サーバ ユーティリティ

この章は、次の項で構成されています。

テクニカル サポート データのエクスポート

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

重要 ファームウェアまたは BIOS の更新が進行中の場合は、それらのタスクが完了するまで、テクニカル サポート データをエクスポートしないでください。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope 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 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 collect-from** {**all** |**cmc** |**peercmc** |**bmc1** |**bmc2**}	テクニカルサポートデータにエクスポートするコンポーネントを指定します。
ステップ 4	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 5	Server /chassis/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 6	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

	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 7	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 8	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 9	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 10	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。

	コマンドまたはアクション	目的
ステップ 11	（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 12	（任意） Server /chassis/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 chassis
Server /chassis # scope tech-support
Server /chassis/tech-support # set collect-from all
Server /chassis/tech-support* # set remote-ip 192.0.20.41
Server /chassis/tech-support* # set remote-protocol tftp
Server /chassis/tech-support *# set remote-path /user/user1/default.tar.gz
Server /chassis/tech-support *# commit
Server /chassis/tech-support # start
Tech Support upload started.

Server /chassis/tech-support # show detail

Tech Support:
 Server Address: 192.0.20.41
    Path('default' for auto-naming): default.tar.gz
    Protocol: tftp
    Username:
    Password: ******
    Collect from: all
    Progress(%): 100
    Status: COMPLETED

Server /chassis/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。

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 server** {**1** | **2**}	サーバ 1 または 2 のサーバ コマンド モードを開始します。
ステップ 2	Server /server # **scope bmc**	bmc コマンド モードを開始します。
ステップ 3	Server /server/bmc # **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 server 1
Server /server # scope bmc
Server /server/bmc # 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 server** {**1** | **2**}	サーバ 1 または 2 のサーバ コマンド モードを開始します。
ステップ 2	Server /server # **scope bios**	bios コマンド モードを開始します。
ステップ 3	Server /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 server 2
Server/server # scope bios
Server /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 /server/bios #
```

BMC 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、BMC 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。BMC をリセットした後は、ログオフしてから再びログインする必要があります。また、接続が失われ、ネットワーク設定を再び指定する必要がある場合もあります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope server** {**1** | **2**}	サーバ 1 または 2 のサーバ コマンド モードを開始します。
ステップ 2	Server /server # **scope bmc**	bmc コマンド モードを開始します。 （注） 選択したサーバ番号に応じて BMC1 または BMC2 モードが開始されます。
ステップ 3	Server /server/bmc # **factory-default**	確認プロンプトの後に、BMC が出荷時デフォルトにリセットされます。すべての BMC 設定が失われ、インベントリの情報の一部は、サーバは電源が投入されているか、電源が再投入するまで、使用できない場合があります。

例

この例では、BMC1 を工場出荷時のデフォルトにリセットします。

```
Server# scope server 1
Server /server # scope bmc
Server /server/bmc # factory-default
This operation will reset the Server BMC configuration to factory default.
All your configuration will be lost. Some inventory information may
not be available until the server is powered on or power cycled.
Continue?[y|N] y
```

出荷時の初期状態へのリセット

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** {**storage** | **vic** | **bmc1** | **bmc2** | **cmc** | **all**}	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、BMC1、BMC2、および CMC の設定を工場出荷時のデフォルトにリセットします。 • **bmc1** ：BMC1 設定が工場出荷時のデフォルトにリセットされます。 • **bmc2** ：BMC2 設定が工場出荷時のデフォルトにリセットされます。 • **cmc**]CMCs 設定が工場出荷時のデフォルトにリセットされます。 • **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。

	コマンドまたはアクション	目的
		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。 （注） CMC をデフォルトにリセットすると、すべての CMC 設定が失われ、ネットワーク設定モードはデフォルトで、**Cisco Card** モードに設定されます。CMC 工場設定デフォルト値には、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。
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
Factory Reset Status:
    Storage: NA
    VIC: Pending
    BMC1: NA
    BMC2: NA
    CMC: NA
Server /chassis #
```

出荷時の初期状態へのリセット

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** {**storage** | **vic** | **bmc1** | **bmc2** | **cmc** | **all**}	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、BMC1、BMC2、および CMC の設定を工場出荷時のデフォルトにリセットします。 • **bmc1** ：BMC1 設定が工場出荷時のデフォルトにリセットされます。

	コマンドまたはアクション	目的
		• **bmc2** ：BMC2 設定が工場出荷時のデフォルトにリセットされます。 • **cmc**]CMCs 設定が工場出荷時のデフォルトにリセットされます。 • **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。

	コマンドまたはアクション	目的
		（注） CMC をデフォルトにリセットすると、すべての CMC 設定が失われ、ネットワーク設定モードはデフォルトで、**Cisco Card** モードに設定されます。CMC 工場設定デフォルト値には、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。
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
Factory Reset Status:
    Storage: NA
    VIC: Pending
    BMC1: NA
    BMC2: NA
    CMC: NA
Server /chassis #
```

Cisco IMC と BMC 設定のエクスポートとインポート

CMC 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、Cisco IMC 設定をインポートしないでください。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	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 import-export**	import-export コマンド モードを開始します。
ステップ 3	Server /chassis/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

	コマンドまたはアクション	目的
		• 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	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 chassis
Server /chassis # scope import-export
Server /chassis/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 /chassis/import-export # show detail
Import Export:
    Operation: Import
    Status: COMPLETED
    Error Code: 100 (No Error)
    Diagnostic Message: NONE
Server /chassis/import-export #
```

BMC 設定のインポート

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope server** {**1** | **2**}	サーバ 1 または 2 のサーバ コマンド モードを開始します。
ステップ 2	Server /server # **scope bmc**	bmc コマンド モードを開始します。
ステップ 3	Server /server/bmc # **scope import-export**	import-export コマンド モードを開始します。
ステップ 4	Server /server/bmc/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

	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 5	[ユーザ名（Username）] と [パスワード（Password）] を入力します。	インポートするファイルのユーザ名とパスワードを設定します。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 server 2
Server /server# scope bmc
Server /server/bmc # scope import-export
Server /server/bmc/import-export # import-config tftp 192.0.2.34 /ucs/backups/cimc5.xml
Username:pynj
Password:****
Import config started. Please check the status using "show detail".
Server /chassis/import-export # show detail
Import Export:
    Operation: Import
```

```
    Status: COMPLETED
    Error Code: 100 (No Error)
    Diagnostic Message: NONE
Server /server/bmc/import-export #
```

BMC 設定のエクスポート

（注） セキュリティ上の理由から、この操作でユーザアカウントやサーバ証明書をエクスポートしないでください。

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

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 server** {**1** | **2**}	サーバ 1 または 2 のサーバ コマンド モードを開始します。
ステップ 2	Server /server # **scope bmc**	bmc コマンド モードを開始します。
ステップ 3	Server /server/bmc # **scope import-export**	import-export コマンド モードを開始します。
ステップ 4	Server /server/bmc/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

	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 5	[ユーザ名（Username）] と [パスワード（Password）] 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 server 2
Server /server# scope bmc
Server /server/bmc # scope import-export
Server /server/bmc/import-export # export-config tftp 192.0.2.34 /ucs/backups/cimc5.xml
Username:pynj
Password:****
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 /server/bmc/import-export #
```

CMC 設定のエクスポート

（注） セキュリティ上の理由から、この操作でユーザアカウントやサーバ証明書をエクスポートしないでください。

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

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 chassis**	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 import-export**	import-export コマンド モードを開始します。
ステップ 3	Server /chassis/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

	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 4	ユーザ名、パスワード、およびパス フレーズを入力します。	エクスポートするファイルのユーザ名、パスワード、およびパスフレーズを設定します。バックアップ操作を開始します。

エクスポート操作が正常に完了したかどうかを確認するには、**show detail** コマンドを使用します。操作を中止するには、CTRL+C を入力します。

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 chassis
Server /chassis # scope import-export
Server /chassis/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 /chassis/import-export # show detail
Import Export:
```

```
    Operation: EXPORT
    Status: COMPLETED
    Error Code: 100 (No Error)
    Diagnostic Message: NONE

Server /chassis/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 • 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。

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 #
```

ホストへのマスク不能割り込みの生成

状況によっては、サーバがハングして、従来のデバッグ メカニズムに応答しない場合があります。ホストへのマスク不能割り込み（NMI）を生成することにより、サーバのクラッシュ ダンプ ファイルを作成および送信して、サーバのデバッグに使用することができます。

サーバに関連付けられたオペレーティング システムの種類によっては、このタスクでOSが再起動される場合があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope chassis**	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 server** {**1** | **2**}	サーバ 1 または 2 のサーバ コマンド モードを開始します。
ステップ 3	Server /chassis/server # **generate-nmi**	サーバのクラッシュ ダンプ ファイルが生成されます。 このコマンドを使用するには、サーバが電源をオンにし、管理者としてログインする必要があります。

例

次に、ホストへの NMI 信号を生成する例を示します。

```
Server # scope chassis
Server /chassis # scope server 2
Server /chassis/server # generate-nmi
This operation will send NMI to host and may cause reboot of OS
OS reboot depends on it's NMI configuration
Do you want to continue? [y|N] y
Server /chassis/server #
```

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 #
```

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 #
```