サーバ ユーティリティ

この章は、次の項で構成されています。

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、**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 サーバでは、リモート サーバからファームウェアを更新したときの、サーバのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバ タイプとして SCP または SFTP を選択した場合にのみ使用できます。 このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」というメッセージが表示されます。サーバフィンガープリントの信頼性に応じて、[y] または [n] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。
ステップ 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。
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。

	コマンドまたはアクション	目的
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、サーバのトラブルシューティング時に、サーバの BIOS CMOS メモリのクリアが必要になることがあります。この手順は、通常のサーバ メンテナンスには含まれません。

手順

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

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。
- サーバのマザーボード上でハードウェア ジャンパの BIOS リカバリ機能を使用する（お使いのサーバ モデルでサポートされている場合）。手順については、お使いのサーバ モデルに対応した『Cisco UCS Server Installation and Service Guide』を参照してください。

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の電源が再投入されるため、サーバのダウンタイムをスケジュール設定します。

手順

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

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、サーバをリセットします。

Cisco IMC の出荷時デフォルトへのリセット

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

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

バージョン 1.5(1) からバージョン 1.5(2) にアップグレードすると、Cisco IMC インターフェイスのホスト名はそのまま保持されます。ただし、バージョン 1.5(2) にアップグレードした後、工場出荷時の状態にリセットすると、ホスト名は CXXX-YYYYYY という形式に変更されます。（XXX はモデル番号、YYYYYY はサーバのシリアル番号）。

バージョン 1.5(2) からバージョン 1.5(1) にダウングレードすると、ホスト名はそのまま保持されます。ただし、工場出荷時の状態にリセットすると、ホスト名は ucs-cxx-mx という形式に変更されます。

（注） Cisco IMC 1.5(x)、2.0、および 2.0(3) バージョンを工場出荷時の初期状態にリセットすると、**Shared LOM** モードがデフォルトで設定されます。C3160 サーバの場合、Cisco IMC を工場出荷時の初期状態にリセットすると、**[Dedicated]** モードが **[Full]** デュプレックス 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。
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 アカウントやサーバ証明書をエクスポートしないでください。

始める前に

バックアップ リモート サーバの IP アドレスを取得します。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope import-export**	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たパスおよびファイル名でエクスポートされます。

	コマンドまたはアクション	目的
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 サーバでは、リモート サーバからファームウェアを更新したときの、サーバのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバ タイプとして SCP または SFTP を選択した場合にのみ使用できます。 このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?」というメッセージが表示されます。サーバ フィンガープリントの信頼性に応じて、[y] または [n] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。
ステップ 4	Server /cimc/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。

	コマンドまたはアクション	目的
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。
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。

	コマンドまたはアクション	目的
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 サーバは次のいずれかになります。 • TFTP • FTP • SFTP • SCP • HTTP （注） Cisco UCS C シリーズ サーバでは、リモート サーバからファームウェアを更新したときの、サーバのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバ タイプとして SCP または SFTP を選択した場合にのみ使用できます。 このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?」というメッセージが表示されます。サーバ フィンガープリントの信頼性に応じて、[y] または [n] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。
ステップ 4	Server /cimc/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。

	コマンドまたはアクション	目的
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のコンフィギュレーション ファイルがインポートされます。リモート サーバは次のいずれかになります。 • TFTP

	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 サーバでは、リモート サーバからファームウェアを更新したときの、サーバのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバ タイプとして SCP または SFTP を選択した場合にのみ使用できます。 このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?」というメッセージが表示されます。サーバ フィンガープリントの信頼性に応じて、[y] または [n] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。

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 サーバは次のいずれかになります。 • TFTP • FTP • SFTP • SCP • HTTP

	コマンドまたはアクション	目的
		（注） Cisco UCS C シリーズ サーバでは、リモート サーバからファームウェアを更新したときの、サーバのフィンガープリントの確認をサポートするようになりました。このオプションは、リモートサーバタイプとして SCP または SFTP を選択した場合にのみ使用できます。 このアクションを実行しながら、リモートサーバタイプとして SCP または SFTP を選択した場合、「Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?」というメッセージが表示されます。サーバ フィンガープリントの信頼性に応じて、[y] または [n] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。
ステップ 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 サーバの IP アドレス、サーバ上のファームウェア ファ

	コマンドまたはアクション	目的
		イルへのファイル パスを指定します。プロトコルは次のいずれかになります。 • TFTP • FTP • SFTP • SCP • HTTP （注） Cisco UCS C シリーズ サーバでは、リモート サーバからファームウェアを更新したときの、サーバのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバ タイプとして SCP または SFTP を選択した場合にのみ使用できます。 このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?」というメッセージが表示されます。サーバ フィンガープリントの信頼性に応じて、[y] または [n] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。
ステップ 4	（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 #
```