サーバ ユーティリティ

この章の内容は、次のとおりです。

- テクニカル サポート データのエクスポート，1 ページ
- 出荷時の初期状態へのリセット，6 ページ
- Cisco IMC 設定のエクスポートとインポート，8 ページ
- ホストへのマスク不能割り込みの生成，15 ページ
- Cisco IMC バナーの追加または更新，16 ページ
- Cisco IMC の最後のリセット理由の表示，17 ページ
- 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，18 ページ
- 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，19 ページ
- PID カタログのアップロード，20 ページ
- PID カタログの有効化，22 ページ
- スマート アクセス USB の有効化，23 ページ
- Starship 管理の有効化と無効化，24 ページ
- デバイス コネクタの HTTPS プロキシ設定の設定，24 ページ
- Starship デバイス コネクタのプロパティの表示，25 ページ

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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [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、[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 [テクニカル サポート データのエクスポート（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（Name）]	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 through）] ドロップダウン リスト	（注） [前面パネルの USB（Front Panel USB）] オプションは、[スマート アクセス USB（Smart Access USB）] が有効になっており、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 データをリモート サーバ、またはサーバに接続している 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 タイプとして SCP または SFTP を選択した場合、「サーバ（*RSA*）キー 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性に応じて、[はい（Yes）] または [いいえ（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。 • [前面パネルの USB（Front Panel USB）]：サーバに接続している USB ストレージ デバイスにテクニカル サポート データを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 ファイルを保存する必要のあるサーバの 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 リストの設定によって、フィールド名は異なる場合があります。

[名前（Name）]	説明
[パスおよびファイル名（Path and Filename）] フィールド	ファイルをリモート サーバにエクスポートするときに、Cisco IMC で使用するパスおよびファイル名。 （注） サーバ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（Username）]	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。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。
[パスワード（Password）]	リモート サーバのユーザ名のパスワード。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 5 [エクスポート（Export）] をクリックします。

次の作業

生成されたレポート ファイルを Cisco TAC に提供します。

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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [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、[ローカル ダウンロード用のテクニカル サポート データの作成（Generate Technical Support Data for Local Download）] をクリックします。

ステップ 4 [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（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（Name）]	説明
[テクニカル サポート データの作成（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 ボタンは無効化されます。 [生成（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 [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（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。
[テクニカル サポート データの再作成（Regenerate Technical Support Data）] オプション ボタン	Cisco IMC テクニカル サポート データ ファイルがダウンロード可能な場合、このオプション ボタンが表示されます。 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、[再作成（Regenerate）] をクリックします。データ収集が完了したら、[アクション（Actions）] 領域の [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（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。
[ローカル ファイルへダウンロード（Download to local file）] オプション ボタン	Cisco IMC テクニカル サポート データ ファイルがダウンロード可能な場合、このオプション ボタンが有効になります。 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、[ダウンロード（Download）] をクリックします。 （注） サーバ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。
[作成およびダウンロード（Generate and Download）] ボタン	テクニカル サポート データ ファイルを作成してダウンロードできます。
[生成（Generate）] ボタン	テクニカル サポート データ ファイルを作成できます。
[ダウンロード（Download）] ボタン	テクニカル サポート データ ファイルを作成後にダウンロードできます。

ステップ 5 [生成（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 [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（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。

次の作業

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

非常に稀なケースですが、現在稼動しているファームウェアで問題が発生した場合やサーバのトラブルシューティング時などに、サーバ 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。サーバ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、ネットワーク設定の再指定が必要になる場合もあります。この移行中、一部のインベントリ情報が使用できないことがあります。

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（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。

はじめる前に

サーバ 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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [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、[工場出荷時のデフォルトにリセット（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にリセット（Reset to Factory Default）] ダイアログボックスで、次の情報を確認します。

名称	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が工場出荷時の設定にリセットされます。 展開して、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します。

名称	説明
[BMC] チェックボックス	オンにすると、BMC が工場出荷時の設定にリセットされます。 （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 はサーバのシリアル番号です。また、リセット時には、デフォルトで Cisco Card モードが設定されます。
[ストレージ（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） ストレージ アダプタを工場出荷時の設定にリセットするには、ホストの電源がオンになっている必要があります。
[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 が工場出荷時の設定にリセットされます。 展開して、工場出荷時の設定にリセットする特定の VIC を選択します。 （注） VIC を工場出荷時の設定にリセットするには、ホストの電源がオンになっている必要があります。
[リセット（Reset）] ボタン	選択したコンポーネントが工場出荷時の設定にリセットされます。

ステップ 5 [リセット（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デフォルトで [シスコ カード（Cisco Card）] モードに設定されます。

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（Network settings）
- 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。

- コミュニケーション 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
- ダイナミック ストレージの設定
- シャーシの説明

Cisco IMC 設定のエクスポート

（注） セキュリティ上の理由から、この操作ではユーザ アカウントやサーバ証明書はエクスポートされません。

はじめる前に

バックアップ リモート サーバの IP アドレスを取得します。

手順

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

ステップ 2 [管理者（Admin）] メニューの [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、[エクスポート設定（Export Configuration）] をクリックします。

ステップ 4 [エクスポート設定（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。

名称	説明
[エクスポート用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 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。

名称	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。 • [リモート サーバ（Remote Server）]：XML 設定ファイルをリモート サーバ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 サーバのフィールドが表示されます。 • [前面パネルの USB（Front Panel USB）]：サーバに接続してい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 [前面パネルの USB（Front Panel USB）] オプションは、[スマート アクセス USB（Smart Access USB）] が有効になっており、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。

名称	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 サーバのタイプ。次のいずれかになります。 • TFTP サーバ（TFTP Server） • FTP サーバ（FTP Server） • SFTP サーバ（SFTP Server） • SCP サーバ • HTTP サーバ（HTTP Server） （注） 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、「サーバ（*RSA*）キー 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性に応じて、[はい（Yes）] または [いいえ（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 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の IPv4 アドレスか 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、フィールド名が異なることがあります。
[パスおよびファイル名（Path and Filename）] フィールド	ファイルをリモート サーバにエクスポートするときに、Cisco IMC で使用するパスおよびファイル名。
[ユーザ名（Username）]	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。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。
[パスワード（Password）]	リモート サーバのユーザ名のパスワード。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。
[パスフレーズ（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 パスワードの暗号化に AES256 アルゴリズムを使用するパスフレーズ。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

はじめる前に

設定ファイルをインポートするときに SNMP 設定情報を復元する必要がある場合は、インポートを実行する前に、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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [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、[インポート設定（Import Configuration）] をクリックします。

ステップ 4 [インポート設定（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。

名称	説明
[インポート用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 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。

名称	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。 • [リモート サーバ（Remote Server）]：XML 設定ファイルをリモート サーバ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 サーバのフィールドが表示されます。 • [前面パネルの USB（Front Panel USB）]：サーバに接続してい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 [前面パネルの USB（Front Panel USB）] オプションは、[スマート アクセス USB（Smart Access USB）] が有効になっており、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。

名称	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 サーバのタイプ。次のいずれかになります。 • TFTP サーバ（TFTP Server） • FTP サーバ（FTP Server） • SFTP サーバ（SFTP Server） • SCP サーバ • HTTP サーバ（HTTP Server） （注） 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、「サーバ（*RSA*）キー 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性に応じて、[はい（Yes）] または [いいえ（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 IP/ホスト名（Server IP/Hostname）] フィールド	設定ファイルが存在するサーバの IPv4 アドレスか 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、フィールド名が異なることがあります。
[パスおよびファイル名（Path and Filename）] フィールド	リモート サーバ上の設定ファイルのパスおよびファイル名。
[ユーザ名（Username）]	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。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。
[パスワード（Password）]	リモートサーバのユーザ名のパスワード。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。

名称	説明
パスフレーズ（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 パスワードの暗号化に AES256 アルゴリズムを使用するパスフレーズ。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 [インポート（Import）] をクリックします。

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。

はじめる前に

- 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。
- サーバの電源をオンに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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [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、[NMI をホストに作成（Generate NMI to Host）] をクリックします。

ステップ 4 [NMI をホストに作成（Generate NMI to Host）] ダイアログボックスで、次の情報を確認します。

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

ステップ 5 [送信（Send）] 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

著作権表記やカスタマイズされ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。

はじめる前に

手順

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

ステップ 2 [管理者（Admin）] メニューの [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、[Cisco IMC バナーの追加/更新（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、次のフィールドに値を入力します。

[名前（Name）]	説明
[バナー（1 行あたり 80 文字。最大 2K 文字。）（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、[バナーの保存（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。

次の作業

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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [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、[最後のリセット理由（Last Reset Reason）] 領域の下にある次の情報を確認します。

[名前（Name）]	**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。
[ステータス（Status）] フィールド	コンポーネントが最後にリセットされた理由。次のいずれかになります。 • [ウォッチドッグによるリセット（watchdog-reset）]：Cisco IMC のメモリが容量一杯に到達した時点でウォッチドッグタイマーがリセットします。 • [ac サイクル（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）。 • [グレースフル リブート（graceful-reboot）]：Cisco IMC のリブートが実行されます。

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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [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、[インベントリ データの生成（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（Name）]	説明
[インベントリ データの生成（Generate Inventory Data）] オプション ボタン	Cisco IMC 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、このオプション ボタンが表示されます。
[ローカル ファイルへダウンロード（Download to local file）] オプション ボタン	Cisco IMC インベントリ データ ファイルがダウンロード可能な場合、このオプション ボタンが有効になります。 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、[ダウンロード（Download）] をクリックします。

ステップ 5 [生成（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、[ローカル ファイルへのインベントリ データのダウンロード（Download Inventory Data to Local File）] オプション ボタンを選択して [ダウンロード（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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [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、[リモートへのハードウェア インベントリ データのエクスポート（Export Hardware Inventory Data 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（Name）]	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（TFTP Server） • FTP サーバ（FTP Server） • SFTP サーバ（SFTP Server） • SCP サーバ • HTTP サーバ（HTTP Server） （注） 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、「サーバ（*RSA*）キー 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性に応じて、[はい（Yes）] または [いいえ（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 リストの設定によって、フィールド名は異なる場合があります。

[名前（Name）]	説明
[パスおよびファイル名（Path and Filename）] フィールド	ファイルをリモート サーバにエクスポートするときに、Cisco IMC で使用するパスおよびファイル名。
[ユーザ名（Username）]	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。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。
[パスワード（Password）]	リモート サーバのユーザ名のパスワード。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 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

はじめる前に

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 [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[ユーティリティ（Utilities）] をクリックします。

ステップ 3 [作業（Work）] 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 ファイルが保管されている場所に応じて、次のいずれかのオプションを選択します。

ステップ 4 [ローカル ファイルからの PID カタログのアップロード（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を選択（Choose File to Upload）] ダイアログボックスを使用してアップロードするカタログ ファイルを選択します。

[名前（Name）]	説明
[ファイル（File）] フィールド	アップロードする PID カタログ ファイル。
[参照（Browse）] ボタン	該当するファイルに移動するためのダイアログボックスが開きます。

ステップ 5 [リモート サーバからの PID カタログのアップロード（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（Name）]	説明
[リモート サーバからの PID カタログのアップロード（Upload PID Catalog from Remote Server）] 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 • FTP • SFTP • SCP • HTTP
[サーバ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の IP アドレスまたはホスト名。[PID カタログのアップロード元（Upload PID Catalog from）] 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。

[名前（Name）]	説明
[アップロード（Upload）] ボタン	選択した PID カタログがアップロードされます。 （注） 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、「サーバ（*RSA*）キー 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性に応じて、[はい（Yes）] または [いいえ（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。
[キャンセル（Cancel）] ボタン	サーバに保存されたファームウェア バージョンを変更せずにウィザードを終了します。

PID カタログの有効化

はじめる前に

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 [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[ユーティリティ（Utilities）] をクリックします。

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

[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（Name）]	説明
[アクティブ化（Activate）] ボタン	PID カタログをアクティブにできます。

（注） 初めてシステムにログインしている場合は、[PID カタログの有効化（Activate PID Catalog）] リンクは無効になっています。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はリンクが有効な状態で維持されるので、PID を何度でもアクティブにすることができます。

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。

はじめる前に

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

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）] メニューの [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。

Starship 管理の有効化と無効化

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

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 [Starship管理（Starship Management）] エリアで、[オン（On）] をクリックして Starship の管理を有効にします。
[接続（Connection）] エリアに Starship 管理の接続状態が表示されます。デバイス コネクタの Starship 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 Starship 管理を無効にするには、[オフ（Off）] をクリックします。
Starship 管理を無効にすると、[接続（Connection）] エリアに接続状態が [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、プロキシサーバのクレデンシャルを提供できます。
[ユーザ名（Username）] フィールド	プロキシ サーバ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。

Starship 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 [Starship管理（Starship Management）] 領域で、次の情報を確認します。

アクション名	説明
[状態（State）] オプション ボタン	Starship 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）]：Starship 管理を有効にします。 • [オフ（Off）]：Starship 管理を無効にします。

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

名称	説明
[ステータス（Status）] フィールド	Starship 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）]：Starship の管理が無効になっ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）]：Starship 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）]Starship でデバイスが登録されましたが、要求されていないことを示します。
[接続再試行（Retry Connection）] リンク	Starship への接続を再試行できます。このオプションは、Starship の接続に問題がある場合のみに表示されます。
[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。

名称	説明
[HTTPSプロキシ設定（HTTPS Proxy Settings）] ダイアログ ボックス	Starship 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。Starship にサーバ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、プロキシサーバのクレデンシャルを提供できます。
[ユーザ名（Username）] フィールド	プロキシ サーバのクレデンシャルです。
[パスワード（Password）] フィールド	