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。

テクニカル サポート データのエクスポート

テクニカル サポート データのエクスポート

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

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [ユーティリティ（Utilities）] ペインの [アクション（Actions）] 領域で、[テクニカルサポート データのエクスポート（Export Technical Support Data）] をクリックします。

ステップ 4 **[Export Technical Support Data]**ダイアログボックスで、次のフィールドに入力します。

名前	説明
[テクニカル サポート データのエクスポート先（Export Technical Support Data to）] ドロップダウン リスト	リモート サーバのタイプ。次のいずれかになります。 • **[TFTP サーバー（TFTP Server）]** • **FTP サーバー（FTP Server）** • **SFTP サーバー（SFTP Server）** • **SCP サーバー（SCP Server）** • **HTTP サーバー（HTTP Server）** （注） このアクションを実行中にリモート サーバのタイプとして SCP または SFTP を選択した場合、ポップアップ ウィンドウが表示され、そこに *[サーバ（RSA）鍵フィンガープリントは <server_finger_print _ID> です。続行しますか?（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度に応じて、[Yes] または [No] 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。

名前	説明
[テクニカル サポート データのエクスポート元（Export Technical Support Data through）] ドロップダウン リスト	（注） [前面パネル USB（Front Panel USB）] オプションは、[スマート アクセス USB（Smart Access USB）] が有効で、USB ストレージ デバイスがサーバに接続されている場合にのみ表示されます。 テクニカル サポート データは、リモート サーバまたはサーバに接続された USB ストレージ デバイスにエクスポートできます。次のいずれかを選択できます。 • [リモート（Remote）]：次のいずれかのプロトコルを使用して、リモート サーバにテクニカル サポート データをエクスポートできます。 • **TFTP** • **FTP** • **SFTP** • **SCP** • **[HTTP]** （注） このアクションを実行しながら、リモート サーバー 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?*」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼度に応じて、[Yes] または [No] 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。 • [Front Panel USB]：これにより、テクニカル サポート データをサーバーに接続された USB ストレージ デバイスにエクスポートできます。
[サーバ IP/ホスト名（Server IP/Hostname）] フィールド	サポート データ ファイルの保存先とするサーバの IP アドレスまたはホスト名。[テクニカル サポート データのエクスポート先（Export Technical Support Data to）] ドロップダウン リストの設定に応じて、フィールドの名前は異なります。

名前	説明
[Path and Filename] フィールド	ファイルをリモート サーバーにエクスポートするときに、Cisco IMC が使用する必要のあるパスおよびファイル名。 （注） サーバーにサポート対象ネットワーク アダプタ カードのいずれかがある場合、データ ファイルにはアダプタ カードからのテクニカル サポート データも含まれています。
ユーザ名	システムがリモート サーバへのログインに使用する必要のあるユーザ名。プロトコルが TFTP または HTTP の場合、このフィールドは適用されません。
パスワード	リモート サーバのユーザ名のパスワード。プロトコルが TFTP または HTTP の場合、このフィールドは適用されません。

ステップ 5 [エクスポート（Export）] をクリックします。

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。

ローカル ファイルへのテクニカル サポート データのダウンロード

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

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Generate Technical Support Data for Local Download] をクリックします。

ステップ 4 **[Download Technical Support Data to Local File]** ダイアログボックスで、次のフィールドに入力します。

名前	説明
[Generate Technical Support Data] オプション ボタン	Cisco IMCダウンロードするテクニカル サポート データ ファイルがない場合、このオプション ボタンは無効にされます。 [Generate] をクリックして、データ ファイルを作成します。データ収集が完了したら、[Actions] 領域の [Download Technical Support Data to Local File] をクリックして、ファイルをダウンロードします。
[Regenerate Technical Support Data] オプション ボタン	Cisco IMCこのオプション ボタンは、ダウンロードするテクニカル サポート データ ファイルがある場合に表示されます。 既存のサポート データ ファイルを新しいものと置き換えるには、このオプションを選択し、[Regenerate] をクリックします。データ収集が完了したら、[Actions] 領域の [Download Technical Support Data to Local File] をクリックして、ファイルをダウンロードします。
[Download to local file] オプション ボタン	Cisco IMCこのオプション ボタンは、ダウンロードするテクニカル サポート データ ファイルがある場合に有効になります。 既存のファイルをダウンロードするには、このオプションを選択し、[Download] をクリックします。 （注） サポートされているネットワーク アダプタ カードがサーバに組み込まれている場合、そのアダプタ カードからの技術サポート データもデータ ファイルに取り込まれます。
[生成（Generate）] ボタン	テクニカル サポート データ ファイルを生成できます。
[Download] ボタン	生成されたテクニカル サポート データ ファイルをダウンロードできます。

ステップ 5 **[Generate]** をクリックして、データ ファイルを作成します。データ収集が完了したら、**[アクション（Actions）]** 領域の **[テクニカル サポート データのローカル ファイルへのダウンロード（Download Technical Support Data to Local File）]**をクリックして、ファイルをダウンロードします。

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。

出荷時の初期状態へのリセット

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やサーバーのトラブルシューティング時など、稀なケースで、サーバーコンポーネントの出荷時デフォルトへのリセットが必要になることがあります。これを行うと、ユーザ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。サーバー コンポーネント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。この移行中、一部のインベントリ情報が使用できない場合があります。

BMC を工場出荷時の設定にリセットすると、シリアル番号が Cisco IMCXXXXXX 形式で表示されます。XXXXXX はサーバーのシリアル番号です。

重要 **VIC アダプタを他の世代の C シリーズ サーバー（たとえば M4）から M5 世代の C シリーズ サーバーまたは M5 サーバーから他の世代のサーバーに移動する際は、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

サーバー コンポーネントを出荷時デフォルトにリセットするには、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

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Reset to Factory Default] をクリックします。

ステップ 4 [工場出荷時のデフォルトへのリセット（Reset to Factory Default）] ダイアログボックスで、次の情報を確認します。

Actions	説明
[次の設定を工場出荷時のデフォルトにリセット（Reset to factory Default Setting of）] ドロップダウン リスト	工場出荷時の設定にリセットするシャーシまたはBMC を選択できます。次のいずれかになります。 • **シャーシ** • **BMC1** • **BMC2**

名前	説明
[すべて（All）] チェックボックス	オンにすると、サーバのすべてのコンポーネントを工場出荷時の設定にリセットします。 展開することで、工場出荷時の設定にリセットする特定のコンポーネントを選択できます。
[BMC] チェックボックス	オンにすると、BMCを工場出荷時の設定にリセットします。 （注） BMC を工場出荷時の設定にリセットすると、シリアル番号がCisco IMCXXXXXX形式で表示されます。XXXXXXはサーバーのシリアル番号です。BMC NIC モードの工場出荷時のデフォルトの後に**共有LOMの拡張**がデフォルトで設定されます。
[Storage] チェックボックス	オンにすると、使用可能なすべてのストレージ アダプタが工場出荷時の設定にリセットされます。ストレージ アダプタをリセットすると、ディスク上のデータは変更されませんが、仮想ドライブのメタ データは消去され、データ損失が発生することがあります。展開して工場出荷時の設定にリセットする特定のストレージ アダプタを選択します。 （注） 工場出荷時のデフォルトにストレージアダプタをリセットするには、ホストの電源をオンにする必要があります。
[VIC] チェックボックス	オンにすると、使用可能なすべての VIC を工場出荷時の設定にリセットします。 展開することで、工場出荷時の設定にリセットする特定のVICを選択できます。 （注） 工場出荷時のデフォルトにVICをリセットするには、ホストの電源をオンにする必要があります。
[Reset] ボタン	選択したコンポーネントを工場出荷時の設定にリセットします。

ステップ 5 [Reset] をクリックして、選択したコンポーネントを工場出荷時の設定にリセットします。

ホストがBIOS POST（電源投入時自己診断テスト）を実行しているとき、またはEFIシェル内にあるときにCisco IMC を再起動すると、ホストの電源が短時間オフになります。準備ができると、Cisco IMC の電源はオンになります。再起動時に、ネットワーク設定モードは **[Cisco カード (Cisco Card)]**モードにデフォルトで設定されます。

Cisco IMC 設定のエクスポートとインポート

Cisco IMC 設定のエクスポートとインポート

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） 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 サーバの IP アドレスを取得します。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Export Configuration] をクリックします。

ステップ 4 **[設定のエクスポート（Export Configuration）]** ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[エクスポートするコンポーネントの選択（Select Component for Export）] ドロップダウンリスト	コンポーネントのタイプ。次のいずれかになります。 • **[BMC]** • **VIC アダプタ** 選択したコンポーネントに応じて、そのコンポーネントの設定がエクスポートされます。

名前	説明
[エクスポート先（Export to）] ドロップダウン リスト	XML 設定ファイルを保存する場所。次のいずれかになります。 • [ローカル（Local）]：Cisco IMC GUI を実行しているコンピュータのローカル ドライブに XML 設定ファイルを保存するには、このオプションを選択して [エクスポート（Export）] をクリックします。 このオプションを選択すると、Cisco IMC GUI に [ファイルのダウンロード（File Download）] ダイアログボックスが表示され、設定ファイルを保存する場所に移動できます。 • [Remote Server]：XML 設定ファイルをリモート サーバーからインポートするには、このオプションを選択します。 このオプションを選択すると、Cisco IMC GUI にリモート サーバーのフィールドが表示されます。 • [Front Panel USB]：サーバーに接続された USB ストレージ デバイスに設定ファイルをエクスポートするには、このオプションを選択します。 （注） • Cisco IMC の設定をエクスポートするための [前面パネル USB（Front Panel USB）] オプションは、スマート アクセス USB が有効で、USB ストレージデバイスがサーバに接続されている場合にのみ使用できます。 • このオプションは、[コンポーネントの選択（Select Component）] ドロップダウン リストで [BMC] を選択した場合にのみ使用できます。

名前	説明
[エクスポート先（Export to）] ドロップダウン リスト	リモート サーバーのタイプ。次のいずれかになります。 • **[TFTP サーバー（TFTP Server）]** • **FTP サーバー（FTP Server）** • **SFTP サーバー（SFTP Server）** • **SCP サーバー（SCP Server）** • **HTTP サーバー（HTTP Server）** （注） このアクションを実行中にリモート サーバのタイプとして SCP または SFTP を選択した場合、ポップアップ ウィンドウが表示され、そこに *[サーバ（RSA）鍵フィンガープリントは <server_finger_print _ID> です。続行しますか?（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度に応じて、[Yes] または [No] 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。
[サーバーIP/ホスト名（Server IP/Hostname）] フィールド	設定ファイルのエクスポート先となるサーバーの IPv4 または IPv6 アドレス、またはホスト名。[エクスポート先（Export to）] ドロップダウン リストで選択したリモート サーバのタイプに応じて、フィールドの名前は異なる場合があります。
[Path and Filename] フィールド	ファイルをリモート サーバーにエクスポートするときに、Cisco IMC が使用する必要のあるパスおよびファイル名。
ユーザ名	システムがリモート サーバへのログインに使用する必要のあるユーザ名。プロトコルが TFTP または HTTP の場合、このフィールドは適用されません。
パスワード	リモート サーバのユーザ名のパスワード。プロトコルが TFTP または HTTP の場合、このフィールドは適用されません。
[Passphrase]	エクスポートした設定ファイル内の LDAP および SNMP v3 ユーザ パスワードを、AES256 アルゴリズムを使用して暗号するためのパスフレーズ。6 ～ 127 文字の文字列を入力します。次の文字は入力しないでください：! # $ & < > ? ; ' | ` ~ \ % ^ ( ) "

ステップ 5 [エクスポート（Export）] をクリックします。

Cisco IMC 設定のインポート

始める前に

コンフィギュレーション ファイルのインポート時に SNMP 設定情報を復元する場合は、インポートを行う前にこのサーバで SNMP がディセーブルになっていることを確認します。インポートを実行するときに SNMP がイネーブルになっている場合、Cisco IMC では設定ファイルに保存されている値によって現在の値は上書きされません。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Import Configuration] をクリックします。

ステップ 4 **[設定のインポート（Import Configuration）]** ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[インポートするコンポーネントの選択（Select Component for Import）] ドロップダウン リスト	コンポーネントのタイプ。次のいずれかになります。 • **[BMC]** • **VIC アダプタ** 選択したコンポーネントに応じて、そのコンポーネントの設定がインポートされます。

名前	説明
[インポート元（Import From）] ドロップダウン リスト	XML 設定ファイルの場所。次のいずれかになります。 • [ローカル（Local）]：Cisco IMC GUI を実行しているコンピュータのローカル ドライブに XML 設定ファイルをインポートするには、このオプションを選択します。 このオプションを選択すると、Cisco IMC GUI に [参照（Browse）] ボタンが表示され、インポートするファイルに移動できます。 • [Remote Server]：XML 設定ファイルをリモート サーバーからインポートするには、このオプションを選択します。 このオプションを選択すると、Cisco IMC GUI にリモート サーバーのフィールドが表示されます。 • [Front Panel USB]：サーバーに接続された USB ストレージ デバイスから設定ファイルをインポートするには、このオプションを選択します。 （注） • Cisco IMC の設定をインポートするための [前面パネル USB（Front Panel USB）] オプションは、スマート アクセス USB が有効で、USB ストレージデバイスがサーバに接続されている場合にのみ使用できます。 • このオプションは、[コンポーネントの選択（Select Component）] ドロップダウン リストで [BMC] を選択した場合にのみ使用できます。

名前	説明
[インポート元（Import From）] ドロップダウン リスト	（注） これらのオプションは、[リモート（Remote）] を選択した場合にのみ使用できます。 リモート サーバーのタイプ。次のいずれかになります。 • **[TFTP サーバー（TFTP Server）]** • **FTP サーバー（FTP Server）** • **SFTP サーバー（SFTP Server）** • **SCP サーバー（SCP Server）** • **HTTP サーバー（HTTP Server）** （注） このアクションを実行中にリモートサーバのタイプとして SCP または SFTP を選択した場合、ポップアップ ウィンドウが表示され、そこに *[サーバ（RSA）鍵フィンガープリントは <server_finger_print _ID> です。続行しますか?（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度に応じて、[Yes] または [No] 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。
[サーバーIP/ホスト名（Server IP/Hostname）] フィールド	設定ファイルを保存するサーバーの IPv4 または IPv6 アドレス、またはホスト名。[インポート元（Import From）] ドロップダウン リストで選択したリモート サーバのタイプに応じて、フィールドの名前は異なる場合があります。
[Path and Filename] フィールド	リモート サーバ上の構成ファイルのパスとファイル名。
ユーザ名	システムがリモート サーバへのログインに使用する必要のあるユーザ名。プロトコルが TFTP または HTTP の場合、このフィールドは適用されません。
パスワード	リモートサーバのユーザ名のパスワード。プロトコルが TFTP または HTTP の場合、このフィールドは適用されません。

名前	説明
[Passphrase]	インポートした設定ファイル内の LDAP および SNMP v3 ユーザ パスワードを AES256 アルゴリズムを使用して暗号化するためのパスフレーズ。6 ～ 127 文字の文字列を入力します。次の文字は入力しないでください：! # $ & < > ? ; ' | ` ~ \ % ^ ( ) " （注） 設定ファイルの暗号化されたセクションを編集しそれをインポートしようとすると、編集内容は無視され、インポート操作画面には部分的な成功メッセージが表示されます。

ステップ 5 [Import] をクリックします。

ホストへのマスク不可能な割り込みの生成

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。

サーバー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。

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。
- サーバの電源が投入されている。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Generate NMI to Host] をクリックします。

ステップ 4 **[ホストへの NMI の生成（Generate NMI to Host）]** ダイアログボックスで、次の情報を確認します。

Actions	説明
[Generate NMI to] ドロップダウン リスト	マスク不能割り込み（NMI）を生成するサーバーを選択できます。次のいずれかになります。 • **[サーバー 1（Server 1）]** • **[サーバー 2（Server 2）]**

ステップ 5 **[送信]**をクリックします。

このアクションは、OS を再起動する可能性のあるホストに NMI 信号を送信します。

Cisco IMC バナーの追加または更新

著作権やカスタマイズしたメッセージなどの重要な情報を入力して、Cisco IMC バナーを追加または更新できます。次の手順を実行します。

始める前に

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Add/Update Cisco IMC Banner] をクリックします。

ステップ 4 **[Cisco IMC バナーの追加/更新（Add/Update Cisco IMC Banner）]**ダイアログボックスで、次のフィールドに入力します。

名前	説明
[Banner (80 Chars per line. Max 2K Chars.)] フィールド	Web UI またはコマンドライン インターフェイスにログインする前に、ログイン画面に表示する著作権情報またはメッセージを入力します。
[SSH の再起動（Restart SSH）] チェックボックス	オンにすると、[Save Banner] ボタンをクリックした後にアクティブな SSH セッションが終了します。

ステップ 5 **[バナーの保存（Save Banner）]**をクリックします。

次のタスク

Cisco IMC の最後のリセット理由の表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。
ステップ 2 [管理（Admin）] メニューで [ユーティリティ（Utilities）] をクリックします。
ステップ 3 [Utilities] ペインの [Actions] 領域で、[Last Reset Reason] 領域の下にある次の情報を確認します。

名前	説明
[コンポーネント（Component）] フィールド	最後にリセットされたコンポーネント。
[Status] フィールド	コンポーネントが前回リセットされた理由。次のいずれかになります。 • **watchdog-reset** — カーネル パニックまたはハング タスクが原因でウォッチドッグ タイマーが期限切れになりました。 • [ac-cycle]：PSU 電源ケーブルが取り外されています（電源入力なし）。 • [graceful-reboot]：Cisco IMC のリブートが実行されます。 • **OOM-reset** — メモリがフル キャパシティに達すると（ウォッチドッグ タイマーなしで）Cisco IMC がリブートします。

ローカル ファイルへのハードウェア インベントリのダウンロード

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。
ステップ 2 [管理（Admin）] メニューで [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Generate Inventory Data] をクリックします。

ステップ 4 **[インベントリ データの生成（Generate Inventory Data）]**ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Generate Inventory Data] オプション ボタン	Cisco IMCこのオプション ボタンは、ダウンロードするハードウェア インベントリ データ ファイルがない場合に表示されます。
[Download to local file] オプション ボタン	Cisco IMCこのオプション ボタンは、ダウンロードするインベントリ データ ファイルがある場合に有効になります。 既存のファイルをダウンロードするには、このオプションを選択し、[Download] をクリックします。

ステップ 5 [Generate] をクリックして、データ ファイルを作成します。データ収集が完了したら、[Download Inventory Data to Local File] オプション ボタンを選択して [Download] をクリックし、ファイルをローカルにダウンロードします。

リモート サーバへのハードウェア インベントリ データのエクスポート

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Export Hardware Inventory Data to Remote] をクリックします。

ステップ 4 **[ハードウェア インベントリ データのエクスポート（Export Hardware Inventory Data）]**ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[ハードウェア インベントリ データのエクスポート先（Export Hardware Inventory Data to）] ドロップダウン リスト	リモート サーバのタイプ。次のいずれかになります。 • **[TFTP サーバー（TFTP Server）]** • **FTP サーバー（FTP Server）** • **SFTP サーバー（SFTP Server）** • **SCP サーバー（SCP Server）** • **HTTP サーバー（HTTP Server）** （注） このアクションを実行中にリモート サーバのタイプとして SCP または SFTP を選択した場合、ポップアップ ウィンドウが表示され、そこに *[サーバ（RSA）鍵フィンガープリントは <server_finger_print _ID> です。続行しますか?（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度に応じて、[Yes] または [No] 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。
[サーバーIP/ホスト名（Server IP/Hostname）] フィールド	データ ファイルを保存する必要のあるサーバーの IP アドレスまたはホスト名。[ハードウェア インベントリ データのエクスポート先（Export Hardware Inventory Data to）] ドロップダウン リストの設定に応じて、フィールドの名前は異なります。
[Path and Filename] フィールド	ファイルをリモート サーバーにエクスポートするときに、Cisco IMC が使用する必要のあるパスおよびファイル名。
ユーザ名	システムがリモート サーバへのログインに使用する必要のあるユーザ名。プロトコルが TFTP または HTTP の場合、このフィールドは適用されません。
パスワード	リモート サーバのユーザ名のパスワード。プロトコルが TFTP または HTTP の場合、このフィールドは適用されません。

ステップ 5 [エクスポート（Export）] をクリックします。

PID カタログのアップロード

始める前に

PID カタログ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。

手順

ステップ 1 **[Navigation]**ペインの **[Admin]**タブをクリックします。

ステップ 2 **[Admin]**タブの**[Utilities]** をクリックします。

ステップ 3 作業ペインで**[PID カタログのアップロード（Upload PID Catalog）]**リンクをクリックします。

[PID カタログのアップロード（Upload PID Catalog）] ダイアログボックスが表示されます。

カタログ ファイルの場所に応じて、いずれかのオプションを選択します。

ステップ 4 **[カタログのアップロード元：ローカル ファイル（Upload PID Catalog from Local File）]** ダイアログボックスで**[参照（Browse）]**をクリックし、**[アップロードするファイルの選択（Choose File to Upload）]**ダイアログボックスでアップロードするカタログ ファイルを選択します。

名前	説明
[File] フィールド	アップロードする PID カタログ ファイル。
[Browse] ボタン	ダイアログボックスが表示され、そこで、該当するファイルにナビゲートすることができます。

ステップ 5 **[カタログのアップロード元：リモート サーバ（Upload PID Catalog from Remote Server）]**ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[PID カタログのアップロード元：リモート サーバ（Upload PID Catalog from Remote Server）]ドロップダウン リスト	リモート サーバーのタイプ。次のいずれかになります。 • **TFTP** • **FTP** • **SFTP** • **SCP** • **[HTTP]**

名前	説明
[サーバーIP/ホスト名（Server IP/Hostname）] フィールド	PID カタログ情報を有効にするサーバーの IP アドレスまたはホスト名。[Upload PID Catalog from Remote Server] ドロップダウン リストの設定によって、フィールド名は異なる場合があります。
[パスおよびファイル名（Path and Filename）] フィールド	リモート サーバー上のカタログ ファイルのパスおよびファイル名。
[ユーザ名（Username）] フィールド	リモート サーバのユーザ名。
[パスワード（Password）]フィールド	リモート サーバのパスワード。
[アップロード（Upload）] ボタン	選択したPIDカタログをアップロードします。 （注） このアクションを実行中にリモート サーバのタイプとして SCP または SFTP を選択した場合、ポップアップ ウィンドウが表示され、そこに *[サーバ（RSA）鍵フィンガープリントは <server_finger_print _ID> です。続行しますか?（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度に応じて、[Yes] または [No] 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をベースにしており、接続先ホストの特定や確認に利用できます。
[Cancel]ボタン	サーバに保管されているファームウェア バージョンには変更を加えることなく、ウィザードを閉じます。

PID カタログの有効化

⚠

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

PIDカタログを有効にするには、admin権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 **[Admin]** タブの**[Utilities]** をクリックします。

ステップ 3 **作業**ペインで **[PID カタログの有効化（Activate PID Catalog）]** タブをクリックします。

[PID カタログの有効化（Activate PID Catalog）] ダイアログボックスが表示されます。次のフィールドに入力します。

名前	説明
[アクティブ化（Activate）] ボタン	PID カタログをアクティベートできます。

（注） 初めてシステムにログオンする場合は、**[PID カタログの有効化（Activate PID Catalog）]**リンクが灰色で表示されます。PID カタログをサーバにアップロードすると、このリンクが有効になります。PIDファイルをアップロードした後もリンクは引き続きアクティブであり、PID を複数回アクティブにできます。

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

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 **[管理 (Admin)]** タブの **[ユーティリティ (Utilities)]** をクリックします。

ステップ 3 [ユーティリティ (Utilities)] ペインの **[アクション (Actions)]** 領域で、**[PID カタログの削除 (Delete PID Catalog)]**] をクリックし、**[OK]** をクリックして確定します。

（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。

スマート アクセス USB の有効化

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 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [アクション（Actions）] 領域で [スマートアクセスUSBの有効化（Enable Smart Access USB）] をクリックします。

これはトグル ボタンです。スマート アクセスを無効にするには、[スマートアクセスUSBの無効化（Disable Smart Access USB）] をクリックします。スマート アクセス USB を有効にした後にのみ、このボタンが表示されます。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 Cisco IMC から切断してホスト オペレーティング システムに接続します。

Cisco Intersight 管理の有効化/無効化

Intersight 管理を有効にすると、Intersight クラウド アプリケーションと M5 サーバー間の双方向通信が確立されます。

（注） ポート番号 8888-8889 は、Intersight 通信を行うために予約されています。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [デバイスコネクタ（Device Connector）] をクリックします。

ステップ 3 **[Intersight Management]** 領域で **[On]** をクリックして Intersight 管理を有効にします。
[Connection] 領域に Intersight 管理の接続状態が表示されます。デバイス コネクタの Intersight 管理への接続が確立できていない場合は、[詳細と推奨事項（Details & Recommendations）] ドロップダウン リストに表示される推奨事項を確認し、接続の問題を修正します。

ステップ 4 [アクセス モード（Access Mode）] で [読み取り専用（Read-only）] または [制御を許可（Allow Control）] を選択します。
[読み取り専用（Read-only）] アクセス モードを選択すると、Intersight を使用してデバイスを構成できなくなります。したがって、クラウドからデバイス コネクタに送信される構成は、エラー コードを伴って拒否されます。[制御を許可（Allow Control）] モードを選択すると、Intersight を使用してデバイスの構成を完全に制御できます。

ステップ 5 Intersight 管理を無効にするには、[オフ（Off）] をクリックします。
Intersight 管理を無効にすると、[接続（Connection）] 領域に接続状態が [管理上無効（Administratively Disabled）] として表示されます。

デバイス コネクタの HTTPS プロキシ設定の設定

サーバーの HTTPS プロキシ設定を手動で構成できます。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [デバイスコネクタ（Device Connector）] をクリックします。

ステップ 3 [接続（Connections）] エリアで、[HTTPSプロキシ設定（HTTPS Proxy Settings）] をクリックしてプロキシ設定を入力します。

アクション名	説明
[オフ（Off）] ボタン	HTTPS プロキシ設定を無効にします。
[手動（Manual）] ボタン	HTTPS プロキシ設定を手動で構成できます。
[プロキシホスト名/IP（Proxy Hostname/IP）] フィールド	プロキシ サーバーの IP アドレスまたはホスト名。
[プロキシポート（Proxy Port）] フィールド	プロキシ サーバーのポート番号。
[認証（Authentication）] トグル ボタン	このオプションを有効にすると、プロキシサーバーのクレデンシャルを提供できます。
[ユーザー名（Username）] フィールド	プロキシ サーバーのクレデンシャルです。
[パスワード（Password）] フィールド	

ステップ 4 [HTTPSプロキシ設定（HTTPS Proxy Settings）] ダイアログ ボックスで、情報を追加してから [保存（Save）] をクリックします。

Intersight デバイス コネクタのプロパティの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [デバイスコネクタ（Device Connector）] をクリックします。

ステップ 3 [Intersight管理（Intersight Management）] 領域で、次の情報を確認します。

アクション名	説明
[Enabled] オプション ボタン	Intersightの管理を有効または無効にできます。次のいずれかになります。 • [オン（On）]：Intersight の管理を有効にします。このシステムを請求してCisco Intersight の機能を活用できます。 • [オフ（Off）]：Intersight の管理を無効にします。Cisco Intersightへの通信は許可されません。

ステップ 4 [接続（Connection）] 領域で、次の情報を確認します。

名前	説明
[Status] フィールド	Intersight への接続の状態を表示します。次のいずれかになります。 • [管理上無効（Administratively Disabled）]：Intersight の管理が無効にされていることを示します。 • [DNS誤設定（DNS Misconfigured）]：BMC で DNS の詳細が設定されていないことを示します。 • [UCS接続ネットワークエラー（UCS Connect Network Error）]：無効なネットワーク構成を示します。 • **[Certificate Error]**—無効な証明書を示します。 • [要求あり（Claimed）]：Intersight でデバイスが要求されていることを示します。 • [要求なし（Not Claimed）]：デバイスが Intersight に登録されているが要求されてはいないことを示します。
[接続再試行（Retry Connection）] リンク	Intersight への接続を再試行できます。このオプションは、Intersight の接続に問題がある場合にのみ表示されます。
[詳細と推奨事項（Details & Recommendations）] ドロップダウン リスト	状態に基づいて接続の問題を修正するための詳細と推奨事項を表示します。

名前	説明
[HTTPSプロキシ設定（HTTPS Proxy Settings）] ダイアログ ボックス	Intersight 接続に必要な HTTPS プロキシ設定を手動で構成できます。
[シリアル番号（Serial Number）] フィールド	BMC のシリアル番号を表示します。
[セキュリティトークン（Security Token）] フィールド	接続ステータスが [要求なし（Not Claimed）] の場合に表示されます。Intersight にサーバーを安全に搭載するにはセキュリティ トークンを使用します。

ステップ 5 [接続（Connections）] エリアで、[HTTPSプロキシ設定（HTTPS Proxy Settings）] をクリックして次の情報を確認します。

アクション名	説明
[オフ（Off）] ボタン	HTTPS プロキシ設定を無効にします。
[手動（Manual）] ボタン	HTTPS プロキシ設定を手動で構成できます。
[プロキシホスト名/IP（Proxy Hostname/IP）] フィールド	プロキシ サーバーの IP アドレスまたはホスト名。
[プロキシポート（Proxy Port）] フィールド	プロキシ サーバーのポート番号。
[認証（Authentication）] トグル ボタン	このオプションを有効にすると、プロキシサーバーのクレデンシャルを提供できます。
[ユーザー名（Username）] フィールド	プロキシ サーバーのクレデンシャルです。
[パスワード（Password）] フィールド	

Intersight デバイス コネクタのプロパティの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理者（Admin）] タブをクリックします。
ステップ 2 [管理者（Admin）] タブの [デバイスコネクタ（Device Connector）] をクリックします。
ステップ 3 [Intersight管理（Intersight Management）] 領域で、次の情報を確認します。

アクション名	説明
[Enabled] オプション ボタン	Intersightの管理を有効または無効にできます。次のいずれかになります。 • [オン（On）]：Intersight の管理を有効にします。このシステムを請求してCisco Intersight の機能を活用できます。 • [オフ（Off）]：Intersight の管理を無効にします。Cisco Intersightへの通信は許可されません。

ステップ 4 [接続（Connection）] 領域で、次の情報を確認します。

名前	説明
[Status] フィールド	Intersight への接続の状態を表示します。次のいずれかになります。 • [管理上無効（Administratively Disabled）]：Intersight の管理が無効にされていることを示します。 • [DNS誤設定（DNS Misconfigured）]：BMC で DNS の詳細が設定されていないことを示します。 • [UCS接続ネットワークエラー（UCS Connect Network Error）]：無効なネットワーク構成を示します。 • [証明書検証エラー（Certification Validation Error）]：無効な証明書を示します。 • [要求あり（Claimed）]：Intersight でデバイスが要求されていることを示します。 • [要求なし（Not Claimed）]：デバイスが Intersight に登録されているが要求されてはいないことを示します。
アクセス モード	デフォルトでは、このモードは [制御を許可（Allow Control）] に設定されます。
[詳細と推奨事項（Details & Recommendations）] ドロップダウン リスト	状態に基づいて接続の問題を修正するための詳細と推奨事項を表示します。
デバイス ID	これはデバイスの ID を示します。

名前	説明
登録コード	これは Intersight からデバイスを要求するために必要なセキュリティ コードです。 （注） このコードは、[接続（Connection）] ステータスが [要求なし（Not Claimed）] のときにのみ使用できます。

ステップ 5 [Settings] 領域で、次の情報を確認します。

名前	説明
[General] タブ	**アクセス モード** • **[Read-only]**：**[Read-only]** アクセス モードを選択すると、Intersight を使用してデバイスを設定できなくなります。 • **[Allow Control]** — **[Allow Control]** モードを選択すると、Intersight を使用したデバイスの構成を完全に制御できます。 **[Intersightだけからの設定（Configuration from Intersight only）]** このオプションは、[制御を許可（Allow Control）] モードが有効になっている場合にのみ設定できます。[ロックアウトの設定（Configure Lockout）] オプションは次のとおりです。 **[OFF]**— デバイスを、ローカルでも Intersight からでも管理するには、オプション **[Configuration from Intersight only] をオフにします。**. この設定により、すべての既存のセッション（webUi、XML および CLI）が終了します。 **[ON:** — Intersight の Cisco IMC 設定をロックするには、オプション **[Configuration from Intersight only]** をオンにします。この設定により、すべての既存のセッション（webUi、XML および CLI）が終了します。 （注） 設定ロック アウト モードで admin としてログインしている場合、admin ロールはユーザー ロールにマッピングされるため、インターフェイスはユーザー ロールでログインしたユーザーとして動作します。
[Proxy Configuration] タブ	Intersight 接続に必要な HTTPS プロキシ設定を手動で構成できます。

名前	説明
[HTTPS プロキシ (HTTPS Proxy)] フィールド オプション ボタンを選択します	OFF - HTTPS プロキシ設定を無効にします。 ON - HTTPS プロキシ設定を有効にします。
[プロキシホスト名/IP（Proxy Hostname/IP）] フィールド	プロキシ サーバーの IP アドレスまたはホスト名。
[プロキシポート（Proxy Port）] フィールド	プロキシ サーバーのポート番号。
[認証（Authentication）] トグル ボタン	このオプションを有効にすると、プロキシサーバーのクレデンシャルを提供できます。 （注） デバイス コネクタには、ログイン クレデンシャルの形式は必須ではありません。これらは設定済みの HTTP プロキシ サーバーにそのまま渡されます。 ユーザー名をドメイン名で限定する必要があるかどうかは、HTTP プロキシ サーバーの構成によって異なります。
[Username] フィールド [Password] フィールド	プロキシ サーバーのクレデンシャルです。

名前	説明
[証明書マネージャ (Certificate Manager)] タブ	信頼できる証明書のリストを表示し、有効な信頼できる証明書をインポートできます。 • **[インポート (Import)]** - CA 署名付き証明書をインポートすることができます。 （注） インポートされた証明書が *.pem (base64 エンコード) 形式である必要があります。 • 次の情報と証明書のリストを表示することができます。 • **[名前 (Name)]**—CA 証明書の共通名。 • **[In Use]** - 信頼ストアで証明書を正常にリモート サーバの確認に使用されたかどうか。 • **[Issued By]**: 証明書の発行認証局。 • **[Expires]**—証明書の有効期限。 （注） バンドルされている証明書 (ロック アイコンが証明書) を削除することはできません。

PCIe スイッチの回復

始める前に

- 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。
- サーバーの電源が投入されている。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理（Admin）] メニューをクリックします。

ステップ 2 [管理（Admin）] メニューで [ユーティリティ（Utilities）] をクリックします。

ステップ 3 **[Utilities (ユーティリティ)]** ペインの **[Actions (アクション)]** 領域で、**[Recover PCIe Switch (PCIe スイッチの回復)]** をクリックします。

ステップ 4 **[Recover PCIe Switch (PCIe スイッチの回復)]** ダイアログ ボックスで、次の情報を確認します。

名前	説明
[Controller] ドロップダウン	サーバで使用可能なPCIeスイッチの一覧を示します。このリストから、[recover controller (コントローラの回復)] アクションを実行するスイッチを選択できます。
[Recover Controller (コントローラの回復)] ボタン	[Recover Controller (コントローラの回復)] ボタンをクリックすると、選択したコントローラのリカバリが開始されます。
[Cancel (キャンセル)] ボタン	アクションをキャンセルし、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。