします。 • [有効（Enabled）]：xHCIレガシーサポートを有効にします。これはデフォルト値です。

名前	説明
[すべてのUSBデバイス（All USB Devices）] ドロップダウン リスト **set AllUsbDevices**	すべての物理および仮想USBデバイスを有効にするか無効にするか。次のいずれかになります。 • [Disabled]：すべての USB デバイスが無効です。 • [Enabled]：すべての USB デバイスが有効になります。
[USB Port: Rear] **set UsbPortRear**	背面パネルのUSBデバイスを有効にするか無効にするか。次のいずれかになります。 • [無効（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。 • [有効（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 ポート：前面（USB Port:Front）] **set UsbPortFront**	前面パネルのUSBデバイスを有効にするか無効にするか。次のいずれかになります。 • [無効（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。 • [有効（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デバイスを有効にするか無効にするか。次のいずれかになります。 • [無効（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。 • [有効（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**	vKVM ポートが有効か無効か。次のいずれかになります。 • **無効**：vKVM キーボードおよびマウス デバイスを無効にします。キーボードとマウスは vKVM ウィンドウで機能しなくなります。 • **有効**：vKVM キーボードとマウス デバイスを有効にします。
[USB Port: vMedia] **set UsbPortVMedia**	仮想メディア デバイスを有効にするか無効にするか。次のいずれかになります。 • [無効（Disabled）]：vMediaデバイスをディセーブルにします。 • [Enabled]：vMedia デバイスを有効にします。

[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]：サーバーでは 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。 • [有効（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**	サーバー上で SR-IOV（Single Root I/O Virtualization）を有効にするか無効にするか。次のいずれかになります。 • [Disabled]：SR-IOV は無効になります。 • [有効（Enabled）]：SR-IOV はイネーブルになります。

サーバー モデル別 BIOS パラメータ

名前	説明
[ASPM サポート（ASPM Support）] ドロップダウン リスト **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]：BIOS での ASPM サポートが無効です。 • [Force L0]：すべてのリンクを強制的に L0 スタンバイ（L0s）状態にします。 • [自動（Auto）]：電力状態を CPU によって判別します。
[NVMe SSD ホットプラグのサポート（NVMe SSD Hot-Plug Support）] ドロップダウン リスト **set PCIeSSDHotPlugSupport**	サーバの電源を切ることなく、NVMe SSD を交換できます。次のいずれかになります。 • [無効（Disabled）]：NVMe SSD ホットプラグ サポートが無効です。これはデフォルト値です。 • [有効（Enabled）]：NVMe SSD ホットプラグ サポートが有効です。
[VGA 優先順位（VGA Priority）] ドロップダウン リスト **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 デバイスの優先順位を設定できます。次のいずれかになります。 • [Onboard]：オンボード VGA デバイスが優先されます。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]：PCIE グラフィックス アダプタが優先されます。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。 • [オンボード VGA 無効（Onboard VGA Disabled）]：PCIE グラフィックス アダプタが優先され、オンボード VGA デバイスは無効になります。

[Serial Configuration] のパラメータ

名前	説明
[Out-of-Band Mgmt Port] **set comSpcrEnable**	Windows 緊急管理サービスで使用可能な 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。 • [有効（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。
[コンソールリダイレクション（Console redirection）] ドロップダウン リスト **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 リダイレクションで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 リダイレクションの関連性はなくなり、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]：POST中に COM ポート 0 でコンソール リダイレクションを有効にします。 • [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有効にします。
[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。

サーバー モデル別 BIOS パラメータ

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] を無効にする場合は、このオプションを使用できません。次のいずれかになります。 • [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。
[フロー制御（Flow Control）] ドロップダウン リスト **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を設定します。送信要求/クリア ツー センド（RTS/CTS）を使用すると、隠れた端末の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 キーによって **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 によって 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 によって **ESC [M** ～ **ESC [X** を生成します。ファンクション キーと Shift キーによって **ESC [Y** ～ **ESC [j** を生成します。Ctrl キーとファンクション キーによって **ESC [k** ～ **ESC [v** を生成します。Shift、Ctrl およびファンクション キーによって **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 キーによって **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 キーはデフォルト モードと同様に動作します。テンキーの最上段のキーによって **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]**：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
[VICに対するCDNサポート（CDN Support for VIC）] ドロップダウン リスト **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。 • [無効（Disabled）]：VICカードに対するCDNサポートは無効です。 • [有効（Enabled）]：CDNサポートはVICカードに対して有効です。 （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 の実行を設定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。
[PCH SATA Mode] **set SataModeSelect**	このオプションでは、PCH SATA モードを選択できます。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 ポートを有効にするか無効にするか。次のいずれかになります。 • [Disabled]：すべての LOM ポートが無効です。 • [Enabled]：すべての LOM ポートが有効になります。

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 をサーバー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 をサーバー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: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。 • **[無効（Disabled）]**：レガシーおよび UEFI の両方のオプション ROM は実行されません。 • **[UEFI のみ（UEFI Only）]**：UEFI オプション ROM のみを実行します。 • [Legacy Only]：レガシー オプション ROM のみを実行します。
[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。 • **[無効（Disabled）]**：レガシーおよび UEFI の両方のオプション ROM は実行されません。 • **[UEFI のみ（UEFI Only）]**：UEFI オプション ROM のみを実行します。 • [Legacy Only]：レガシー オプション ROM のみを実行します。
[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。 • **[無効（Disabled）]**：レガシーおよび UEFI の両方のオプション ROM は実行されません。 • **[UEFI のみ（UEFI Only）]**：UEFI オプション ROM のみを実行します。 • [Legacy Only]：レガシー オプション ROM のみを実行します。

名前	説明
[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。 • **[無効（Disabled）]**：レガシーおよび UEFI の両方のオプション ROM は実行されません。 • **[UEFI のみ（UEFI Only）]**：UEFI オプション ROM のみを実行します。 • [Legacy Only]：レガシー オプション ROM のみを実行します。
[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。 • [自動（Auto）]：システムは許可される最大速度を選択します。 • [GEN1]：最大 2.5 GT/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 5 GT/s までの速度が許可されます。 • [GEN3]：最大 8 GT/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。

名前	説明
[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 [サーバ管理（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、[Save Changes] 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 中にシステムがハングアップした場合に、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。 • [無効（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 ウォッチドッグ タイマー（OS Watchdog Timer）] ドロップダウン リスト **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]：サーバーのブートにかかる時間をトラッキングするためにウォッチドッグ タイマーは使用されません。 • [Enabled]：サーバーのブートにかかる時間をウォッチドッグタイマーでトラッキングします。サーバーが **set OSBootWatchdogTimerTimeout** コマンドにより、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ウォッチドッグタイマータイムアウト（OS Watchdog Timer Timeout）] ドロップダウン リスト **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ウォッチドッグタイマーポリシー（OS Watchdog Timer Policy）] ドロップダウン リスト **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、サーバー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、サーバーはリセットされます。 （注） このオプションは [OS Boot Watchdog Timer] を有効にする場合にのみ適用されます。

[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。

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