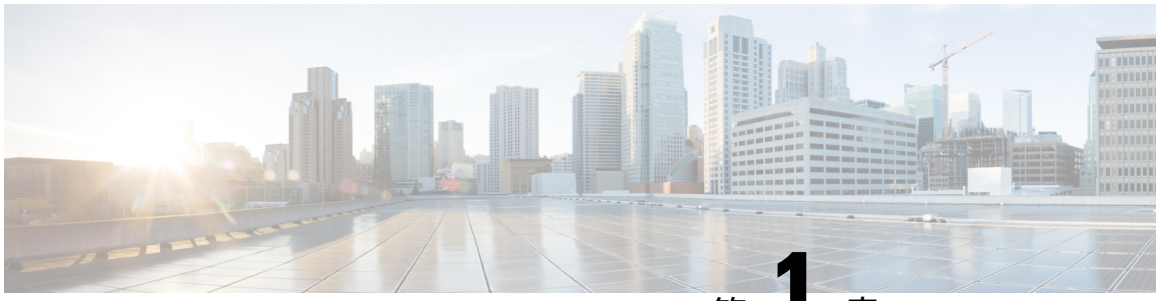
Cisco IMC Supervisor ラックマウント サーバ管理ガイド、リリース 2.2(0.3)

初版：2018 年 6 月 6 日

最終更新：2018 年 8 月 23 日

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

目 次



第 1 章

このリリースの新規情報および変更情報

この章の内容は、次のとおりです。

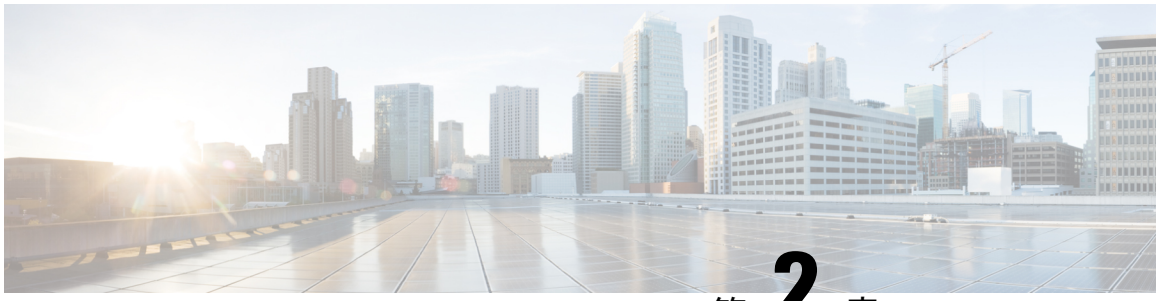
このリリースの新規情報および変更情報

次の表は、この最新リリースに関するマニュアルでの主な変更点の概要を示したものです。この表は、このマニュアルに加えられた変更やこのリリースの新しい機能をすべて網羅するものではありません。

表 *1 : Cisco IMC Supervisor* リリース *2.2(0.3)* の新機能と変更された動作

機能	説明	参照先
ホストイメージマッピングの機能拡張	ホストイメージマッピングは、E シリーズ サーバを対象としたよく利用される機能であり、Cisco IMC にファームウェア ファイルをダウンロードし、ファームウェアをアップグレードできます。 このリリースでは、次のいずれかのイメージをダウンロードおよびアップグレードする場合にホストイメージマッピング プロファイルを作成できます。 • ISO ファームウェア イメージ • CIMC イメージ • BIOS イメージ	ホストイメージマッピング （165 ページ） ネットワーク ホストイメージ マッピング プロファイルの追加 （166 ページ） ホストイメージマッピングのアップロード プロファイルの作成 （169 ページ） ホストのイメージ マッピングの Cisco.com プロファイルの作成 （172 ページ） ホストイメージプロファイルの適用 （176 ページ）

機能	説明	参照先
E シリーズ サーバの電力復元ポリシーの概要	このリリースで導入された電力復元ポリシーでは、E シリーズ サーバの Cisco IMC にログインせずに、そのサーバの電力復元ポリシーに設定されている値を変更できます。	電力復元ポリシー （127 ページ）
ファームウェアのアップグレード プロセスを開始する前にホスト システムをシャットダウンするためのタイムアウトの設定がサポートされています。	ファームウェア イメージをローカル サーバまたはネットワーク サーバからアップロードするときに、ホストがグレースフル シャットダウンする必要があるタイムアウト期間（分単位）を指定できるようになりました。 ファームウェア アップグレード プロセスの開始前にホスト システムを強制的にシャットダウンすることもできます。	ローカル サーバへのイメージの追加 （157 ページ） ネットワーク サーバからのイメージの追加 （161 ページ）
システム タスクのスケジューリング機能の強化。	このリリースでは、**固定遅延**オプションを使用してシステム タスクをスケジュールするオプションが導入されました。このオプションは、連続するシステム タスクの実行の間に、一定時間の間隔を設けることを意味します。 デフォルトでは、ほとんどのシステム タスクには [固定遅延（Fixed Delay）] オプションが設定されます。ただし、[固定レート（Fixed Rate）] オプションのみが設定されているタスクもいくつかあります。 また、このリリースでは、システム タスクにカスタムの頻度を設定する機能も導入されています。	システム タスクの管理 （100 ページ）



第 2 章

概要

この章は次のトピックで構成されています。

Cisco IMC Supervisor について

Cisco IMC Supervisor は、大規模なラック マウント サーバを管理できる管理システムです。ラック マウント サーバのグループを作成して、グループ単位でモニタリングや資産管理を行うことができます。

Cisco IMC Supervisorでは次のタスクも実行できます。

- サーバの論理的なグループ化とグループごとの要約の表示
- 管理対象サーバのインベントリの収集
- サーバとグループのモニタリング
- ファームウェアのダウンロード、アップグレードおよびアクティベーションを含むファームウェア管理
- サーバの検出、モニタ、管理とファームウェアアップグレードのプログラムによる実行のためのノースバウンド REST API の提供
- 電源制御、LED 制御、ログの収集、KVM の起動、CIMC UI の起動など、スタンドアロン サーバのアクションの管理

- ロールベース アクセス コントロール（RBAC）を使用したアクセスの制限
- 電子メール アラートの設定
- ポリシーおよびプロファイルを使用したサーバプロパティの設定
- ファームウェアのアップデートまたはサーバ検出などのタスクを延期するためのスケジュールの定義
- UCS サーバ設定ユーティリティを使用したサーバのハードウェア問題の診断
- Cisco Smart Call Home による、プロアクティブな診断、アラート、修復案の提供
- Cisco UCS S3260 高密度ストレージ ラック サーバの管理
- ネットワーク設定ポリシーよる DNS サーバおよびその他のネットワーク設定の設定
- ゾーン分割ポリシーによるサーバへの物理ドライブの割り当て
- さまざまな地理的ロケーションにわたる複数の診断イメージの設定
- 個々のサーバを 1 つのグループに含めるための電子メール ルールのカスタマイズ

ライセンスについて

Cisco IMC Supervisor では次の有効なライセンスが必要です。

- Cisco IMC Supervisor 基本ライセンス。
- Cisco IMC Supervisor 基本ライセンスの後にインストールする Cisco IMC Supervisor バルク エンドポイント イネーブルメント ライセンス。
- Cisco IMC Supervisor Advanced ライセンス。ポリシーやプロファイルの追加、編集、および削除は基本ライセンスで行えますが、サーバへのポリシーまたはプロファイルの適用には Advanced ライセンスが必要です。ポリシーを適用する際にこのライセンスがないとエラーが発生します。
- デフォルトの組み込み Cisco IMC Supervisor 評価ライセンス。評価ライセンスは、エンドユーザが Cisco IMC Supervisor をインストールし、すべてのサービスを初めて起動するときに自動的に生成されます。これは 50 台のサーバに適用可能です。

重要

- Cisco IMC Supervisor の評価ライセンスを使用している場合は、このライセンスの有効期限（ライセンスが生成されてから 90 日）が切れると、インベントリおよびシステム ヘルス情報（障害など）を取得できなくなることに注意してください。システムデータの更新だけでなく、新しいアカウントの追加もできなくなります。その時点で、Cisco IMC Supervisor のすべての機能を使用するには、永久ライセンスをインストールする必要があります。
- 評価時に追加したサーバの数が購入したサーバライセンスの数を超えると、インベントリ収集は評価時にすでに追加されているサーバについても行われますが、新しいサーバを追加することはできません。たとえば、評価時に約 100 台のサーバを追加し、購入しているライセンスが 25 サーバ ライセンスの場合は、評価ライセンスの期限が切れた後に、新しいサーバを追加できなくなります。また、Advanced ライセンスなしでは設定に関連する操作を実行できなくなります。
- サーバの検出およびインポートの際に、インポートされた数のサーバがライセンス使用制限を超えると、Cisco IMC Supervisor は、制限を超えない範囲内でのみサーバをインポートし、追加のサーバではエラー メッセージを表示します。
- Cisco IMC Supervisor のライセンスはサーバの数に基づきます。Cisco UCS S3260 シャーシは 2 サーバ ノードです。このため Cisco IMC Supervisor では、このシャーシのライセンス使用数が 2 サーバとして見なされます。

ライセンスの取得およびインストールのプロセスは同じです。ライセンスを取得するには、次の手順を実行します。

1. Cisco IMC Supervisor をインストールする前に、Cisco IMC Supervisor ライセンス キーを生成し、証明書（製品アクセス キー）を要求します。
2. シスコのソフトウェア ライセンス サイトに製品アクセス キー（PAK）を登録します（製品アクセス キーの契約履行 （5 ページ） を参照してください）。
3. Cisco IMC Supervisor をインストールした後、ライセンスの更新 （17 ページ）の手順に従ってライセンスを更新します。
4. ライセンスが検証されると、Cisco IMC Supervisor の使用を開始できます。

実行可能な他のさまざまなライセンス タスクについては、ライセンス タスク （17 ページ）を参照してください。

製品アクセス キーの契約履行

シスコのソフトウェア ライセンス サイトに製品アクセス キー（PAK）を登録するには、次の手順を実行します。

始める前に

PAK 番号が必要です。

手順

ステップ 1 シスコのソフトウェア ライセンス Web サイト に移動します。

ステップ 2 [製品ライセンスの登録（Product License Registration）] ページが表示されたら、トレーニングを受けるか、または [製品ライセンスの登録を続ける（Continue to Product License Registration）] をクリックします。

ステップ 3 [製品ライセンスの登録（Product License Registration）] ページの [PAK またはトークンからの新規ライセンスの取得（Get New Licenses from a PAK or Token）] をクリックします。

ステップ 4 **[契約を履行する単一 PAK またはトークンの入力（Enter a Single PAK or TOKEN to Fulfill）]** フィールドに PAK 番号を入力します。

ステップ 5 **[単一 PAK/トークンの契約履行（Fulfill Single PAK/TOKEN）]** をクリックします。

ステップ 6 PAK を登録するために、[ライセンス情報（License Information）] でその他のフィールドに情報を入力します。

フィールド	説明
[組織名（Organization Name）]	組織名。
[サイトの連絡先の名前（Site Contact Name）]	サイトの連絡先の名前。
[組織の番地（Street Address）]	組織の番地。
[市区町村（City/Town）]	市区町村名。
[州/都道府県（State/Province）]	州/都道府県。
[郵便番号（Zip/Postal Code）]	郵便番号。
国（Country）	国名。

ステップ 7 **[キーの発行（Issue Key）]** をクリックします。

ライセンス契約した機能が表示され、デジタル ライセンス契約書と zip 圧縮のライセンス ファイルが、ユーザ指定の電子メール アドレスに電子メールの添付として送信されます。

Cisco IMC Supervisor ユーザ インターフェイスの共通用語

ラックグループ

ラック グループとは、物理ラックマウント サーバの論理グループです。ラック グループは、C シリーズまたは E シリーズ（またはその両方）サーバの単一のコンバージド インフラストラクチャ スタックを表します。必要に応じて、ラック グループを追加、変更、および削除することができます。

（注） 初回ログイン時に、Cisco IMC Supervisorにより [デフォルト グループ（Default Group）] というラック グループが示されます。このラック グループにラック アカウントを追加するか、または新しいラック グループを作成してラック アカウントをそのグループに追加できます。ただし、このデフォルト ラック グループ アカウントは削除できません。

ラックアカウント

ラック アカウントは、Cisco IMC Supervisorに追加されるスタンドアロン ラックマウント サーバです。複数のラック マウント サーバを Cisco IMC Supervisor に追加できます。ラック マウント サーバを Cisco IMC Supervisor にアカウントとして追加すると、Cisco IMC Supervisorによってラック マウント サーバの設定が完全に可視化されます。また、Cisco IMC Supervisorを使用して、C シリーズおよび E シリーズ ラックマウント サーバをモニタおよび管理できます。ラック アカウントは、ラック グループ（デフォルト グループまたは作成したグループ）に追加する必要があります。

ポリシー

ポリシーは、Cisco IMC でのさまざまな属性設定を定義するための主要なメカニズムです。ポリシーは、サーバ間で設定の一貫性と再現性を実現するのに役立ちます。包括的なポリシー セットを定義して使用すると、一貫性、制御性、予測可能性、自動化機能が向上します。

プロファイル

ハードウェア プロファイルは、複数のポリシーを組み合わせたものです。たとえば、1 つのラック ハードウェア プロファイル設定の詳細情報を複数のラックマウント サーバに適用することができます。いくつかの特定のラックマウント サーバにこのハードウェア プロファイルを関連付けることができます。これは、サーバ間で設定の一貫性と再現性を実現するのに役立ちます。プロファイルを定義して使用すると、一貫性、制御性、予測可能性、自動化機能が向上します。

Cisco IMC Supervisor ユーザ インターフェイス

Cisco IMC Supervisor では、管理ポータルに新しいユーザ インターフェイスが導入されています。ここでは、ユーザ インターフェイスの主な機能の一部を紹介します。

ナビゲーションの変更

古いリリースでは、メイン メニューバーから画面にアクセスしました。このリリース以降は、水平のメイン メニュー バーからではなく、サイド バーからすべてのナビゲーション オプションにアクセスできます。結果として、メイン メニュー バーはユーザ インターフェイスには表示されません。マウスまたはカーソルを使用してサイド ナビゲーション バーのオプションにマウスオーバーすると、任意のメニュー オプションをクリックできます。

ユーザ インターフェイス ラベルの廃止

ユーザ インターフェイスではアクションのラベル（[追加（Add）]、[編集（Edit）]、[削除（Delete）]、[エクスポート（Export）]、[フィルタ（Filter）] など）が廃止されました。これらの操作はアイコン形式でのみ表示されます。マウスまたはカーソルを使用してアイコンにマウスオーバーすると、ラベルにそのアイコンを使用して実行できる操作が表示されます。

[ダッシュボード（Dashboard）] を使用した詳細レポートへのアクセス

[ダッシュボード（Dashboard）] を有効にしている場合は、Cisco IMC Supervisorにログインすると最初にダッシュボードが表示されます。通常、この [ダッシュボード（Dashboard）] を使用して、重要または頻繁にアクセスされるレポート ウィジェットを追加できます。[ダッシュボード（Dashboard）] に表示されるレポートをクリックすると、詳細な情報を表示する画面がユーザ インターフェイスに即時に表示されます。ダッシュボード ビューの有効化 （209 ページ）を参照してください。さらに、複数のダッシュボードを作成したり、必要がなくなった場合はそれらを削除することができます。追加ダッシュボードの作成 （210 ページ） およびダッシュボードの削除 （211 ページ） を参照してください。

表形式レポートの拡張機能

以下は、ユーザ インターフェイスで使用できる表形式レポートの拡張機能の一部です。

- 右クリックによる追加オプションの表示

  行を選択してからマウスで右クリックすると、選択した行に関連するオプションのリストが表示されます。

- フィルタおよび検索

  Cisco IMC Supervisor インターフェイスの表形式レポートで [フィルタ（Filter）] オプション、または [検索（Search）] オプションを使用できます。表形式レポートの任意のページで [フィルタ（Filter）] オプションを使用すると、特定条件で表形式レポートの結果を絞り込むことができます。この [フィルタ（Filter）] オプションは、複数ページにまたがらない表形式レポートに使用できます。複数ページにまたがる表形式レポートの場合は、[検索（Search）] オプションを使用して検索結果の絞り込みができます。

- [お気に入り（Favorites）] メニューへの表形式レポートの追加

  ユーザインターフェイスに表示されるすべての表形式レポートをお気に入りとして追加できます。レポートをお気に入りとして追加することで、[お気に入り（Favorites）] メニューからそのレポートにアクセスできます。

- カラムのサイズ変更

  表形式レポートに表示されたカラムは、最後のカラムを含めて、すべてサイズを変更できます。カラムを展開した後、水平スクロール バーを使用すると、画面全体を表示できます。

- データがないときに表示される情報メッセージ

  レポートに表示する情報がない場合、次のメッセージが表示されます。

  データがありません

タブの削除と復元

使用可能なタブが複数ある画面では、その画面に表示するタブの数を選択できます。その画面であるタブを閉じると、そのタブはユーザインターフェイスに表示されるタブの行には表示されなくなります。そのタブを画面に復元したい場合は、画面の右端に表示される下向きの矢印をクリックします。非表示になっている使用可能なタブがドロップダウンリストに表示されます。復元するタブを選択します。

（注） 画面上のタブの削除と復元は、少なくとも2つのタブがある場合にのみ実行できます。この機能は、インターフェイスの画面に表示されているタブが 1 つだけの場合は使用できません。

レポート機能の強化

以下は、ユーザ インターフェイスで使用できる強化されたレポート機能の一部です。

- 円グラフと棒グラフの導入

  各円グラフまたは棒グラフは、PDF、CSV、またはXLS形式でシステムからエクスポートでき、[ダッシュボード（Dashboard）] に追加することもできます。

- [その他のレポート（More Reports）] オプションの可用性

  [その他のレポート（More Reports）] オプションを使用して、[障害（Faults）]、[サーバの状態（Server Health）]、[シャーシの状態（Chassis Health）]、[ファームウェア バージョン（Firmware Versions）]、[サーバ モデル（Server Models）]、[電源の状態（Power State）]、[サーバ接続のステータス（Server Connection Status）] の各レポートを生成できます。

ランディング ページ

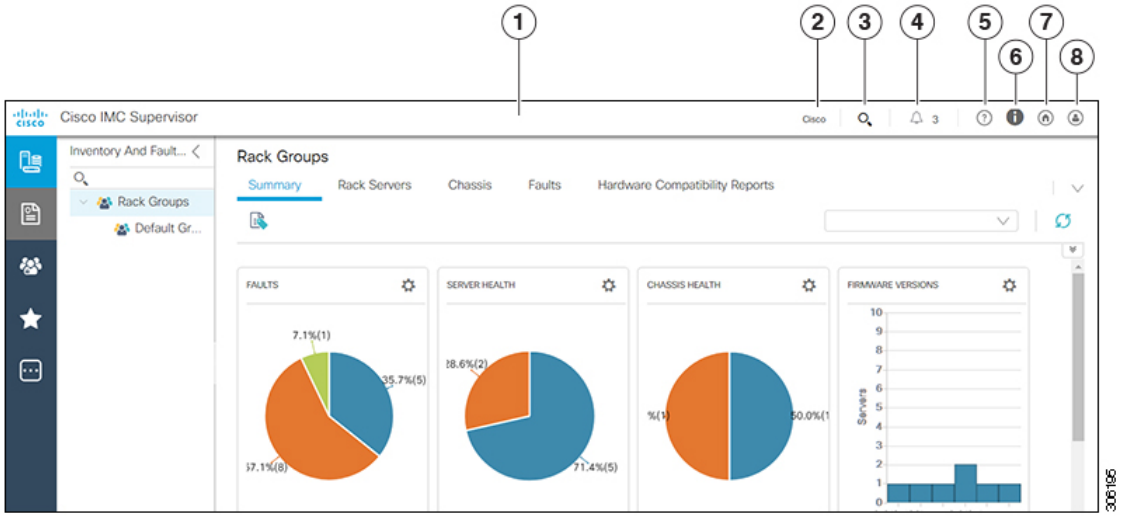
Cisco IMC Supervisor の管理者ポータルにログインすると、ランディング ページが開きます。ランディング ページに表示される要素は、表示内容の設定方法によって異なります。デフォルトでは、ポータルにログインしたときに統合ビューが表示されます。

ランディング ページで使用可能な要素は次のとおりです。

- ヘッダー：画面の上部に表示されます。
- ナビゲーション メニュー：メインのナビゲーション バーは画面の上部には表示されなくなりました。現在は、画面左側に垂直メニューとして表示されています。

（注） このメニューにはスクロールバーはありません。このメニューは、使用可能なスペースに収まる数のオプションを表示します。画面を最小化またはズームインすると、一部のオプションが表示されないことがあります。使用可能なすべてのオプションを表示するには、[サイト マップ（Site Map）] をクリックします。

図 *1* : 新しいユーザ インターフェイス



番号	名前	説明
1	ヘッダー	よくアクセスする要素（メニューなど）が含まれています。ヘッダーは常に表示されます。
2	リンク	ソフトウェアの使用に関する情報にアクセスできる、シスコの Web サイトへのリンクを提供します。

番号	名前	説明
3	検索アイコン	ポータル内の特定のレポートを検索し、そのレポートに直接移動できます。
4	[診断システム メッセージ（Diagnostic System Messages）] アイコン	ログに記録された診断システム メッセージの数が表示されます。このリンクをクリックすると、詳細情報を表示できる [診断システム メッセージ（Diagnostic System Messages）] 画面に移動します。
5	[ヘルプ（Help）] アイコン	管理者ポータルのオンライン ヘルプ システムへのリンクです。
6	[バージョン情報（About）] アイコン	ソフトウェアに関する情報、および現在インストールされているバージョンが表示されます。
7	[ホーム（Home）] アイコン	ユーザ インターフェイスの任意の場所からランディング ページに戻ることができます。
8	[ユーザ（User）] アイコン	プロファイルの編集、ダッシュボードの有効化と無効化、ユーザインターフェイスのクラシック表示へのアクセス、およびログアウトの各操作ができます。

共通のユーザ インターフェイス オプション

次の表は、アプリケーションユーザインターフェイスのすべてのページで利用できるオプションについて説明します。これらのオプションは、すべてのページで同じタスクを実行します。

アイコン	ラベル	説明
	**更新**	ページ上の報告されたデータを更新します。
	**[お気に入り（Favorite）]**	[お気に入り（Favorite）] メニューにページを追加します。 このオプションを使用すると、頻繁にアクセスするページを簡単に表示できるようになります。

アイコン	ラベル	説明
	追加	[追加（Add）] ダイアログ ボックスが表示されます。このダイアログ ボックスで新しいリソースを追加できます。
	編集	[編集（Edit）] ダイアログ ボックスが表示されます。このダイアログ ボックスでリソースを編集できます。
	テーブルのカスタマイズ	[レポートテーブルのカスタマイズ（Customize Report Table）] ダイアログ ボックスが表示されます。このダイアログ ボックスで表示する列を選択できます。
	レポートのエクスポート	[レポートのエクスポート（Export Report）] ダイアログ ボックスが表示されます。このダイアログ ボックスでレポートをシステムにダウンロードできます。 次のいずれかの形式でレポートを生成できます。 • PDF • CSV • XLS
	展開	ページに表示されているすべてのフォルダを展開します。
	折りたたむ	ページに表示されているすべてのフォルダを折りたたみます。
	高度な検索フィルタを追加	ページにフィルタリング パラメータを追加します。
	検索フィールド	ページ上の特定のレコードをフィルタリングするためのキーワードを入力します。

Cisco IMC Supervisor ユーザ インターフェイスへのセキュアな接続の設定

システムへのセキュアな接続を設定するには、次の手順を実行します。

手順

ステップ 1 server.xml ファイルで、redirectPort パラメータの値を **443** に更新します。

このファイルは、/opt/infra/web_cloudmgr/apache-tomcat/conf/ ディレクトリにあります。

```
<Connector port="80" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="443"
maxHttpHeaderSize="65536"/>
```

ステップ 2 web.xml ファイルの次の行をアンコメントします。

```
<security-constraint>
<web-resource-collection>
<web-resource-name>HTTPSOnly</web-resource-name>
<url-pattern>/*</url-pattern>
</web-resource-collection>
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
```

これらの行は、 ファイルの任意の場所に追加できます。

ステップ 3 ユーザ インターフェイスを起動してシステムにログインします。

Cisco IMC Supervisor ユーザ インターフェイスへの非セキュアな接続の設定

デフォルトでは、Cisco IMC Supervisorユーザ インターフェイスはセキュア モードで起動します。セキュア モードをバイパスして非セキュア モード（HTTP）でユーザ インターフェイスを起動する場合は、次の手順に従う必要があります。

手順

ステップ 1 root としてログ インします。

ステップ 2 /opt/infra/web_cloudmgr/apache-tomcat/conf/server.xml ファイルで次の変更を行います。

a) 既存のポート 8080 のコネクタ タグをコメント アウトします。

```
<!--
<Connector port="8080" protocol="HTTP/1.1"
redirectPort="443" maxHttpHeaderSize="65536"
URIEncoding = "UTF-8"/>
-->
```

b) 新しいポート 8080 のコネクタ タグとして以下を追加します。

```
<Connector port="8080" protocol="HTTP/1.1"
maxThreads="150" minSpareThreads="4"
connectionTimeout="20000"
URIEncoding = "UTF-8" />
```

ステップ 3 /opt/infra/web_cloudmgr/apache-tomcat/webapps/app/WEB-INF/web.xml ファイルの <security-constraint> タグをコメントにします。

```
<!--
<security-constraint>
<web-resource-collection>
<web-resource-name>HTTPSOnly</web-resource-name>
<url-pattern>/*</url-pattern>
</web-resource-collection>
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
-->
```

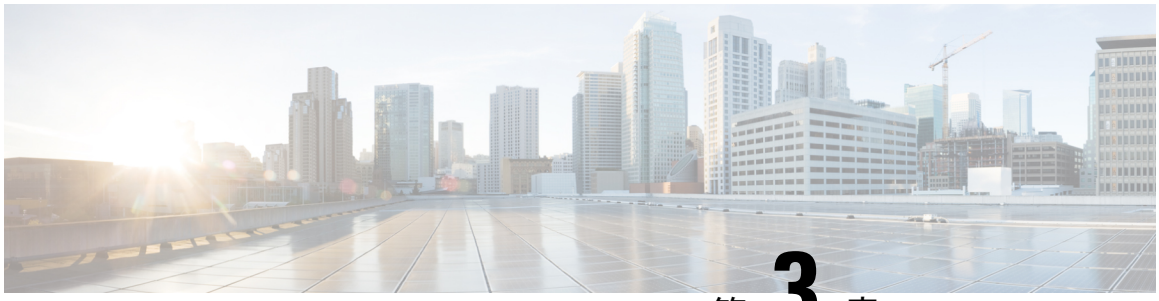
ステップ 4 サービスを再起動します。

ステップ 5 ユーザ インターフェイスを起動してシステムにログインします。

これで、次の URL 形式を使用して、非セキュア モードでシステムにログインできます。

http://<IP-Address>:8080 または http://<IP-Address>

セキュア モードでも非セキュア モードでもユーザ インターフェイスを起動できます。



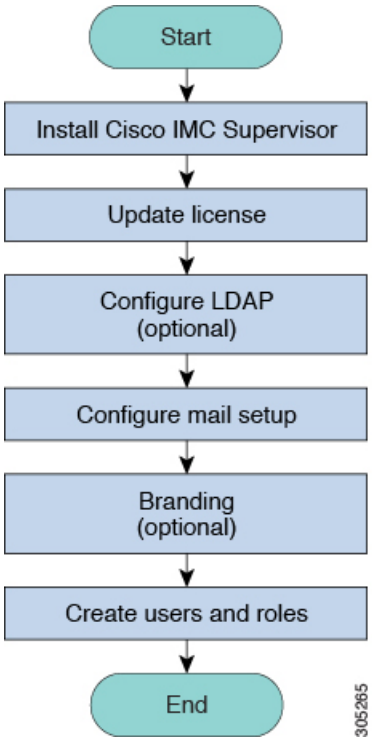
第 3 章

はじめに

この章は次のトピックで構成されています。

概要

次の図は、Cisco IMC Supervisorを使用した環境設定のワークフローを示しています。



起動 Cisco IMC Supervisor

Cisco IMC Supervisor が、正しく設定された IP アドレスを使用してインストールされている必要があります。

始める前に

- Cisco IMC Supervisor が正常にインストールされたことを確認します。
- Cisco IMC Supervisor のインストール時に IP アドレスが設定されていることを確認します。

手順

ブラウザの URL に Cisco IMC Supervisor の IP アドレスを入力して、次のクレデンシャルでログインします。

- [ユーザ名（User Name）]：**admin**
- [パスワード（Password）]：**admin**

ログインすると Cisco IMC Supervisor が起動します。Cisco IMC Supervisor のデフォルト ダッシュボードビューが表示されます。

ライセンス タスク

[ライセンス（License）]メニューを使用して、ライセンスの詳細とリソースの使用状況を表示できます。次のライセンス手順は、**[管理（Administration）]** > **[ライセンス（License）]** メニューから実行できます。

タブ	説明
[ライセンス キー（License Keys）]	このタブには、Cisco IMC Supervisor で使用されるライセンスの詳細が表示されます。このタブでは、ライセンスを更新、交換、移行することもできます。Cisco IMC Supervisor の新しいバージョンが利用可能になったら、ライセンスを更新できます。
[ライセンス使用率（License Utilization）]	このタブには、使用中のライセンスおよび各ライセンスの詳細（ライセンスの制限、使用可能期間、ステータス、備考など）が表示されます。ライセンスの監査もこのページから実行できます。 （注） Cisco IMC Supervisor のライセンスはサーバの数に基づきます。Cisco UCS S3260 シャーシは 2 サーバノードです。このため Cisco IMC Supervisor では、このシャーシのライセンス使用数が 2 サーバとして見なされます。
[リソース使用率のデータ（Resource Usage Data）]	このタブには、使用される各種リソースの詳細が表示されます。
非アクティブ化されたライセンス	このタブには、非アクティブにされたライセンスのリストが表示されます。

ライセンスの更新

Cisco IMC Supervisor の使用を開始する前に、次の手順を実行してライセンスを更新する必要があります。有効なライセンスのリストについては、ライセンスについて （4 ページ）を参照してください。ライセンス キーを生成し、製品アクセス キーを請求及び登録します。Cisco IMC Supervisor のインストールが完了すると、ライセンスが検証されているため、Cisco IMC Supervisor を使用できます。

始める前に

ライセンス ファイルを圧縮ファイルで受け取った場合は、展開して **.lic** ファイルをローカルマシンに保存します。

手順

ステップ 1 **[管理（Administration）]** > **[ライセンス（License）]** の順に選択します。

ステップ 2 [ライセンス（License）] ページで [ライセンス キー（License Keys）] を選択します。

ステップ 3 [ライセンス キー（License Keys）] ページで [ライセンスの更新（Update License）] をクリックします。

ステップ 4 [ライセンスの更新（Update License）] 画面で次のいずれかの操作を行います。

- **.lic** ファイルをアップロードするには、[参照（Browse）] をクリックして **.lic** ファイルを探して選択してから、[アップロード（Upload）] をクリックします。
- ライセンス キーの場合は、**[ライセンステキストの入力]** チェックボックスをオンにし、ライセンス キーのみをコピーして **[ライセンステキスト]** フィールドに貼り付けます。ライセンス キーは通常、ファイルの先頭の Key -> の後にあります。

  ライセンス ファイルのフルテキストをコピーして **[ライセンステキスト（License Text）]** フィールドに貼り付けることもできます。

ステップ 5 [送信（Submit）] をクリックします。
ライセンス ファイルが処理されて、更新の成功を確認するメッセージが表示されます。

ライセンスの置換

システムでライセンスを置換するには、この手順を使用します。この操作を行うと、システムのその他の既存のライセンスが非アクティブになります。

手順

ステップ 1 **[管理（Administration）]** > **[ライセンス（License）]** の順に選択します。

ステップ 2 [ライセンス（License）] ページで [ライセンス キー（License Keys）] を選択します。

ステップ 3 [ライセンスの交換（Replace License）] を選択します。

ステップ 4 [ライセンスのアップロード（Upload License）] フィールドで、PAK ファイルをドラッグ アンド ドロップするか、または [ファイルを選択（Select a File）] をクリックしてファイルを参照して選択します。

ステップ 5 （任意） [ライセンス テキストの入力（Enter License Text）] をオンにし、ライセンス テキストをコピーして貼り付けます。

ステップ 6 [送信（Submit）] をクリックします。

既存のライセンスはすべて新しいライセンスに置き換えられます。

非アクティブ化されたライセンスの表示

非アクティブ ライセンスのリストはユーザ インターフェイスから表示できます。非アクティブ ライセンスに関する次の情報を表示できます。

- PAK ファイル名
- ファイル ID
- ライセンス エントリ
- ライセンス値
- 有効期限日
- 非アクティブ化された時刻
- ライセンスを非アクティブ化したユーザの名前

手順

ステップ 1 **[管理（Administration）] > [ライセンス（License）]** の順に選択します。

ステップ 2 [ライセンス（License）] ページで [非アクティブ化されたライセンス（Deactivated Licenses）] を選択します。

ステップ 3 すべての非アクティブ ライセンスに関して表示された情報を確認します。

ライセンスの移行

Cisco IMC Supervisor では、グラフィカル ユーザ インターフェイスを使用してライセンスを移行できます。たとえば、永久ライセンスからサブスクリプション ライセンスに移行できます。

手順

ステップ 1 **[管理（Administration）] > [ライセンス（License）]** の順に選択します。

ステップ 2 [ライセンス（License）] ページで [ライセンス キー（License Keys）] を選択します。

ステップ 3 [ライセンス キー（License Keys）] ページで [ライセンスの移行（Migrate License）] をクリックします。

ステップ 4 [ライセンスのアップロード（Upload License）] フィールドで、PAK ファイルをドラッグ アンド ドロップするか、または [ファイルを選択（Select a File）] をクリックしてファイルを参照して選択します。

ステップ 5 （任意）[ライセンス テキストの入力（Enter License Text）] をオンにし、ライセンス テキストをコピーして貼り付けます。

ステップ 6 [送信（Submit）] をクリックします。

ライセンス監査の実行

ライセンスの監査を実行するには、この手順を実行します。

始める前に

ライセンスを更新する必要があります。ライセンスをアップグレードするには、ライセンスの更新 （17 ページ）を参照してください。

手順

ステップ 1 **[管理（Administration）] > [ライセンス（License）]** の順に選択します。

ステップ 2 [ライセンス（License）] ページで [ライセンス使用率（License Utilization）] をクリックします。

ステップ 3 [その他の操作（More Actions）] ドロップダウンリストから [ライセンス監査の実行（Run License Audit）] を選択します。

ステップ 4 [ライセンス監査の実行（Run License Audit）] 画面で、[送信（Submit）] をクリックします。このプロセスは完了するまでに時間がかかります。

ユーザ アクセス プロファイルの管理

マルチロール アクセス プロファイル

1 人のユーザを複数のロールに割り当てることができます。これは、1 つのユーザ アクセス プロファイルとしてシステム内で反映されます。たとえば、あるユーザが、グループ管理者、および全ポリシーの管理者として Cisco IMC Supervisor にログインしようとした場合、両方のタイプのアクセスが適切であれば、いずれのログインも可能です。アクセス プロファイルは、ユーザごとに表示できるリソースも定義します。

LDAP ユーザを Cisco IMC Supervisor に統合するときにユーザが複数のグループに属している場合、システムにより各グループのプロファイルが作成されます。ただし、デフォルトでは、ドメイン ユーザ プロファイルが LDAP ユーザに追加されます。

（注） [プロファイルの管理（Manage Profiles）]機能を使用して、ユーザ アクセス プロファイルに対して追加、ログイン、編集、または削除を行うことができます。

ユーザ アクセス プロファイルの作成

手順

ステップ 1 **[管理（Administration）] > [ユーザとグループ（Users and Groups）]** を選択します。

ステップ 2 [ユーザとグループ（Users and Groups）] ページで [ユーザ（User）] をクリックします。

ステップ 3 リストからユーザを選択します。

ステップ 4 [その他の操作（More Actions）] ドロップダウンリストから [プロファイルの管理（Manage Profiles）] を選択します。

ステップ 5 [プロファイルの管理（Manage Profile）] ページで、[追加+（Add +）] をクリックします。

ステップ 6 [アクセス プロファイルへのエントリの追加（Add Entry to Access Profiles）] ページで、次のフィールドに入力します。

フィールド名	説明
[名前（Name）] フィールド	プロファイル名。
[説明（Description）] フィールド	プロファイルの説明です。
[タイプ（Type）] ドロップダウンリスト	ユーザ ロールのタイプを選択します。
[顧客組織（Customer Organizations）] ドロップダウンリスト	このユーザ プロファイルを適用する組織を選択します。
[ユーザがアクセスできる他のすべてのグループからのリソースを表示（Show Resources From All Other Groups the User Has Access）] チェックボックス	ユーザがアクセス可能なまたはユーザが属している他のすべてのグループからのリソースを表示できるように指定する場合に、このチェックボックスをオンにします。
[共有グループ（Shared Groups）] フィールド	[選択（Select）] をクリックして、ユーザ プロファイルを適用するグループを選択します。 ユーザは、選択されたグループに関連付けられたすべてのリソースにアクセスできます。
[デフォルトプロファイル（Default Profile）] チェックボックス	デフォルトのユーザ アクセス プロファイルである場合は、このチェックボックスをオンにします。デフォルトでない場合は、このチェックボックスをオフにします。

ステップ 7 [送信（Submit）] をクリックします。

次のタスク

必要に応じて、追加のユーザ プロファイルを作成します。

プロファイルへのログイン

システムのユーザは、自分のアカウントに複数のプロファイルが存在する場合は、特定のプロファイルを使ってシステムにログインできます。

手順

ステップ 1 [Cisco IMC Supervisor ログイン（Cisco IMC Supervisor login）] ページの [ユーザ名（Username）] フィールドに、ユーザ名を「ユーザ名: アクセス プロファイル名」の形式で入力します。

例：Alex: GrpAdmin

ステップ 2 [パスワード（Password）] フィールドにパスワードを入力します。

ステップ 3 [ログイン（Login）] をクリックします。

デフォルト プロファイル

デフォルト プロファイルは、システムで作成した最初のプロファイルです。デフォルト プロファイルを別のプロファイルに変更できます。新しいデフォルトプロファイルを使用し、ユーザ名とパスワードを入力してログインします。

デフォルト プロファイルの変更

手順

ステップ 1 ユーザ インターフェイスで、右上隅に表示されたユーザ名をクリックします。

ユーザ名は [ログアウト（logout）] オプションの左側に表示されます。

ステップ 2 [ユーザ情報（User Information）] ページの [アクセス プロファイル（Access Profiles）] タブを選択します。

ステップ 3 ユーザ プロファイルを選択し、[デフォルトプロファイルとして設定（Set as Default Profile）] をクリックします。

（注）　プロファイルは、追加時または編集時にデフォルトとして設定することもできます。

認証および LDAP 統合

LDAP のフォールバックを選択して、認証を設定できます。また、フォールバックを行わない VeriSign ID 保護（VIP）認証を設定できます。

名前	説明
ローカルが最初、LDAPにフォールバック（Local First, fallback to LDAP）	認証は最初にローカル サーバで実行されます（Cisco IMC Supervisor）。ユーザがローカル サーバにない場合、LDAP サーバが確認されます。
[VeriSign ID保護（Verisign Identity Protection）]	VIP 認証サービス（2 要素認証）が有効化されます。

認証の環境設定

ログイン認証タイプを変更する場合は、次の手順を実行します。

手順

ステップ 1　**[管理（Administration）] > [ユーザとグループ（Users and Groups）]** を選択します。

ステップ 2　[認証の環境設定（Authentication Preferences）] を選択します。

ステップ 3　[認証の環境設定（Authentication Preferences）] ドロップダウンリストから、次のいずれかのオプションを選択します。

- **ローカルが最初、LDAPにフォールバック（Local First, fallback to LDAP）**

  このオプションを選択する場合は、LDAP サーバを設定する必要があります。詳細については、LDAP サーバの設定 （29 ページ）を参照してください。

- [VeriSign ID 保護（Verisign Identity Protection）]：このオプションを選択した場合は、次のステップに進みます。

ステップ 4　[VeriSign ID 保護（Verisign Identity Protection）] を選択した場合は、次の手順を実行します。

a)　VIP 証明書をアップロードするには、[参照（Browse）] をクリックします。
　証明書を見つけて選択し、[アップロード（Upload）] をクリックします。

b)　[パスワード（Password）] を入力します。

ステップ 5 [保存（Save）] をクリックします。

LDAP の設定

Cisco IMC Supervisorでの LDAP の設定には、LDAP 設定の追加と LDAP サーバの設定が含まれますまた、LDAP の接続をテストし、LDAP の概要情報を表示できます。以降のセクションでは、これらの手順の実行方法について説明します。

LDAP の統合

LDAP 統合を使用して、LDAP サーバのユーザを Cisco IMC Supervisor と同期することができます。LDAP 認証により、同期されたユーザを LDAP サーバで認証することができます。LDAP ユーザを自動または手動で同期できます。LDAP アカウントの追加中に、LDAP アカウントが Cisco IMC Supervisor と自動的に同期される頻度を指定できます。オプションで **LDAPSyncTask** システム タスクを使用して、LDAP 同期を手動でトリガーすることもできます。

LDAP ディレクトリに新しい組織単位（OU）を追加し、手動または自動で同期プロセスを実行している場合は、最近追加された LDAP ユーザが Cisco IMC Supervisor に表示されます。

システム タスクを実行する機能に加えて、Cisco IMC Supervisorには LDAP ディレクトリとシステムを同期するための追加オプションもあります。

[LDAP ユーザのクリーンアップ（Cleanup LDAP Users）] システム タスク：このシステム タスクは、システム内で同期されたユーザがLDAPディレクトリから削除されたかどうかを判別します。LDAPディレクトリから削除されたユーザのレコードが存在する場合、このシステム タスクの実行後に、これらのユーザはシステム内で無効としてマークされます。管理者は、これらの非アクティブユーザのリソース割り当てを解除できます。デフォルトでは、このタスクは有効モードになっています。このシステム タスクが無効モードに設定されるのは、サービスを 2 回再起動した後だけです。

ローカルに存在している、または Cisco IMC Supervisor で外部から同期されているユーザは選択できません。

重要 グループ、またはドメイン ユーザのグループに属していないユーザは、[グループに属していないユーザ（Users with No Group）] として LDAP に表示されます。これらのユーザは、Cisco IMC Supervisor のドメイン ユーザのグループの下に追加されます。

異なる LDAP サーバ アカウントに所属し、同じ名前を持った LDAP ユーザを追加できます。複数のユーザ レコードを区別するために、ログイン ユーザ名の末尾にドメイン名が追加されます。たとえば、abc@vxedomain.com などです。このルールは、ユーザ グループにも適用されます。

単一のLDAPアカウントが追加され、ユーザがユーザ名のみを指定してログインすると、Cisco IMC Supervisorは最初にそのユーザがローカル ユーザまたは LDAP ユーザのどちらであるかを判別します。ユーザがローカルユーザおよび外部LDAPユーザの両方として識別された場合、ログイン段階でユーザ名がローカルユーザ名に一致すると、そのローカルユーザが Cisco IMC Supervisor に対して認証されます。あるいは、ユーザ名が外部ユーザの名前に一致すると、その LDAP ユーザが Cisco IMC Supervisor に対して認証されます。

LDAP 統合の規則と制限事項

グループの同期規則

- 選択した LDAP グループが Cisco IMC Supervisor にすでに存在しており、ソースのタイプが [ローカル（Local）] の場合、そのグループは同期中に無視されます。
- 選択した LDAP グループが Cisco IMC Supervisor にすでに存在しており、グループソースのタイプが [外部（External）] の場合、そのグループの説明および電子メール属性が Cisco IMC Supervisor で更新されます。
- LDAP サーバを追加する際には、ユーザ フィルタとグループ フィルタを指定できます。グループ フィルタを指定すると、指定したグループに属するすべてのユーザがシステムに追加されます。さらに、次のような操作も行えます。
  - 指定したグループにサブグループが含まれている場合には、グループ、サブグループ、およびそれらのサブグループ内のユーザがシステムに追加されます（これが該当するのは、手動で LDAP ディレクトリを同期した場合のみです）。
  - ユーザが複数のグループの一部であり、グループ フィルタとして指定されたグループに他のグループが一致しない場合、それらの追加グループはシステムに追加されません。
- ユーザは複数の設定グループに属することができます。ただし、ユーザが属するグループのリストで最初に表示されているグループが、そのユーザのデフォルトのプライマリ グループとして設定されます。ユーザがどのグループにも属していない場合は、デフォルトのプライマリ グループが [ドメイン ユーザ（Domain Users）] として設定されます。

（注） ユーザが属するすべてのグループに関する情報は、**LDAPSyncTask** システム タスクの実行後にのみ表示できます。

- LDAP グループを同期すると、グループ内のすべてのユーザが最初にシステムに追加されます。また、指定された LDAP グループ内のユーザが同じ OU 内の（または異なる OU 内の）他のグループに関連付けられている場合には、それらのグループも取得され、システムに追加されます。
- LDAP 同期プロセスでは、システムの指定された LDAP グループ、およびネストされたグループがあればそれも併せて取得されます。
- このリリースより前のリリースでは、ユーザは 1 つのグループにのみ属していました。ユーザが属するその他のグループは、最新リリースにアップグレードし、**LDAPSyncTask** システムタスクを実行した場合にのみ、[プロファイルの管理（Manage Profiles）] ダイアログ ボックスに表示されます。これは、他のグループが、LDAP サーバの設定時に指定したグループ フィルタの条件に一致する場合のみ該当します。

ユーザの同期規則

- 名前に特殊文字が含まれている LDAP ユーザは Cisco IMC Supervisor に追加されます。
- LDAP サーバを追加する際には、ユーザ フィルタとグループ フィルタを指定できます。ユーザ フィルタを指定すると、指定したフィルタと一致するすべてのユーザと、それらのユーザが属しているグループがシステムに取得されます。
- Cisco IMC Supervisor では、システムに追加された各ユーザのユーザ プリンシパル名（UPN）が表示されるようになりました。これは、以前のリリースでシステムに追加されたユーザに適用可能です。ユーザは、ログイン名またはユーザ プリンシパル名を使用してシステムにログインできます。ユーザ プリンシパル名とプロファイル名の両方を使用したログインはサポートされていません。
- 選択した LDAP ユーザが Cisco IMC Supervisor にすでに存在しており、ソースのタイプが [ローカル] の場合、そのユーザは同期中に無視されます。
- 選択した LDAP ユーザが Cisco IMC Supervisor にすでに存在しており、ソースのタイプが [外部] の場合、そのユーザの名前、説明、電子メール、および他の属性が更新されて使用できるようになります。
- ユーザ アカウントが 2 つの異なる LDAP ディレクトリで作成されている場合は、最初に同期された LDAP ディレクトリのユーザ詳細が表示されます。他の LDAP ディレクトリのユーザ詳細は表示されません。
- 複数の LDAP ディレクトリが同期された後、LDAP 外部ユーザは、完全なドメイン名をユーザ名と共に指定して Cisco IMC Supervisor にログインする必要があります。たとえば vxedomain.cisco.com\username のように指定します。ただし、Cisco IMC Supervisorに追加されている LDAP サーバ ディレクトリが 1 つしかない場合には、この規則は適用されません。

ユーザ同期の制限事項

- あるユーザが複数のグループ メンバーシップを持っていても、そのユーザは Cisco IMC Supervisor では単一のグループ メンバーシップを持つことになります。

（注）
- Cisco IMC Supervisor 内のユーザとグループ（ローカルと LDAP の両方）の合計数を 10,000 以下に保つことをお勧めします。この数値を超えると、アプライアンスが遅くなったり応答しなくなることがあります。
- LDAP 同期プロセス後に、ユーザが正しいグループに割り当てられていることを確認します。

ベスト プラクティス

何千もの LDAP オブジェクトを Cisco IMC Supervisor と同期すると、アプライアンスのパフォーマンスに問題が発生する可能性があります。必要な LDAP オブジェクトのみを同期するには、次の手順を実行します。

1. Cisco IMC Supervisor へのアクセス権が必要なすべてのユーザを含む LDAP グループを作成します。
2. それらのグループのみを Cisco IMC Supervisor と同期します。

LDAP 設定の追加

LDAP 設定を追加するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [LDAP 統合（LDAP Integration）]** を選択します。

ステップ 2 LDAP 設定を追加するには [+] をクリックします。

ステップ 3 [LDAP 設定の追加（Add LDAP Configurations）] ページで、次のフィールドに入力します。

フィールド	説明
[アカウント名（Account Name）] フィールド	LDAP アカウント名。
[サーバ タイプ（Server Type）] ドロップダウンリスト	[Microsoft Active Directory] または [Open LDAP] を選択します。
[サーバ（Server）] フィールド	サーバのホスト名または IP アドレス。
[SSLの有効化（Enable SSL）] チェックボックス	LDAP サーバに対するセキュアな接続を有効にします。

フィールド	説明
[ポート（Port）] フィールド	ポート番号 SSL では 636 に、非セキュア モードでは 389 に自動的に設定されます。
[ドメイン名（Domain Name）] フィールド	LDAP ユーザのドメイン名。
[ユーザ名（Username）] フィールド	LDAP ユーザの名前を入力します。
[パスワード（Password）] フィールド	ユーザ名に関連付けられるパスワードを入力します。
[同期頻度（Synchronization Frequency）] ドロップダウンリスト	LDAP サーバを同期する頻度（時間単位）を選択します。次のいずれかを指定できます。 • 1 • 4 • 12 • 24

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 [LDAP 検索ベース（LDAP Search Base）] ページで [選択（Select）] をクリックし、表示されているテーブルから OU に基づいてユーザを取得するための検索条件を選択します。

（注） Cisco IMC Supervisor ではユーザはサポートされていますが、グループはサポートされていません。**OU** に基づく検索条件は必須ではありません（ユーザとグループの両方が含まれる可能性があるため）。システム同期タスクが 24 時間ごとに実行され、検索基準に基づいて LDAP ユーザが同期されます。このため、ユーザ情報のみの手動同期を実行する必要があります。LDAP の手動同期を実行するには、LDAP の手動同期のリクエスト （34 ページ）を参照してください。

ステップ 6 [選択（Select）] ダイアログボックスで [選択（Select）] をクリックします。

選択した検索条件が、[検索ベース（Search Base）] フィールドの横に表示されます。

ステップ 7 [LDAP 検索ベース（LDAP Search Base）] ダイアログボックスの [次へ（Next）] をクリックします。

ステップ 8 [+] をクリックし、[LDAP ユーザ ロール フィルタ（LDAP User Role Filter）] ダイアログボックスでユーザ ロール フィルタ テーブルにエントリを追加します。

ステップ 9 [ユーザ ロール フィルタへのエントリの追加（Add Entry to User Role Filters）] ダイアログボックスで、ユーザ ロールの詳細を入力します。

ステップ 10 [送信（Submit）] をクリックします。

これらのフィルタは編集または削除できます。また、上矢印と下矢印を使ってフィルタを移動して、フィルタの優先順位を設定できます。

ステップ 11 [LDAP ユーザ ロール フィルタ（LDAP User Role Filter）] ダイアログボックスで、[送信（Submit）] をクリックします。

LDAP サーバの設定

Cisco IMC Supervisorでは複数の LDAP サーバとアカウントを設定できます。LDAP アカウントを追加するときに、次の項目を指定できます。

- 検索ベース識別名（DN）に含まれている組織単位（OU）。
- LDAP アカウントがシステムと自動的に同期される頻度。
- 結果を絞り込み、グループおよびユーザに LDAP ロール フィルタを指定する、グループ フィルタまたはユーザ フィルタ。

LDAP サーバ アカウントが追加されると直ちにこのアカウントのシステム タスクが自動的に作成され、データ同期を即時に開始します。LDAP サーバ アカウントのすべてのユーザとグループがシステムに追加されます。デフォルトでは、LDAP アカウントのすべてのユーザに対して、自動的にサービス エンド ユーザ プロファイルが割り当てられます。

始める前に

認証設定を [ローカルが最初、LDAP にフォールバック（Local First, fallback to LDAP）] に設定している必要があります。

手順

ステップ 1 **[管理（Administration）] > [LDAP 統合（LDAP Integration）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [LDAP サーバの設定（LDAP Server Configuration）] ページで、次のフィールドに入力します。

名前	説明
[アカウント名（Account Name）] フィールド	アカウント名。 この名前は一意である必要があります。
[サーバタイプ（Server Type）] フィールド	LDAP サーバのタイプ。次のいずれかを指定できます。 • OpenLDAP • MSAD - Microsoft Active Directory
[サーバ（Server）] フィールド	LDAP サーバの IP アドレスまたはホスト名。

名前	説明
[SSLの有効化（Enable SSL）] チェックボックス	LDAP サーバに対するセキュアな接続を有効にします。
[ポート（Port）] フィールド	ポート番号 SSL では 636 に、非セキュア モードでは 389 に自動的に設定されます。
[ドメイン名（Domain Name）] フィールド	ドメイン名。 LDAP ディレクトリのタイプとして [OpenLDAP] を選択した場合は、このドメイン名が、ユーザ名で指定されたドメインと一致している必要があります。 **重要** 完全なドメイン名を指定する必要があります。たとえば、vxedomain.com などです。
[ユーザ名（Username）] フィールド	ユーザ名。 LDAP ディレクトリのタイプとして [OpenLDAP] を選択した場合は、ユーザ名を次の形式で指定します。 **uid=users,ou=People,dc=ucsd,dc=com** ここに指定する **ou** は、ディレクトリ階層でその他のすべてのユーザが配置される場所です。
[パスワード（Password）] フィールド	ユーザのパスワード。
[同期頻度（Synchronization Frequency）] ドロップダウンリスト	LDAP サーバが同期される頻度（時間）を選択します。次のいずれかを指定できます。 • 1 • 4 • 12 • 24

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 [LDAP 検索ベース（LDAP Search Base）] ペインで [選択（Select）] をクリックし、LDAP 検索ベースのエントリを指定して、[選択（Select）] をクリックします。

このリストには、Cisco IMC Supervisor で利用できるすべての組織単位（OU）が表示されます。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 [ユーザとグループのフィルタの設定（Configure User and Group Filters）] ペインで、次のフィールドに入力します。

名前	説明
ユーザフィルタ（User Filters）	[+] 記号をクリックして、システムと同期する必要がある特定のユーザを選択します。 選択したユーザが属するグループがすべて取得され、システムに追加されます。
グループ フィルタ（Group Filters）	[+] 記号をクリックして、システムと同期する必要があるグループを選択します。 選択したグループに属するユーザがすべて取得され、システムに追加されます。ただし、選択したグループのユーザが、選択していないその他のグループにも属している場合、それらのグループは、このフィールドで選択されている場合を除き取得されません。
[ユーザフィルタへのエントリの追加（Add Entry to User Filters）] または [グループフィルタへのエントリの追加（Add Entry to Group Filters）] ダイアログボックス（前の選択に応じて表示されます）	
[属性名（Attribute Name）] ドロップダウンリスト	[グループ名（Group Name）] または [ユーザ名（User Name）] を選択します。
[オペレータ（Operator）] ドロップダウンリスト	グループおよびユーザを取得する際に適用するフィルタを選択します。次のいずれかを指定できます。 • **等しい（Equals to）** • **開始（Starts with）**
[属性値（Attribute Value）] フィールド	検索に含めるキーワードまたは値を指定します。

フィルタに基づいて、グループまたはユーザが取得されます。

ステップ 8 [次へ（Next）] をクリックします。

ステップ 9 [LDAP ユーザ ロール フィルタ（LDAP User Role Filter）] ペインで、[+] 記号をクリックして、ユーザ ロール フィルタを追加します。

ステップ 10 [ユーザロールフィルタへのエントリの追加（Add Entry to User Role Filters）] 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
[属性名（Attribute Name）] フィールド	属性の名前。これには、**グループ名**を指定できます。
[オペレータ（Operator）] ドロップダウンリスト	ドロップダウンリストは次のいずれかになります。 • **次の値と等しい（Equal to）** • **開始（Starts with）**
[属性値（Attribute Value）] フィールド	このフィールドで値を指定します [オペレータ（Operator）] フィールドと [属性値（Attribute Value）] フィールドの値に一致するすべてのユーザが、[ユーザロールのマッピング（Map User Role）] ドロップダウンリストで選択するユーザ ロールに割り当てられます。
[ユーザロールのマップ（Map User Role）] ドロップダウンリスト	ユーザのマップ先とするユーザ ロールを選択します。デフォルトのロールまたはユーザ定義のロールを選択できます。 Cisco IMC Supervisor に用意されているデフォルトのロールは以下のとおりです。 • グループ管理者 • 演算子 • システム管理者（System Admin）

ステップ 11 [送信（Submit）] をクリックします。

ユーザ ロール フィルタが [ユーザ ロール フィルタ（User Role Filters）] テーブルに追加されます。

（注） 複数のユーザ ロール フィルタが指定されている場合は、最初の行のフィルタが適用されます。

ユーザのロールを手動で更新すると、そのユーザには、グループをマップしたユーザロールが適用されなくなります。

次のタスク

LDAP に認証の環境設定を設定していない場合は、認証の環境設定を変更するように指示されます。認証の環境設定 （23 ページ）を参照してください。

LDAP サーバのサマリー情報の表示

LDAP サーバのサマリー情報を表示するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [LDAP 統合（LDAP Integration）]** を選択します。

ステップ 2 テーブルから LDAP のアカウント名を選択します。

ステップ 3 [表示（View）] をクリックします。

[LDAP アカウント情報の表示（View LDAP Account Information）] 画面に、LDAP アカウントのサマリー情報が表示されます。

ステップ 4 [閉じる（Close）] をクリックします。

LDAP サーバの接続のテスト

LDAP 接続をテストするには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [LDAP 統合（LDAP Integration）]** を選択します。

ステップ 2 テーブルから LDAP のアカウント名を選択します。

ステップ 3 [テスト接続（Test Connection）] をクリックします。

接続のステータスが表示されます。

ステップ 4 [LDAP 接続のテスト（Test LDAP Connectivity）] ダイアログボックスで、[閉じる（Close）] をクリックします。

ベース DN の検索

ベース DN を検索するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [LDAP 統合（LDAP Integration）]** を選択します。

ステップ 2 [ベースDNの検索（Search BaseDN）] をクリックします。

（注） Cisco IMC Supervisor ではユーザはサポートされていますが、グループはサポートされていません。**OU** に基づく検索条件は必須ではありません（ユーザとグループの両方が含まれる可能性があるため）。

ステップ 3 [LDAP 検索ベース（LDAP Search Base）] ダイアログボックスで [選択（Select）] をクリックします。

ステップ 4 [選択（Select）] ダイアログボックスで、1 つ以上のユーザを選択して [選択（Select）] をクリックします。

ステップ 5 [LDAP 検索ベース（LDAP Search Base）] ダイアログボックスで [送信（Submit）] をクリックします。

LDAP の手動同期のリクエスト

LDAP の手動同期のリクエストでは、LDAP ユーザおよびグループを取得するための基本検索条件または詳細検索条件を指定できます。LDAP の手動同期を行うには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [LDAP 統合（LDAP Integration）]** を選択します。

ステップ 2 [Request Manual LDAP Sync] をクリックします。

ステップ 3 [LDAP の手動同期のリクエスト（Request Manual LDAP Sync）] ページで、次のフィールドに情報を入力します。

名前	説明
[基本検索（Basic Search）] チェックボックス	組織単位ごとの基本検索を可能にします。
[詳細検索（Advanced Search）] チェックボックス	詳細検索を可能にします。

（注） いずれかの検索オプションを使用する時点ですでにユーザおよびグループが Cisco IMC Supervisor に存在する場合、検索を実行しても同じユーザとグループは読み込まれません。

ステップ 4 基本検索の場合は、[選択（Select）] をクリックして検索ベースを指定します。

ステップ 5 検索ベース DN を選択し、[選択（Select）] をクリックして、ステップ 9 に進みます。

ステップ 6 詳細検索の場合は、[詳細なフィルタ オプション（Advanced Filtering Options）] ペインで、[ユーザ フィルタ（User Filters）] と [グループ フィルタ（Group Filters）] の属性名を追加または編集します。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 [ユーザとグループの選択（Select Users and Groups）] ページで、次のフィールドに入力します。

名前	説明
[LDAP グループ（LDAP Groups）] フィールド	ユーザを同期する必要がある LDAP グループ。
[LDAP ユーザ（LDAP Users）] フィールド	同期する必要がある LDAP ユーザ。

ステップ 9 [送信（Submit）] をクリックします。

[管理（Administration）] > [ユーザとグループ（Users and Groups）] を選択し、[ユーザ（Users）] をクリックして同期されたユーザを確認します。

LDAP 同期の実行と LDAP 同期結果の表示

LDAP の同期を実行し、結果を表示するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [システム（System）]** を選択します。

ステップ 2 [システム（System）] ページで [システムのタスク（System Tasks）] をクリックします。

ステップ 3 [ユーザとグループのタスク（User and Group Tasks）] を展開し、[LDAPSyncTask] を選択します。

ステップ 4 [今すぐ実行（Run Now）] をクリックします。

ステップ 5 [送信（Submit）] をクリックします。

ステップ 6 （オプション）[タスクの管理（Manage Task）] をクリックして、同期処理を有効または無効にします。

次のタスク

同期プロセスの結果が Cisco IMC Supervisor に表示されます。[LDAP 統合（LDAP Integration）] ページで LDAP アカウントを選択し、[結果（Results）] をクリックすると、同期プロセスの概要が表示されます。

LDAP サーバの詳細の変更

構成済み LDAP サーバで変更できる詳細は以下のみです。

- ポート番号および SSL 設定
- ユーザ名およびパスワード

- 同期頻度
- 検索ベース DN の選択
- マッピングされたユーザ ロールとグループ

LDAP サーバの詳細を変更するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [LDAP 統合（LDAP Integration）]** を選択します。

ステップ 2 LDAP アカウントを選択します。

ステップ 3 [変更（Modify）] をクリックします。

ステップ 4 [LDAP サーバの設定（LDAP Server Configuration）] ページで、次のフィールドを編集します。

名前	説明
[SSLの有効化（Enable SSL）] チェックボックス	LDAP サーバに対するセキュアな接続を有効にします。
[ポート（Port）] フィールド	ポート番号 SSL では 636 に、非セキュア モードでは 389 に自動的に設定されます。
[ユーザ名（Username）] フィールド	ユーザ名。 LDAP ディレクトリのタイプとして [OpenLDAP] を選択した場合は、ユーザ名を次の形式で指定します。 **uid=users,ou=People,dc=ucsd,dc=com** ここに指定する **ou** は、ディレクトリ階層でその他のすべてのユーザが配置される場所です。
[パスワード（Password）] フィールド	ユーザのパスワード。
[同期頻度（Synchronization Frequency）] ドロップダウンリスト	LDAP サーバがシステム データベースと同期される頻度（時間単位）を選択します。次のいずれかを指定できます。 • 1 • 4 • 12 • 24

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [LDAP 検索ベース（LDAP Search Base）] エントリを編集し、[次へ（Next）] をクリックします。

ステップ 7 [ユーザ フィルタ（User Filters）] および [グループ フィルタ（Group Filters）] テーブルで必要な属性を選択して編集し、[次へ（Next）] をクリックします。

ステップ 8 [LDAP ユーザ ロール フィルタ（LDAP User Role Filter）] テーブルでエントリを選択して編集します。

ステップ 9 上矢印と下矢印を使用して、テーブルエントリの追加、編集、削除、または移動をクリックします。

ステップ 10 [送信（Submit）] をクリックします。

グループ メンバーシップ情報の表示

システム内のユーザは、複数のユーザ グループに属することができます。ユーザがシステムに追加されると、ユーザが属するすべてのグループもシステムに追加されます。ただし、最後にユーザが追加されたグループは、ユーザのデフォルトのプライマリ グループとして設定されます。ユーザがどのグループにも属していない場合は、デフォルトのプライマリ グループが [ドメイン ユーザ（Domain Users）] として設定されます。[プロファイルの管理（Manage Profiles）] オプションを使用して、ユーザのグループ メンバーシップを表示し変更することができますが、Cisco IMC Supervisor では特定のユーザが属しているすべてのグループのリストを表示する追加オプションもあります。

手順

ステップ 1 **[管理（Administration）] > [ユーザとグループ（Users and Groups）]** を選択します。

ステップ 2 [Users] をクリックします。

ステップ 3 テーブルからユーザを選択します。

ステップ 4 [グループメンバーシップ（Group Membership）] をクリックします。

[以下のメンバー（Member Of）] 画面に、ユーザが属するすべてのグループが表示されます。

ステップ 5 [閉じる（Close）] をクリックします。

LDAP サーバ情報の削除

LDAP サーバのアカウントを削除すると、検索基準、BaseDN および対象の LDAP サーバに関するシステム エントリのみが削除されます。LDAP サーバに割り当てられているユーザは削除されません。LDAP サーバの情報を削除するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [ユーザとグループ（Users and Groups）]** を選択します。
ステップ 2 [LDAP 統合（LDAP Integration）] を選択します。
ステップ 3 テーブルから LDAP のアカウント名を選択します。
ステップ 4 [削除（Delete）] をクリックします。
ステップ 5 確認のダイアログボックスで [削除] をクリックします。

それにより、Cisco IMC Supervisor の LDAP アカウントの削除が開始されます。LDAP アカウント内のユーザの数によっては、この削除プロセスは完了するまで数分かかる場合があります。その間、LDAP アカウントは Cisco IMC Supervisor で表示されたままになります。[更新（Refresh）] をクリックして、アカウントの削除を確定します。

SCP ユーザの設定

SCP ユーザは、サーバ診断やテクニカル サポートのアップロード操作で、SCP プロトコルを使用して Cisco IMC Supervisor アプライアンスにファイルを転送する際に使用されます。SCP ユーザ アカウントは、Cisco IMC SupervisorUI または shelladmin へのログインには使用できません。SCP ユーザ パスワードを設定するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [ユーザとグループ（Users and Groups）]** を選択します。
ステップ 2 [SCP ユーザ設定（SCP User Configuration）] をクリックします。
ステップ 3 [パスワード（Password）] フィールドに SCP ユーザ パスワードを入力します。
ステップ 4 [送信（Submit）] をクリックします。

電子メール設定の設定

Cisco IMC Supervisor から送信されるすべての電子メールに SMTP サーバが必要です。障害のアラートなどの Cisco IMC Supervisor によって生成される電子メールは、次の手順を使用して設定した電子メール設定に送信されます。電子メールアラートのルールを追加する方法の詳細については、サーバ障害に関する電子メール アラート ルールの追加 （78 ページ）を参照してください。

手順

ステップ 1 **[管理（Administration）] > [システム（System）]** を選択します。

ステップ 2 [電子メール設定（Mail Setup）] をクリックします。

ステップ 3 [電子メール設定（Mail Setup）] ページで、次のフィールドに入力します。

フィールド	説明
送信電子メール サーバ（SMTP）（Outgoing Email Server (SMTP)）	サーバの IP アドレスまたはドメイン名。
送信 SMTP ポート（Outgoing SMTP Port）	SMTP サーバのポート番号。
送信 SMTP ユーザ（Outgoing SMTP User）	（オプション）SMTP 認証で使用する送信 SMTP ユーザ ID。
送信 SMTP パスワード（Outgoing SMTP Password）	（オプション）SMTP 認証で使用する送信 SMTP ユーザ ID のパスワード。
送信者の電子メールアドレス（Outgoing Email Sender Email Address）	Cisco IMC Supervisor によって生成される送信電子メールの送信者アドレス。
サーバIPアドレス	Cisco IMC Supervisor を実行しているサーバの IP アドレス。
[テスト メールの送信（Send Test Email）] チェックボックス	設定されたアドレスにテスト メールを送信するには、このチェックボックスをオンにします。

ステップ 4 [保存（Save）] をクリックします。

Cisco.com ユーザ資格情報とプロキシ設定

[管理（Administration）] > [システム（System）] から、Cisco ユーザ資格情報とプロキシの詳細を設定することができます。Cisco.com ユーザとプロキシの資格情報は、アプリケーション全体の設定です。これらの資格情報は、ファームウェア イメージのダウンロードと Cisco IMC Supervisor の更新に自動的に使用されます。Cisco Smart Call Home でも、これらのプロキシの詳細を使用します。

Cisco.com ユーザの設定

Cisco.com ユーザの名前とパスワードを設定するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [システム（System）]** を選択します。

ステップ 2 [システム（System）] ページで、[Cisco.com ユーザ設定（Cisco.com User Configuration）] をクリックします。

ステップ 3 Cisco.com ユーザを設定するため、次のフィールドに情報を入力します。

フィールド	説明
[ユーザ名（cisco.com）（User Name (cisco.com)）] フィールド	シスコのログイン ユーザ名を入力します。
[パスワード（cisco.com）（Password (cisco.com)] フィールド	シスコのログイン パスワードを入力します。

ステップ 4 [保存（Save）] をクリックします。

プロキシ設定

プロキシ設定を構成する場合は、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [システム（System）]** を選択します。

ステップ 2 [システム（System）] ページで、[プロキシ設定（Proxy Configuration）] をクリックします。

ステップ 3 プロキシ設定の次のフィールドに入力します。

フィールド	説明
[プロキシ設定の有効化（Enable Proxy Configuration）] チェックボックス	（オプション）このチェックボックスをオンにしてプロキシを有効化し、次の情報を入力します。 • [ホスト名（Host Name）] フィールド：プロキシ設定用のホスト名を入力します。 • [ポート（Port）] フィールド：プロキシ設定用のポートを入力します。

フィールド	説明
[プロキシ認証の有効化（Enable Proxy Authentication）] チェックボックス	（オプション）このチェックボックスをオンにしてプロキシ認証を有効にし、次の情報を入力します。 • [プロキシ ユーザ名（Proxy User Name）] フィールド：プロキシ認証用のプロキシ ユーザ名を入力します。 • [プロキシ パスワード（Proxy Password）] フィールド：プロキシ ユーザ名のパスワードを入力します。

ステップ 4 [保存（Save）] をクリックします。

CMDB 統合の設定

構成管理データベース（CMDB）は、システムの変更を追跡および管理するために使用されます。CMDB には通常、サービス リクエスト、グループなどのリソースに対する追加、削除、または変更のイベント タイプが表示されます。

手順

ステップ 1 **[管理（Administration）] > [統合（Integration）]** を選択します。

ステップ 2 [統合（Integration）] ページで [CMDB 統合の設定（CMDB Integration Setup）] をクリックします。

ステップ 3 [CMDB 統合の設定（CMDB Integration Setup）] 画面で、次を含む必須フィールドに入力します。

名前	説明
[FTP サーバにエクスポート] チェックボックス	FTP サーバに変更記録をエクスポートするには、このチェックボックスをオンにします。
[エクスポート形式（Export Format）] ドロップダウンリスト	エクスポート形式の種類（CSV または XML）を選択します。
[FTP Server] フィールド	FTP サーバのアドレス。
[FTP Port] フィールド	FTP サーバ ポート番号。
[FTP User] フィールド	FTP ユーザ ID。
[FTP パスワード] フィールド	FTP ユーザ パスワード。

名前	説明
[FTP Export Frequency] ドロップダウンリスト	変更記録を FTP サーバにエクスポートする頻度を選択します。
[FTP File Name] フィールド	エクスポートされる変更記録のファイル名。ファイルがターゲットFTPサーバにエクスポートされるたびに、次の変数を使用して新しいファイル名を作成できます。 MONTH、WEEK、DAY、YEAR、HOUR、MIN、SEC、MLLIS 例：XYZ-$DAY-$HOUR-$MIN-$SEC
[FTP のテスト] チェックボックス	FTP の設定をテストするには、このチェックボックスをオンにします。

ステップ 4 [保存（Save）] をクリックします。

ブランディング

ログインページは、ドメイン名に関連付けられているロゴを示すように設定できます。エンドユーザがそのドメインからログインすると、ログイン ページでそのカスタム ロゴが表示されます。ロゴの最適なイメージのサイズは幅 890 ピクセル、高さ 470 ピクセルで、余白に 255 ピクセルが割り当てられています。シスコは、より高速なダウンロードを実現するために、イメージ サイズを小さくすることを推奨しています。

新しいログイン ブランディング ページの追加

新しいログイン ブランディング ページを追加する場合は、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [ユーザとグループ（Users and Groups）]** を選択します。
ステップ 2 [ログイン ページのブランディング（Login Page Branding）] をクリックします。
ステップ 3 [追加（Add）] をクリックします。
ステップ 4 [ドメイン ブランディング（Domain Branding）] ページで、次のフィールドに入力します。

フィールド	説明
[ドメイン名（Domain Name）] フィールド	ブランディング用ドメイン名。たとえば、imcs.xxxx.com です。 （注） ローカル マシンでドメイン名を作成するには、C:\Windows\System32\drivers\etc に移動して、ホスト ファイルで <*ipaddress*> と <*domainname*> を指定します。たとえば、10.10.10.10 imcs.xxxx.com です。
[カスタム ドメイン ロゴ（Custom Domain Logo）] チェックボックス	（オプション）ロゴを追加する場合は、このチェックボックスをオンにして、以下を実行します。 1. **[参照（Browse）]**をクリックします。 2. ロゴに移動してファイルを選択します。 3. [開く（Open）] をクリックします。

ステップ 5 [送信（Submit）] をクリックします。

ステップ 6 確認ダイアログボックスで、[OK] をクリックします。

（注） 作成したカスタマイズ済みのログイン ページを編集、削除、複製できます。

ユーザ インターフェイス設定の設定

Cisco IMC Supervisor アプリケーションをカスタマイズするには、次の手順を使用します。要件に基づいて、アプリケーション ヘッダー、管理者およびエンドユーザのポータルを変更できます。ロゴ、アプリケーション名、ログアウトなどのリンクを含むヘッダーも非表示にできます。

手順

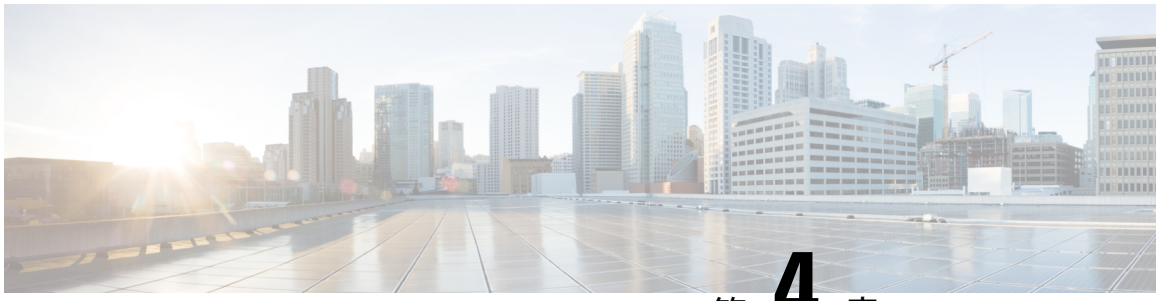
ステップ 1 **[管理（Administration）] > [ユーザ インターフェイス設定（Interface Settings）]** を選択します。

ステップ 2 [ユーザ インターフェイス設定（User Interface Settings）] ページで、次を実行します。

フィールド	説明
[ヘッダー全体の非表示] チェックボックス	ヘッダーを有効または無効にするには、このチェックボックスを使用します。
[Product Name] フィールド	ヘッダーのメイン タイトル。

フィールド	説明
[Product Name 2nd Line] フィールド	ヘッダーのサブタイトル。
[バージョン情報ダイアログの有効化（Enable About Dialog）] チェックボックス	このチェックボックスを使用して、Cisco IMC Supervisorの[バージョン情報（About）] ダイアログボックスを有効または無効にします。
管理者ポータル	
[カスタムリンク 1 のラベル（Custom Link 1 Label）] フィールド	ヘッダー バーのテキストを変更するには、このフィールドを設定します。
[カスタムリンク1のURL（Custom Link 1 URL）] フィールド	**カスタム リンク 1 ラベル**の URL を設定できます。
[カスタムリンク 2 のラベル（Custom Link 2 Label）] フィールド	ヘッダー バーのテキストを変更するには、このフィールドを設定します。
[カスタムリンク2のURL（Custom Link 1 URL）] フィールド	**カスタム リンク 2 ラベル**の URL を設定できます。
エンド ユーザ ポータル	
[カスタムリンク 1 のラベル（Custom Link 1 Label）] フィールド	ヘッダー バーのテキストを変更するには、このフィールドを設定します。
[カスタムリンク1のURL（Custom Link 1 URL）] フィールド	**カスタム リンク 1 ラベル**の URL を設定できます。
[カスタムリンク 2 のラベル（Custom Link 2 Label）] フィールド	ヘッダー バーのテキストを変更するには、このフィールドを設定します。
[カスタムリンク2のURL（Custom Link 1 URL）] フィールド	**カスタム リンク 2 ラベル**の URL を設定できます。

ステップ 3 [保存（Save）] をクリックします。



第 4 章

ユーザ、ユーザ ロール、およびグループの管理

この章は次のトピックで構成されています。

概要

Cisco IMC Supervisor は、次のシステム定義のユーザ ロールをデフォルトでサポートしています。

- [システム管理者（System Admin）]：ユーザの追加などすべての権限を持つユーザ。Cisco IMC Supervisor の管理者は、システムが提供するユーザ ロールまたはカスタム定義のユーザ ロールをユーザに割り当てることができます。また、割り当てられているロールの情報を後で確認できます。次の割り当てを行うことができます。
  - システム内でカスタム ユーザ ロールを作成し、このロールを持つ新しいユーザ アカウントを作成するか、既存のユーザにこのロールを割り当てます。

    新しいユーザ ロールを作成する場合は、そのユーザ ロールを管理者にするかオペレータにするかを指定できます。ユーザ アカウントの作成の詳細については、ユーザ アカウントの作成 （47 ページ）を参照してください。ユーザ ロールの作成方法については、ユーザ ロールの追加 （50 ページ）を参照してください。

- 既存のユーザ ロール（デフォルトのロールを含む）を変更し、そのロールに関連付けられているユーザのメニュー設定と読み取り/書き込み権限を変更する。

  ロールのメニュー設定と権限を変更する手順は、ユーザ ロールを作成する手順と同じです。

- [グループ管理者（Group Admin）]：すべての権限を持つユーザ。システム定義のユーザ グループ [デフォルト グループ（Default Group）] は、Cisco IMC Supervisorではデフォルトで使用できます。グループ管理者として、ユーザアカウントを作成してこのグループに割り当てたり、作成済みのグループにユーザアカウントを割り当てたりできます。ユーザは複数の設定グループに属することができます。ただし、最後にユーザが追加されたグループは、ユーザのデフォルトのプライマリ グループとして設定されます。
- [オペレータ（Operator）]：システム管理者のロール タイプは admin であるため、アクセス制限（メニュー設定とユーザ権限）の任意の組み合せを使用して、既存のオペレータ（Operator）ロールを必要に応じて変更できます。デフォルトでは、以下のメニュー設定とユーザ権限がオペレータ（Operator）に割り当てられます。

メニュー設定	ユーザの権限
[システム（Systems）]： • [インベントリと障害のステータス（Inventory and Fault Status）] • 物理アカウント • ファームウェア管理 • サーバ診断	• [読み取り：物理コンピューティング（Read - Physical Computing）] • [書き込み：物理コンピューティング（Write - Physical Computing）] • [読み取り：システム管理者（Read - System Admin）] • [読み取り：ユーザ（Read - Users）] • [読み取り：タグ ライブラリの読み取り（Read - Read Tag Library）] • [書き込み：タグ ライブラリの書き込み（Write - Write Tag Library）] • [読み取り：オーケストレーション（Read - Orchestration）] • [書き込み：オーケストレーション（Write - Orchestration）]
ポリシー: • スケジュールの管理 • APIとオーケストレーション	
[管理（Administration）] • ユーザとグループ • 統合	

（注） レポート（[SCP ユーザ設定（SCP User Configuration）]、[認証の環境設定（Authentication Preferences）]、[パスワード ポリシー（Password Policy）] など）は、[ユーザとグループ（Users and Groups）] でオペレータ（Operator）ロールに対して有効になっています。

ユーザ アカウントの作成

（注） [ユーザの編集（Edit User）] ダイアログボックスの [ユーザ ロール（User Role）] および [ログイン名（Login Name）] フィールドは編集できません。

手順

ステップ 1 **[管理（Administration）] > [ユーザとグループ（Users and Groups）]** を選択します。

ステップ 2 [Users] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [ユーザの追加（Add User）] ページで、次のフィールドに入力します。

フィールド	説明
[ユーザロール（User Role）] ドロップダウンリスト	[グループ管理者（Group Admin）]、[オペレータ（Operator）]、[システム管理者（System Admin）] のいずれかを選択します。
[ユーザ グループ] ドロップダウンリスト	アクセスを許可するグループを選択します。既存のグループを選択したり、新しいグループを追加したりできます。 （注） このフィールドは、ユーザ ロールとして [グループ管理者（Group Admin)] を選択している場合にのみ表示されます。
[ログイン名（Login Name）] フィールド	ユーザのログイン名。
[パスワード（Password）] フィールド	ユーザのパスワード。Lightweight Directory Access Protocol（LDAP）認証が設定されているユーザの場合、パスワードはローカル サーバではなく、LDAP サーバでのみ検証されます。
[パスワードの確認（Confirm Password）] フィールド	前のフィールドと同じパスワードを入力します。
[ユーザの連絡先電子メール（User Contact Email）] フィールド	電子メール アドレスを入力します。
[名（First Name）] フィールド	（オプション）ユーザの名。

フィールド	説明
[姓（Last Name）] フィールド	（オプション）ユーザの姓。
[電話（Phone）] フィールド	（オプション）ユーザの電話番号。
[アドレス（Address）] フィールド	（オプション）ユーザの住所。

ステップ 5 [追加（Add）] をクリックします。

ステップ 6 [OK] をクリックします。

オンライン ユーザの表示

現在オンラインであるユーザを表示するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [ユーザとグループ（Users and Groups）]** を選択します。

ステップ 2 [現在のオンライン ユーザ（Current Online Users）] をクリックします。
現在 Cisco IMC Supervisor にログインしているユーザのユーザ名、IP アドレス、セッション開始時刻などの詳細を確認できます。

ユーザの最近のログイン履歴の確認

システム管理者は、すべてのユーザの最近のログイン履歴を確認できます。すべてのログイン試行操作について次の詳細情報が記録されます。

- [ログイン名（Login Name）]
- リモート アドレス（Remote Address）
- クライアント詳細
- クライアント タイプ
- Authentication Status
- コメント
- アクセス日

手順

ステップ 1 **[管理（Administration）] > [ユーザとグループ（Users and Groups）]** を選択します。

ステップ 2 [ユーザとグループ（Users and Groups）] ページで [すべてのユーザのログイン履歴（All Users Login History）] をクリックします。

ステップ 3 画面に表示される情報を確認します。

ユーザのセッション制限の設定

システム上でユーザが開始できる REST API 要求とユーザ インターフェイスのセッションの数を設定できます。

手順

ステップ 1 **[管理（Administration）] > [ユーザとグループ（Users and Groups）]** を選択します。

ステップ 2 [ユーザとグループ（Users and Groups）] ページで [セッション管理（Session Management）] をクリックします。

ステップ 3 [セッション管理（Session Management）] 画面で、次を含む必須フィールドに入力します。

名前	説明
[ユーザあたりの同時セッションの最大数（Maximum Concurrent Sessions Per User）] フィールド	ユーザごとにサポートされる同時GUIセッションの最大数。1 ～ 128 の数値を入力します。 デフォルト値は 16 です。
[ユーザあたりの同時 REST API 要求の最大数（Maximum Concurrent REST API Requests Per User）] フィールド	ユーザごとにサポートされる同時 REST API 要求の最大数。1 ～ 256 の範囲内の数を入力してください。 デフォルト値は 128 です。

ステップ 4 [送信（Submit）] をクリックします。

次のタスク

ユーザがこの画面で指定した制限値を超える GUI セッションまたは REST API 要求を開始すると、[システム メッセージ（System Messages）] 画面にエラー メッセージが表示されます。このシナリオでは、ユーザが自分のセッションや API 要求をクリアするか、または管理者がシェルユーティリティを使用してユーザのセッションや要求をクリアします。詳細については、『*Cisco IMC Supervisor Shell Guide*』を参照してください。

ユーザ ロールの追加

新しくインストールされた Cisco IMC Supervisor アプライアンスでは、デフォルトで [グループ管理者（GroupAdmin）] と [オペレータ（Operator）] ロールが使用可能になっています。グループ管理者のロール タイプは admin であるため、アクセス制限（メニュー設定とユーザ権限）の任意の組み合せを使用して、既存のオペレータ（Operator）ロールを必要に応じて変更できます。同様に、次の手順で新しいロールを作成し、ユーザを割り当てることができます。

手順

ステップ 1 **[管理（Administration）] > [システム（System）]** を選択します。

ステップ 2 [User Roles] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [ユーザ ロールの追加（Add User Role）] ページの [ユーザ ロール（User Role）] ペインで、次のフィールドに入力します。

フィールド	説明
[ユーザ ロール（User Role）] フィールド	ユーザ ロールの記述名。
[ロール タイプ（Role Type）] ドロップダウンリスト	[管理者（Admin）] を選択します。
[説明（Description）] フィールド	（オプション）ユーザ ロールの説明。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [メニュー設定（Menu Settings）] ペインで、必要なメニュー オプションを選択します。

メニュー オプションを選択するには、メニュー設定フィールドのチェックボックスをオンにします。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 [ユーザの権限（User Permissions））] ペインで、必要な操作を選択します。

操作を選択するには、その操作のチェックボックスをオンにします。

ステップ 9 [送信（Submit）] をクリックします。

（注） ユーザ ロールの編集、複製、または削除も実行できます。

ユーザ グループの追加

新しいユーザ グループを追加する場合は、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [ユーザとグループ（Users and Groups）]** を選択します。

ステップ 2 [ユーザ グループ（User Groups）] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [ユーザ グループの追加（Add User Group）] ページで、次のフィールドに入力します。

フィールド	説明
[名前（Name）] フィールド	ユーザ グループの名前。
[説明（Description）] フィールド	（オプション）ユーザ グループの説明。
[コード（Code）] フィールド	（オプション）グループの短い名前またはコード名。
[コスト センター（Cost Center）] フィールド	コストセンターの名前または番号（必要な場合）。グループに関連付けられているコスト センターの名前または番号です。
[連絡先の電子メール（Contact Email）] フィールド	この電子メール アドレスは、必要に応じてサービス リクエストとリクエスト承認のステータスをグループ所有者に通知するために使用されます。
[名（First Name）] フィールド	（オプション）連絡先の名。
[姓（Last Name）] フィールド	（オプション）連絡先の姓。
[電話（Phone）] フィールド	（オプション）連絡先の電話番号。
[アドレス（Address）] フィールド	（オプション）連絡先の住所。
[グループ共有ポリシー（Group Share Policy）] ドロップダウンリスト	（オプション）このグループ内のユーザのグループ共有ポリシーを選択します。 このドロップダウンリストには、作成済みのグループ共有ポリシーが表示されます。

フィールド	説明
[ユーザへのリソース割り当てを許可（Allow Resource Assignment To Users）] チェックボックス	（オプション）オンにすると、このグループのユーザにリソースが割り当てられ、それらのリソースをユーザが所有できます。またこれらのユーザは、グループに属しているリソースを表示できます。ただし、ユーザ間でリソースを共有することはできません。

ステップ 5 [追加（Add）] をクリックします。

ステップ 6 [OK] をクリックします。

（注） これらのユーザ グループを選択し、それらを表示、編集、削除、有効または無効にすることにより管理できます。[ユーザ グループ（User Groups）] タブからタグを管理することもできます。

ユーザ グループのブランディング

ユーザ グループの Cisco IMC Supervisor アプリケーションをカスタマイズするには、次の手順を実行します。選択したグループに属するユーザがシステムにログインすると、カスタマイズされたページが表示されます。

手順

ステップ 1 **[管理（Administration）] > [ユーザとグループ（Users and Groups）]** を選択します。

ステップ 2 [ユーザ グループ（User Groups）] をクリックします。

ステップ 3 ユーザ グループを選択します。

ステップ 4 [ブランディング（Branding）] をクリックします。

ステップ 5 [グループ ブランディング（Group Branding）] ページで、次のフィールドに入力します。

フィールド	説明
[ロゴ イメージ（Logo Image）] チェックボックス	オンにすると、ロゴがアプリケーションの左上隅に表示されます。
[アプリケーション ラベル（Application Labels）] チェックボックス	オンにすると、アプリケーションのラベルがアプリケーション上部のヘッダー セクションに表示されます。

フィールド	説明
[ログアウト時のURL転送（URL Forwarding on Logout）] チェックボックス	オンにすると、ユーザはログアウト時に指定された URL に転送されます。
[カスタムリンク（Custom Links）] チェックボックス	オンにすると、カスタムリンクがアプリケーションの右上隅に表示されます。

ステップ 6 [送信（Submit）] をクリックします。

グループ共有ポリシー

グループの共有ポリシーによって、ユーザはリソースと、他のユーザと共有するものを高度に制御できるようになります。このポリシーでは、ユーザは現在自分だけに割り当てられているリソースを表示し、またユーザが属するすべてのグループに割り当てられているリソースを表示できます。

グループを作成する場合は、グループの共有ポリシーを定義して、どのグループが読み取り/書き込み権限を持つかを決定できます。後にユーザがこのグループに追加されると、リソースに対するそのユーザのアクセス権は、グループに適用されるグループの共有ポリシーによって決定されます。

グループ共有ポリシーの追加

ポリシーを追加してユーザ グループと共有する場合は、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [ユーザとグループ（Users and Groups）]** を選択します。

ステップ 2 [グループ共有ポリシー（Group Share Policy）] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [グループ共有ポリシーの追加（Add Group Share Policy）] ページで、次のフィールドに入力します。

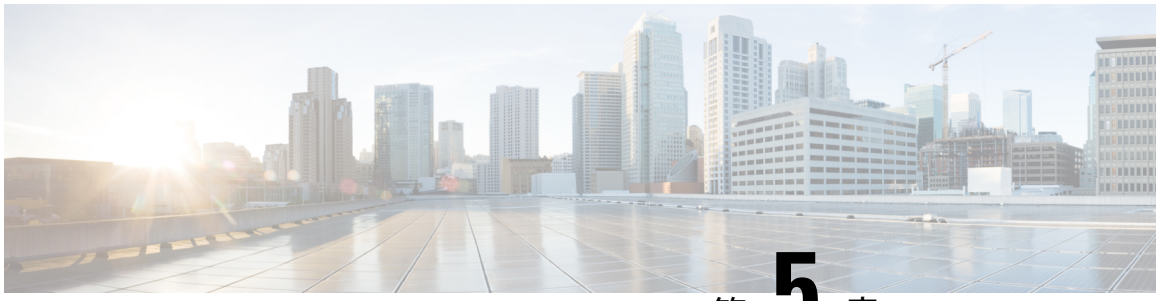
フィールド	説明
[ポリシー名（Policy Name）] フィールド	グループ共有ポリシーの名前。

フィールド	説明
[ポリシーの説明（Policy Description）] フィールド	ポリシーの説明。
[グループの選択（Select Groups）] ドロップダウンリスト	作成したポリシーを共有するグループを選択します。

ステップ 5 [送信（Submit）] をクリックします。

ステップ 6 [送信結果（Submit Result） ダイアログボックスで [OK] をクリックします。

（注） 既存のポリシーを選択して、表示、編集、削除、複製することもできます。



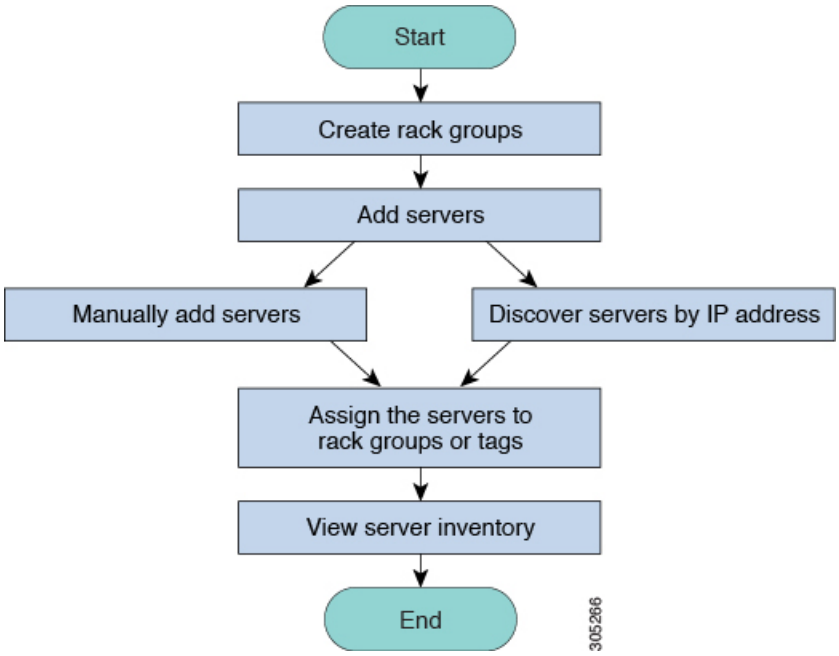
第 5 章

サーバ検出、ラック グループ、およびラック アカウントの管理

この章は次のトピックで構成されています。

概要

次の図は、Cisco IMC Supervisorでのグループの管理、ラック アカウントおよびサーバ検出のワークフローを示します。理想的には、ラック グループを作成し、サーバをこれらのラック グループに追加します。サーバを手動で追加するか、またはサーバを検出することができます。これらのサーバの詳細インベントリを確認できます。



使用例：初めて Cisco IMC Supervisor をインストールする場合は、何も事前設定されていないため、環境をセットアップする必要があります。管理の必要なシステムが世界中で何百もある可能性があります。これらのサーバを Cisco IMC Supervisor に導入するには、手動で追加するか、またはIPアドレスによって検出します。その前に、組織の要件に基づいて、これらのサーバの論理的なフィルタ処理とタグ付けについて検討できます。たとえば、サーバを地域、建物番号、オペレーティング システムなどでグループ化できます。タグ管理によって、Cisco IMC Supervisorに導入されるサーバをより細かくグループ化できます。たとえば、Windows、Linux などを含むサーバにタグを追加して、オペレーティング システムのラック グループでサーバをグループ化できます。また、既存のサーバにタグをオンザフライで追加する柔軟性もあります。

ラック グループまたはタグに名前を付ける決まった方法はありません。必要に応じて自由に名前を決めることができます。ラック グループおよびタグの名前は相互互換的に使用できます。たとえば、Windows、Linux などという名前のラック グループを作成し、オペレーティング システムのタグ名でそれらのグループをタグ付けできます。

サーバの検出およびインポート

ラック マウント サーバを自動的に検出して Cisco IMC Supervisor にインポートできます。以降のセクションでは、自動ディスカバリ プロファイルの設定、自動検出の実行、自動検出されたサーバのインポートなどについて説明します。

自動検出プロファイルの設定

Cisco IMC Supervisor がデバイスを検出するための基盤となる自動検出プロファイルを設定する必要があります。Cisco IMC Supervisor に設定できるプロファイル数に制限はありません。

自動検出プロファイルを追加または編集する場合は、次の手順を実行します。

手順

ステップ 1 **[システム（Systems）] > [物理アカウント（Physical Accounts）]** を選択します。

ステップ 2 [検出プロファイル（Discovery Profiles）] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [検出プロファイルの追加（Add Discovery Profile）] ページで、次のフィールドに入力します。

フィールド	説明
[プロファイル名（Profile Name）] フィールド	プロファイルの記述名。
[検索条件（Search Criteria）] ドロップダウンリスト	このドロップダウンリストから [IP アドレス範囲（IP Address Range）]、[サブネットマスク範囲（Subnet Mask Range）]、[IP アドレスの CSV ファイル（IP Address CSV File）]、または [IP アドレス リスト（IP Address List）] を選択します。
[開始 IP（Starting IP）] フィールド	有効な IP アドレス
[終了 IP（Ending IP）] フィールド	有効な IP アドレス
[クレデンシャル ポリシーの使用（Use Credential Policy）] チェックボックスがオンの場合	
[クレデンシャルポリシー（Credential Policy）] ドロップダウンリスト	ポリシーをドロップダウンリストから選択するか、[+] アイコンをクリックして新しいポリシーを作成します。新しいポリシーの作成については、クレデンシャル ポリシーの作成 （104 ページ）を参照してください。
[クレデンシャル ポリシーの使用（Use Credential Policy）] チェックボックスがオフの場合	
[ユーザ名（User Name）] フィールド	サーバのログイン名。
[パスワード（Password）] フィールド	サーバのログイン パスワード **重要** パスワードには+などの特殊文字を使用しないでください。
[プロトコル（Protocol）] ドロップダウンリスト	リストから [https] または [http] を選択します。
[ポート（Port）] フィールド	ポート番号を入力します。

フィールド	説明
次のフィールドは、[検索条件（Search Criteria）] に [IP アドレス範囲（IP Address Range）]、[サブネット マスク範囲（Subnet Mask Range）] 、および [IP アドレス リスト（IP Address List）] を選択した場合にのみ使用できます。 （注） [IP アドレスの CSV ファイル（IP Address CSV File）] を選択した場合は、CSV ファイルに次の形式でこれらのフィールドを指定できます。[ファイルテンプレート（File Template）] をクリックすると、サンプル CSV ファイルを使用できます。見出しなしで CSV ファイルの最初の行からエントリを追加する必要があります。 • <*ip*> • （オプション）<説明> • （オプション） <ロケーション> • （オプション）<連絡先> • （オプション） <ラック グループ> • （オプション）<タグ名:タグ値>;<タグ名:タグ値> （注） • [ラック グループ（Rack Group）] と [タグ（Tags）] には、既存の値または新しい値を指定できます。これらのフィールドの指定はオプションです。CSV ファイルで [ラック グループ（Rack Group）] の値を指定しない場合、[デフォルト グループ（Default Group）] が使用されます。 • 現在の Cisco IMC Supervisor バージョンにアップグレードする場合は、既存の CSV ファイルを、[ファイルを選択（Select a File）] オプションを使用して新しい形式で作成した CSV ファイルに置き換えます。 • タグのタイプは **STRING** タイプのみです。	
[説明（Description）] フィールド	サーバの説明を入力します。
[連絡先（Contact）] フィールド	サーバの連絡先の詳細を入力します。
[ロケーション（Location）] フィールド	サーバのアドレスを入力します。
[ラック グループの選択（Select Rack Group）] ドロップダウン リストまたは [+] アイコン	ラック グループを選択するか、ラック グループを作成します。

ステップ 5 [送信（Submit）] をクリックします。

（注） プロファイルを変更、削除、表示することもできます。これらの操作を実行するには、[編集（Edit）]、[クリア（Clear）]、[削除（Delete）]、または [表示（View）] をクリックします。

自動検出の実行

ラックマウント サーバを自動的に検出して Cisco IMC Supervisor にインポートする場合は、次の手順を実行します。

始める前に

Cisco IMC Supervisor がデバイスを検出するための基盤となるプロファイルを設定する必要があります。

手順

ステップ 1 **[システム（Systems）] > [物理アカウント（Physical Accounts）]** を選択します。

ステップ 2 [デバイスの検出（Discover Devices）] をクリックします。

ステップ 3 [検出（Discover）] をクリックします。

ステップ 4 [デバイスの検出（Discover Devices）] ページで、次のフィールドに入力します。

フィールド	説明
[プロファイルの選択（Select Profile）] ドロップダウンリスト	[選択（Select）] をクリックし、検出するプロファイルを選択します。検出するすべてのプロファイルのチェックボックスをオンにします。
[後でスケジュール（Schedule Later）] チェックボックス	このチェックボックスをオンにして、後でサーバを自動検出するための既存のスケジュールを選択するか、または [+] をクリックして新しいスケジュールを作成します。スケジュールの作成の詳細については、スケジュールの作成 （183 ページ） を参照してください。**[ポリシー（Policies）] > [スケジュールの管理（Manage Schedules）]** の順に移動して、スケジュールを選択し、[スケジュール タスクを表示する（View Scheduled Tasks）] をクリックしてスケジュールされたタスクを表示するか、または [スケジュール タスクの削除（Remove Scheduled Tasks）] をクリックしてスケジュールされたタスクを削除できます。

フィールド	説明
[スケジュール（Schedule(s)）] ドロップダウンリスト	[後でスケジュール（Schedule Later）] チェックボックスを選択している場合、ドロップダウンリストから作成したスケジュールを選択できます。 （注） また、このダイアログボックスから新しいスケジュールを作成することもできます。

ステップ 5 [送信（Submit）] をクリックします。

サーバのインポート

自動検出を使用してサーバをインポートする場合は、次の手順を実行します。

始める前に

- Cisco IMC Supervisor がデバイスを検出するための基盤となるプロファイルを設定する必要があります。
- すでに自動検出を実行済みです。

手順

ステップ 1 **[システム（Systems）] > [物理アカウント（Physical Accounts）]** を選択します。

ステップ 2 [デバイスの検出（Discover Devices）] をクリックします。

ステップ 3 [インポート（Import）] をクリックします。

ステップ 4 [検出されたデバイスのインポート（Import Discovered Device）] ページで、次のフィールドに入力します。

フィールド	説明
[デバイスの選択（Select Device(s)）] フィールド	[選択（Select）] をクリックしてインポートするデバイスを選択します。インポートするすべてのサーバのチェックボックスをオンにします。 （注） 特定のラック アカウントの [インポートのステータス（Import Status）] が [インポート済み（imported）] である場合、ステータスは [インポート済み（imported）] になりますが、そのラック アカウントはインポート対象として表示されません。
ユーザ プレフィックス（User Prefix）	ユーザのプレフィックスを入力します。

ステップ 5 [送信（Submit）] をクリックします。

（注） 前のインポート プロセスが完了するのを待たずに、検出されたデバイスを複数回インポートすることができます。

検出されたデバイスのプロパティの設定

検出されたデバイスのプロパティを設定するには、次の手順を実行します。

始める前に

Cisco IMC Supervisor がデバイスを検出するための基盤となるプロファイルを設定する必要があります。

手順

ステップ 1 **[システム（Systems）] > [物理アカウント（Physical Accounts）]** を選択します。
ステップ 2 [デバイスの検出（Discover Devices）] をクリックします。
ステップ 3 [検出されたデバイス（Discovered Devices）)] テーブルでデバイスを選択します。
ステップ 4 [プロパティの設定（Set Properties）] をクリックします。
ステップ 5 [プロパティの設定（Set Properties）] ページで、次のフィールドに入力します。

フィールド	説明
[説明（Description）] フィールド	サーバの説明を入力します。

フィールド	説明
[連絡先（Contact）] フィールド	サーバの連絡先の詳細を入力します。
[ロケーション（Location）] フィールド	サーバのアドレスを入力します。
[ラック グループの選択（Select Rack Group）] ドロップダウンリストまたは [+] アイコン	ラック グループを選択するか、ラック グループを作成します。

ステップ 6 [送信（Submit）] をクリックします。

ラック グループの追加

新しいラック グループを Cisco IMC Supervisor に追加する場合は、次の手順を実行します。デフォルトで、システム定義グループ [デフォルト グループ（Default Group）] を使用できます。

始める前に

初めてログインする場合は、Cisco IMC Supervisor用にライセンスが更新されていることを確認します。ライセンスをアップグレードするには、ライセンスの更新 （17 ページ）を参照してください。

手順

ステップ 1 **[システム（Systems）] > [物理アカウント（Physical Accounts）]** を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 [ラックグループの作成（Create Rack Group）] ページで、次のフィールドに入力します。

フィールド	説明
[グループ名（Group Name）]フィールド	ラック グループの記述名。
[説明（Description）] フィールド	（オプション）ラック グループの説明。

ステップ 4 [作成（Create）] をクリックします。

次のタスク

ラック グループに 1 つ以上のラック アカウントを追加します。

ラック アカウントの追加

作成済みの既存のラック グループにラックマウント サーバを追加することも、新しいラック グループを作成してラックマウントサーバを追加することもできます。アカウントを追加したら、Cisco IMC Supervisorを使用してそのサーバを管理することができます。

既存のラック グループに新しいラックマウント サーバを追加する場合は、次の手順を実行します。

始める前に

- 初めてログインする場合は、Cisco IMC Supervisor用にライセンスがアップグレードされていることを確認します。ライセンスをアップグレードするには、ライセンスの更新 （17 ページ）を参照してください。
- ラック グループが存在することを確認します。

（注） システム提供のデフォルト グループまたは作成済みのラック グループの下にラック アカウントを追加できます。

- Cisco IMC Supervisor で XML API が有効になっていることを確認します。これによって、Cisco IMC Supervisorからラックマウント サーバを追加して管理できるようになります。

手順

ステップ 1 **[システム（Systems）] > [物理アカウント（Physical Accounts）]** を選択します。

ステップ 2 [ラック アカウント（Rack Accounts）] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [アカウントの作成（Create Account）] ページで、次のフィールドに入力します。

フィールド	説明
[アカウント名（Account Name）] フィールド	ラック アカウントの記述名。
[サーバ IP/ホスト名（Server IP or Hostname）] フィールド	ラックマウント サーバの IP アドレス、または Cisco UCS S3260 高密度ストレージ ラック サーバの仮想管理 IP アドレス。 （注） 完全修飾ドメイン名（FQDN）またはホスト名も入力できます。
[説明（Description）] フィールド	（オプション）ラック アカウントの説明。

フィールド	説明
[クレデンシャルポリシーの使用（Use Credential Policy）] チェック ボックス	（オプション）すでにクレデンシャルポリシーを作成している場合は、このチェックボックスをオンにして、ドロップダウンリストからポリシーを選択します。
[クレデンシャル ポリシーの使用（Use Credential Policy）] チェックボックスがオンの場合	
[クレデンシャルポリシー（Credential Policy）] ドロップダウンリスト	ドロップダウンリストからポリシーを選択します。
[クレデンシャル ポリシーの使用（Use Credential Policy）] チェックボックスがオフの場合	
[ユーザ名（User Name）] フィールド	ラックマウント サーバのログイン ID。
[パスワード（Password）] フィールド	ラックマウント サーバのログイン ID のパスワード。
[プロトコル（Protocol）] ドロップダウンリスト	リストから [https] または [http] を選択します。
[ポート（Port）] フィールド	選択したプロトコルに関連付けられたポート番号。
[ラック グループ（Rack Group）] ドロップダウンリストまたは [+] アイコン	リストからラック グループを選択するか、[+] をクリックしてラック グループを作成します。 ラック グループの作成の詳細については、ラック グループの追加 （62 ページ）を参照してください。
[連絡先（Contact）] フィールド	（オプション）アカウントの連絡先電子メール アドレス。
[ロケーション（Location）] フィールド	（オプション）アカウントの場所。

ステップ 5 [送信（Submit）] をクリックします。

（注）
- 前に実行されたラック アカウントを作成するコマンドが完了するまで待つことなく、ラック アカウントを再び作成できます。
- インベントリの編集、削除、収集、ラック サーバへのラック アカウントの割り当て、アカウント接続のテストを行うことができます。
- 複数のラック アカウントを選択して削除できます。インベントリ収集、障害状況の収集、ファームウェア アップグレード、ポリシーまたはプロファイルの適用、サーバ診断のタスクがアカウントのいずれかで実行されている場合は、アカウントを削除できません。

次のタスク

ラック サーバ接続をテストします。アカウント接続のテスト （66 ページ） を参照してください。

ラック アカウントまたはラック グループのインベントリの収集

ラック アカウントまたはラック グループのインベントリを収集するには、次の手順を実行します。

始める前に

ラック アカウントまたはラック グループがラック アカウントの下にすでに作成されています。

手順

ステップ 1 **[システム（Systems）] > [物理アカウント（Physical Accounts）]** を選択します。
ステップ 2 [ラック アカウント（Rack Accounts）] をクリックします。
ステップ 3 ラック アカウントのリストが表示されます。
ステップ 4 [インベントリ（Inventory）] をクリックします。
ステップ 5 [アカウントのインベントリ収集（Collect Inventory for Account(s)）] ページで、[ラック グループ（Rack Group）] または [ラック アカウント（Rack Account）] を選択して、ドロップダウン リストからサーバを選択します。
ステップ 6 [選択（Select）] をクリックしてサーバを選択します。
ステップ 7 [選択（Select）] ダイアログボックスで、サーバを選択して [選択（Select）] をクリックします。

（注） 選択対象となるラック グループまたはラック アカウントをフィルタリングするには、レポート上部にある検索バーを使用できます。

ステップ 8 [送信（Submit）] をクリックします。

ラック グループへのラック アカウントの割り当て

ラック グループにサーバを割り当てるには、次の手順を実行します。

始める前に

ラック アカウントまたはサーバは、[ラック アカウント（Rack Accounts）] ですでに作成されています。

手順

ステップ 1 **[システム（Systems）] > [物理アカウント（Physical Accounts）]** を選択します。

ステップ 2 [ラック アカウント（Rack Accounts）] をクリックします。

ステップ 3 サーバのリストが表示されます。

ステップ 4 1 つ以上のサーバを選択して、[ラック グループの割り当て（Assign Rack Group）] をクリックします。

ステップ 5 [ラック グループの割り当て（Assign Rack Group）] ページで、サーバを割り当てるラック グループを選択します。

（注） ラック グループを作成するには、[選択したサーバへのラックグループの割り当て（Assign Rack Group to selected server(s)）] ドロップダウンリストの横にある [+] アイコンをクリックします。

ステップ 6 [送信（Submit）] をクリックします。

アカウント接続のテスト

1 つ以上のラック アカウントの接続をテストする場合は、次の手順を実行します。Cisco IMC Supervisor に追加されたすべての新しいアカウントに対して、この手順を実行することを推奨します。

手順

ステップ 1 **[システム（Systems）] > [物理アカウント（Physical Accounts）]** を選択します。

ステップ 2 [ラック アカウント（Rack Accounts）] をクリックします。

ステップ 3 ラック アカウントのリストから、接続をテストするアカウントを選択します。

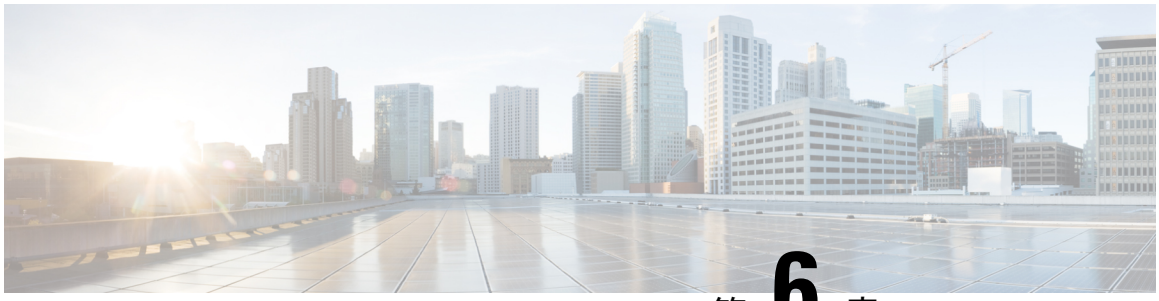
ステップ 4 [テスト接続（Test Connection）] をクリックします。

（注） リストから 1 つ以上のラック アカウントを選択するまでは、[接続のテスト（Test Connection）] ボタンは表示されません。

ステップ 5 [接続のテスト（Test Connection）] ダイアログボックスで、[送信（Submit）] をクリックします。

接続のテストには数分かかる場合があります。

接続ステータスと、成功または失敗の理由が [ラックアカウント（Rack Accounts）] ページに表示されます。



第 6 章

インベントリ データおよび障害の表示

この章は次のトピックで構成されています。

ラックマウント サーバの詳細の表示

ラックマウント サーバの詳細（サーバで使用されているメモリ、CPU、PSU など）を表示する場合は、次の手順を実行します。

（注） [ラック グループ（Rack Groups）] を選択し、ラックマウント サーバの詳細を表示する手順を実行することもできます。

始める前に

サーバがラック アカウントとしてラック グループに追加されていることを確認します。

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [ラック グループ（Rack Groups）] を展開し、サーバが含まれているラック グループを選択します。

ステップ 3 選択したラック グループのページで、[ラック サーバ（Rack Servers）] をクリックします。

ステップ 4 リストでサーバをダブルクリックしてその詳細を確認するか、リストでサーバを選択し、右端の下矢印をクリックして [詳細の表示（View Details）] を選択します。

（注） リストからサーバを選択するまでは、右端に下向き矢印は表示されません。

ラックマウント サーバに関する次の詳細が表示されます。

タブ	説明
要約	ラック アカウントの概要。
CPU	サーバで使用されている CPU の詳細。
メモリ	サーバで使用されているメモリの詳細。
PSUs	サーバで使用されている電源モジュールの詳細。 （注） Cisco UCS S3260 高密度ストレージ ラック サーバには適用されません。
PCIアダプタ	サーバで使用されている PCI アダプタの詳細。
VICアダプタ	サーバで使用されている VIC アダプタの詳細。 リストされている VIC アダプタのいずれかを選択して [詳細の表示（View Details）] をクリックすると、[外部イーサネット インターフェイス（External Ethernet Interfaces）] と [VM FEX（VM FEXs）] の情報が表示されます。
ネットワークアダプタ	サーバで使用されているネットワーク アダプタの詳細。 リストされているネットワーク アダプタのいずれかを選択して [詳細の表示（View Details）] をクリックすると、[外部イーサネット インターフェイス（External Ethernet Interfaces）] の情報が表示されます。
ストレージアダプタ	サーバで使用されているストレージ アダプタの詳細。 リストされているストレージ アダプタのいずれかを選択して [詳細の表示（View Details）] をクリックすると、[コントローラ情報（Controller Info）]、[物理ドライブ（Physical Drives）]、[仮想ドライブ（Virtual Drives）] などの情報が表示されます。SSD のスマート情報の表示 （72 ページ）を参照してください。.
FlexFlashアダプタ	サーバで使用されている FlexFlash アダプタの詳細。 リストされている FlexFlash アダプタのいずれかを選択して [詳細の表示（View Details）] をクリックすると、[コントローラ情報（Controller Info）]、[物理ドライブ（Physical Drives）] などの情報が表示されます。 Cisco IMC Supervisor を旧バージョンからアップグレードしている場合、FlexFlash の詳細をレポートに表示するには [システム（Systems）] > [物理アカウント（Physical Accounts）] > [ラック アカウント（Rack Accounts）] > [インベントリ（Inventory）] に移動してインベントリを実行するか、定期的なインベントリが実行されるのを待つ必要があります。 （注） Cisco UCS S3260 高密度ストレージ ラック サーバには適用されません。

タブ	説明
通信	HTTP、HTTPS、SSH、IPMI Over LAN、NTP、SNMP などのプロトコルに関する情報。
リモート プレゼンス	VKVM、Serial Over LAN、および vMedia の詳細。
障害	サーバで記録された障害の詳細。
ユーザ数	**デフォルト グループ**のユーザに関する詳細。ユーザ ポリシーおよびパスワードの有効期限ポリシーの作成時に設定した強力なパスワード ポリシーとパスワード有効期限の詳細も確認できます。ユーザ ポリシー （134 ページ）およびパスワードの有効期限ポリシー （125 ページ）を参照してください。 （注） Cisco UCS S3260 高密度ストレージ ラック サーバには適用されません。
Cisco IMC ログ	サーバの Cisco IMC ログの詳細。 （注） Cisco UCS S3260 高密度ストレージ ラック サーバには適用されません。
システム イベント ログ	サーバ ログの詳細。 （注） Cisco UCS S3260 高密度ストレージ ラック サーバには適用されません。
TPM	TPM インベントリに関する情報。
BIOS	サーバの BIOS 設定とブート順序の詳細。 サーバを選択し、[BIOS 設定の表示（View BIOS Settings）]、[ブート設定の表示（View Boot Settings）]、[ブート順序の表示（View Boot Order）] のいずれかをクリックします。
障害履歴	サーバで発生した障害の履歴情報。
テクニカル サポート	ファイル名、宛先タイプ、アップロードのステータスなどのテクニカル サポート ログ ファイルに関する詳細は、[テクニカル サポート（Tech Support）] テーブルに表示されます。 リモート サーバまたはローカルの Cisco IMC Supervisor アプライアンスへテクニカル サポート ログ ファイルをエクスポートするオプションがあります。エクスポートの詳細については、リモート サーバへのテクニカル サポート データのエクスポート （97 ページ）を参照してください。 （注） Cisco UCS S3260 高密度ストレージ ラック サーバには適用されません。

タブ	説明
ホストイメージ	イメージの詳細（名前、サイズ、MD5チェックサム、最終変更時刻、イメージがマップされているかどうかなど）が表示されます。イメージを選択し、[イメージのマッピング（Map Image）]、[イメージのマップ解除（Unmap Image）]、または[イメージの削除（Delete Image）]を選択して、それぞれのアクションを実行できます。 （注） ホスト イメージ マッピングは、E シリーズ サーバにのみ適用できます。
関連付けられているハードウェアプロファイル	ハードウェア プロファイルに関連付けられているポリシーの詳細。

ステップ 5 右端の [戻る（Back）] ボタンをクリックして前のウィンドウに戻ります。

SSD のスマート情報の表示

ストレージ コントローラの下にソリッド ステート ドライブ（SSD）のスマート情報を表示するには、次の手順を実行します。

始める前に

サーバがラック アカウントとしてラック グループに追加されていることを確認します。

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [ラック グループ（Rack Groups）] を展開し、SSD ドライブが含まれているラック グループを選択します。

ステップ 3 選択したラック グループのページで、[ラック サーバ（Rack Servers）] をクリックします。

（注） また、[ラック グループ（Rack Groups）] でサブ グループを選択することもできます。

ステップ 4 リストに SSD が含まれているサーバをダブルクリックします。

ステップ 5 [ラック サーバ（Rack Server）] ページで [ストレージ アダプタ（Storage Adapters）] をクリックします。

ステップ 6 SSD ドライブをダブルクリックし、[コントローラ情報（Controller Info）] をクリックします。

次のコントローラ設定を使用できます。

- **SMART でのコピーバックの有効化（Enable Copyback on SMART）**

- **SMART エラーでの SSD へのコピーバックの有効化（Enable Copyback to SSD on SMART Error）**

ステップ 7 SSD ドライブをダブルクリックし、[物理ドライブ（Physical Drives）] をクリックします。

ステップ 8 SSD 物理ドライブをダブルクリックし、[スマート情報の表示（View Smart Information）] をクリックします。

SSD ドライブに関する次の詳細が表示されます。

タブ	説明
[電源再投入カウント（Power Cycle Count）] フィールド	ドライブが製造されてから現在までに電源の再投入が行われた回数。
[電源オン時間（Power on Hours）] フィールド	ドライブが「電源オン」モードになっている合計時間数。
[残量（パーセンテージ）（Percentage Life Left）] フィールド	半導体ドライブ（SSD）のライフタイムで残っている書き込みサイクルの回数。たとえば、ライフタイムを通して 100 回の書き込みサイクルに対応できる SSD で 15 回の書き込みが行われた場合、ドライブのライフタイムの残りのパーセンテージは85%となります。パーセンテージの各範囲は異なる色で表されます。たとえば、75% ～ 100% は緑、1% ～ 25% は赤で表されます。 （注） [コントローラ情報（Controller Info）] の下の [SD - 残量（パーセンテージ）（SSD - Percentage Life Left）] に、SSD の棒グラフが追加されます。
[消耗ステータス（日数）（Wear Status in Days）] フィールド	SSD で書き込みサイクルが行われた日数。 SSD ベンダーが提示する 1 日あたりの SSD 書き込みの有限回数に基づいて、SSD が機能し続ける合計年数を計算できます。
[動作温度（Operating Temperature）] フィールド	選択した SSD が、それを選択した時点で動作していたドライブの温度。
[消費された予約済みの容量の割合（Percentage Reserved Capacity Consumed）] フィールド	（SSD 用に予約されているパーセンテージのうち）SSD が消費した容量の合計。

タブ	説明
[前回の更新時刻（Time of Last Refresh）] フィールド	ドライブが最後に更新されてからの時間。

ステップ 9 [閉じる（Close）] をクリックします。

（注） [ストレージ アダプタ（Storage Adapter）] ページで [コントローラ情報（Controller Info）] をクリックし、[残量（パーセンテージ）（Percentage LIFE LEFT）]、[SMART でのコピーバックの有効化（Enable Copy back on SMART）]、[SMART エラーでの SSD へのコピーバックの有効化（Enable Copy back to SSD on SMART Error）] などのコントローラ設定を表示します。

コントローラ ドライブ セキュリティの概要

自己暗号化ドライブ（SED）は、データをドライブに書き込む際にデータを暗号化し、データを読み取る前に復号するために使用されます。これにより、ドライブのデータのセキュリティが確保されます。Cisco IMC Supervisor は、この機能のためにコントローラ、物理ドライブ、および仮想ドライブの各レベルでのセキュリティの有効化をサポートしています。

コントローラ レベルのセキュリティには、リモート キー管理とローカル キー管理の 2 つのオプションがあります。リモート キー管理では、KMIP サーバからセキュリティ キー ID とセキュリティ キーが取得されます。ローカル キー管理では、セキュリティ キー ID とセキュリティ キーはユーザが指定するか、または CIMC サーバから提案されます。これらのパラメータはドライブのデータを保護する目的で使用されます。

物理ドライブ レベルのセキュリティでは、SED ドライブをロック状態または外部ロック状態にできます。ロック状態では、このサーバでコントローラのセキュリティ キーを使用してドライブがロックされています。外部ロック状態では、別のコントローラのセキュリティ キーを使用してドライブがロックされていますが、ドライブはこのコントローラに配置されています。外部ロック状態のドライブをロック解除するには、そのコントローラのセキュリティ キーが必要です。ロック解除後には、ドライブに対して任意のセキュリティ関連の操作を実行できます。

（注） Cisco IMC Supervisor ではローカル キー管理だけがサポートされており、リモート キー管理はサポートされていません。コントローラ ドライブ セキュリティの詳細の表示 （75 ページ）を参照してください。.

コントローラ ドライブ セキュリティの詳細の表示

[コントローラ情報（Controller Info）]、[物理ドライブ（Physical Drives）]、および[仮想ドライブ（Virtual Drives）]でコントローラ ドライブのセキュリティの詳細を表示するには、次の手順を実行します。

始める前に

M4 ラックマウント サーバまたは UCS S3260 ストレージ サーバには SED が接続されている必要があります。

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [ラック グループ（Rack Groups）] を展開し、サブ ラック グループを選択します。

ステップ 3 [ラック サーバ（Rack Servers）] をクリックします。

ステップ 4 サーバをダブルクリックします。

ステップ 5 [ラック サーバ（Rack Server）] ページで [ストレージ アダプタ（Storage Adapters）] をクリックします。

ステップ 6 選択したサーバをダブルクリックするか、[詳細の表示（View Details）] をクリックします。

ステップ 7 [ストレージ アダプタ（Storage Adapter）] ページで [コントローラ情報（Controller Info）] をクリックします。
SSD ドライブに関する次の詳細が表示されます。

タブ	説明
[電源再投入カウント（Power Cycle Count）] フィールド	ドライブが製造されてから現在までに電源の再投入が行われた回数。
[電源オン時間（Power on Hours）] フィールド	ドライブが電源オン モードになっている合計時間数。

タブ	説明
[残量（パーセンテージ）（Percentage Life Left）] フィールド	半導体ドライブ（SSD）のライフタイムで残っている書き込みサイクルの回数。たとえば、ライフタイムを通して 100 回の書き込みサイクルに対応できる SSD で 15 回の書き込みが行われた場合、ドライブのライフタイムの残りのパーセンテージは 85% となります。パーセンテージの各範囲は異なる色で表されます。たとえば、75% ～ 100% は緑、1% ～ 25% は赤で表されます。 （注） [コントローラ情報（Controller Info）] の下の [SD - 残量（パーセンテージ）（SSD - Percentage Life Left）] に、SSD の棒グラフが追加されます。
[消耗ステータス（日数）（Wear Status in Days）] フィールド	SSD で書き込みサイクルが行われた日数。 SSD ベンダーが提示する 1 日あたりの SSD 書き込みの有限回数に基づいて、SSD が機能し続ける合計年数を計算できます。
[動作温度（Operating Temperature）] フィールド	選択した SSD が、それを選択した時点で動作していたドライブの温度。
[消費された予約済みの容量の割合（Percentage Reserved Capacity Consumed）] フィールド	（SSD 用に予約されているパーセンテージのうち）SSD が消費する合計容量。
[前回の更新時刻（Time of Last Refresh）] フィールド	ドライブが最後に更新されてからの時間。

ステップ 8 [ストレージアダプタ（Storage Adapter）] ページで [物理ドライブ（Physical Drives）] をクリックします。
コントローラ名、物理ドライブ番号、ステータス、ヘルス、シリアル番号、ファームウェア、FDE 対応、FDE 有効、保護済み、ロック済み、外部ロック済みなどの詳細が表示されます。

ステップ 9 [ストレージアダプタ（Storage Adapter）] ページで [仮想ドライブ（Virtuall Drives）] をクリックします。
仮想ドライブ番号、名前、ステータス、ヘルス、サイズ、RAID レベル、ブート ドライブ、FDE 対応、FDE 有効などの詳細が表示されます。

ステップ 10 [送信（Submit）] をクリックします。

ラック マウント サーバの障害の詳細の表示

問題の原因や問題解決のための推奨手順など、ラック マウント サーバの障害の詳細を表示する場合は、次の手順を実行します。

始める前に

サーバはすでに、ラック アカウントとしてラック グループに追加されています。

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [ラック グループ（Rack Groups）] ページで、[障害（Faults）] をクリックします。

ステップ 3 リストでサーバをダブルクリックし、詳細を表示します。リストでサーバをクリックし、右端の下矢印をクリックして [詳細の表示（View Details）] を選択することもできます。

（注） リストからサーバを選択するまでは、右端に下矢印は表示されません。

ラックマウント サーバに関する次の詳細が表示されます。

タブ	説明
説明	問題の原因の要約。
推奨	問題を解決する手順。

ステップ 4 [閉じる（Close）] をクリックします。

ラック グループの要約レポート

[インベントリと障害のステータス（Inventory and Fault Status for Rack Groups）] ページには、ラック グループのリストが表示されます。[ラック グループ（Rack Groups）] でグループを選択すると、選択したラック グループのページに、次のレポートを示す [要約（Summary）] レポートが表示されます。

- [障害（Faults）]：選択したラック グループの障害数の合計を示します。障害の数は、[クリティカル（Critical）]、[メジャー（Major）]、[警告（Warnings）]、[マイナー（Minor）]、[通知（Info）] などの重大度に基づいて分類されます。
- [サーバの状態（Server Health）]：サーバ全体のヘルス ステータスを表します。サーバ全体のヘルス ステータスは、[良好（Good）]、[メモリ テストが進行中です（Memory Test

In Progress）]、[中程度の障害（Moderate Fault）]、[重大な障害（Severe Fault）] などの状態のいずれかになります。

（注） [中程度の障害（Moderate Fault）] と [重大な障害（Severe Fault）] は、それぞれ、重大度が [メジャー（Major）] および [重大（Critical）] の障害と関連します。ただし、サーバのヘルス ステータスは CIMC によって報告されるステータスに基づいて決定され、上記の障害の重大度に対して、常に直接的にマッピングされるわけではないことに注意してください。障害のタイプや関連コンポーネントなどの他の要素がサーバ全体のヘルス ステータスに影響します。

- [シャーシの状態（Chassis Health）]：シャーシのヘルス ステータスを表します。ヘルス ステータスは、[良好（Good）]、[メモリ テストが進行中です（Memory Test In Progress）]、[中程度の障害（Moderate Fault）]、[重大な障害（Severe Fault）] などの状態のいずれかになります。
- [ファームウェアのバージョン（Firmware Versions）]：選択されたラック グループに対し、そのファームウェア バージョンで管理されているサーバの合計数を表します。
- [サーバ モデル（Server Models）]：選択されたラック グループに対し、そのモデルで管理されているサーバの合計数を表します。
- [電源の状態（Power State）]：選択されたラック グループに対し、その電源状態で管理されているサーバの合計数を表します。電源の状態は [オン（On）] または [オフ（Off）] のいずれかです。
- [サーバ接続のステータス（Server Connection Status）]：選択されたラック グループに対し、その接続ステータスをもつサーバの合計数を表します。接続ステータスは [成功（Success）] または [失敗（Failed）] のいずれかです。
- [概要（Overview）]：サーバの合計数と重大な障害の数を示します。

サーバ障害に関する電子メール アラート ルールの追加

1 つ以上の電子メール ルールを作成できます。各ルールでは、指定した条件に一致する障害が定期的な検査で見つかると、電子メール アラートが送信されます。このような障害に関する電子メール アラートを受信するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）]** > **[システム（System）]** を選択します。

ステップ 2 [電子メール アラート ルール（Email Alert Rules）] をクリックします。

（注） [電子メール アラート ルール（Email Alert Rules）] テーブルには、電子メール アラート ルール名、アラート範囲、アラート ルールで選択されたサーバとサーバ グループなどのアラート ルールの詳細が表示されます。

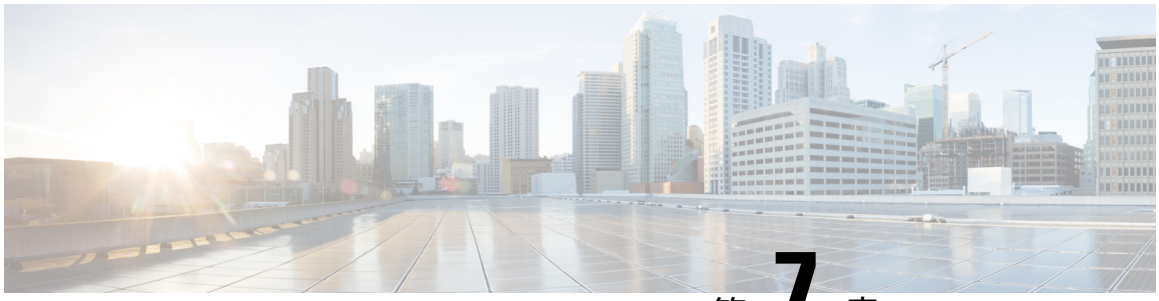
ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [電子メール アラート ルールの追加（Add Email Alert Rule）] ページで、次のフィールドに入力します。

フィールド	説明
名前	ルールの一意の名前を入力します。
アラート範囲	任意のサーバで検出された新しい障害に関するすべてのシステム レベルのアラートを受信するには[システム（System）]を選択します。特定のラック グループの一部であるサーバで検出された新しい障害に関する電子メール アラートを受信するには [サーバ グループ（ServerGroup）]を選択します。特定のサーバで検出された新しい障害に関する電子メール アラートを受信するには[サーバ（Server）]を選択します。
サーバグループ	アラート レベルとして [サーバ グループ（ServerGroup）]を選択すると、このオプションが表示されます。 **1.** [選択（Select）] をクリックします。 **2.** [選択（Select）] ダイアログボックスで 1 つ以上のラック サーバ グループをオンにし、[選択（Select）] をクリックします。電子メール アラートの送信対象となる選択されたサーバ グループの名前が、このフィールドの横にリストされます。
サーバ	アラート レベルとして [サーバ（Server）] を選択すると、このオプションが表示されます。 **1.** [選択（Select）] をクリックします。 **2.** [選択（Select）] ダイアログボックスで 1 つ以上のサーバをオンにし、[選択（Select）] をクリックします。電子メール アラートの送信対象となる選択されたサーバの名前が、このフィールドの横にリストされます。

フィールド	説明
[電子メール アドレス（Email Addresses）] フィールド	電子メール アラートの対象受信者の電子メール アドレス。電子メール アドレスが複数ある場合は、カンマで区切って入力できます。
重大度	[電子メール アドレス（Email Addresses）] フィールドで設定された電子メール アドレスに電子メール アラートを送信する対象となる障害重大度レベルを選択するには、次の手順を実行します。 **1.** [選択...] をクリックします。 **2.** リストから 1 つ以上の重大度レベルをオンにし、[選択（Select）] をクリックします。 （注） 選択した値が [選択...（Select...）] ボタンの横に表示されます。
[ルール有効（Rule Enabled）] チェックボックス	このチェックボックスをオンにして、設定された電子メール アドレスへの電子メール アラートを有効にします。

（注）
- 電子メール アラート ルールを修正および削除できます。[編集（Edit）] および [削除（Delete）] オプションは、ルールを選択した場合にのみ表示されます。[編集（Edit）] をクリックし、表示されているフィールドを必要に応じて変更するか、[削除（Delete）] をクリックして、削除することを確認します。
- 同時に複数のルールを選択して [削除（Delete）] をクリックし、それらを削除できます。
- 送信される電子メール アラートの数は、作成したルールの数に基づいています。
- 1.0 または 1.0.0.1 でシステム レベル ルールが存在する場合、1.1 にアップグレードすると、デフォルトでのそのルールの名前が **system-default** として追加されたことを確認できます。このグループの [アラート レベル（Alert Level）] フィールドは変更できませんが、このシステム レベル ルールを削除することは可能です。



第 7 章

ラック サーバの管理

この章は次のトピックで構成されています。

ラックマウント サーバの詳細の表示

ラックマウント サーバの詳細（サーバで使用されているメモリ、CPU、PSU など）を表示する場合は、次の手順を実行します。

（注） [ラック グループ（Rack Groups）] を選択し、ラックマウント サーバの詳細を表示する手順を実行することもできます。

始める前に

サーバがラック アカウントとしてラック グループに追加されていることを確認します。

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [ラック グループ（Rack Groups）] を展開し、サーバが含まれているラック グループを選択します。

ステップ 3 選択したラック グループのページで、[ラック サーバ（Rack Servers）] をクリックします。

ステップ 4 リストでサーバをダブルクリックしてその詳細を確認するか、リストでサーバを選択し、右端の下矢印をクリックして [詳細の表示（View Details）] を選択します。

（注） リストからサーバを選択するまでは、右端に下向き矢印は表示されません。

ラックマウント サーバに関する次の詳細が表示されます。

タブ	説明
要約	ラック アカウントの概要。
CPU	サーバで使用されている CPU の詳細。
メモリ	サーバで使用されているメモリの詳細。
PSUs	サーバで使用されている電源モジュールの詳細。 （注） Cisco UCS S3260 高密度ストレージ ラック サーバには適用されません。
PCIアダプタ	サーバで使用されている PCI アダプタの詳細。
VICアダプタ	サーバで使用されている VIC アダプタの詳細。 リストされている VIC アダプタのいずれかを選択して [詳細の表示（View Details）] をクリックすると、[外部イーサネット インターフェイス（External Ethernet Interfaces）] と [VM FEX（VM FEXs）] の情報が表示されます。
ネットワークアダプタ	サーバで使用されているネットワーク アダプタの詳細。 リストされているネットワーク アダプタのいずれかを選択して [詳細の表示（View Details）] をクリックすると、[外部イーサネット インターフェイス（External Ethernet Interfaces）] の情報が表示されます。

タブ	説明
ストレージアダプタ	サーバで使用されているストレージ アダプタの詳細。 リストされているストレージ アダプタのいずれかを選択して [詳細の表示（View Details）] をクリックすると、[コントローラ情報（Controller Info）]、[物理ドライブ（Physical Drives）]、[仮想ドライブ（Virtual Drives）] などの情報が表示されます。SSD のスマート情報の表示 （72 ページ）を参照してください。.
FlexFlashアダプタ	サーバで使用されている FlexFlash アダプタの詳細。 リストされている FlexFlash アダプタのいずれかを選択して [詳細の表示（View Details）] をクリックすると、[コントローラ情報（Controller Info）]、[物理ドライブ（Physical Drives）] などの情報が表示されます。 Cisco IMC Supervisor を旧バージョンからアップグレードしている場合、FlexFlash の詳細をレポートに表示するには [システム（Systems）] > [物理アカウント（Physical Accounts）] > [ラック アカウント（Rack Accounts）] > [インベントリ（Inventory）] に移動してインベントリを実行するか、定期的なインベントリが実行されるのを待つ必要があります。 （注） Cisco UCS S3260 高密度ストレージ ラック サーバには適用されません。
通信	HTTP、HTTPS、SSH、IPMI Over LAN、NTP、SNMP などのプロトコルに関する情報。
リモート プレゼンス	VKVM、Serial Over LAN、および vMedia の詳細。
障害	サーバで記録された障害の詳細。
ユーザ数	**デフォルト グループ**のユーザに関する詳細。ユーザ ポリシーおよびパスワードの有効期限ポリシーの作成時に設定した強力なパスワード ポリシーとパスワード有効期限の詳細も確認できます。ユーザ ポリシー （134 ページ）およびパスワードの有効期限ポリシー （125 ページ）を参照してください。 （注） Cisco UCS S3260 高密度ストレージ ラック サーバには適用されません。
Cisco IMC ログ	サーバの Cisco IMC ログの詳細。 （注） Cisco UCS S3260 高密度ストレージ ラック サーバには適用されません。

タブ	説明
システム イベント ログ	サーバ ログの詳細。 （注） Cisco UCS S3260 高密度ストレージ ラック サーバには適用されません。
TPM	TPM インベントリに関する情報。
BIOS	サーバの BIOS 設定とブート順序の詳細。 サーバを選択し、[BIOS 設定の表示（View BIOS Settings）]、[ブート設定の表示（View Boot Settings）]、[ブート順序の表示（View Boot Order）]のいずれかをクリックします。
障害履歴	サーバで発生した障害の履歴情報。
テクニカル サポート	ファイル名、宛先タイプ、アップロードのステータスなどのテクニカル サポート ログ ファイルに関する詳細は、[テクニカル サポート（Tech Support）] テーブルに表示されます。 リモート サーバまたはローカルの Cisco IMC Supervisorアプライアンスへテクニカル サポート ログ ファイルをエクスポートするオプションがあります。エクスポートの詳細については、リモート サーバへのテクニカル サポート データのエクスポート （97 ページ）を参照してください。 （注） Cisco UCS S3260 高密度ストレージ ラック サーバには適用されません。
ホストイメージ	イメージの詳細（名前、サイズ、MD5 チェックサム、最終変更時刻、イメージがマップされているかどうかなど）が表示されます。イメージを選択し、[イメージのマッピング（Map Image）]、[イメージのマップ解除（Unmap Image）]、または [イメージの削除（Delete Image）]を選択して、それぞれのアクションを実行できます。 （注） ホスト イメージ マッピングは、E シリーズ サーバにのみ適用できます。
関連付けられているハードウェア プロファイル	ハードウェア プロファイルに関連付けられているポリシーの詳細。

ステップ 5 右端の [戻る（Back）] ボタンをクリックして前のウィンドウに戻ります。

ラック マウント サーバの障害の詳細の表示

問題の原因や問題解決のための推奨手順など、ラック マウント サーバの障害の詳細を表示する場合は、次の手順を実行します。

始める前に

サーバはすでに、ラック アカウントとしてラック グループに追加されています。

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [ラック グループ（Rack Groups）] ページで、[障害（Faults）] をクリックします。

ステップ 3 リストでサーバをダブルクリックし、詳細を表示します。リストでサーバをクリックし、右端の下矢印をクリックして [詳細の表示（View Details）] を選択することもできます。

（注） リストからサーバを選択するまでは、右端に下矢印は表示されません。

ラックマウント サーバに関する次の詳細が表示されます。

タブ	説明
説明	問題の原因の要約。
推奨	問題を解決する手順。

ステップ 4 [閉じる（Close）] をクリックします。

ラックマウント サーバの電源オン/オフ

ラックマウント サーバの電源をオンまたはオフにする場合は、次の手順を実行します。

始める前に

サーバはすでに、ラック アカウントとしてラック グループに追加されています。

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [ラック グループ（Rack Groups）] を選択します。

（注） [ラック グループ（Rack Groups）] を展開し、サーバを含むラック グループを選択することもできます。

ステップ 3 選択したラック グループのページで、[ラック サーバ（Rack Servers）] をクリックします。

（注） また、[ラック グループ（Rack Groups）] でサブ グループを選択することもできます。

ステップ 4 サーバのリストから、電源をオンまたはオフにするサーバを選択します。

（注） 複数のラック サーバを選択することもできます。

ステップ 5 [電源オン（Power ON）] をクリックします。[その他の操作（More Actions）] ドロップダウン リストから [電源オフ（Power OFF）] を選択します。

（注） 右クリックしてオプションを選択することもできます。

ステップ 6 確認ダイアログボックスで、[OK] をクリックします。

（注） サーバの電源がオンまたはオフになったことを示すメッセージが表示されます。このメッセージは、いずれかのサーバの電源オン/オフを実行できなかったかどうかも示します。少し時間が経過した後でテーブルを更新すると、現在の電源状態が反映されます。

ラック マウント サーバのアセットのタグ付け

アセット タグは、サーバのユーザ定義タグです。[アセット タグ（Asset Tag）] オプションを使用し、Cisco IMC Supervisorで Cisco IMC サーバ プロパティを追加できます。

ラック サーバとシャーシの両方でアセットをタグ付けできます。シャーシのアセットにタグを付けるには、Cisco UCS S3260 ラック サーバのアセットのタグ付け （196 ページ）を参照してください。アセットにタグを付けるには、次の手順を実行します。

始める前に

サーバはすでに、ラック アカウントとしてラック グループに追加されています。

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [ラック グループ（Rack Groups）] ページで [ラック サーバ（Rack Servers）] をクリックします。

（注） また、[インベントリと障害のステータス（Inventory and Fault Status）] ペインの [ラック グループ（Rack Groups）] でサブ グループを選択することもできます。

ステップ 3 タグを付けるサーバを選択します。

ステップ 4 [その他の操作（More Actions）] ドロップダウンリストから [アセット タグ（Asset Tag）] を選択します。

（注） 右クリックしてオプションを選択することもできます。

ステップ 5 [送信（Submit）] をクリックします。

（注） [アセット タグ（Asset Tag）] オプションは、Cisco IMCリリース 3.0.(1c) 以降でのみ使用可能です。これよりも古いバージョンのプラットフォームでは、[ラック グループ（Rack Groups）] ページの [アセット タグ（Asset Tag）] カラムは空白になります。

ラックマウント サーバのシャットダウン

ラックマウント サーバをシャット ダウンする場合は、次の手順を実行します。

（注） 複数のラック サーバを選択することもできます。

始める前に

サーバはすでに、ラック アカウントとしてラック グループに追加されています。

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [インベントリと障害のステータス（Inventory and Fault Status）] ペインで [ラック グループ（Rack Groups）] を選択します。

（注） [ラック グループ（Rack Groups）] を展開し、サーバを含むラック グループを選択することもできます。

ステップ 3 選択したラック グループのページで、[ラック サーバ（Rack Servers）] をクリックします。

（注） また、[ラック グループ（Rack Groups）] でサブ グループを選択することもできます。

ステップ 4 リストからサーバを選択します。

ステップ 5 [その他の操作（More Actions）] ドロップダウンリストから [シャットダウン（Shut Down）] を選択します。

（注） 右クリックしてオプションを選択することもできます。

ステップ 6 [OK] をクリックします。

ラックマウント サーバのハード リセットの実行

サーバをリセットするには、次の手順を実行します。

（注） 複数のラック サーバを選択することもできます。

始める前に

サーバはすでに、ラック アカウントとしてラック グループに追加されています。

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [インベントリと障害のステータス（Inventory and Fault Status）] ペインで [ラック グループ（Rack Groups）] を選択します。

（注） [ラック グループ（Rack Groups）] を展開し、サーバを含むラック グループを選択することもできます。

ステップ 3 選択したラック グループのページで、[ラック サーバ（Rack Servers）] をクリックします。

（注） また、[ラック グループ（Rack Groups）] でサブ グループを選択することもできます。

ステップ 4 リストからサーバを選択します。

ステップ 5 [その他の操作（More Actions）] ドロップダウンリストから [ハード リセット（Hard Reset）] を選択します。

（注） 右クリックしてオプションを選択することもできます。

ステップ 6 [OK] をクリックします。

ラックマウント サーバの電源再投入の実行

ラック マウント サーバの電源を 1 サイクルでオンまたはオフにするには、次の手順を実行します。

（注） 複数のラック サーバを選択することもできます。

始める前に

サーバはすでに、ラック アカウントとしてラック グループに追加されています。

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [インベントリと障害のステータス（Inventory and Fault Status）] ペインで [ラック グループ（Rack Groups）] を選択します。

（注） [ラック グループ（Rack Groups）] を展開し、サーバを含むラック グループを選択することもできます。

ステップ 3 選択したラック グループのページで、[ラック サーバ（Rack Servers）] をクリックします。

（注） また、[ラック グループ（Rack Groups）] でサブ グループを選択することもできます。

ステップ 4 リストからサーバを選択します。

ステップ 5 [その他の操作（More Actions）] ドロップダウンリストから [電源の再投入（Power Cycle）] を選択します。

（注） 右クリックしてオプションを選択することもできます。

ステップ 6 [OK] をクリックします。

ラックマウント サーバの KVM コンソールの起動

kvm.jnlp ファイルをダウンロードし、KVM コンソールを開くには、次の手順を実行します。

始める前に

- サーバがラック アカウントとしてラック グループに追加されていることを確認します。
- KVM 機能が機能するために必要な有効な Java Runtime Environment（JRE）がインストールされていることを確認します。

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [インベントリと障害のステータス（Inventory and Fault Status）] ペインで [ラック グループ（Rack Groups）] を選択します。

（注） [ラック グループ（Rack Groups）] を展開し、サーバを含むラック グループを選択することもできます。

ステップ 3 選択したラック グループのページで、[ラック サーバ（Rack Servers）] をクリックします。

（注） また、[ラック グループ（Rack Groups）] でサブ グループを選択することもできます。

ステップ 4 リストからサーバを選択します。

ステップ 5 [その他の操作（More Actions）] ドロップダウンリストから [KVM コンソール（KVM Console）] を選択します。

（注）
- 右クリックしてオプションを選択することもできます。
- KVM コンソールを起動するサーバは最大 5 台まで選択できます。

ステップ 6 [送信（Submit）] をクリックします。

Cisco IMC Supervisor によって *kvm.jnlp* ファイルがダウンロードされます。

ステップ 7 ダウンロード フォルダ内の *kvm.jnlp* ファイルをダブルクリックします。

[KVMコンソール] が別ウィンドウで開きます。

（注） 別ウィンドウで開く `launcher.jsp` ファイルにより、選択したサーバのリストが表示されます。KVM コンソールが正常に起動したかどうかも確認できます。

ラックマウント サーバの GUI の起動

別のブラウザで Cisco IMC Supervisor GUI を起動するには、次の手順を実行します。

始める前に

サーバはすでに、ラック アカウントとしてラック グループに追加されています。

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [インベントリと障害のステータス（Inventory and Fault Status）] ペインで [ラック グループ（Rack Groups）] を選択します。

（注） [ラック グループ（Rack Groups）] を展開し、サーバを含むラック グループを選択することもできます。

ステップ 3 選択したラック グループのページで、[ラック サーバ（Rack Servers）] をクリックします。

（注） また、[ラック グループ（Rack Groups）] でサブ グループを選択することもできます。

ステップ 4 リストからサーバを選択します。

ステップ 5 [その他の操作（More Actions）] ドロップダウンリストから [GUI の起動（Launch GUI）] を選択します。

（注） 右クリックしてオプションを選択することもできます。

ステップ 6 [送信（Submit）] をクリックします。

サーバの GUI が別のブラウザで起動します。

ラックマウント サーバのロケータ LED の設定

サーバ ロケータ LED を使用すると、データセンター内の多数のサーバ間で特定のサーバを識別できます。LED をオンまたはオフに設定するには、次の手順を実行します。

（注） 複数のラック サーバを選択することもできます。

始める前に

サーバはすでに、ラック アカウントとしてラック グループに追加されています。

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [インベントリと障害のステータス（Inventory and Fault Status）] ペインで [ラック グループ（Rack Groups）] を選択します。

（注） [ラック グループ（Rack Groups）] を展開し、サーバを含むラック グループを選択することもできます。

ステップ 3 選択したラック グループのページで、[ラック サーバ（Rack Servers）] をクリックします。

（注） また、[ラック グループ（Rack Groups）] でサブ グループを選択することもできます。

ステップ 4 リストからサーバを選択します。

ステップ 5 [その他の操作（More Actions）] ドロップダウンリストから [ロケータ LED（Locator LED）] を選択します。

（注） 右クリックしてオプションを選択することもできます。

ステップ 6 [オン/オフ（Turn）] ドロップダウンリストから、[オン（ON）] または [オフ（OFF）] を選択します。

ステップ 7 [送信（Submit）] をクリックします。

ラックマウント サーバのラベルの設定

サーバにラベル名を設定すると、サーバの分類に役立ちます。これにより、必要なサーバの検索、確認、比較が容易になります。ラック マウント サーバにラベルを設定するには、次の手順を実行します。

始める前に

サーバはすでに、ラック アカウントとしてラック グループに追加されています。

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [インベントリと障害のステータス（Inventory and Fault Status）] ペインで [ラック グループ（Rack Groups）] を選択します。

（注） [ラック グループ（Rack Groups）] を展開し、サーバを含むラック グループを選択することもできます。

ステップ 3 選択したラック グループのページで、[ラック サーバ（Rack Servers）] をクリックします。

（注） また、[ラック グループ（Rack Groups）] でサブ グループを選択することもできます。

ステップ 4 リストからサーバを選択します。

ステップ 5 [その他の操作（More Actions）] ドロップダウンリストから [ラベルの設定（Set Label）] を選択します。

（注）　右クリックしてオプションを選択することもできます。

ステップ 6 新しいラベルを入力します。

ステップ 7 [送信（Submit）] をクリックします。

ラック マウント サーバのタグの管理

タグは、オブジェクト（リソース グループ、ラック サーバなど）にラベルを割り当てる場合に使用されます。タグは、ラックの位置、担当サポート グループ、目的、またはオペレーティング システムなどの情報を提供するために使用できます。タグを追加または変更するには、次の手順を実行します。

始める前に

サーバはすでに、ラック アカウントとしてラック グループに追加されています。

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [インベントリと障害のステータス（Inventory and Fault Status）] ペインで [ラック グループ（Rack Groups）] を展開し、サーバを含むラック グループを選択します。

ステップ 3 [ラック サーバ（Rack Servers）] または [シャーシ（Chassis）] をクリックします。

（注）　[ラック グループ（Rack Groups）] ではサブ グループを選択できます。

ステップ 4 [その他のアクション（More Actions）] ドロップダウンリストから [タグの管理（Manage Tags）] を選択します。

（注）　右クリックしてオプションを選択することもできます。

ステップ 5 [+] をクリックして、[タグの管理（Manage Tags）] テーブルにエントリを追加します。

ステップ 6 [タグへのエントリの追加（Add Entry to Tag）] 画面で、次のフィールドに入力します。

フィールド	説明
タグ名	

フィールド	説明
	ドロップダウンリストからタグ名を選択して [送信（Submit）] をクリックするか、または新しいタグを作成します。 **1.** **[+]** アイコンをクリックします。 **2.** [タグの作成（Create Tag）] ウィンドウで、次の手順を実行します。 **1.** [名前（Name）] フィールドにタグのわかりやすい名前を入力します。 **2.** [説明（Description）] フィールドにタグの説明を入力します。 **3.** [タイプ（Type）] フィールドで、ドロップダウンリストから [文字列（String）] または [整数（Integer）] を選択します。 **4.** [使用できるタグ値（Possible Tag Values）] フィールドに、タグに使用できる値を入力します。 **5.** [次へ（Next）] をクリックします。 **6.** [+] アイコンをクリックして、新しいカテゴリを追加します。 **3.** [エンティティへのエントリの追加（Add Entry to Entities）] ウィンドウで、[カテゴリ（Category）] ドロップダウンリストからカテゴリを選択します。次のいずれかを指定できます。 • [Physical_Compute] カテゴリの場合、ラック サーバのタグ エンティティが作成されます。 • [管理（Administration）] カテゴリの場合、ユーザのタグ エンティティが作成されます。 （注） シャーシのタグも追加できます。シャーシのタグの追加の詳細については、Cisco UCS S3260 ラック サーバのタグの追加 （198 ページ）を参照してくださ

フィールド	説明
	い。 **4.** [ラック サーバ（Rack Servers）] または [シャーシ（Chassis）] チェックボックスをオンにします。 **5.** [送信（Submit）] をクリックします。 （注） タグは、セットになったタグ付け可能なエンティティに応じてそれぞれのカテゴリの下に表示されます。 **6.** 確認ダイアログボックスで、[OK] をクリックします。
タグ値	ドロップダウンリストからタグ値を選択します。

ステップ 7 [送信（Submit）] をクリックします。

ステップ 8 [タグの管理（Manage Tags）] 画面でタグを選択し、[編集（Edit）] をクリックしてタグを編集します。

ステップ 9 タグ名とタグ値を選択してタグを変更します。

ステップ 10 [送信（Submit）] をクリックします。

ラック マウント サーバのタグの追加

タグは、オブジェクト（リソース グループ、ラック サーバなど）にラベルを割り当てる場合に使用されます。タグは、ラックの位置、担当サポート グループ、目的、またはオペレーティング システムなどの情報を提供するために使用できます。ラック マウント サーバにタグを追加するには、次の手順を実行します。

始める前に

サーバはすでに、ラック アカウントとしてラック グループに追加されています。

（注） 複数のラック サーバを選択することもできます。

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [インベントリと障害のステータス（Inventory and Fault Status）] ペインで [ラック グループ（Rack Groups）] を選択します。

（注） [ラック グループ（Rack Groups）] を展開し、サーバを含むラック グループを選択することもできます。

ステップ 3 選択したラック グループのページで、[ラック サーバ（Rack Servers）] をクリックします。

（注） また、[ラック グループ（Rack Groups）] でサブ グループを選択することもできます。

ステップ 4 [その他の操作（More Actions）] ドロップダウンリストから [タグの追加（Add Tags）] を選択します。

（注） 右クリックしてオプションを選択することもできます。

ステップ 5 ドロップダウンリストから [タグ名（Tag Name）] を選択します。

ステップ 6 ドロップダウンリストから [タグ値（Tag Value）] を選択します。

ステップ 7 プラス アイコンをクリックして新しいタグを作成します。タグの作成については、ラック マウント サーバのタグの管理 （93 ページ）を参照してください。

（注） タグの詳細を複製、編集、削除、および表示することもできます。

リモート サーバへのテクニカル サポート データのエクスポート

指定したサーバにテクニカル サポート ファイルをアップロードするには、次の手順を実行します。

（注） テクニカル サポートのエクスポート オプションでは、Cisco UCS S3260 高密度ストレージ ラック サーバはサポートされていません。

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [インベントリと障害のステータス（Inventory and Fault Status）] ペインで [ラック グループ（Rack Groups）] を選択します。

（注） [ラック グループ（Rack Groups）] を展開し、サーバを含むラック グループを選択することもできます。

ステップ 3 選択したラック グループのページで、[ラック サーバ（Rack Servers）] をクリックします。

（注） また、[ラック グループ（Rack Groups）] でサブ グループを選択することもできます。

ステップ 4 リストでラックマウント サーバをダブルクリックしてその詳細を確認するか、リストでラックマウント サーバをクリックし、右端の下矢印をクリックして [詳細の表示（View Details）] を選択します。

ステップ 5 [テクニカル サポート（Tech Support）] をクリックします。

ステップ 6 [Create Tech Support] をクリックします。

ステップ 7 [テクニカル サポートの作成（Create Tech Support）] 画面で、次のフィールドに入力します。

名前	説明
[宛先タイプ（Destination Type）] ドロップダウンリスト	リモート サーバまたはローカルの Cisco IMC Supervisor アプライアンスにファイルをエクスポートできます。[REMOTE] または [LOCAL] を選択します。
[ネットワークタイプ（Network Type）] ドロップダウンリスト	ネットワーク タイプ。次のいずれかになります。 • **SCP** • **SFTP** • **FTP** • **TFTP**
[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。[ネットワーク タイプ（Network Type）] ドロップダウンリストの設定によって、このフィールドの名前が異なります。
[Path and Filename] フィールド	ファイルをリモート サーバにエクスポートする際に必要な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。ネットワーク タイプが TFTP 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。ネットワーク タイプが TFTP の場合、このフィールドは適用されません。

ステップ 8 [送信（Submit）] をクリックします。

（注）
- 選択してダウンロードできるテクニカル サポート ファイルは、[宛先タイプ（Destination Type）] として [LOCAL] を選択して作成されたものだけです。
- 既存のテクニカル サポート ファイルを選択し、Cisco IMC Supervisorアプライアンス内に保存されているファイルのみをダウンロードできます。特定のファイルを選択し、[ダウンロード（Download）] をクリックします。これにより、<ホスト名>_<タイムスタンプ>. tar.gz ファイルが作成されます。

SEL のクリア

システム イベント ログ（SEL）は、問題のトラブルシューティングに使用できるほとんどのサーバ関連イベントを記録します。SEL ログをクリアするには、次の手順を実行します。

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [インベントリと障害のステータス（Inventory and Fault Status）] ペインで [ラック グループ（Rack Groups）] を選択します。

（注） [ラック グループ（Rack Groups）] を展開し、サーバを含むラック グループを選択することもできます。

ステップ 3 選択したラック グループのページで、[ラック サーバ（Rack Servers）] をクリックします。

（注） また、[ラック グループ（Rack Groups）] でサブ グループを選択することもできます。

ステップ 4 リストでラックマウント サーバをダブルクリックしてその詳細を確認するか、リストでラックマウント サーバをクリックし、右端の下矢印をクリックして [詳細の表示（View Details）] を選択します。

ステップ 5 [システム イベント ログ（System Event Log）] をクリックします。

ステップ 6 [IMC SEL ログのクリア（Clear IMC SEL Logs）] をクリックします。

ステップ 7 （任意） [IMC SEL ログのクリア（Clear IMC SEL Logs）] ダイアログボックスで、[Cisco IMC Supervisor から履歴ログを削除する（Delete historical logs from Cisco IMC Supervisor）] チェックボックスをオンにします。

このオプションを選択すると、Cisco IMC SupervisorGUI からシステム イベント ログがクリアされます。

ステップ 8 [送信（Submit）] をクリックします。

システム タスクの管理

[システムのタスク（System Tasks）] タブには、現在 Cisco IMC Supervisor で利用可能なすべてのシステム タスクが表示されます。ただし、このシステム タスクのリストは、Cisco IMC Supervisorで作成したアカウントのタイプにリンクされています。たとえば、初めてログインした場合は、一連の汎用システム関連のタスクだけがこのページに表示されます。ラック アカウントや Cisco IMC Supervisor アカウントなどのアカウントを追加した時点から、これらのアカウントに関連するシステムのタスクがこのページに読み込まれます。

左側のペインでタスクを展開し、消去、ラック サーバ、ユーザ、グループ タスクなどの個々のタスクを選択して、それらを管理します。

アプライアンスで実行しているプロセスまたはタスクが複数ある状況において、システム タスクの無効化を選択することができます。無効にすると、手動で有効にするまで、システム タスクは実行されません。これは他のレポートに入力されるデータに影響します。たとえば、インベントリ収集のシステム タスクを無効にすると、このデータが必要なレポートに正確なデータが表示されない場合があります。この場合、インベントリ収集プロセスを手動で実行するか、またはシステム タスクを有効にする必要があります。

（注） システム タスクの編集は推奨されません。

手順

ステップ 1 **[管理（Administration）] > [システム（System）]** を選択します。

ステップ 2 [システムのタスク（System Tasks）] をクリックします。

ステップ 3 リストからタスクを選択し、[タスクの管理（Manage Task）] をクリックします。

ステップ 4 [タスクの管理（Manage Task）] 画面で、次のフィールドに入力します。

フィールド	説明
[タスクの実行（Task Execution）] ドロップダウンリスト	（オプション）[有効（Enable）] または [無効（Disable）] を選択します。
[システム タスク ポリシー（System Task Policy）] ドロップダウンリスト	次のいずれかのオプションを選択します。 • **default-system-task-policy** • **local-run-policy**

フィールド	説明
[スケジュールのタイプ（Schedule Type）] ドロップダウンリスト	システム タスクのスケジュール タイプを指定します。次のいずれかの頻度を指定できます。 • [固定遅延（Fixed Delay）] : 1 つのタスクの実行完了後、次のタスクの実行開始までの時間を指します。 • [固定レート（Fixed Rate）] : 連続的なタスクの実行と実行の間の時間を指します。1つのタスクの実行に遅延がある場合、またはスケジュール時間よりタスクの実行に時間がかかる場合は、後続のタスクの実行に遅れが出ます。この設定で設定されているシステム タスクは、同時に実行されません。これらのタスクは、同時には実行されません。
[時間（Hours）] ドロップダウンリスト	タスクを実行する間隔を時間単位で選択します。 [固定遅延（Fixed Delay）] をスケジュール タイプとして選択した場合、この数字は1つのタスクの実行を完了し、次のタスクの実行を開始するまでの時間間隔を示します（時間単位）。 [固定レート（Fixed Rate）] を選択した場合、この数字は連続したタスクの実行の時間間隔を示します（時間単位）。
[分（Minutes）] ドロップダウンリスト	分単位のタスク実行頻度を選択します。
[カスタム頻度の有効化（Enable Custom Frequenc）] チェックボックス	システム タスクのカスタム頻度を有効にするには、このチェックボックスをオンにします。
[繰り返しタイプ（Recurrence Type）] ドロップダウンリスト	システム タスクの定期スケジュールを指定します。次のいずれかを指定できます。 • **無期限** • **1回のみ**
[開始時間] フィールド	定期スケジュールの日付と時刻を特定します。

フィールド	説明
[頻度] ドロップダウンリスト	システム タスクの頻度を選択します。次のいずれかを指定できます。 • **Hourly** • **毎日** • **週 1 回** • **月 1 回** （注） このフィールドは、[繰り返しタイプ（Recurrence Type）] ドロップダウンリストから [無期限（No End）] を選択した場合にのみ表示されます。
[頻度の間隔] ドロップダウンリスト	ドロップダウンリストから頻度の間隔を選択します。このリスト内の値は、指定した頻度によって異なります。

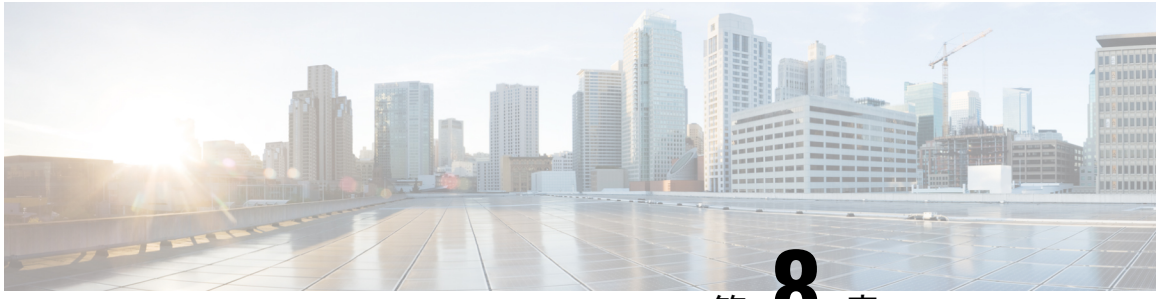
ステップ 5 [送信（Submit）] をクリックします。

タスクの実行

各タスクは、ユーザが定義した間隔で実行するようにスケジュールされます。ただし、これを上書きして手動で実行することができます。手動で実行したタスクは、再度頻度カラムの定義に従って実行するようにスケジュールされます。システム タスクを手動で実行する場合は、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [システム（System）]** を選択します。
ステップ 2 [システムのタスク（System Tasks）] をクリックします。
ステップ 3 テーブルからシステム タスクを選択します。
ステップ 4 [今すぐ実行（Run Now）] をクリックします。
ステップ 5 [送信（Submit）] をクリックします。



第 8 章

ポリシーとプロファイルの管理

この章は次のトピックで構成されています。

クレデンシャル ポリシー

ポリシーには、システムまたはネットワーク リソースへのアクセスを制御する一連のルールが含まれます。クレデンシャル ポリシーは、ユーザ アカウントのパスワードの要件とアカウント ロックアウトを定義します。ユーザ アカウントに割り当てられたクレデンシャル ポリシーは、Cisco IMC Supervisor の認証プロセスを制御します。クレデンシャル ポリシーを追加した後、クレデンシャルの種類または個々のアプリケーションに対して新しいポリシーをデフォルト ポリシーとして指定することができます。

[クレデンシャル ポリシー（Credential Policies）] ページには、次の詳細情報が表示されます。

フィールド	説明
ポリシー名	ポリシーのユーザ定義名。
説明	ポリシーのユーザ定義の簡単な説明。
ユーザ名	シスコ ユーザ名。
プロトコル	ポリシーが準拠するプロトコル。
[ポート（Port）]	ポリシーのポート。

このページから、ポリシーの追加、編集、削除など、さまざまなタスクを実行できます。クレデンシャル ポリシーの作成については、クレデンシャル ポリシーの作成 （104 ページ）を参照してください。

クレデンシャル ポリシーの作成

クレデンシャル ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 **[ポリシー（Policies）] > [ポリシーとプロファイルの管理（Manage Policies and Profiles）]** を選択します。

ステップ 2 [ポリシーとプロファイルの管理（Manage Policies and Profiles）] ページで [クレデンシャル ポリシー（Credential Policies）] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [クレデンシャル ポリシーの追加（Add Credential Policy）] 画面で、次のフィールドに入力します。

フィールド	説明
[ポリシー名（Policy Name）] フィールド	ポリシーの記述名。
[説明（Description）] フィールド	（オプション）ポリシーの説明。
[ユーザ名（User Name）] フィールド	Cisco IMC ユーザ名またはラックマウント サーバのユーザ名。
[パスワード（Password）] フィールド	Cisco IMC パスワードまたはラックマウント サーバのパスワード。
[プロトコル（Protocol）] ドロップダウンリスト	ドロップダウンリストからプロトコルを選択します。
[ポート（Port）] フィールド	ポリシーのポート番号を入力します。

ステップ 5 [送信（Submit）] をクリックします。

（注） 作成したクレデンシャル ポリシーのサーバ マッピングの編集、複製、削除、表示、適用、確認ができます。

ハードウェアポリシー

ポリシーとは、Cisco IMCでのさまざまな属性の設定を定義する主なメカニズムです。ポリシーは、サーバ間で設定の一貫性と再現性を実現するのに役立ちます。包括的なポリシーセットを定義して使用すると、一貫性、制御性、予測可能性、自動化機能が向上します。

使用例：自身が管理者である場合、適切なネットワーキング、BIOS、RAID設定などの必要な設定を含んだ「ゴールデンサーバ」が特定できている場合があります。これらの設定を、ポリ

シーに準拠していない他のサーバ全体に複製することができます。今後、新しいサーバの追加が必要になる場合や、設定済みサーバを展開する場合に備えて、Cisco IMC内この設定を保持することができます。また、同じ内容を適用する前に、その設定をオンザフライで変更することも可能です。たとえば、コンポーネントに更新が必要となったり、NTP IP アドレス、ボーレートなどが必要となったりする場合があります。「ゴールデンサーバ」での設定を失念していた場合や、他のサーバへの適用前にその内容を確認したい場合もあります。

個々のポリシーは1つずつ処理されます。プロファイルにバンドルされているポリシーはマルチスレッド化されており、一連のプロセスを同時に開始するのに役立ちます。

Cisco IMC Supervisor でハードウェア ポリシーを使用する方法を次のワークフローで説明します。

1. BIOS ポリシー、NTP ポリシーなどのハードウェア ポリシーを作成します。次のいずれかの方法でポリシーを作成できます。
    1. 新しいポリシーを作成します。さまざまなポリシー タイプ、および新しいポリシーの作成方法の詳細については、ハードウェア ポリシーの作成 （105 ページ）を参照してください。
    2. サーバの既存の設定からポリシーを作成します。サーバの既存の設定からポリシーを作成する方法については、既存の設定からのポリシーの作成 （140 ページ）を参照してください。
2. サーバにポリシーを適用します。ポリシーの適用については、ハードウェア ポリシーの適用 （142 ページ）を参照してください。
3. ポリシーで、必要に応じて次のオプション作業を実行します。
    1. 編集
    2. 削除
    3. 複製
    4. 特定のポリシーにマッピングされているサーバのリストを表示することもできます。これらの作業の実行の詳細については、ハードウェア ポリシーの一般タスク （143 ページ）を参照してください。
    5. さまざまなポリシーを作成して、それらをプロファイルにグループ化した後で、そのプロファイルをサーバに適用できます。プロファイルの適用については、ハードウェア プロファイルの適用 （148 ページ）を参照してください。

ハードウェア ポリシーの作成

ハードウェア ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 **[ポリシー（Policies）] > [ポリシーとプロファイルの管理（Manage Policies and Profiles）]** を選択します。

ステップ 2 [ポリシーとプロファイルの管理（Manage Policies and Profiles）] ページで [ハードウェア ポリシー（Hardware Policies）] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [追加（Add）] 画面で、ドロップダウンリストからポリシー タイプを選択します。

ポリシー タイプに基づくポリシーの作成の詳細については、次の表でポリシー タイプを選択してください。これらのポリシーの設定に必要なさまざまなプロパティは、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』で確認できます。このマニュアルでは、ポリシー タイプごとにセクションがリストされています。

（注） ポリシーを作成する Cisco UCS S3260 プラットフォームを選択するためのチェックボックスが導入されました。このオプションは、デフォルトで無効です。Cisco UCS S3260 のポリシーを作成する必要がある場合、このチェックボックスをオンにして、同様に有効にする必要があります。

ポリシータイプ	『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』のセクション
BIOS ポリシー （107 ページ）	*BIOS* の設定
ディスクグループポリシー （109 ページ）	ストレージ アダプタの管理
FlexFlash ポリシー （109 ページ）	*Flexible Flash* コントローラの管理
IPMI Over LANポリシー （115 ページ）	*IPMI* の設定
LDAPポリシー （117 ページ）	*LDAP* サーバの設定
レガシー ブート順序ポリシー （118 ページ）	サーバのブート順
ネットワーク構成ポリシー （119 ページ）	ネットワーク関連の設定
ネットワークセキュリティポリシー （123 ページ）	ネットワーク セキュリティの設定
NTPポリシー （124 ページ）	*Network Time Protocol* 設定の指定
パスワードの有効期限ポリシー （125 ページ）	パスワード有効期限
高精度のブート順序ポリシー （126 ページ）	高精度ブート順の設定
電力復元ポリシー （127 ページ）	電力復元ポリシーの設定
RAIDポリシー （128 ページ）	ストレージ アダプタの管理

ポリシータイプ	『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』のセクション
Serial Over LANポリシー （132 ページ）	*Serial over LAN* の設定
SNMPポリシー （132 ページ）	*SNMP* の設定
SSHポリシー （134 ページ）	*SSH* の設定
ユーザ ポリシー （134 ページ）	ローカル ユーザの設定
VIC アダプタ ポリシー （137 ページ）	*VIC* アダプタのプロパティの表示
仮想KVMポリシー （136 ページ）	仮想 *KVM* の設定
vMedia ポリシー （138 ページ）	仮想メディアの設定
ゾーン分割ポリシー （139 ページ）	『*Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide for S3260 Storage Servers*』の「*Dynamic Storage*」

次のタスク

サーバにポリシーを適用します。ハードウェア ポリシーの適用 （142 ページ）を参照してください。

BIOS ポリシー

BIOS ポリシーは、サーバに対する BIOS 設定の設定を自動化します。1 つのサーバまたはサーバ セットのニーズに適合する特定の BIOS 設定のグループを含む、1 つ以上の BIOS ポリシーを作成できます。サーバの BIOS ポリシーを指定しない場合、BIOS 設定はデフォルト値のセット（新品のベア メタル サーバの場合）、あるいは以前に Cisco IMC を使用して設定した値のセットになります。BIOS ポリシーを指定すると、それまでにサーバに設定されているすべての値はその値に置き換えられます。

さまざまな BIOS プロパティの設定の詳細については、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』の「*Configuring BIOS Settings*」の項を参照してください。

手順

ステップ 1 [ハードウェア ポリシー（Hardware Policies）] を選択した後で [追加（Add）] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [追加（Add）] 画面で、ドロップダウンリストから [BIOS ポリシー（BIOS Policy）] を選択して [送信（Submit）] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドに名前を入力します。

[サーバの現在の設定からポリシーを作成（Create policy from current configuration of the server）] チェックボックスをオンにして、[次へ（Next）] をクリックすることもできます。[サーバの詳細（Server Details）] 画面が表示されます。既存の設定からのポリシーの作成（140 ページ）を参照してください。

ステップ 4 ポリシーが Cisco UCS S3260 サーバのポリシーの場合は [Cisco UCS S3260] チェック ボックスをオンにし、[次へ（Next）] をクリックします。

ステップ 5 [メイン（Main）] 画面で、主要な BIOS プロパティ（[ブート オプション再試行（Boot Option Retry）]、[Post エラー一時停止（Post Error Pause）]、および [TPM サポート（TPM Support）] ドロップダウンリストのエントリなど）の値を選択します。[電源オンパスワードのサポート（Power ON Password Support）] ドロップダウンリストでは電源オン時のパスワード サポートを有効または無効にすることができます。デフォルトのプラットフォーム設定を選択することもできます。これを有効にすると、設定の変更や BIOS セットアップへのアクセスなど、サーバに変更を加えることができません。

（注） CIMC UI を使用し、[BIOS 設定（BIOS Configuration）] 画面で BIOS パスワードが設定されていることを確認します。

ステップ 6 [詳細設定（Advanced）] 画面で、BIOS のプロパティ値をドロップダウンリストから選択して [次へ（Next）] をクリックします。

ステップ 7 [サーバ管理（Server Management）] 画面で、サーバのプロパティ値をドロップダウンリストから選択して [送信（Submit）] をクリックします。

（注） BIOS ポリシーには、すべての使用可能なプラットフォームのためのトークンが表示されます。

- 属性が特定のサーバプラットフォームに対して有効でない場合、トークンは無視されます。たとえば、Power On Password Support BIOS トークンは、3.x ファームウェアを実行しているサーバにのみ適用されます。このトークンは、3.x より前のファームウェアを実行しているサーバに適用されると、無視されます。
- 属性がターゲットプラットフォームに存在しており、その値が該当しない場合、エラーが発生します。たとえば、Extended APIC BIOS トークンには Enabled および Disabled という値がありますが、これは、プラットフォーム A に基づくサーバモデルにのみ該当します。ただし、このトークンがプラットフォーム B のサーバモデルに適用されると、xml 解析エラーが表示されます。

ディスクグループポリシー

ディスク グループ ポリシーを使用すると、仮想ドライブに使われる物理ディスクを選択することができ、特定の仮想ドライブに関連するさまざまな属性の設定もできます。仮想ドライブの作成に使用される物理ディスクのグループをディスクグループと呼びます。

ディスク グループポリシーは、ディスク グループの作成方法と設定方法を定義します。このポリシーでは、仮想ドライブに使用する RAID レベルを指定します。1 つのディスク グループポリシーを使用して、複数のディスク グループを管理できます。1 つのディスク グループ ポリシーを複数の仮想ドライブに関連付けることができます。この場合、仮想ドライブは同じ仮想ドライブ グループ スペースを共有します。RAIDポリシーで複数の仮想ドライブに関連付けられたディスク グループ ポリシーには、複数のディスク グループ ポリシーで繰り返し使用される物理ディスクは含まれません。RAID ポリシーの詳細については、RAIDポリシー （128 ページ）を参照してください。

ディスク グループの各種プロパティの設定に関する詳細は、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』の「*Managing Storage Adapters*」の項を参照してください。

ディスク グループ ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [ハードウェア ポリシー（Hardware Policies）] を選択した後で [追加（Add）] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [追加（Add）] 画面でドロップダウンリストから [ディスク グループ ポリシー（Disk Group Policy）] を選択し、[送信（Submit）] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドに名前を入力して、[次へ（Next）] をクリックします。

ステップ 4 [仮想ドライブ設定（Virtual Drive Configuration）] 画面で、[RAID レベル（RAID Level）] ドロップダウンリストから RAID レベルを選択し、[次へ（Next）] をクリックします。

ステップ 5 [ローカル ディスク設定（Local Disk Configuration）] 画面で、[+] をクリックしてローカル ディスク設定を参照するエントリを追加し、[送信（Submit）] をクリックします。

（注）
- サーバの現在の設定からディスク グループ ポリシーを作成することはできません。
- RAID ポリシーをサーバの現在の設定から作成すると、ディスク グループ ポリシーもサーバの設定から自動的に作成されます。

FlexFlash ポリシー

FlexFlash ポリシーでは、SD カードを設定して有効にできます。

各種プロパティの設定に関する詳細については、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』の「*Managing the Flexible Flash Controller*」の項を参照してください。

（注）

- FlexFlash をサポートする最小の Cisco Integrated Management Controller のファームウェア バージョンは 2.0(2c) です。
- FlexFlash ポリシーは、Cisco UCS S3260 ラック サーバでは使用できません。

FlexFlash ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [ハードウェア ポリシー（Hardware Policies）] を選択した後で [追加（Add）] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [追加（Add）] 画面で、ドロップダウンリストから [FlexFlash ポリシー（FlexFlash Policy）] を選択して [送信（Submit）] をクリックします。

ステップ 3 **[ポリシー名（Policy Name）]** フィールドに名前を入力して、**[次へ（Next）]** をクリックします。

[サーバの現在の設定からポリシーを作成（Create policy from current configuration of the server）] チェックボックスをオンにして、**[次へ（Next）]** をクリックすることもできます。[サーバの詳細（Server Details）] 画面が表示されます。既存の設定からのポリシーの作成（140 ページ）を参照してください。

ステップ 4 [カードの設定（Configure Cards）] ページで、次のフィールドに入力します。

フィールド	説明
[ファームウェア モード（Firmware Mode）] ペイン	以下のファームウェア動作モードのいずれかを選択します。 • [ミラーモード（Mirror Mode）]：このモードはミラー設定であり、C220 M4 および C240 M4 サーバのみで使用できます。 • [Util モード（Util Mode）]：このモードでは、4 つのパーティションがある 1 枚のカードおよび 1 つのパーティションがある 1 枚のカードが作成されます。このモードを使用できるのは C220 M4 および C240 M4 サーバのみです。 • [適用なし（Not Applicable）]：ファームウェア動作モードは選択されません。[適用なし（Not Applicable）] を選択した場合はステップ 5 に進みます。このモードが使用できるのは、C220 M3、C240 M3、C22、C24、および C460 M4 サーバのみです。
[ミラー（Mirror）] オプション ボタン	[仮想ドライブの有効化（Enable Virtual Drive）] チェックボックスをオンにして [Hypervisor] 仮想ドライブを有効にするか、または [仮想ドライブの消去（Erase Virtual Drive）] チェックボックスをオンにして仮想ドライブを消去します。
[ユーティリティ（Util）] オプション ボタン	[仮想ドライブの有効化（Enable Virtual Drive）] をオンにして仮想ドライブ（[SCU]、[Hypervisor]、[ドライバ（Drivers）]、[HUU]、および [ユーザ パーティション（User Partition）]）を有効にするか、または [仮想ドライブの消去（Erase Virtual Drive）] チェックボックスをオンにして仮想ドライブを消去します。 （注） 複数の仮想ドライブを選択できます。

フィールド	説明
[適用なし（Not Applicable）] ラジオボタン	[仮想ドライブの有効化（Enable Virtual Drive）] オンにして仮想ドライブ（[SCU]、[HV]、[ドライバ（Drivers）]、および [HUU]）を有効にします。 （注） • 複数の仮想ドライブを選択できます。 • [仮想ドライブの消去（Erase Virtual Drive）] チェックボックスは使用できません。
[パーティション名（Partition Name）] フィールド（[ミラー（Mirror）] および [Util] モードでのみ使用可能）	パーティションの名前。
[非 Util カード パーティション名（Non Util Card Partition Name）] フィールド	2 枚目のカード（ある場合）の単一パーティションに割り当てる名前。 （注） このオプションは、ユーティリティモードの場合にのみ使用できます。
[プライマリ カードの選択（Select Primary Card）]（ミラーモードの場合に使用可能）または [Util カードの選択（Select Util Card）]（Util モードの場合に使用可能）ドロップダウンリスト。	SD カードがある場合は [スロット 1（Slot 1）] または [スロット 2（Slot 2）] を選択し、SD カードがサーバに 1 枚しかない場合は [なし（None）] を選択します。 （注） [なし（None）] は [Util カードの選択（Select Util Card）] オプションの場合にのみ選択できます。
[自動同期（Auto Sync）] チェックボックス	選択されたスロットで使用できる SD カードを自動的に同期します。 （注） このオプションは、ミラーモードの場合にのみ使用できます。

フィールド	説明
[スロット 1 読み取りエラーしきい値（Slot-1 Read Error Threshold）] フィールド	Cisco FlexFlash カードのスロット 1 へのアクセス中に許容される読み取りエラーの数。あるカードでの読み取りエラーの数がこのしきい値を超えた場合、そのカードには正常でないというマークが付けられます。 読み取りエラーしきい値を指定するには、1以上 255 以下の整数を入力します。検出されたエラー数に関係なく、カードが無効にならないように指定するには、0（ゼロ）を入力します。
[スロット 1 書き込みエラーしきい値（Slot-1 Write Error Threshold）] フィールド	Cisco Flexible Flash カードのスロット 1 へのアクセス中に許容される読み取りエラーの数。あるカードでの書き込みエラーの数がこのしきい値を超えた場合、そのカードには正常でないというマークが付けられます。 書き込みエラーしきい値を指定するには、1以上 255 以下の整数を入力します。検出されたエラー数に関係なく、カードが無効にならないように指定するには、0（ゼロ）を入力します。
[スロット 2 読み取りエラーしきい値（Slot-2 Read Error Threshold）] フィールド	Cisco FlexFlash カードのスロット 2 へのアクセス中に許容される読み取りエラーの数。あるカードでの読み取りエラーの数がこのしきい値を超えた場合、そのカードには正常でないというマークが付けられます。 読み取りエラーしきい値を指定するには、1以上 255 以下の整数を入力します。検出されたエラー数に関係なく、カードが無効にならないように指定するには、0（ゼロ）を入力します。 （注） このオプションは、ユーティリティモードの場合にのみ使用できます。ミラーモードの場合、スロット 1 の読み取り/書き込みしきい値はスロット 2 にも適用されます。

フィールド	説明
[スロット 2 書き込みエラーしきい値（Slot-2 Write Error Threshold）] フィールド	Cisco Flexible Flash カードのスロット 2 へのアクセス中に許容される読み取りエラーの数。あるカードでの書き込みエラーの数がこのしきい値を超えた場合、そのカードには正常でないというマークが付けられます。 書き込みエラーしきい値を指定するには、1以上 255 以下の整数を入力します。検出されたエラー数に関係なく、カードが無効にならないように指定するには、0（ゼロ）を入力します。 （注） このオプションは、ユーティリティモードの場合にのみ使用できます。ミラーモードの場合、スロット1の読み取り/書き込みしきい値はスロット 2 にも適用されます。

ステップ 5 ステップ 4 の [詳細（Details）] ペインで [適用なし（Not Applicable）] を選択した場合は、以下のフィールドを入力します。

フィールド	説明
[仮想ドライブの有効化（Virtual Drive Enable）] ドロップダウンリスト	USB 形式のドライブとして、サーバに対して使用可能にできる仮想ドライブ。
[RAID プライマリ メンバー（RAID Primary Member）] ドロップダウンリスト	プライマリ RAID メンバが存在するスロット。
[RAID セカンダリ ロール（RAID Secondary Role）] ドロップダウンリスト	セカンダリ RAID の役割です。
[I/O 読み取りエラーしきい値（I/O Read Error Threshold）] フィールド	Cisco FlexFlash カードへのアクセス時の読み取りエラーの許容数。あるカードでの読み取りエラーの数がこのしきい値を超えた場合、そのカードには正常でないというマークが付けられます。 読み取りエラーしきい値を指定するには、1以上 255 以下の整数を入力します。検出されたエラー数に関係なく、カードが無効にならないように指定するには、0（ゼロ）を入力します。

フィールド	説明
[I/O 書き込みエラーしきい値（I/O Write Error Threshold）] フィールド	Cisco FlexFlash カードへのアクセス時の書き込みエラーの許容数。あるカードでの書き込みエラーの数がこのしきい値を超えた場合、そのカードには正常でないというマークが付けられます。 Cisco FlexFlash カードへのアクセス時の書き込みエラーの許容数。あるカードでの書き込みエラーの数がこのしきい値を超えた場合、そのカードには正常でないというマークが付けられます。
[エラーをクリア（Clear Errors）] チェックボックス	オンにした場合、[送信（Submit）] をクリックすると、読み取り/書き込みエラーがクリアされます。

ステップ 6 [送信（Submit）] をクリックします。

[ハードウェア ポリシー（Hardware Policies）] テーブルで既存の FlexFlash ポリシーを選択後、ユーザ インターフェイスで各操作オプションを選択すれば、そのポリシーの削除、編集、複製、適用や、適用状況の表示を実施することができます。

（注） FlexFlash のポリシーの適用は、以下の 2 つのステップで行われます。

1. サーバの設定がデフォルトに設定されます。
2. ポリシーの新しい設定が適用されます。そのため、このステップで何らかの障害が発生した場合、既存の設定はポリシーに適用される前に失われます。

IPMI Over LANポリシー

インテリジェント プラットフォーム管理インターフェイス（IPMI）では、サーバ プラットフォームに組み込まれているサービス プロセッサとのインターフェイスのためのプロトコルを定義しています。このサービス プロセッサはベースボード管理コントローラ（BMC）と呼ばれ、サーバのマザーボードに存在します。BMC は、メイン プロセッサおよびボード上の他の要素に、簡単なシリアル バスを使用してリンクします。IPMI メッセージで Cisco IMC を管理する場合は IPMI over LAN ポリシーを設定します。

各種プロパティの設定の詳細については、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』の「*Configuring IPMI*」の項を参照してください。

IPMI Over LAN ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [ハードウェア ポリシー（Hardware Policies）] を選択した後で [追加（Add）] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [追加（Add）] 画面で、ドロップダウンリストから [IPMI Over LAN ポリシー（IPMI Over LAN Policy）] を選択して [送信（Submit）] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドに名前を入力して、[次へ（Next）] をクリックします。

[サーバの現在の設定からポリシーを作成（Create policy from current configuration of the server）] チェックボックスをオンにして、[次へ（Next）] をクリックすることもできます。[サーバの詳細（Server Details）] 画面が表示されます。既存の設定からのポリシーの作成（140 ページ）を参照してください。

ステップ 4 ラックマウント サーバ用にこのポリシーを作成している場合は、次の手順を実行します。

a) [メイン（Main）] ダイアログボックスで、次のフィールドに情報を入力します。

オプション	説明
IPMI Over LANの有効化	IPMI プロパティを設定するには、このチェックボックスをオンにします。
権限レベル制限	ドロップダウンリストから権限レベルを選択します。
暗号化キー	このフィールドにキーを入力します。

（注） 暗号キーは 40 文字を超えない偶数の 16 進数文字である必要があります。指定した文字数が 40 未満の場合、キーの長さが 40 文字になるようゼロが追加されます。

b) [次へ（Next）] をクリックします。

c) [確認（Confirm）] 画面で [送信（Submit）] をクリックします。
[ハードウェア ポリシー（Hardware Policies）] ページの [サーバ プラットフォーム（Server Platform）] カラムにラックマウント サーバが一覧表示されます。

ステップ 5 ポリシーが Cisco UCS S3260 サーバのポリシーの場合は [Cisco UCS S3260] チェック ボックスをオンにし、[次へ（Next）] をクリックします。

ステップ 6 [CMS 設定（CMC Settings）] 画面で、必要に応じて、CMC 1 と CMC 2 の両方の [IPMI Over LAN の有効化（Enable IPMI Over LAN）] チェックボックスをオンにします。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 [BMC 設定（BMC Settings）] 画面で、必要に応じて、BMC 1 と BMC2 の両方の [IPMI Over LAN の有効化（Enable IPMI Over LAN）] チェックボックスをオンにします。

ステップ 9 [確認（Confirm）] 画面で [送信（Submit）] をクリックします。

[ハードウェア ポリシー（Hardware Policies）] ページの [サーバ プラットフォーム（Server Platform）] カラムに Cisco UCS S3260 高密度ストレージ ラック サーバが一覧表示されます。

LDAPポリシー

Cisco C シリーズ サーバと E シリーズ サーバは LDAP をサポートしています。Cisco IMC Supervisor は LDAP ポリシーを使用したサーバでの LDAP 設定をサポートしています。1 つのサーバまたはサーバ セットのニーズに適合する特定の LDAP 設定のグループを含む、1 つ以上の LDAP ポリシーを作成できます。

各種 LDAP プロパティの設定の詳細については、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』の「*Configuring LDAP Server*」を参照してください。

手順

ステップ 1 [ハードウェア ポリシー（Hardware Policies）] を選択した後で [追加（Add）] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [追加（Add）] 画面で、ドロップダウンリストから [LDAP ポリシー（LDAP Policy）] を選択して [送信（Submit）] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドに名前を入力します。

[サーバの現在の設定からポリシーを作成（Create policy from current configuration of the server）] チェックボックスをオンにして、[次へ（Next）] をクリックすることもできます。[サーバの詳細（Server Details）] 画面が表示されます。既存の設定からのポリシーの作成（140 ページ）を参照してください。

ステップ 4 ポリシーが Cisco UCS S3260 サーバのポリシーの場合は [Cisco UCS S3260] チェック ボックスをオンにし、[次へ（Next）] をクリックします。

ステップ 5 [メイン（Main）] 画面で、LDAP のプロパティを入力し、[次へ（Next）] をクリックします。

ステップ 6 [LDAP サーバの設定（Configure LDAP Servers）] 画面で、LDAP サーバの詳細を入力し、[次へ（Next）] をクリックします。

ステップ 7 [グループ認証（Group Authorization））] 画面でグループ認証の詳細を入力し、[+] をクリックして LDAP グループ エントリをテーブルに追加します。

ステップ 8 [LDAP グループへのエントリの追加（Add Entry to LDAP Groups）]画面で、グループの詳細を入力し、[送信（Submit）] をクリックします。

（注）
- それまでにサーバで設定した既存の LDAP ロール グループが削除され、ポリシーで設定したロール グループに置き換えられます。ポリシーにロール グループを追加していない場合、サーバの既存のロール グループはただ削除されます。
- [検索するグループのネスト レベル（Nested Group Search Depth）] は、Cisco IMC バージョン 2.0(4c) 以降のみに適用されます。バージョン 2.0(4c) より古い Cisco IMC が稼働しているサーバでポリシーを使用してこの値を適用することはできません。

レガシー ブート順序ポリシー

レガシー ブート順序ポリシーはブート順序設定の構成を自動化します。1 つのサーバまたはサーバのセットの要件に対応するブート順序設定の特定のグループ化を含む、1 つまたは複数のレガシー ブート順序ポリシーを作成できます。Cisco IMC Supervisor を使用して、使用可能なブート デバイス タイプからサーバがブートを試行する順序を設定できます。デバイスの線形順序付けを可能にする高精度ブート順序を設定することもできます。高精度のブート順序ポリシー （126 ページ）を参照してください。

サーバ ブート順序の各種プロパティの設定に関する詳細については、『Cisco UCS C-Series Servers Integrated Management ControllerGUI Configuration Guide』の「*ServerBoot Order*」のセクションを参照してください。

（注） レガシー ブート順序ポリシーは Cisco UCS S3260 Rack Server では使用できません。

手順

ステップ 1 [ハードウェア ポリシー（Hardware Policies）] を選択した後で [追加（Add）] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [追加（Add）] 画面で、ドロップダウンリストから [レガシー ブート順序ポリシー（Legacy Boot Order Policy）] を選択し、[送信（Submit）] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドに名前を入力して、[次へ（Next）] をクリックします。

[サーバの現在の設定からポリシーを作成（Create policy from current configuration of the server）] チェックボックスをオンにして、[次へ（Next）] をクリックすることもできます。[サーバの詳細（Server Details）] 画面が表示されます。既存の設定からのポリシーの作成 （140 ページ）を参照してください。

ステップ 4 [メイン（Main）] 画面で、[+] をクリックし、ドロップダウンリストからデバイス タイプを選択します。追加したデバイスがテーブルに一覧表示されます。

[デバイスの選択（Select Devices）]テーブルで、既存のデバイスを選択し、[x]をクリックしてデバイスを削除します。上下の矢印アイコンを使用して、エントリの順序を変更します。テーブル内のエントリの順序によってブート順序が定まります。

同じデバイス タイプを再度追加することはできません。

ステップ 5 [選択デバイスへのエントリの追加（Add Entry to Select Devices）] 画面で [送信（Submit）] をクリックします。

（注） このポリシーは 2.0 より前の Cisco IMC バージョンにのみ適用されます。これよりも高い Cisco IMC バージョンを実行しているサーバにポリシーが適用された場合、エラー メッセージが表示されます。代わりに高精度ブート順序ポリシーを使用します。

ネットワーク構成ポリシー

Cisco IMC Supervisor では、サーバの以下のネットワーク設定を指定できるネットワーク構成ポリシーを作成できます。

- DNS Domain
- IPv4 および IPv6 用の DNS サーバ
- VLAN の設定

さまざまなネットワーク構成プロパティの設定の詳細については、『 Integrated Management Controller GUI Guide』の「 *Network-Related Settings*」の項を参照してください。

ネットワーク構成ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [ハードウェア ポリシー（Hardware Policies）] を選択した後で [追加（Add）] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [追加（Add）]ダイアログボックスで、ドロップダウンリストから[ネットワーク構成ポリシー（Network Configuration Policy）] を選択し、[送信（Submit）] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドに名前を入力して、[次へ（Next）] をクリックします。

[サーバの現在の設定からポリシーを作成（Create policy from current configuration of the server）] チェックボックスをオンにして、[次へ（Next）]をクリックすることもできます。[サーバの詳細（Server Details）] ウィンドウが表示されます。「既存の設定からのポリシーの作成 （140 ページ）」を参照してください。

ステップ 4 ラックマウント サーバ用にこのポリシーを作成している場合は、次の手順を実行します。

a) [メイン（Main）] 画面で、次のフィールドに情報を入力します。

フィールド	説明
共通プロパティ	
[ダイナミック DNS の使用（Use Dynamic DNS）] チェックボックス	ダイナミック DNS は、DNS サーバのリソース レコードを追加または更新するために使用されます。 Cisco IMC Supervisor
[ダイナミック DNS の使用（Use Dynamic DNS）] チェックボックスをオンにする場合	
[**Dynamic DNS Update Domain**] フィールド	ドメインを指定できます。ドメインは、メイン ドメインまたはサブ ドメインのどちらでも可です。このドメイン名は、DDNS 更新のため Cisco IMC Supervisor のホスト名に付加されます。
IPv4 のプロパティ	
[Obtain DNS Server Addresses from DHCP] チェックボックス	オンにすると、Cisco IMC Supervisor は DNS サーバ アドレスを DHCP から取得します。
[DHCP から DNS サーバ アドレスを取得する（Obtain DNS Server Addresses from DHCP）] チェックボックスをオフにする場合	
[Preferred DNS Server] フィールド	プライマリ DNS サーバの IP アドレス。
[Alternate DNS Server] フィールド	セカンダリ DNS サーバの IP アドレス。
IPv6 のプロパティ	
[Obtain DNS Server Addresses from DHCP] チェックボックス	オンにすると、Cisco IMC Supervisor は DNS サーバ アドレスを DHCP から取得します。
[DHCP から DNS サーバ アドレスを取得する（Obtain DNS Server Addresses from DHCP）] チェックボックスをオフにする場合	
[Preferred DNS Server] フィールド	プライマリ DNS サーバの IP アドレス。
[Alternate DNS Server] フィールド	セカンダリ DNS サーバの IP アドレス。
VLAN のプロパティ	
[Enable VLAN] チェックボックス	オンにすると、仮想 LAN に接続されます。
[VLAN の有効化（Enable VLAN）] チェックボックスをオンにする場合	
[VLAN ID] フィールド	VLAN ID。
[優先順位（Priority）] フィールド	VLAN でのこのシステムのプライオリティ。

b) [次へ（Next）] をクリックします。

c) [確認（Confirm）] 画面で [送信（Submit）] をクリックします。
[ハードウェア ポリシー（Hardware Policies）] ページの [サーバ プラットフォーム（Server Platform）] カラムにラックマウント サーバがリストされます。

ステップ 5 ポリシーが Cisco UCS S3260 サーバのポリシーの場合は [Cisco UCS S3260] チェック ボックスをオンにし、[次へ（Next）] をクリックします。

ステップ 6 [メイン（Main）] 画面で、次のフィールドに情報を入力します。

フィールド	説明
共通プロパティ	
[ダイナミック DNS の使用（Use Dynamic DNS）] チェックボックス	ダイナミック DNS は、DNS サーバのリソース レコードを追加または更新するために使用されます。 Cisco IMC Supervisor
[ダイナミック DNS の使用（Use Dynamic DNS）] チェックボックスをオンにする場合	
[**Dynamic DNS Update Domain**] フィールド	ドメインを指定できます。ドメインは、メイン ドメインまたはサブ ドメインのどちらでも可です。このドメイン名は、DDNS 更新のため Cisco IMC Supervisor のホスト名に付加されます。
IPv4 のプロパティ	
[Use DHCP] チェックボックス	オンにすると、[DHCP から DNS サーバ アドレスを取得する（Obtain DNS Server Addresses from DHCP）] チェックボックスが表示されます。
[Obtain DNS Server Addresses from DHCP] チェックボックス	オンにすると、DNS の DHCP が有効になります。
[DHCP から DNS サーバ アドレスを取得する（Obtain DNS Server Addresses from DHCP）] チェックボックスをオフにする場合	
[Preferred DNS Server] フィールド	プライマリ DNS サーバの IP アドレス。
[Alternate DNS Server] フィールド	セカンダリ DNS サーバの IP アドレス。
IPv6 のプロパティ	
[IPv6の有効化（Enable IPv6）] チェックボックス	オンにすると、[DHCP を使用する（Use DHCP）] チェックボックスが表示されます。
[Use DHCP] チェックボックス	オンにすると、[DHCP から DNS サーバ アドレスを取得する（Obtain DNS Server Addresses from DHCP）] チェックボックスが表示されます。

フィールド	説明
[Obtain DNS Server Addresses from DHCP] チェックボックス	オンにすると、Cisco IMC Supervisor は DNS サーバ アドレスを DHCP から取得します。
[DHCP を使用する（Use DHCP）] チェックボックスをオンにしない場合	
[管理 IP アドレス（Management IP Address）] フィールド	管理 IP アドレスを入力します。
[プレフィクス長（Prefix Length）]フィールド	プレフィックス長の文字数を入力します。
[ゲートウェイ（Gateway）]フィールド	ゲートウェイの IP アドレスを入力します。
[DHCP から DNS サーバ アドレスを取得する（Obtain DNS Server Addresses from DHCP）] チェックボックスをオフにする場合	
[Preferred DNS Server] フィールド	プライマリ DNS サーバの IP アドレス。
[Alternate DNS Server] フィールド	セカンダリ DNS サーバの IP アドレス。
VLAN のプロパティ	
[Enable VLAN] チェックボックス	オンにすると、仮想 LAN に接続されます。
[VLAN の有効化（Enable VLAN）] チェックボックスをオンにする場合	
[VLAN ID] フィールド	VLAN ID。
[優先順位（Priority）] フィールド	VLAN でのこのシステムのプライオリティ。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 [CMC 設定（CMC Settings）] 画面で、必要に応じて、CMC 1 と CMC 2 の両方の以下のフィールドに入力します。

フィールド	説明
[Hostname] フィールド	サーバのホスト名。
[IPv4アドレス（IPv4 Address）]フィールド	IPv4 IP アドレス。
[IPv6 アドレス（IPv6 Address）] フィールド	IPv6 IP アドレス。

ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 [BMC 設定（CMC Settings）] 画面で、必要に応じて、BMC 1 と BMC 2 の両方の以下のフィールドに入力します。

フィールド	説明
[Hostname] フィールド	サーバのホスト名。

フィールド	説明
[IPv4アドレス（IPv4 Address）]フィールド	IPv4 IP アドレス。
[IPv6 アドレス（IPv6 Address）] フィールド	IPv6 IP アドレス。

ステップ 11 [次へ（Next）] をクリックします。

ステップ 12 [確認（Confirm）] 画面で [送信（Submit）] をクリックします。

注意 Cisco IMC Supervisor とラック サーバの間のネットワークの DHCP 設定に依存する通信が遮断されないようにするため、次の設定を使用するときには注意してください

DNS IP アドレスを取得するために DHCP を使用すると、システムはサーバの管理 IP アドレスの取得にも DHCP を使用するようにラック サーバ（このポリシーが適用される）を設定します。

ネットワークセキュリティポリシー

Cisco IMC Supervisor は、IP ブロッキングをネットワーク セキュリティとして使用します。IP ブロッキングは、サーバまたは Web サイトと、特定の IP アドレスまたはアドレス範囲との間の接続を防ぎます。IP ブロッキングは、これらのコンピュータから Web サイト、メール サーバ、またはその他のインターネット サーバへの不要な接続を効果的に禁止します。1 台のサーバまたは複数台のサーバのセットの要件に一致する、IP プロパティの特定のグループ化を含む、1 つまたは複数のネットワーク セキュリティ ポリシーを作成できます。

ネットワーク セキュリティ ポリシーを作成する際に 4 つの IP フィルタリング プロパティを設定できます。IP フィルタリングにより選択済みの IP のセットでサーバにアクセスできます。4 つあるフィルタ フィールドのいずれかに単一の IP アドレスを入力するか、または IP アドレスの範囲をハイフンで区切って入力できます。IP アドレスには IPv4 アドレスまたは IPv6 アドレスを使用できます。

さまざまなネットワーク セキュリティ プロパティの設定の詳細については、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』の「*Network Security Configuration*」の項を参照してください。

ネットワーク セキュリティ ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [ハードウェア ポリシー（Hardware Policies）] を選択した後で [追加（Add）] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [追加（Add）] 画面で、ドロップダウンリストから [ネットワーク セキュリティ（Network Security）] を選択し、[送信（Submit）] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドに名前を入力します。

[サーバの現在の設定からポリシーを作成（Create policy from current configuration of the server）] チェックボックスをオンにして、[次へ（Next）] をクリックすることもできます。[サーバの詳細（Server Details）] ウィンドウが表示されます。既存の設定からのポリシーの作成（140 ページ）を参照してください。

ステップ 4 ポリシーが Cisco UCS S3260 サーバのポリシーの場合は [Cisco UCS S3260] チェック ボックスをオンにし、[次へ（Next）] をクリックします。

ステップ 5 [IP ブロッキング（IP Blocking）] ウィンドウで、IP をブロックするために [IP ブロッキングの有効化（Enable IP Blocking）] チェックボックスをオンにし、IP ブロック プロパティを設定するために属性を入力します。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 [IP フィルタリング（IP Filtering）] 画面で、[IP フィルタリングの有効化（Enable IP Filtering）] チェックボックスをオンにして IP を有効にし、単一の IP アドレスまたは IP アドレスの範囲を入力します。

（注） [フィルタ 1（Filter 1）] はデフォルトで Cisco IMC Supervisor の IP アドレスを表示します。

ステップ 8 [送信（Submit）] をクリックします。

NTPポリシー

NTP サービスにより、Cisco IMC Supervisorが管理するサーバを設定して NTP サーバとの間で時刻を同期することができます。デフォルトでは、NTP サーバは Cisco IMC Supervisor では動作しません。NTP サービスを有効化するには、NTP サーバとして動作する 1 ～ 4 台のサーバの IP/DNS アドレスを指定する必要があります。NTP サービスを有効にすると、Cisco IMC Supervisor は設定された NTP サーバと時刻を同期します。

さまざまな NTP プロパティの設定の詳細については、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』の「*Configuring NetworkTime Protocol Settings*」の項を参照してください。

NTP ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [ハードウェア ポリシー（Hardware Policies）] を選択した後で [追加（Add）] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [追加（Add）] 画面で、ドロップダウンリストから [NTP ポリシー（NTP Policy）] を選択して [送信（Submit）] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドに名前を入力します。

[サーバの現在の設定からポリシーを作成（Create policy from current configuration of the server）] チェックボックスをオンにして、[次へ（Next）] をクリックすることもできます。[サーバの詳

細（Server Details）]画面が表示されます。既存の設定からのポリシーの作成（140ページ）を参照してください。

ステップ 4 ポリシーが Cisco UCS S3260 サーバのポリシーの場合は [Cisco UCS S3260] チェック ボックスをオンにし、[次へ（Next）] をクリックします。

ステップ 5 [メイン（Main）] 画面で [NTP の有効化（Enable NTP）] チェックボックスをオンにして代替サーバを有効にし、NTP サーバを 4 つまで指定します。

ステップ 6 [送信（Submit）] をクリックします。

（注） このポリシーは、E シリーズ サーバ モデルには適用できません。

パスワードの有効期限ポリシー

パスワードが期限切れになる有効期限を設定できます。管理者はこの期間を日単位で設定できます。この設定はすべてのユーザに対して共通です。ユーザは、ユーザ ポリシーの一部として構成を設定して派生させ、パスワード有効期限ポリシーを作成することができます。

さまざまなプロパティの設定の詳細については、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』の「*Configuring Password Expiry for Users*」の項を参照してください。

パスワード有効期限ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [ハードウェア ポリシー（Hardware Policies）] を選択した後で [追加（Add）] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [追加（Add）]画面で、ドロップダウンリストから [パスワードの有効期限ポリシー（Password Expiration Policy）] を選択して [送信（Submit）] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドに名前を入力します。

ステップ 4 [メイン（Main）] 画面で、次のフィールドに情報を入力します。

フィールド	説明
[パスワード有効期日を有効にする（Enable Password Expiry）] チェックボックス	指定したパスワードの有効期限を有効にするには、このチェックボックスをオンにして、次の項目を入力します。 [パスワードの有効期間（Password Expiry Duration）]：パスワードが期限切れになる日数を設定します。
[パスワード履歴（Password History）] フィールド	パスワード履歴を表示するときに表示される件数を設定します。

フィールド	説明
[通知期間（Notification Period）] フィールド	パスワードの有効期限について通知されるまでの日数を設定します。
[猶予期間（Grace Period）] フィールド	パスワードの期限が切れるまでの猶予期間を設定します。

ステップ 5 [送信（Submit）] をクリックします。

（注）
- 既存のポリシーを選択し、[プロパティ（Properties）] または [削除（Delete）] をクリックして、[その他のアクション（More Actions）] ドロップダウンリストからポリシーを編集または削除することもできます。
- このポリシーは、ユーザポリシーとともに適用する必要があります。パスワード有効期限ポリシーを個別に適用することはできません。
- E シリーズ サーバは、パスワード有効期限ポリシーをサポートしていません。

高精度のブート順序ポリシー

高精度ブート順序を設定すると、デバイスの線形順序付けが可能になります。Cisco IMC Supervisor では、ブート順およびブート モードの変更、各デバイス タイプ下への複数のデバイスの追加、ブート順の並び替え、各デバイス タイプのパラメータの設定ができます。

ブート順序の各種プロパティの設定に関する詳細については、『Cisco UCS C-Series Servers Integrated Management ControllerGUI Configuration Guide』の「*Configuring the Precision Boot Order*」のセクションを参照してください。

このポリシーは、Cisco IMCバージョン 2.x 以降を実行しているサーバで作成できます。2.x より前のバージョンを実行しているサーバでは、レガシーブート順序ポリシーを代わりに設定してください。

高精度ブート順序ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [ハードウェア ポリシー（Hardware Policies）] を選択した後で [追加（Add）] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [追加（Add）] ウィンドウで、ドロップダウンリストから [高精度ブート順序ポリシー（Precision Boot Order Policy）] を選択し、[送信（Submit）] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドに名前を入力します。

[サーバの現在の設定からポリシーを作成（Create policy from current configuration of the server）] チェックボックスをオンにして、**[次へ（Next）]** をクリックすることもできます。

[サーバの詳細（Server Details）] ウィンドウが表示されます。既存の設定からのポリシーの作成 （140 ページ）を参照してください。

ステップ 4 ポリシーが Cisco UCS S3260 サーバのポリシーの場合は [Cisco UCS S3260] チェック ボックスをオンにし、[次へ（Next）] をクリックします。

ステップ 5 [メイン（Main）] ウィンドウで、[UEFI セキュア ブート（UEFI Secure Boot）] チェックボックスをオンにするか、[ブート モードの設定（Configure Boot Mode）] ドロップダウンリストからブート モードを選択します。

ステップ 6 [+] をクリックし、デバイスの詳細を選択または入力します。追加したデバイスがテーブルに一覧表示されます。

また、[デバイスの選択（Select Devices）]テーブルで既存のデバイスを選択し、[x] をクリックして削除したり、編集アイコンをクリックしてデバイスを編集したりすることもできます。上下の矢印アイコンを使用して、エントリの順序を変更します。テーブル内のエントリの順序によってブート順序が定まります。

ステップ 7 [選択デバイスへのエントリの追加（Add Entry to Select Devices）] ページで [送信（Submit）] をクリックします。

ステップ 8 サーバを 1 回起動する必要があるデバイスを設定するには、[ワンタイム ブート デバイスの設定（Configure One Time Boot Device）] チェックボックスをオンにします。

ステップ 9 [ワンタイム ブート デバイス（One Time Boot Device）] ドロップダウンリストから、1 回限り設定するブート デバイスを選択します。

（注） [ワンタイムブートデバイスの設定（ One Device）] は、3.0(1c)より古いバージョンのCIMCには適用されません。

ステップ 10 選択したサーバでワンタイム ブート デバイスが更新された後でサーバをリブートするには、[更新時に再起動（Reboot On Update）] チェックボックスをオンにします。

ステップ 11 [送信（Submit）] をクリックします。

電力復元ポリシー

E シリーズ サーバの Cisco IMC にログインせずに、そのサーバで設定されている電力復元ポリシーの値を変更する場合に、このポリシーを作成します。

（注） E シリーズのサーバに対してのみこのポリシーを作成することができます。このポリシーは ENCS サーバまたは C シリーズ サーバでのみ作成できます。

手順

ステップ 1 [ハードウェア ポリシー（Hardware Policies）] を選択した後で [追加（Add）] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [追加（Add）] 画面で、ドロップダウンリストから [電力復元ポリシー（Power Restore Policy）] を選択して [送信（Submit）] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドに名前を入力します。

[サーバの現在の設定からポリシーを作成（Create policy from current configuration of the server）] チェックボックスをオンにして、[次へ（Next）] をクリックすることもできます。[サーバの詳細（Server Details）] 画面が表示されます。既存の設定からのポリシーの作成（140 ページ）を参照してください。

ステップ 4 [電力復元ポリシー（Power Restore Policy）] リストから設定を選択します。

次のいずれかの頻度を指定できます。

- [電源オフ（Power-off）]
- 電源投入
- [最後の状態の復元（Restore-last-state）]

ステップ 5 [送信（Submit）] をクリックします。

次のタスク

このポリシーを適用する必要があります。詳細については、ハードウェア ポリシーの適用（142 ページ）を参照してください。

RAIDポリシー

RAID ポリシーを使用して、サーバで仮想ドライブを作成できます。仮想ドライブのストレージ容量も設定できます。RAIDポリシーの各仮想ドライブはディスク グループポリシーに関連付けられます。ディスク グループ ポリシーを使用して、特定の仮想ドライブに使用するディスクを選択および設定できます。

RAID ポリシーは、次でのみサポートされます。

- RAID 設定をサポートするストレージ コントローラ。
- Cisco IMC ファームウェア バージョン 2.0(4c) 以降。
- 単一のストレージコントローラを含むサーバ。複数のストレージコントローラを含むサーバでは、最初のスロットのストレージ コントローラにのみ RAID ポリシーが適用されます。

各種プロパティの設定の詳細については、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』の「*Managing Storage Adapters*」の項を参照してください。

RAID ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [ハードウェア ポリシー（Hardware Policies）] を選択した後で [追加（Add）] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [追加（Add）] ウィンドウで、ドロップダウンリストから [RAID ポリシー（RAID Policy）] を選択し、[送信（Submit）] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドに名前を入力します。

[サーバの現在の設定からポリシーを作成（Create policy from current configuration of the server）] チェックボックスをオンにして、**[次へ（Next）]** をクリックすることもできます。[サーバの詳細（Server Details）] ウィンドウが表示されます。既存の設定からのポリシーの作成 （140 ページ）を参照してください。

ステップ 4 ポリシーが Cisco UCS S3260 サーバのポリシーの場合は [Cisco UCS S3260] チェック ボックスをオンにし、[次へ（Next）] をクリックします。

ステップ 5 [ドライブ セキュリティ（Drive Security）] ウィンドウで、[ドライブセキュリティの設定（Configure Drive Security）] チェックボックスをオンにしてドライブのセキュリティを設定します。

ステップ 6 [ドライブ セキュリティの有効化（Enable Drive Security）] または [ドライブ セキュリティの無効化（Disable Drive Security）] ラジオボタンを選択して、ドライブのセキュリティを有効または無効にします。

（注） ドライブのセキュリティを有効にすると、セキュリティ キーの詳細を入力できるようになります。

ステップ 7 [ドライブ セキュリティの有効化（Enable Drive Security）] を選択して次のフィールドに情報を入力します。

フィールド	説明
[ローカル鍵管理（Local Key Management）] チェックボックス	このチェックボックスは、デフォルトでオンになっています。
[セキュリティキー（Security Key）] フィールド	セキュリティキーを入力します。
[セキュリティ キー ID（Security Key Identifier）] フィールド	セキュリティ キー ID を入力します。
[セキュリティ キーの確認（Confirm Security Key）] フィールド	先ほど入力したセキュリティ キーを確認します。

フィールド	説明
[現在のセキュリティ キー（Current Security Key）] フィールド	セキュリティ キーを変更する場合のみ、キーを入力します。

（注） Cisco IMC Supervisor が RAID ポリシーとセキュリティ キーをエクスポートすると、Cisco IMC Supervisorによるセキュリティ キーの露出を防ぐため、セキュリティ キー パラメータは空のままになります。このため、値は手動で入力する必要があります。

ステップ 8 [仮想ドライブ設定（Virtual Drive Configuration）] ウィンドウで [+] をクリックして、サーバ上に設定する仮想ドライブを追加します。

ステップ 9 [+] をクリックして、仮想ドライブテーブルにエントリを追加します。[仮想ドライブへのエントリの追加（Add Entry to Virtual Drives）] ページで次のフィールドに情報を入力します。

フィールド	説明
[仮想ドライブ名（Virtual Drive Name）] フィールド	指定したパスワードの有効期限を有効にするには、このチェックボックスをオンにして、次の項目を入力します。 [パスワードの有効期間（Password Expiry Duration）]：パスワードが期限切れになる日数を設定します。
[仮想ドライブ サイズ（Virtual Drive Size）]	
[ディスク グループ ポリシー（Disk Group Policy）] ドロップダウンリスト	[ディスク グループ ポリシー（Disk Group Policy）] ドロップダウンリストから既存のディスク グループ ポリシーを選択するか、[+] をクリックし、新しいディスク グループ ポリシーを追加してローカル ディスクを指定することができます。ディスクグループポリシー（109 ページ）を参照してください。 （注） 2 つの仮想ドライブを作成して同じディスク グループ ポリシーに関連付けると、同じ仮想ドライブ グループ スペースを共有します
[Access Policy] ドロップダウンリスト	表示されるオプションから選択します。
[読み取りポリシー（Read Policy）] ドロップダウンリスト	表示されるオプションから選択します。
[書き込みポリシー（Write Policy）] ドロップダウンリスト	表示されるオプションから選択します。

フィールド	説明
[IO ポリシー（IO Policy）] ドロップダウンリスト	表示されるオプションから選択します。
[ドライブ キャッシュ（Drive Cache）] ドロップダウンリスト	表示されるオプションから選択します。
[拡張して使用可能（Expand to available）] チェックボックス	ディスクで使用可能な最大容量を使用するために、仮想ドライブ サイズを拡張します。
[ブート ドライブ（Boot Drive）] チェックボックス	作成する仮想ドライブをブート ドライブとして設定します。 （注） 複数のブート ドライブを設定することはできません。
[JBOD 状態のディスクを未構成で良好に設定（Set disks in JBOD state to Unconfigured Good）] チェックボックス	JBOD状態であるディスクを、仮想ドライブの作成に使用される前に未設定の良好状態に設定します。
[完全なディスク暗号化を有効にする（Enable Full Disk Encryption）] チェックボックス	未使用の物理ドライブから仮想ドライブを作成します。

ステップ 10 [送信（Submit）] をクリックします。
[仮想ドライブ（Virtual Drive）] テーブルに、作成した仮想ドライブが表示されます。

ステップ 11 サーバの既存の仮想ドライブをすべて削除するには、[既存の仮想ドライブの削除（Delete existing Virtual Drives）] チェックボックスをオンにします。

このチェックボックスをオンにすると、サーバの既存の仮想ドライブは、ポリシーの適用時にすべて削除されます。これにより、既存のデータが失われる可能性があります。

ステップ 12 [次へ（Next）] をクリックします。

ステップ 13 [物理ドライブ設定（Physical Drive Configuration）] ページで次のようにします。

ステップ 14 [未使用ディスクを設定する（Configure Unused Disks）] チェックボックスをオンにして、未使用ディスクを [未設定で良好（Unconfigured Good）] または [JBOD] 状態として設定するオプションを選択します。

（注） [未設定で良好（Unconfigured Good）] を選択すると、[セキュア ドライブのクリア（Clear Secure Drive）] チェックボックスが表示されます。[JBOD] を選択すると、[セキュア ドライブの有効化（Enable Secure Drive）] チェックボックスが表示されます。

ステップ 15 [セキュア ドライブのクリア（Clear Secure Drive）] をオンにして物理ディスク上のすべてのデータを削除するか、[セキュア ドライブの有効化（Enable Secure Drive）] をオンにしてセキュア ドライブを有効にします。

ステップ 16 [送信（Submit）] をクリックします。

Serial Over LANポリシー

Serial over LAN を使用すると、管理対象システムのシリアル ポートの入出力を IP 経由でリダイレクトできます。ホストコンソールへCisco IMC Supervisor を使用して到達する場合は、サーバで Serial over LAN を設定して使用します。サーバ/サーバ群のニーズを条件に特定の Serial Over LAN 属性を分類する Serial over LAN ポリシーを 1 つ以上作成できます。

各種プロパティの設定の詳細については、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』の「*Configuring Serial Over LAN*」の項を参照してください。

Serial over LAN ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [ハードウェア ポリシー（Hardware Policies）] を選択した後で [追加（Add）] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [追加（Add）] 画面で、ドロップダウンリストから [Serial Over LAN ポリシー（Serial Over LAN Policy）] を選択して [送信（Submit）] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドに名前を入力します。

[サーバの現在の設定からポリシーを作成（Create policy from current configuration of the server）] チェックボックスをオンにして、[次へ（Next）] をクリックすることもできます。[サーバの詳細（Server Details）] ウィンドウが表示されます。既存の設定からのポリシーの作成（140 ページ）を参照してください。

ステップ 4 ポリシーが Cisco UCS S3260 サーバのポリシーの場合は [Cisco UCS S3260] チェック ボックスをオンにし、[次へ（Next）] をクリックします。

ステップ 5 [メイン（Main）] ウィンドウで、[SoL の有効化（Enable SoL）] チェックボックスをオンにして、ドロップダウンリストから [CoM ポート（CoM Port）] 値と [ボー レート（Baud Rate）] 値を選択するか、既存の値を使用します。

ステップ 6 [送信（Submit）] をクリックします。

SNMPポリシー

Cisco IMC Supervisor は、Simple Network Management Protocol（SNMP）設定、および管理対象サーバからSNMP トラップによって障害およびアラート情報を送信するための設定をサポートします。

SNMP の各種プロパティの設定に関する詳細は、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』の「*Configuring SNMP*」のセクションを参照してください。

SNMP ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [ハードウェア ポリシー（Hardware Policies）] を選択した後で [追加（Add）] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [追加（Add）] 画面で、ドロップダウンリストから [SNMP ポリシー（SNMP Policy）] を選択して [送信（Submit）] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドに名前を入力します。

[サーバの現在の設定からポリシーを作成（Create policy from current configuration of the server）] チェックボックスをオンにして、[次へ（Next）] をクリックすることもできます。[サーバの詳細（Server Details）] ウィンドウが表示されます。既存の設定からのポリシーの作成（140 ページ）を参照してください。

ステップ 4 ポリシーが Cisco UCS S3260 サーバのポリシーの場合は [Cisco UCS S3260] チェック ボックスをオンにし、[次へ（Next）] をクリックします。

ステップ 5 [SNMP ユーザ（SNMP Users）] ウィンドウで [+] をクリックして SNMP ユーザを追加し、ユーザの詳細を入力します。[+] アイコンを使用して最大 15 の SNMP ユーザを追加できます。

既存の SNMP エントリを選択し、エントリを編集するかテーブルから削除します。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 [SNMP トラップ（SNMP Traps）] ウィンドウで [+] をクリックして SNMP トラップを追加し、トラップの詳細を入力します。[+] アイコンを使用して最大 15 の SNMP トラップを追加できます。

既存の SNMP エントリを選択し、エントリを編集するかテーブルから削除します。

ステップ 8 [次へ（Next）] をクリックします。

ステップ 9 [SNMP 設定（SNMP Settings）] ウィンドウで 、SNMP のプロパティを設定します。

ステップ 10 [送信（Submit）] をクリックします。

（注）
- それまでにサーバで設定した既存の [SNMP ユーザ（SNMP Users）] または [SNMP トラップ（SNMP Traps）] が削除され、ポリシーで設定したユーザまたはトラップに置き換えられます。ポリシーにユーザやトラップを追加していない場合、サーバ上の既存のユーザやトラップは削除されますが、置き換えられません。
- 2.x より前のバージョンの Cisco IMC を実行している C シリーズ サーバで **SNMP ポート**を設定することはできません。該当するサーバではチェックボックスを使用して除外する必要があります。
- バージョン 2.x の Cisco IMC を実行している E シリーズ サーバで **SNMP ポート**を設定することはできません。該当するサーバではチェックボックスを使用して除外する必要があります。

SSHポリシー

SSHサーバにより、SSHクライアントは暗号化された安全な接続を確立できます。SSHクライアントはSSHプロトコルで動作するアプリケーションで、デバイスの認証と暗号化を行います。サーバまたはサーバの集合のニーズに合う特定のSSHプロパティグループを含むSSHポリシーを1つ以上作成できます。

SSHの各種プロパティの設定に関する詳細は、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』の「*Configuring SSH*」のセクションを参照してください。

SSHポリシーを作成するには、次の手順を実行します。

手順

ステップ1 [ハードウェア ポリシー（Hardware Policies）] を選択した後で [追加（Add）] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81ページ）を参照してください。

ステップ2 [追加（Add）] ウィンドウで、ドロップダウンリストから [SSH ポリシー（SSH Policy）] を選択し、[送信（Submit）] をクリックします。

ステップ3 [ポリシー名（Policy Name）] フィールドに名前を入力します。

[サーバの現在の設定からポリシーを作成（Create policy from current configuration of the server）] チェックボックスをオンにして、[次へ（Next）] をクリックすることもできます。[サーバの詳細（Server Details）] ウィンドウが表示されます。既存の設定からのポリシーの作成（140ページ）を参照してください。

ステップ4 ポリシーがCisco UCS S3260サーバのポリシーの場合は [Cisco UCS S3260] チェック ボックスをオンにし、[次へ（Next）] をクリックします。

ステップ5 [メイン（Main）] ウィンドウで [SSHの有効化（Enable SSH）] チェックボックスをオンにし、SSHプロパティを入力するか、既存のプロパティを使用します。

ステップ6 [送信（Submit）] をクリックします。

ユーザ ポリシー

ユーザ ポリシーは、ローカル ユーザ設定の構成を自動化します。サーバまたはサーバ群に対して設定する必要があるローカルユーザのリストを含む、1つ以上のユーザ ポリシーを作成できます。

各種プロパティの設定の詳細については、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』の「*Configuring Local Users*」の項を参照してください。

ユーザ ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [ハードウェア ポリシー（Hardware Policies）] を選択した後で [追加（Add）] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [追加（Add）] ウィンドウで、ドロップダウンリストから [ユーザ ポリシー（User Policy）] を選択し、[送信（Submit）] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドに名前を入力します。

[サーバの現在の設定からポリシーを作成（Create policy from current configuration of the server）] チェックボックスをオンにして、[次へ（Next）] をクリックすることもできます。[サーバの詳細（Server Details）] ウィンドウが表示されます。既存の設定からのポリシーの作成（140 ページ）を参照してください。

ステップ 4 ポリシーが Cisco UCS S3260 サーバのポリシーの場合は [Cisco UCS S3260] チェック ボックスをオンにし、[次へ（Next）] をクリックします。

ステップ 5 [メイン（Main）] ウィンドウで、サーバに瀬亭する必要があるユーザを [ユーザ（Users）] リストに追加できます。

ステップ 6 次のステップで設定するユーザに強力なパスワードを強制する場合は、[強力なパスワードを強制する（Enforce Strong Password）] チェックボックスをオンにします。

この機能は、CIMC 2.0(9c) 以降を実行するサーバにのみ適用できます。

ステップ 7 [+] をクリックしてユーザを追加します。

ステップ 8 [エントリの追加（Add Entry）] ウィンドウで、次のフィールドに入力します。

フィールド	説明
ユーザ名	このフィールドにはユーザ名を入力します。
ロール	ドロップダウンリストから、[読み取り専用（read-only）]、[管理者（admin）] などのユーザ ロールを選択します。
ユーザアカウントの有効化	ユーザをアクティブにするには、このチェックボックスをオンにします。
新しいパスワード	ユーザ名に関連付けられるパスワードを入力します。
新しいパスワードの確認	前のフィールドと同じパスワードを入力します。

ステップ 9 [送信（Submit）] をクリックします。

ステップ 10 パスワード有効期限ポリシーを適用するには、[パスワードの有効期限ポリシーの追加（Add Password Expiration Policy）] チェックボックスをオンにします。

（注）　パスワード有効期限ポリシーを個別に適用することはできません。

ステップ 11　ドロップダウンリストから既存のパスワードの有効期限ポリシーを選択するか、[+] をクリックして新しいパスワードの有効期限ポリシーを追加します。パスワードの有効期限ポリシー（125 ページ）を参照してください。

ステップ 12　[送信（Submit）] をクリックします。

また、[メイン（Main）] ウィンドウの [ユーザ（Users）] テーブルで既存のユーザを選択し、[編集（Edit）] または [削除（Delete）] アイコンをクリックしてユーザを編集/削除することもできます。

（注）
- [ユーザ（Users）] テーブルの先頭のユーザは admin ユーザです。この admin ユーザは削除できませんが、パスワードを変更することはできます
- 2.0(8d) より古いバージョンの CIMC を実行しているサーバの場合、Cisco IMC Supervisorにより、ポリシーで定義されているものとともに、サーバにダミーのユーザエントリが作成されています。CIMC 2.0(8d) 以降を実行しているサーバにこのポリシーを適用すると、空白のユーザエントリは作成されなくなります。以前の既存のダミー ユーザ エントリ（以前のポリシーによって適用された）は消去されます。
- Cisco IMC Supervisor の管理に使用されるアカウントが、ポリシーのユーザ リストから削除されていないことを確認します。削除されている場合、Cisco IMC Supervisorは管理対象サーバへの接続を失います。

仮想KVMポリシー

KVM コンソールは Cisco IMC Supervisor からアクセス可能なインターフェイスであり、サーバへのキーボード、ビデオ、マウス（KVM）の直接接続をエミュレートします。KVM コンソールを使用すると、リモートの場所からサーバに接続できます。サーバまたはサーバの集合のニーズに合う特定の KVM プロパティ グループを含む KVM ポリシーを 1 つ以上作成できます。

KVM の各種プロパティの設定の詳細については、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』の「*Configuring the Virtual KVM*」のセクションを参照してください。

仮想 KVM ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1　[ハードウェア ポリシー（Hardware Policies）] を選択した後で [追加（Add）] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [追加（Add）] ウィンドウで、ドロップダウンリストから [仮想 KVM ポリシー（Virtual KVM Policy）] を選択し、[送信（Submit）] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドに名前を入力します。

[サーバの現在の設定からポリシーを作成（Create policy from current configuration of the server）] チェックボックスをオンにして、[次へ（Next）] をクリックすることもできます。[サーバの詳細（Server Details）] ウィンドウが表示されます。既存の設定からのポリシーの作成（140 ページ）を参照してください。

ステップ 4 ポリシーが Cisco UCS S3260 サーバのポリシーの場合は [Cisco UCS S3260] チェック ボックスをオンにし、[次へ（Next）] をクリックします。

ステップ 5 [vKVM の有効化（Enable vKVM）] チェック ボックスをオンにします。

ステップ 6 仮想サーバのプロパティを選択または入力するか、既存のプロパティを使用します。

ステップ 7 [送信（Submit）] をクリックします。

VIC アダプタ ポリシー

各種 VIC プロパティの設定の詳細については、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』の「*Viewing VIC Adapter Properties*」を参照してください。

手順

ステップ 1 [ハードウェア ポリシー（Hardware Policies）] を選択した後で [追加（Add）] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [追加（Add）] 画面で、ドロップダウンリストから [VIC アダプター ポリシー（VIC Adapter Policy）] を選択して [送信（Submit）] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドに名前を入力します。

[サーバの現在の設定からポリシーを作成（Create policy from current configuration of the server）] チェックボックスをオンにして、[次へ（Next）] をクリックすることもできます。[サーバの詳細（Server Details）] 画面が表示されます。既存の設定からのポリシーの作成（140 ページ）を参照してください。

ステップ 4 ポリシーが Cisco UCS S3260 サーバのポリシーの場合は [Cisco UCS S3260] チェック ボックスをオンにし、[次へ（Next）] をクリックします。

ステップ 5 [メイン（Main）] 画面で [+] をクリックし、VIC アダプタ エントリをテーブルに追加します。

ステップ 6 [VIC アダプタへのエントリの追加（Add Entry to VIC Adapters）] 画面で、アダプタの詳細を入力または選択します。

- [vNIC]：デフォルト プロパティは eth0 および eth1 です。これらのプロパティは編集できますが、削除することはできません。これらのプロパティは、usNIC プロパティにも使用できます。

- [vHBA]：デフォルト プロパティは fc0 および fc1 です。これらのプロパティは編集できますが、削除することはできません。

ステップ 7 [送信（Submit）] をクリックします。

vMedia ポリシー

KVM コンソールおよび vMedia を使ってサーバに OS をインストールするために、Cisco IMC Supervisorを使用できます。サーバまたはサーバの集合のニーズに合う、複数の OS イメージの vMedia マッピングを含む vMedia ポリシーを 1 つ以上作成できます。Cisco IMC Supervisor では、ISO ファイル（CDD を使用）と IMG ファイル（HDD を使用）でそれぞれ 1 つずつ、最大 2 つの vMedia マッピングを設定できます。

vMedia の各種プロパティの設定の詳細については、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』の「*Configuring the Virtual Media*」のセクションを参照してください。

vMedia ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [ハードウェア ポリシー（Hardware Policies）] を選択した後で [追加（Add）] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [追加（Add）] 画面で、ドロップダウンリストから [vMedia ポリシー（vMedia Policy）] を選択して [送信（Submit）] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドに名前を入力します。

[サーバの現在の設定からポリシーを作成（Create policy from current configuration of the server）] チェックボックスをオンにして、[次へ（Next）] をクリックすることもできます。[サーバの詳細（Server Details）] ウィンドウが表示されます。既存の設定からのポリシーの作成（140 ページ）を参照してください。

ステップ 4 ポリシーが Cisco UCS S3260 サーバのポリシーの場合は [Cisco UCS S3260] チェック ボックスをオンにし、[次へ（Next）] をクリックします。

ステップ 5 [メイン（Main）] ウィンドウで [vMedia の有効化（Enable vMedia）] チェックボックスをオンにして vMedia を有効にし、[仮想メディア暗号化の有効化（Enable Virtual Media Encryption）] をオンにして vMedia 暗号化を有効にします。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 [CDD vMedia マッピングの追加（Add CDD vMedia Mapping）] チェックボックスをオンにして、CDD マッピングの詳細を入力します。

ステップ 8 [次へ（Next）] をクリックします。

ステップ 9 [HDD vMedia マッピングの追加（Add CDD vMedia Mapping）] チェックボックスをオンにして、HDD マッピングの詳細を入力します。

ステップ 10 [送信（Submit）] をクリックします。

（注）
- 現在、Cisco IMC Supervisorで [低電力 USB 状態（Low Power USB State）] を設定することはできません。
- vMedia ポリシーを適用すると、そのポリシーに vMedia マッピングが含まれていなくても、サーバで設定した既存の vMedia マッピングがすべて削除されます。

ゾーン分割ポリシー

ゾーン分割ポリシーは、サーバに物理ドライブを割り当てるために使用されます。Cisco UCS S3260 高密度ストレージ ラック サーバは、Cisco Management Controller（CMC）の Serial Attached SCSI（SAS）ドライブの動的ストレージをサポートしています。この動的ストレージサポートは、CMC にある SAS ファブリック マネージャにより提供されます。動的ストレージでは次のオプションがサポートされています。

- サーバ 1 とサーバ 2 への物理ディスクの割り当て
- シャーシ規模のホットスペア（RAID コントローラでのみサポート）
- 共有モード（HBA でのみサポート）
- 物理ディスクの割り当て解除
- SAS エクスパンダのプロパティの表示
- サーバへの物理ドライブの割り当て
- シャーシ幅ホット スペアとしての物理ドライブの移動
- 物理ドライブの割り当て解除

ディスク グループの各種プロパティの設定に関する詳細は、『Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide for S3260 Servers』の「*DynamicStorage*」の項を参照してください。

ゾーン分割ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [ハードウェア ポリシー（Hardware Policies）] を選択した後で [追加（Add）] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [追加（Add）] 画面で、ドロップダウンリストから [ゾーン分割ポリシー（Zoning Policy）] を選択して [送信（Submit）] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドに名前を入力します。

[サーバの現在の設定からポリシーを作成（Create policy from current configuration of the server）] チェックボックスをオンにして、[次へ（Next）] をクリックすることもできます。[サーバの詳細（Server Details）] ウィンドウが表示されます。既存の設定からのポリシーの作成（140 ページ）を参照してください。

（注） ゾーン分割ポリシーは Cisco UCS 3260 ラック サーバにのみ適用でき、UI の [Cisco UCS S3260] チェックボックスがデフォルトでオンになっています。

ステップ 4 [ゾーン分割（Zoning）] ウィンドウで [+] をクリックして、サーバ上で設定するローカル ディスクを追加します。

ステップ 5 [ローカル ディスクへのエントリの追加（Add Entry to Local Disks）] ウィンドウで、ローカル ディスクが装着されているスロット番号を [スロット番号（Slot Number）] に入力します。

ステップ 6 ローカル ディスクの所有権を割り当てる [所有権（Ownership）] などのローカル ディスクの詳細を選択します。

ステップ 7 あるサーバが所有するディスクを別のサーバに割り当てる場合は、[強制（Force）] チェックボックスをオンにします。

ステップ 8 [送信（Submit）] をクリックします。

ステップ 9 [物理ドライブ電源ポリシーを変更する（Modify Physical Drive Power Policy）] チェックボックスをオンにしてポリシーを設定します。

ステップ 10 [物理ドライブ電源状態（Physical Drive Power State）] ドロップダウンリストから電源の状態を選択します。

ステップ 11 [送信（Submit）] をクリックします。

既存の設定からのポリシーの作成

以前に設定したサーバを使用してポリシーを作成することもできます。サーバの既存の設定を再利用することで、類似した設定の作成にかかる時間と手間を削減できます。

（注） サーバの現在の設定からポリシーを作成する場合、パスワードフィールドはサーバから取得されません。

サーバの現在の設定からポリシーを作成する場合は、次の手順を実行します。

手順

ステップ 1 [ハードウェア ポリシー（Hardware Policies）] を選択した後で [追加（Add）] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [サーバの現在の設定からポリシーを作成（Create policy from current configuration of the server）] チェックボックスをオンにし、[次へ（Next）] をクリックします。

ステップ 3 [サーバの詳細（Server Details）] 画面で、次のいずれかの方法でサーバの詳細を指定します。

（注） Cisco UCS S326 サーバのポリシーを作成している場合は、ステップ 5 に進みます。

a) [サーバの詳細を手動で入力（Enter Server Details Manually）] チェックボックスをオンにし、次のフィールドに情報を入力します。

1. [サーバ IP（Server IP）] フィールドに IP アドレスを入力します。
2. 既存のポリシーを選択するために [クレデンシャル ポリシーの使用（Use Credential Policy）] チェックボックスをオンにして [クレデンシャル ポリシー（Credential Policy）] ドロップダウンリストからポリシーを選択するか、[クレデンシャルポリシー（Credential Policy）] ドロップダウンリストの横にある [+] をクリックし、[クレデンシャルポリシー追加フォーム（Credential Policy Add Form）] 画面で詳細を入力して新規ポリシーを作成します。
3. [ユーザ名（User Name）] フィールドに、サーバ ログイン名を入力します。
4. [パスワード（Password）] フィールドに、サーバ ログインのパスワードを入力します。
5. [プロトコル（Protocol）] ドロップダウンリストから http または https を選択します。
6. [ポート（Port）] フィールドに、選択したプロトコルに関連付けられたポート番号を入力します。

b) [選択（Select）] をクリックして、設定を取得するサーバを選択します。

ステップ 4 [次へ（Next）] をクリックします。

[メイン（Main）] 画面に進みます。ポリシーの作成を続行します。

ステップ 5 Cisco UCS S3260 サーバの場合は、[サーバの現在の設定からポリシーを作成（Create policy from current configuration of the server）] および [Cisco UCS S3260] チェックボックスの両方をオンにして、[次へ（Next）] をクリックします。

注目 Cisco UCS S3260 サーバでは電力復元ポリシーを作成できません。E シリーズのサーバに対してのみこのポリシーを作成することができます。

ステップ 6 [サーバの詳細（Server Details）] 画面で [サーバの詳細を手動で入力（Enter Server Details Manually）] チェックボックスをオンにして、以下のフィールドに入力するか、または [選択（Select）] をクリックして、ポリシーを適用する Cisco UCS S3260 サーバを選択します。

1. Cisco UCS S3260 プラットフォームの [サーバ IP（Server IP）] フィールドに仮想的な管理 IP アドレスを入力します。
2. 既存のポリシーを選択するために [クレデンシャル ポリシーの使用（Use Credential Policy）] チェックボックスをオンにして [クレデンシャル ポリシー（Credential Policy）] ドロップダウンリストからポリシーを選択するか、[クレデンシャル ポリシー（Credential Policy）] ドロップダウンリストの横にある [+] をクリックし、[クレデンシャルポリシー追加フォーム（Credential Policy Add Form）] ダイアログボックスで詳細を入力して新規ポリシーを作成します。

3. [ユーザ名（User Name）] フィールドに、サーバ ログイン名を入力します。
4. [パスワード（Password）] フィールドに、サーバ ログインのパスワードを入力します。
5. [プロトコル（Protocol）] ドロップダウンリストから http または https を選択します。
6. [ポート（Port）] フィールドに、選択したプロトコルに関連付けられたポート番号を入力します。

ステップ 7 [サーバ ノード 1（Server Node 1）] または [サーバ ノード 2（Server Node 2）] のいずれかのラジオボタンを選択します。

ステップ 8 [次へ（Next）] をクリックします。

[メイン（Main）] 画面に進みます。ポリシーの作成を続行します。

ハードウェア ポリシーの適用

既存のポリシーをサーバに適用するには、次の手順を実行します。

手順

ステップ 1 **[ポリシー（Policies）] > [ポリシーとプロファイルの管理（Manage Policies and Profiles）]** を選択します。

ステップ 2 [ポリシーとプロファイルの管理（Manage Policies and Profiles）] ページで [ハードウェア ポリシー（Hardware Policies）] をクリックします。

ステップ 3 適用するポリシーを選択します。

ステップ 4 上部に表示されるオプションから [適用（Apply）] をクリックします。
[ポリシーの適用（Apply Policy）] 画面で、ポリシー適用対象として [シャーシ（Chassis）] または [サーバ（Server(s)）] を選択できます。これらのオプションは、選択したユーザ管理ポリシーまたはコンピューティング ノード ポリシーに基づいて表示されます。

ステップ 5 [選択（Select）] をクリックして、そのポリシーを適用するシャーシまたはサーバを選択します。

（注） [選択（Select）] をクリックすると、C シリーズ サーバや E シリーズ サーバなどのすべてのサーバが表示されます。電源復元ポリシーを適用する場合は、E シリーズ サーバのみを選択する必要があります。電力復元ポリシーの適用対象として他のサーバを選択すると、エラー メッセージが表示されます。

Cisco UCS 3260 タイプのポリシーの場合、シャーシは管理ポリシーとして、サーバはコンピューティング ノード ポリシーとして表示されます。ポリシーとプロファイル（199 ページ）を参照してください。

ステップ 6 ポリシーの適用タスクを後で実行するようスケジュールするには、[後にスケジュール（Schedule Later）] チェックボックスをオンにします。

ステップ 7 [スケジュール（Schedule）] ドロップダウンリストから既存のスケジュールを選択するか、[+] をクリックして新しいスケジュールを作成します。スケジュールの作成 （183 ページ）を参照してください。

（注） [ポリシー（Policies）]>[スケジュールの管理（Manage Schedules）] の順に移動して、スケジュールを選択し、[スケジュール タスクを表示する（View Scheduled Tasks）] をクリックしてスケジュールされたタスクを表示するか、または [スケジュール タスクの削除（Remove Scheduled Tasks）] をクリックしてスケジュールされたタスクを削除できます。

ステップ 8 [送信（Submit）] をクリックします。

指定した一連のサーバにポリシーを適用するプロセスが開始されます。ポリシータイプ、およびポリシーを適用するサーバへのネットワーク接続によっては、このプロセスに数分かかる場合があります。

ハードウェア ポリシーの一般タスク

既存のポリシーのサーバマッピングの詳細を編集、削除、複製、または表示するには、次の手順を実行します。

手順

ステップ 1 **[ポリシー（Policies）]>[ポリシーとプロファイルの管理（Manage Policies and Profiles）]** を選択します。

ステップ 2 [ポリシーとプロファイルの管理（Manage Policies and Profiles）] ページで [ハードウェア ポリシー（Hardware Policies）] をクリックします。

ステップ 3 [ハードウェア ポリシー（Hardware Policies）] ページで、左側ペインのポリシーを展開して、ポリシーを選択します。次の手順を必要に応じて実行します。

a) （任意） ポリシーを削除するには、[削除（Delete）] をクリックします。[ポリシーの削除（Delete Policy）] ダイアログボックスで、[選択（Select）] をクリックして削除するポリシーを選択します。[選択（Select）] をクリックし、次に [送信（Submit）] をクリックします。

ポリシーがサーバに関連付けられていても、選択した 1 つ以上のポリシーを削除できます。プロファイルに関連付けられたポリシーを削除しようとすると、エラーが発生します。

b) （任意） ポリシーを変更するには、[プロパティ（Properties）] をクリックして必要なプロパティを変更します。

ポリシー名を変更する場合は、すでに存在する名前を指定しないようにしてください。

c) （任意） ポリシーを複製するには、[複製（Clone）] をクリックして選択したポリシーの詳細を新しいポリシーにコピーします。

d) （任意） [詳細の表示（View Details）] をクリックすると、適用したポリシーのステータス、およびポリシーを適用したサーバのIPアドレスが表示されます。ポリシーが正常に適用されていない場合、[ステータスメッセージ（Status Message）] カラムにエラーメッセージが表示されます。

ステップ 4 ポリシーをサーバまたはサーバグループに適用するには、[適用（Apply）] をクリックします。プロファイルの適用については、ハードウェア ポリシーの適用 （142 ページ）を参照してください。

ステップ 5 状況に応じて、[送信（Submit）] または [閉じる（Close）] をクリックします。

ハードウェアプロファイル

ハードウェア プロファイルは、複数のポリシーを組み合わせたものです。たとえば、1 つのラック ハードウェア プロファイル設定の詳細情報を複数のラックマウント サーバに適用することができます。いくつかの特定のラックマウント サーバにこのハードウェア プロファイルを関連付けることができます。これは、サーバ間で設定の一貫性と再現性を実現するのに役立ちます。プロファイルを定義して使用すると、一貫性、制御性、予測可能性、自動化機能が向上します。

Cisco IMC Supervisor でハードウェア プロファイルを使用する方法を次のワークフローで説明します。

1. ハードウェアプロファイルを作成します。次のいずれかの方法でプロファイルを作成できます。
    1. 新しいプロファイルを作成します。新しいプロファイルの作成方法の詳細については、ハードウェア プロファイルの作成 （145 ページ）を参照してください。
    2. サーバの既存の設定からプロファイルを作成します。サーバの既存の設定からプロファイルを作成する方法については、既存の設定からのプロファイルの作成（146ページ）を参照してください。
2. サーバで、プロファイルを適用します。プロファイルの適用については、ハードウェア プロファイルの適用 （148 ページ）を参照してください。
3. プロファイルで、必要に応じて次のオプション作業を実行します。
    1. 編集
    2. 削除
    3. 複製

特定のプロファイルにマッピングされたサーバのリスト、およびこのプロファイルに関連付けられたポリシーの詳細を表示することもできます。これらの作業の実行の詳細については、ハードウェア プロファイルの一般タスク （149 ページ）を参照してください。

ハードウェア プロファイルの作成

手順

ステップ 1 **[ポリシー（Policies）] > [ポリシーとプロファイルの管理（Manage Policies and Profiles）]** を選択します。

ステップ 2 [ポリシーとプロファイルの管理（Manage Policies and Profiles）] ページで [ハードウェア プロファイル（Hardware Profiles）] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [ハードウェア プロファイル（Hardware Profile）] 画面で、作成するプロファイルの名前を [プロファイル名（Profile Name）] フィールドに入力します。

既存のサーバ設定を使用したい場合は、[サーバの現在の設定からプロファイルを作成する（Create profile from current configuration of the server）] チェックボックスをオンにすることもできます。[サーバの詳細（Server Details）] 画面が表示されます。既存の設定からのプロファイルの作成を確認します。

ステップ 5 ポリシーが Cisco UCS S3260 サーバのポリシーの場合は [Cisco UCS S3260] チェックボックスをオンにし、[次へ（Next）] をクリックします。

ステップ 6 [プロファイルのエンティティ（Profile Entities）] ウィンドウで [+] をクリックし、プロファイル エントリを追加します。

既存のエンティティを削除するには、削除アイコンをクリックします。

ステップ 7 [プロファイル名へのエントリの追加（Add Entry to Profile Name）] ウィンドウで、[ポリシー タイプ（Policy Type）] を選択します。

ステップ 8 [ポリシー名（Policy Name）] ドロップダウンリストからポリシー名を選択します。このリストには作成済みのポリシーの名前が表示されます。

[ポリシー名（Policy Name）] の横にある [+] をクリックすると、先に選択したポリシー タイプに基づいて新しいポリシーを作成できます。「ハードウェア ポリシーの作成 （105 ページ）」を参照してください。

ステップ 9 [次にポリシーを適用（Apply Policy To）] ドロップダウンリストからポリシーを適用するサーバを選択します。

ステップ 10 [送信（Submit）] をクリックします。

次のタスク

また、プロファイルを編集、削除、複製したり、選択したプロファイルにマップされているサーバを表示したりすることもできます。「ハードウェア プロファイルの一般タスク （149 ページ）」を参照してください。

既存の設定からのプロファイルの作成

以前に設定したサーバを使用してプロファイルを作成することもできます。サーバの既存の設定を再利用することで、類似した設定の作成にかかる時間と手間を削減できます。

（注） サーバの現在の設定からプロファイルを作成する場合、パスワードフィールドはサーバから取得されません。

サーバの現在の設定からプロファイルを作成する場合は、次の手順を実行します。

手順

ステップ 1 **[ポリシー（Policies）] > [ポリシーとプロファイルの管理（Manage Policies and Profiles）]** を選択します。

ステップ 2 [ポリシーとプロファイルの管理（Manage Policies and Profiles）] ページで [ハードウェア プロファイル（Hardware Profiles）] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [プロファイル名（Profile Name）] フィールドにプロファイル名を入力します。

ステップ 5 [サーバの現在の設定からプロファイルを作成（Create profile from current configuration of the server）] チェックボックスをオンにします。次の方法でサーバの詳細情報を使用できます。Cisco UCS S3260 サーバの場合はステップ 10 に進みます。

a) [サーバの詳細を手動で入力（Enter Server Details Manually）] チェックボックスをオンにし、次のフィールドに情報を入力します。

1. [サーバ IP（Server IP）] フィールドに IP アドレスを入力します。
2. 既存のポリシーを選択するために [クレデンシャル ポリシーの使用（Use Credential Policy）] チェックボックスをオンにして [クレデンシャル ポリシー（Credential Policy）] ドロップダウンリストからポリシーを選択するか、[クレデンシャル ポリシー（Credential Policy）] ドロップダウンリストの横にある [+] をクリックし、[クレデンシャルポリシー追加フォーム（Credential Policy Add Form）] ダイアログボックスで詳細を入力して新規ポリシーを作成します。
3. [ユーザ名（User Name）] フィールドに、サーバ ログイン名を入力します。
4. [パスワード（Password）] フィールドに、サーバ ログインのパスワードを入力します。
5. [プロトコル（Protocol）] ドロップダウンリストから http または https を選択します。

6. [ポート（Port）]フィールドに、選択したプロトコルに関連付けられたポート番号を入力します。
7. [選択（Select）] をクリックし、ポリシーを選択し、[選択（Select）] をクリックします。

b) [選択（Select）] をクリックして、設定を取得するサーバを選択します。
c) [選択（Select）] をクリックし、ポリシーを選択し、[選択（Select）] をクリックします。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 プロファイル名にエントリを追加するには、[プロファイルのエンティティ（Profile Entities）] ウィンドウで [+] をクリックします。

[x] をクリックし、[プロファイル名（Profile Name）] テーブルから既存のエントリを削除します。

ステップ 8 [送信（Submit）] をクリックします。

ステップ 9 Cisco UCS S3260 サーバの場合は、[Cisco UCS S3260] チェックボックスをオンにし、[次へ（Next）] をクリックします。

a) [サーバの詳細を手動で入力（Enter Server Details Manually）] チェックボックスをオンにし、次のフィールドに情報を入力します。
   1. Cisco UCS S3260 プラットフォームの [サーバ IP（Server IP）] フィールドに仮想的な管理 IP アドレスを入力します。
   2. 既存のポリシーを選択するために [クレデンシャル ポリシーの使用（Use Credential Policy）]チェックボックスをオンにして[クレデンシャル ポリシー（Credential Policy）] ドロップダウンリストからポリシーを選択するか、[クレデンシャルポリシー（Credential Policy）] ドロップダウンリストの横にある [+] をクリックし、[クレデンシャルポリシー追加フォーム（Credential Policy Add Form）] ダイアログ ボックスで詳細を入力して新規ポリシーを作成します。
   3. [ユーザ名（User Name）] フィールドに、サーバ ログイン名を入力します。
   4. [パスワード（Password）]フィールドに、サーバログインのパスワードを入力します。
   5. [プロトコル（Protocol）] ドロップダウンリストから http または https を選択します。
   6. [ポート（Port）]フィールドに、選択したプロトコルに関連付けられたポート番号を入力します。
   7. [選択（Select）] をクリックし、ポリシーを選択し、[選択（Select）] をクリックします。

b) [選択（Select）] をクリックして、設定を取得するサーバを選択します。
c) [選択（Select）] をクリックし、サーバから作成するポリシーを選択し、[選択（Select）] をクリックします。

ステップ 10 [次へ（Next）] をクリックします。

ステップ 11 プロファイル名にエントリを追加するには、[プロファイルのエンティティ（Profile Entities）] ウィンドウで [+] をクリックします。

[x] をクリックし、[プロファイル名（Profile Name）] テーブルから既存のエントリを削除します。

（注） Cisco UCS S3260 のプロファイル タイプの場合、プラットフォーム タイプが Cisco UCS S3260 のポリシーのみ追加できます。ポリシーがコンピューティング ノード タイプの場合、[次にポリシーを適用（Apply Policy To）] フィールドにサーバ ノードを指定する必要があります。たとえば、[サーバ 1（Server-1）]、[サーバ 2（Server-2）]、[両方（Both）] などです。管理ポリシーの場合、このフィールドは該当しません。

ステップ 12 [送信（Submit）] をクリックします。

ハードウェア プロファイルの適用

ハードウェア プロファイルをラック サーバに適用するには、次の手順を実行します。

手順

ステップ 1 **[ポリシー（Policies）] > [ポリシーとプロファイルの管理（Manage Policies and Profiles）]** を選択します。

ステップ 2 [ポリシーとプロファイルの管理（Manage Policies and Profiles）] ページで [ハードウェア プロファイル（Hardware Profiles）] をクリックします。

ステップ 3 既存のハードウェア プロファイルを選択し、[適用（Apply）] をクリックします。
[プロファイルの適用（Apply Profile）] 画面で、プロファイルの適用先として [シャーシ（Chassis）]（Cisco UCS S3260 タイプのプロファイルに適用可能）または [サーバ（Server(s)）] を選択できます。これらのオプションは、選択したサーバプラットフォームに基づいて表示されます。

ステップ 4 [プロファイルの適用（Apply Profile）] 画面で、[選択（Select）] をクリックしてプロファイルを適用するシャーシまたはサーバを選択します。

ステップ 5 プロファイルの適用タスクを後で実行するようスケジュールするには、[後にスケジュール（Schedule Later）] チェックボックスをオンにします。

ステップ 6 [スケジュール（Schedule）] ドロップダウンリストから既存のスケジュールを選択するか、[+] をクリックして新しいスケジュールを作成します。スケジュールの作成（183 ページ）を参照してください。

（注） [ポリシー（Policies）] > [スケジュールの管理（Manage Schedules）] の順に移動して、スケジュールを選択し、[スケジュール タスクを表示する（View Scheduled Tasks）] をクリックしてスケジュールされたタスクを表示するか、または [スケジュール タスクの削除（Remove Scheduled Tasks）] をクリックしてスケジュールされたタスクを削除できます。

ステップ 7 [送信（Submit）] をクリックします。

指定した一連のサーバにプロファイルを適用するプロセスが開始されます。プロファイル タイプ、およびプロファイルを適用するサーバへのネットワーク接続によっては、このプロセスに数分かかる場合があります。

ハードウェア プロファイルの一般タスク

既存のプロファイルのサーバマッピングの詳細を編集、削除、複製、または表示するには、次の手順を実行します。

手順

ステップ 1 **[ポリシー（Policies）] > [ポリシーとプロファイルの管理（Manage Policies and Profiles）]** を選択します。

ステップ 2 [ポリシーとプロファイルの管理（Manage Policies and Profiles）] ページで [ハードウェア プロファイル（Hardware Profiles）] をクリックします。

ステップ 3 [ハードウェア プロファイル（Hardware Profile）] を展開し、プロファイルを選択します。オプションで次の作業を行うことができます。

a) （任意） プロファイルを削除するには、[削除（Delete）] をクリックします。[プロファイルの削除（Delete Profile）] ダイアログボックスの [選択（Select）] をクリックし、1 つ以上のプロファイルを選択して、[選択（Select）] をクリックします。[送信（Submit）] をクリックしてプロファイルを削除します。

サーバに関連付けられていても、プロファイルを削除できます。

b) （任意） プロファイルを変更するには、プロファイルを選択し、[編集（Edit）] をクリックして必要なプロパティを変更します。

プロファイル名を変更する場合は、すでに存在する名前を指定しないようにしてください。

c) （任意） 既存のプロファイルの詳細を新しいプロファイルにコピーするには、[クローン（Clone）] をクリックします。

d) （任意） プロファイルをサーバまたはサーバ グループに適用するには、[適用（Apply）] をクリックします。ハードウェア プロファイルの適用（148ページ）を参照してください。

e) （任意）[詳細の表示（View Details）] をクリックすると、適用したプロファイルのステータス、およびプロファイルを適用したサーバの IP アドレスが表示されます。プロファイルが正常に適用されていない場合、[ステータスメッセージ（Status Message）] カラムにエラー メッセージが表示されます。

ステップ 4 状況に応じて、[送信（Submit）] または [閉じる（Close）] をクリックします。

タグ ライブラリ

タグ付けは、オブジェクトにラベルを割り当てるときに行います。管理者は、Cisco IMC Supervisorのリソース グループやユーザ グループなどのオブジェクトにタグ付けするかどうかを決定できます。ラック アカウントなどのカテゴリにタグを割り当てることができます。また、選択したカテゴリの特定タイプのアカウントにタグを適用することもできます。

[タグ ライブラリ（Tag Library）] の唯一のタブには、次の詳細が表示されます。

フィールド	説明
名前	タグ ライブラリのユーザ定義名。
説明	タグ ライブラリのユーザ定義の簡単な説明。
[タイプ（Type）]	文字列または整数。
使用できるタグ値	ユーザ定義のタグ値。
適用先	ラックマウント サーバまたはユーザ。

タグ ライブラリの作成

タグ ライブラリを作成する場合は、次の手順を実行します。

手順

ステップ 1 **[ポリシー（Policies）] > [タグ ライブラリ（Tag Library）]** を選択します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 [タグの作成（Create Tag）] 画面で、[タグの詳細（Tag Details）] のフィールドに値を入力します。

フィールド	説明
[名前（Name）] フィールド	タグの記述名。
[説明（Description）] フィールド	（オプション）タグの説明。
[タイプ（Type）] ドロップダウンリスト	文字列または整数を選択します。
[使用できるタグ値（Possible Tag Values）] フィールド	タグに設定可能な値。

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 [適用可能なルール（Applicability Rules）] 画面で、次の手順を実行します。

名前	説明
[タグ付け可能なエンティティ（Taggable Entities）] フィールド	タグの適用が必要なエンティティを選択します。 エンティティを追加するには、次の手順に従います。 **1.** [+] アイコンをクリックします。 **2.** [カテゴリ（Category）] ドロップダウンリストからカテゴリを選択します。次のいずれかを指定できます。 • **Physical_Compute** • **管理（Administration）** **3.** テーブルからタグ付け可能なエンティティを選択します。 **4.** [送信（Submit）] をクリックします。 （注） タグは、セットになったタグ付け可能なエンティティに応じてそれぞれのカテゴリの下に表示されます。

ステップ 6 [送信（Submit）] をクリックします。

（注） 使用可能なオプションをクリックすることで、タグおよびタグの関連付けの詳細を複製、編集、削除、表示するといった、さまざまなタスクを実行できます。

REST API とオーケストレーション

[REST API ブラウザ（REST API Browser）] 画面には、Cisco IMC Supervisor で提供されておりユーザが使用できる API のリストが表示されます。API は次のグループに分類されます。

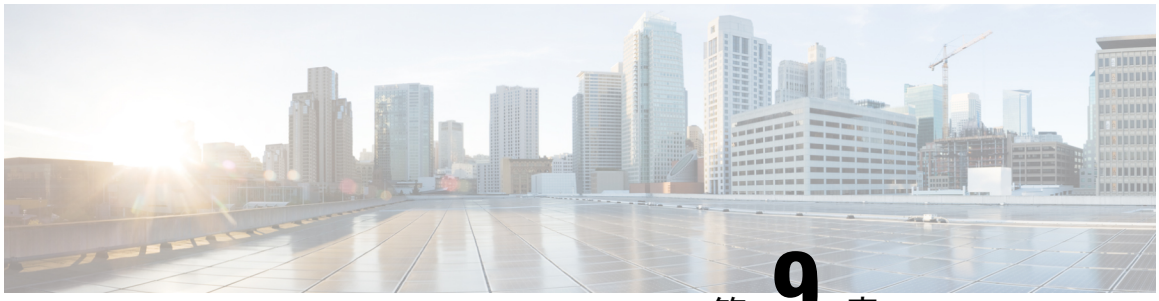
- ファームウェア管理のタスク
- 一般タスク
- プラットフォームタスク
- ポリシー タスク
- ポリシーおよびプロファイルのタスク
- サーバタスク

- ユーザ タスクとグループ タスク

次の操作を実行するには、画面上のコントロールを使用できます。

- リスト全体の展開と折りたたみ
- この画面を [お気に入り（Favorites）] に追加する
- [検索（Search）] または [高度なフィルタ（Advanced Filter）] オプションを使用した特定の API の検出
- レポートのエクスポート
- 管理対象サーバの追加

これらの API の使用法の詳細については、『*Cisco IMC Supervisor REST API Cookbook*』を参照してください。この資料は http://www.cisco.com/c/en/us/support/servers-unified-computing/integrated-management-controller-imc-supervisor/products-programming-reference-guides-list.html から入手できます。



第 9 章

Cisco UCS ハードウェア互換性レポートの管理

この章は次のトピックで構成されています。

概要

Cisco UCS のハードウェア互換性レポートでは、シスコまたはシスコ パートナー（あるいはその両方）によってテストおよび検証された、Cisco UCS のコンポーネントおよび設定に関する相互運用性情報を確認できます。レポートを実行し、現在のソフトウェア バージョンまたはターゲットのソフトウェア バージョンと照らし合わせてステータスを確認することができます。

ハードウェア互換性レポートでは、サーバのオペレーティング システムの互換性がチェックされます。さらに、そのオペレーティング システムに関連付けられているアダプタ ドライバがチェックされます。

Cisco IMC Supervisor は、Cisco UCS ハードウェア互換性レポート ツールと統合して、サーバ、ファームウェア、および関連コンポーネント（ストレージ、ネットワーク アダプタ、VIC アダプタ）が特定のサーバ モデル、OS ベンダ、バージョン、およびプロセッサの組み合わせでサポートされているかどうかに関する情報を提供します。

（注） Cisco UCS ハードウェア互換性レポート ツールは、Cisco C シリーズ/S シリーズ サーバでのみ使用可能です。

このツールの独立バージョンは https://ucshcltool.cloudapps.cisco.com/public から入手できます。Cisco IMC Supervisor コネクタは、このツールが公開する REST API を使用して互換性レポートを取得できます。

Cisco UCS ハードウェア互換性レポート ツールを使用するには、次の点を確認する必要があります。

- DNS が正しく設定されており、Cisco IMC Supervisor アプライアンスから URL https://ucshcltool.cloudapps.cisco.com/ に到達できる。
- cisco.com のクレデンシャルを入力している。Cisco.com ユーザの設定 （40 ページ）を参照してください。

OS ベンダーおよびバージョンのタグ付け

ラック サーバには、オペレーティング システムのベンダーとバージョンでタグ付けする必要があります。次の手順で、システム レベル、ラック グループ レベル、またはラック サーバ レベルでサーバを選択して、サーバにタグを付けることができます。

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [ラック サーバ（Rack Servers）] でラック サーバを選択するか、[ラック グループ（Rack Groups）] を展開してタグ付けするラック サーバを選択します。

ステップ 3 [HCR の OS タグを管理（Manage OS Tag For HCR）] をクリックします。

（注） OS タグは E シリーズ サーバには適用できません。

ステップ 4 ドロップダウンリストから [オペレーティング システムのベンダー（Operating System Vendor）] を選択します。

ステップ 5 ドロップダウンリストから [オペレーティング システムのバージョン（Operating System Version）] を選択します。

（注） OS ベンダーまたは OS バージョンがドロップダウンリストに表示されていない場合は、DNS が正しく設定されており、Cisco IMC Supervisor アプライアンスから URL https://ucshcltool.cloudapps.cisco.com/ に到達できることを確認します。また、**[管理（Administration）] > [システム（System）] > [システム タスク（System Tasks）]** 画面にある [ハードウェア互換性レポートの同期（Synchronize Hardware Compatibility Reports）] システム タスクを手動で実行します。

ステップ 6 [送信（Submit）] をクリックします。

（注） ラック サーバを選択して [HCR の OS タグを削除（Delete OS Tag For HCR）] をクリックし、作成したタグを削除できます。

ハードウェア互換性レポートの作成

タグを追加し、cisco.com クレデンシャルを入力したら、互換性レポートを生成できます。

始める前に

- レポートを生成する前に、cisco.comのクレデンシャルを入力していることを確認します。Cisco.com ユーザの設定 （40 ページ）を参照してください。
- ラック サーバにオペレーティング システム ベンダーとバージョンのタグを付けていることを確認します。OSベンダーおよびバージョンのタグ付け （154ページ）を参照してください。

手順

ステップ 1 **[ポリシー（Policies）] > [ハードウェア互換性レポート（Hardware Compatibility Report）]** を選択します。

ステップ 2 [+] をクリックしてハードウェア互換性レポートを作成します。

ステップ 3 [プロファイルの選択（Select Profile）] フィールドにプロファイル名を入力します。

ステップ 4 [サーバの選択（Choose Server）] を展開し、設定を取得するサーバを選択します。

ステップ 5 **[Validate]** をクリックします。

ステップ 6 [送信（Submit）] をクリックします。
[ハードウェア互換性レポート（Hardware Compatibility Report）] 画面で、作成したレポートを確認します。ラック グループまたはラック サーバを選択し、[ハードウェア互換性レポート（Hardware Compatibility Report）] をクリックして、レポートを表示することもできます。

次のタスク

作成したレポートを選択し、[削除（Delete）]、[編集（Edit）]、[HCL レポートを同期（Synchronize HCL Report(s)）]、または [ステータス詳細の表示（View Status Details）] を選択できます。レポートでは、サーバがサポートされているかどうか、サーバに互換性があるかどうかが示されます。[コンプライアンス（Compliance）] は次のいずれかの状態になります。

- [完全に準拠（Fully Compliant）] : サーバの OS ベンダー、バージョン、またはプロセッサーと、その関連コンポーネントが完全にサポートされています。

- [部分的に準拠（Partially Compliant）]：いくつかのコンポーネントがサポートされていないことが検出されています。
- [非準拠（Not Compliant）]：準拠エラーが発生しているか、またはサーバと関連コンポーネントの特定の組み合わせが無効です。
- [エラー（Error）] または [決定不能（Cannot Determine）]：特定のサーバがタグ付けされていないか、またはバックエンドから応答を取得する際にエラーが発生しました。

ハードウェア互換性レポートの同期

[ハードウェア互換性レポートの同期（Synchronize Hardware Compatibility Reports）] システムタスクは毎週実行され、定期的にハードウェア互換性レポートをバックエンドと同期します。レポートを手動で同期するには、次の手順を実行します。

始める前に

- URL https://ucshcltool.cloudapps.cisco.com を設定します。
- cisco.com のクレデンシャルを設定します。Cisco.com ユーザの設定 （40 ページ）を参照してください。

手順

ステップ 1 **[管理（Administration）] > [システム（System）]** を選択します。

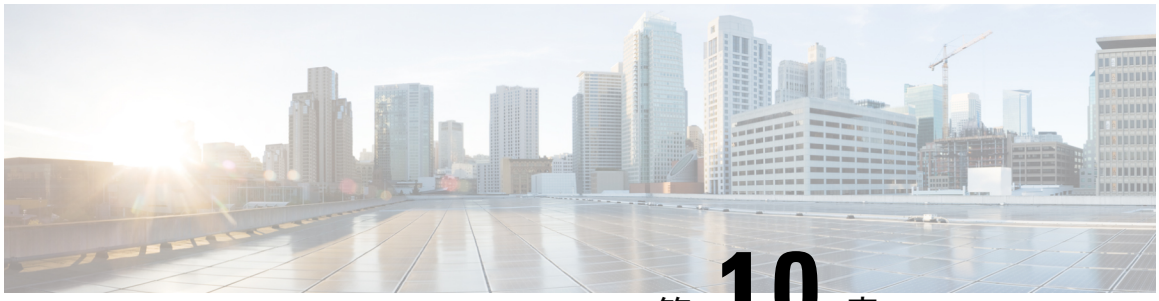
ステップ 2 [システム（System）] ページで [システムのタスク（System Tasks）] をクリックします。

ステップ 3 [ラック サーバ タスク（Rack Server Tasks）] を展開し、[ハードウェア互換性レポートの同期（Synchronize Hardware Compatibility Reports）] を選択します。

ステップ 4 [今すぐ実行（Run Now）] をクリックします。

ステップ 5 [送信（Submit）] をクリックします。

（注） [ハードウェア互換性レポート（Hardware Compatibility Report）] ページからレポートを手動で同期するには、[HCL レポートを同期（Synchronize HCL Report）] オプションも使用できます。



第 10 章

ファームウェア プロファイル

この章は次のトピックで構成されています。

ファームウェア管理メニュー

ファームウェア イメージは、ローカル サーバまたはネットワーク サーバからアップロードできます。プロファイル名は、ローカルおよびネットワークの両方のイメージプロファイルの間で一意である必要があります。

シスコは、すべての Cisco IMC Supervisor コンポーネントをアップグレードするためのファームウェアのアップデートをまとめて提供します。ファームウェアのアップデートは、cisco.com からダウンロードできます。サーバが Cisco IMC Supervisor で管理されていない場合はアップグレードできません。E シリーズのファームウェアイメージをダウンロードするには、cisco.com アカウントに契約アクセスを関連付ける必要があります。

ローカル サーバへのイメージの追加

ローカル マシンからファームウェア イメージを追加するには、次の手順を実行します。

（注） Cisco IMC Supervisor バージョン 2.2(0.3) 以降、イメージ（ローカル イメージ、または 3.0(3e) より古いバージョンの Cisco IMC ではイメージのアップロード）を使用してファームウェア アップグレードを実行するには、シェル メニューを使用して HTTP を有効にする必要があります。

手順

ステップ 1 **[システム（Systems）] > [ファームウェア管理（Firmware Management）]** を選択します。

ステップ 2 [イメージ - ローカル（Images - Local）] タブをクリックし、[+] をクリックしてイメージを追加します。

ステップ 3 [ファームウェアイメージの追加 - ローカル（Add Firmware Image - Local）] 画面で次のフィールドに情報を入力します。

フィールド	説明
[プロファイル名（Profile Name）] フィールド	プロファイルの内容がわかる一意の名前を入力します。
[プロキシ設定（Proxy Configuration）] チェックボックス	（オプション）このチェックボックスをオンにすると、設定したプロキシ設定の詳細が取得されます。 （注） すでに設定している Cisco.com のユーザ クレデンシャルとプロキシ設定の詳細が自動的に取得されます。Cisco.com クレデンシャルの設定については Cisco.com ユーザの設定 （40 ページ） を参照してください。プロキシ設定については、プロキシ設定 （40 ページ） を参照してください。
[プラットフォーム（Platform）] ドロップダウンリスト	ドロップダウンリストからプラットフォームを選択します。 ここでは、1 台以上のサーバを管理しているプラットフォームだけがリストされます。
[使用可能なイメージ（Available Image）] ドロップダウンリスト	ドロップダウンリストから .iso イメージを選択します。
[今すぐダウンロード（Download Now）] チェックボックス	プロファイルの追加直後に .iso イメージをダウンロードするには、このチェックボックスをオンにします。直後にダウンロードしない場合は、[イメージのダウンロード（Download Image）] をクリックして後でイメージをダウンロードできます。
[グレースフルタイムアウト (Graceful Timeout）] チェックボックス	ファームウェアアップグレードプロセスを開始するためにホストシステムがシャットダウンする必要がある期間を指定するには、このチェックボックスをオンにします。 （注） グレースフル タイムアウトは、Cisco IMC 3.1(3a) 以降が稼働しているシステムで設定できます。 タイムアウト期間を指定しない場合、システムは 120 秒後に強制的にシャット ダウンされます。

フィールド	説明
[タイムアウト（分）（Timeout (in mins)）] フィールド	ファームウェアアップグレードプロセスを開始するためにホスト システムがシャットダウンする必要がある期間を指定します。 指定できる値は 0 ～ 60 の範囲内の値です。
[サーバの強制シャットダウン（Force Shutdown Server）] チェックボックス	[グレースフル タイムアウト（分）（Graceful Timeout (in mins)）] フィールドに指定した時間内にホスト システムがシャットダウンしなかった場合に、ホスト システムを強制的にシャットダウンするには、このチェックボックスをオンにします。 このオプションは、デフォルトで有効です。
ライセンス契約書に同意	ライセンス契約書に同意するには、このチェックボックスをオンにします。契約条件のリンクをクリックし、エンドユーザ ライセンス契約書を読みます。 （注） ライセンス契約書に合意しない場合、イメージを後でダウンロードする予定であっても、ファームウェア プロファイルを作成することはできません。

ステップ 4 [送信（Submit）] をクリックします。

（注）
- プロファイル設定の詳細を表示し、ファームウェアイメージの詳細を変更し、イメージプロファイルを削除できます。同時に複数のプロファイルを選択して削除することもできます。
- Cisco IMC Supervisor アプライアンスが、これらのイメージにリモートでマッピングできる必要があります。
- [イメージ - ローカル（Images - Local）] ウィンドウからイメージを選択し、cisco.comからイメージをダウンロードできます。イメージのダウンロードが必要なファームウェア プロファイルの場合は、[イメージのダウンロード（Download Image）] オプションを使用してダウンロード プロセスを延期し、後で開始することができます。また、[イメージの削除（Delete Image）] オプションを使用して、cisco.com からダウンロードしたイメージを削除することもできます。

ローカル ファイル システムからのイメージのアップロード

ローカル ファイル システムから Cisco IMC Supervisor システムへ ISO イメージをアップロードするには、次の手順を実行します。

（注） Cisco IMC Supervisor バージョン 2.2(0.3) 以降、イメージ（ローカル イメージ、または 3.0(3e) より古いバージョンの Cisco IMC ではイメージのアップロード）を使用してファームウェア アップグレードを実行するには、シェル メニューを使用して HTTP を有効にする必要があります。

手順

ステップ 1 **[システム（Systems）] > [ファームウェア管理（Firmware Management）]** を選択します。

ステップ 2 [アップロード（Upload）] を選択してイメージを追加します。

ステップ 3 [ファームウェアイメージのアップロード - ローカル（Upload Firmware Image - Local）] 画面で次のフィールドに入力します。

フィールド	説明
[プロファイル名（Profile Name）] フィールド	プロファイルの内容がわかる一意の名前を入力します。
[プラットフォーム（Platform）] ドロップダウンリスト	C シリーズまたは E シリーズ プラットフォームを選択します。
[File] フィールド	ファイルを選択してこのフィールドにドロップするか、[ファイルを選択（Select a File）] をクリックしてローカル ファイル システムにアップロードします。
[グレースフルタイムアウト（Graceful Timeout）] チェックボックス	ファームウェアアップグレードプロセスを開始するためにホスト システムがシャットダウンする必要がある期間を指定するには、このチェックボックスをオンにします。 （注） グレースフル タイムアウトは、Cisco IMC 3.1(3a) 以降が稼働しているシステムで設定できます。 タイムアウト期間を指定しない場合、システムは 120 秒後に強制的にシャット ダウンされます。
[タイムアウト（分）（Timeout (in mins)）] フィールド	ファームウェアアップグレードプロセスを開始するためにホスト システムがシャットダウンする必要がある期間を指定します。 指定できる値は 0 ～ 60 の範囲内の値です。

フィールド	説明
[サーバの強制シャットダウン（Force Shutdown Server）] チェックボックス	[グレースフル タイムアウト（分）（Graceful Timeout (in mins)）] フィールドに指定した時間内にホスト システムがシャットダウンしなかった場合に、ホストシステムを強制的にシャットダウンするには、このチェックボックスをオンにします。 このオプションは、デフォルトで有効です。

ステップ 4 [送信（Submit）] をクリックします。

（注）
- プロファイル設定の詳細を表示し、ファームウェアイメージの詳細を変更し、イメージプロファイルを削除できます。同時に複数のプロファイルを選択して削除することもできます。
- [プロファイルの削除（Delete Profile）] オプションは、プロファイルに関連付けられたイメージを削除します。誤ったイメージをアップロードしたり、ファイルがプロファイルに関連付けられていない場合は、定期的に（月に1回）実行されるシステム消去タスクによって、Cisco IMC Supervisorアプライアンスからファイルが削除されます。

ネットワーク サーバからのイメージの追加

プロファイル名、リモート IP、リモート ファイル名などを指定してネットワーク サーバからファームウェア イメージを追加するには、次の手順を実行します。

手順

ステップ 1 **[システム（Systems）] > [ファームウェア管理（Firmware Management）]** を選択します。

ステップ 2 [ファームウェア管理（Firmware Management）] ページで [イメージ - ネットワーク（Images - Network）] を選択します。

ステップ 3 [+] をクリックして、イメージを追加します。

ステップ 4 [ファームウェアイメージの追加 - ネットワーク（Add Firmware Image - Network）] 画面で次のフィールドに入力します。

フィールド	説明
[プロファイル名（Profile Name）] フィールド	プロファイルの内容がわかる一意の名前。プロファイル名は固有である必要があります。

フィールド	説明
[プラットフォーム（Platform）] ドロップダウンリスト	ドロップダウンリストからプラットフォームを選択します。 ここでは、1 台以上のサーバを管理しているプラットフォームだけがリストされます。
[Mount Type] ドロップダウンリスト	[ネットワーク ファイル システム（NFS）（Network File System (NFS)）]、[Common Internet File System（CIFS）]、[HTTP] のいずれかのサーバ タイプを選択します。
[リモート IP（Remote IP）] フィールド（NFS および CIFS サーバ タイプの場合のみ）	リモート IP アドレスを入力します。
[リモート共有（Remote Share）] フィールド（NFS および CIFS サーバ タイプの場合のみ）	リモート共有パスを入力します。
[リモート ファイル名（Remote File Name）] フィールド（NFS および CIFS サーバ タイプの場合のみ）	リモート ファイル名を入力します。 （注） リモート ファイル名は Host Upgrade Utility ISO ファイルです。
[ロケーション リンク（Location Link）] フィールド（HTTP サーバ タイプの場合のみ）	イメージの場所の有効な http または https URL リンクを入力します。
[ユーザ名（User Name）] フィールド	ネットワーク パスのユーザ名を入力します。
[パスワード（Password）] フィールド	ネットワーク パスのパスワードを入力します。
[マウント オプション（Mount Options）] ドロップダウンリスト（CIFS サーバ タイプのみ）	[マウント オプション（Mount Options）] ドロップダウンリストから有効なマウント オプションを選択します。 （注） Cisco IMC バージョン 2.0(8) 以降を実行しているサーバ用にマウント オプションを選択できます。
[グレースフルタイムアウト (Graceful Timeout）] チェックボックス	ファームウェア アップグレード プロセスを開始するためにホスト システムがシャットダウンする必要がある期間を指定するには、このチェックボックスをオンにします。 （注） グレースフル タイムアウトは、Cisco IMC 3.1(3a) 以降が稼働しているシステムで設定できます。 タイムアウト期間を指定しない場合、システムは 120 秒後に強制的にシャット ダウンされます。

フィールド	説明
[タイムアウト（分）（Timeout (in mins)）] フィールド	ファームウェアアップグレードプロセスを開始するためにホストシステムがシャットダウンする必要がある期間を指定します。 指定できる値は 0 ～ 60 の範囲内の値です。
[サーバの強制シャットダウン（Force Shutdown Server）] チェックボックス	[グレースフル タイムアウト（分）（Graceful Timeout (in mins)）] フィールドに指定した時間内にホスト システムがシャットダウンしなかった場合に、ホストシステムを強制的にシャットダウンするには、このチェックボックスをオンにします。 このオプションは、デフォルトで有効です。

ステップ 5 [送信（Submit）] をクリックします。

（注）
- プロファイル設定の詳細を表示し、ファームウェアイメージの詳細を変更し、イメージプロファイルを削除できます。同時に複数のプロファイルを選択して削除することもできます。
- Cisco IMC Supervisor アプライアンスが、これらのイメージにリモートでマッピングできる必要があります。

ファームウェアのアップグレード

始める前に

- Cisco IMC バージョン 2.0(x) にアップグレードする場合、デフォルトの Cisco IMC パスワードを変更する必要があります。
- 3.0(3e) より古いバージョンの Cisco IMC が稼働しているサーバのローカル ファームウェア イメージプロファイルを使用してファームウェアをアップグレードする場合は、Cisco IMC Supervisor で HTTP を有効にする必要があります。Cisco IMC Supervisor Shell Admin コンソールで HTTP を有効または無効にする方法については、『Cisco IMC Supervisor Shell Guide, Release 2.2』を参照してください。

（注） 1 つの Cisco UCS S3260 高密度ストレージ ラック サーバ シャーシに設置されている両方のサーバを同時にアップグレードすることは推奨されません。

Cisco IMC Supervisor をアップグレードする前に、ファームウェア プロファイルがすでに設定されている場合は、CCO クレデンシャルとプロキシの詳細が設定されていることを確認してください。Cisco.com ユーザの設定 （40 ページ） およびプロキシ設定 （40 ページ） を参照してください。

手順

ステップ 1 **[システム（Systems）] > [ファームウェア管理（Firmware Management）]** を選択します。

ステップ 2 [ファームウェア管理（Firmware Management）] 画面で [ファームウェア アップグレード（Firmware Upgrades）] をクリックします。

ステップ 3 [アップグレードの実行（Run Upgrade）] をクリックします。
警告メッセージが表示され、選択したサーバのアップグレードを実行すると、ホストがリブートしてファームウェア更新ツールが起動することが通知されます。ファームウェアのアップデートが完了すると、サーバはホスト OS を再起動します。

ステップ 4 **[OK]** をクリックして確定します。

ステップ 5 [ファームウェアのアップグレード （Upgrade Firmware）] 画面で次のフィールドに入力します。

フィールド	説明
[プロファイルの選択（Select Profile）] ドロップダウンリスト	ドロップダウンリストからプロファイルを選択します。
プラットフォーム（Platform）	サーバ プラットフォーム、ファームウェア イメージのバージョン、選択したファームウェア プロファイルのパスなどの詳細を表示できます。
イメージ バージョン	
画像パス	
[サーバ（Server(s)）] ボタン	[Select] をクリックして、リストからサーバを選択します。選択したプロファイルで設定されているプラットフォームに一致するサーバだけがリストに表示されます

フィールド	説明
[後でスケジュール（Schedule later）] チェックボックス	このチェックボックスをオンにして、アップグレードを実行する既存のスケジュールを選択します。あるいは、[+]アイコンをクリックして新しいスケジュールを作成することもできます。スケジュールの作成の詳細については、スケジュールの作成 （183 ページ）を参照してください。**[ポリシー（Policies）] > [スケジュールの管理（Manage Schedules）]** の順に移動してスケジュールを選択し、[スケジュール タスクを表示する（View Scheduled Tasks）] をクリックして、スケジュールされたタスクを表示するか、または [スケジュール タスクの削除（Remove Scheduled Tasks）] をクリックしてスケジュールされたタスクを削除できます。スケジュールされたタスクを選択し、[スケジュール済みのタスクの削除（Remove Scheduled Tasks）] をクリックして、関連付けられているスケジュール済みタスクを削除することもできます。

ステップ 6 [送信（Submit）] をクリックします。

（注） ファームウェア アップグレードの詳細を表示したり、指定したアップグレード操作のステータス レコードを削除することもできます。

ホスト イメージ マッピング

ホスト イメージ マッピングは、E シリーズ サーバを対象としたよく利用される機能であり、Cisco IMC にファームウェア ファイルをダウンロードし、ファームウェアをアップグレードできます。次のいずれかをダウンロードおよびアップグレードするには、Cisco IMC Supervisorを使用してホスト イメージ マッピング プロファイルを作成できます。

- ISO ファームウェア イメージ
- CIMC イメージ
- BIOS イメージ

次のいずれかの方法でファームウェア イメージを Cisco IMC にダウンロードできます。

- ファームウェア ファイルを入手できるネットワーク上の場所（FTP、FTPS、HTTP、または HTTPS サーバ）を入力します。

  詳細については、ネットワーク ホストイメージマッピングプロファイルの追加（166 ページ）を参照してください。

- システム上の場所からファームウェア ファイルを選択します。

詳細については、ホスト イメージ マッピングのアップロード プロファイルの作成 （169 ページ）を参照してください。

- www.cisco.com からファームウェア イメージをダウンロードします。

  詳細については、ホストのイメージマッピングの Cisco.com プロファイルの作成 （172 ページ）を参照してください。

重要 これらのタスクを実行するには、Cisco IMCバージョン 3.2.4 が E シリーズ サーバにインストールされている必要があります。以前のバージョンの Cisco IMC ではこの機能は動作しません。

ファームウェアのアップグレードのためにプロファイルを作成する方法については、ネットワーク ホスト イメージ マッピング プロファイルの追加 （166 ページ）を参照してください。

ネットワーク ホスト イメージ マッピング プロファイルの追加

始める前に

システムで UCS E シリーズ サーバのラック アカウントを作成している必要があります。

手順

ステップ 1 **[システム（Systems）] > [ファームウェア管理（Firmware Management）]** を選択します。

ステップ 2 [ファームウェア管理（Firmware Management）] ページで、[ホスト イメージ マッピング（Host Image Mapping）] クリックします。

ステップ 3 [ネットワーク プロファイル（Network Profile）] を選択します。

ネットワーク上の特定の場所からファームウェア イメージをダウンロードした場合は、このボタンをクリックします。

ステップ 4 [ホスト イメージ マッピングのプロファイル - ネットワーク（Create Host Image Mapping Profile - Network）] 画面で、次を含む必須フィールドに入力します。

フィールド	説明
[プロファイル名（Profile Name）] フィールド	プロファイルの記述名。

[プラットフォーム（Platform）] ドロップダウンリスト	サーバ プラットフォームを選択します。 このプロファイルを適用するときに、このドロップダウンリストから選択したプラットフォームに基づいて、使用可能なサーバのリストにエントリが取り込まれます。 **注目** このドロップダウンリストには、UCS E シリーズ サーバに対して作成したラック アカウントが取り込まれます。
[イメージのダウンロード元（Download Image From）] ドロップダウンリスト	ファームウェア イメージが使用可能なサーバのタイプを選択します。次のいずれかを指定できます。 • FTP サーバ • FTPS サーバ • HTTP サーバ • [HTTPSサーバ（HTTPS Server）]
[Server IP Address] フィールド	サーバの IP アドレス。
[File Path] フィールド	ファームウェア ファイルが使用可能な場所のパス。
[ファイルタイプ（File Type）] ドロップダウンリスト	イメージのファイル タイプを選択します次のいずれかを指定できます。 • **ISO** • **CIMC** • **BIOS**
[ファイル名（File Name）] フィールド	ファイルの名前を入力します。
[ユーザ名（User name）] フィールド	ユーザ名。 （注） このフィールドは、[イメージのダウンロード元（Download Image From）] ドロップダウンリストで [FTP サーバ（FTP Server）] または [FTPS サーバ（FTPS Server）] を選択した場合にのみ表示されます。

[パスワード（Password）] フィールド	ユーザのパスワード。 （注） このフィールドは、[イメージのダウンロード元（Download Image From）] ドロップダウンリストで [FTP サーバ（FTP Server）] または [FTPS サーバ（FTPS Server）] を選択した場合にのみ表示されます。
[ダウンロード後のマッピング（Map After Download）] チェックボックス	ダウンロードしたイメージをマッピングします。 重要 このチェックボックスは、[ファイルタイプ（File Type）] ドロップダウンリストで [ISO] を選択した場合にのみ表示されます。 プロファイルの作成時または作成後にイメージをマッピングできます。サーバでアップグレードを開始するためには、ISO イメージのマッピングが必須です。サーバでイメージをマッピングしていない場合にファームウェアをアップグレードしようとすると、イメージがマッピングされていないことを通知するエラー メッセージが表示されます。このシナリオでのイメージのマッピングについては、ホスト イメージのマッピングおよびマップ解除（179 ページ）を参照してください。
[既存のすべてのイメージを削除（Delete All Existing Images）] チェックボックス	ファームウェア アップグレード対象として選択されたサーバの Cisco IMC で使用可能なダウンロード済みイメージをすべて削除します。

[ダウンロード後にアップグレードを実行（Run Upgrade After Download）] チェックボックス	ファームウェア ファイルのダウンロード後すぐにアップグレード プロセスを開始する場合は、このチェックボックスをオンにします。 アップグレード プロセスを後で手動で開始する場合は、このチェックボックスをオンにしないでください。後でこのプロセスを実行するには、ホストイメージアップグレードの手動での実行 （177 ページ）を参照してください。 **重要** [ファイル タイプ（File Type）] ドロップダウンリストで [ISO] を選択した場合、およびこのチェックボックスをオンにした場合、続行するには、[ダウンロード後のマッピング（Map After Download）] チェックボックスもオンにする必要があります。これら両方のチェックボックスをオンにすると、ファームウェア ファイルがダウンロードされ、Cisco IMC にマッピングされます。

ステップ 5 [送信（Submit）] をクリックします。

次のタスク

プロファイルが作成されたら、このプロファイルを実行するサーバを選択する必要があります。詳細については、ホスト イメージ プロファイルの適用 （176 ページ）を参照してください。

プロファイルの作成後に実行できるその他の操作の一部を次に示します。

- プロファイルの編集または削除
- プロファイルのステータス情報の表示
- アップグレード プロセスの開始（プロファイルの作成中に指定しなかった場合）

ホスト イメージ マッピングのアップロード プロファイルの作成

システムから Cisco IMC にファームウェア ファイルをアップロードするには、次の手順を実行します。

始める前に

システムで UCS E シリーズ サーバのラック アカウントを作成している必要があります。

手順

ステップ 1 **[システム（Systems）] > [ファームウェア管理（Firmware Management）]** を選択します。

ステップ 2 [ファームウェア管理（Firmware Management）] ページで、[ホスト イメージ マッピング（Host Image Mapping）] クリックします。

ステップ 3 [プロファイルのアップロード（Upload Proifle）] を選択します。

ステップ 4 [ホスト イメージ マッピングのプロファイル - アップロード（Create Host Image Mapping Profile - Upload）] 画面で、次を含む必須フィールドに入力します。

フィールド	説明
[プロファイル名（Profile Name）] フィールド	プロファイルの内容がわかる一意の名前。プロファイル名は固有である必要があります。
[プラットフォーム（Platform）] ドロップダウンリスト	ドロップダウンリストからプラットフォームを選択します。 このプロファイルを適用するときに、このドロップダウンリストから選択したプラットフォームに基づいて、使用可能なサーバのリストにエントリが取り込まれます。 **注目** このドロップダウンリストには、UCS E シリーズ サーバに対して作成したラック アカウントが取り込まれます。
[ファイルタイプ（File Type）] ドロップダウンリスト	イメージのファイル タイプを選択します 次のいずれかを指定できます。 • ISO • CIMC • BIOS
[ファイル名（File Name）] フィールド	[ファイルを選択（Select a File）] をクリックして、システムからファイルを参照して選択します。

フィールド	説明
[ダウンロード後のマッピング（Map After Download）] チェックボックス	ダウンロードしたイメージをマッピングします。 **重要** このチェックボックスは、[ファイル タイプ（File Type）] ドロップダウン リストで [ISO] を選択した場合にのみ表示されます。 プロファイルの作成時または作成後にイメージをマッピングできます。サーバでアップグレードを開始するためには、ISO イメージのマッピングが必須です。サーバでイメージをマッピングしていない場合にファームウェアをアップグレードしようとすると、イメージがマッピングされていないことを通知するエラー メッセージが表示されます。このシナリオでのイメージのマッピングについては、ホスト イメージのマッピングおよびマップ解除（179 ページ）を参照してください。
[既存のすべてのイメージを削除（Delete All Existing Images）] チェックボックス	ファームウェア アップグレード対象として選択されたサーバの Cisco IMC で使用可能なダウンロード済みイメージをすべて削除します。

フィールド	説明
[ダウンロード後にアップグレードを実行（Run Upgrade After Download）] チェックボックス	ファームウェア ファイルのダウンロード後すぐにアップグレード プロセスを開始する場合は、このチェックボックスをオンにします。 アップグレード プロセスを後で手動で開始する場合は、このチェックボックスをオンにしないでください。後でこのプロセスを実行するには、ホストイメージアップグレードの手動での実行 （177 ページ）を参照してください。 **重要** [ファイル タイプ（File Type）] ドロップダウンリストで [ISO] を選択した場合、およびこのチェックボックスをオンにした場合、続行するには、[ダウンロード後のマッピング（Map After Download）] チェックボックスもオンにする必要があります。これら両方のチェックボックスをオンにすると、ファームウェア ファイルがダウンロードされ、Cisco IMC にマッピングされます。

ステップ 5 [送信（Submit）] をクリックします。

次のタスク

プロファイルが作成されたら、このプロファイルを実行するサーバを選択する必要があります。詳細については、ホスト イメージ プロファイルの適用 （176 ページ）を参照してください。

プロファイルの作成後に実行できるその他の操作の一部を次に示します。

- プロファイルの編集または削除
- プロファイルのステータス情報の表示
- アップグレード プロセスの開始（プロファイルの作成中に指定しなかった場合）

ホストのイメージ マッピングの Cisco.com プロファイルの作成

www.cisco.com からイメージをダウンロードするためのプロファイルを作成するには、次の手順を実行します。

始める前に

- Cisco.com ユーザ クレデンシャルを設定している必要があります。詳細については、Cisco.com ユーザの設定 （40 ページ）を参照してください。
- システムでプロキシ設定を有効にしている必要があります。詳細については、プロキシ設定 （40 ページ）を参照してください。

手順

ステップ 1 **[システム（Systems）] > [ファームウェア管理（Firmware Management）]** を選択します。

ステップ 2 [ファームウェア管理（Firmware Management）] ページで、[ホスト イメージ マッピング（Host Image Mapping）] クリックします。

ステップ 3 [CCO プロファイル（CCO Profile）] を選択します。

ステップ 4 [ホスト イメージ マッピングのプロファイル - CCO（Create Host Image Mapping Profile - CCO）] 画面で、次を含む必須フィールドに入力します。

フィールド	説明
[プロファイル名（Profile Name）] フィールド	プロファイルの内容がわかる一意の名前。プロファイル名は固有である必要があります。
[プロキシ設定（Proxy Configuration）] チェックボックス	プロキシ設定が行われているかどうかを示します。このチェックボックスがオンの場合は、プロキシ設定は行われています。
[プラットフォーム（Platform）] ドロップダウンリスト	ドロップダウンリストからプラットフォームを選択します。 このプロファイルを適用するときに、このドロップダウンリストから選択したプラットフォームに基づいて、使用可能なサーバのリストにエントリが取り込まれます。 **注目** このドロップダウンリストには、UCS E シリーズ サーバに対して作成したラック アカウントが取り込まれます。

フィールド	説明
[今すぐダウンロード（Download Now）] チェックボックス	プロファイルの作成後すぐにファームウェア イメージのダウンロードを開始するには、このチェックボックスをオンにします。 このチェックボックスをこの時点でオンにしない場合は、後でイメージをダウンロードできます。これを行うには、[ホスト イメージ マッピング（Host Image Mapping）] 画面でプロファイル名を選択し、[その他の操作（More Actions）] ドロップダウンリストから [イメージのダウンロード（Download Image）] を選択します。イメージがダウンロードされたら、プロファイルを適用する必要があります。詳細については、ホストイメージプロファイルの適用 （176 ページ）を参照してください。
[使用可能なイメージ（Available Image）] ドロップダウンリスト	ドロップダウンリストからイメージを選択します。 このリストには、[プラットフォーム（Platform）] ドロップダウンリストで選択したサーバ プラットフォームに関連するイメージが取り込まれます。
[ダウンロード後のマッピング（Map After Download）] チェックボックス	ダウンロードしたイメージをマッピングします。 **重要** このチェックボックスは、[ファイル タイプ（File Type）] ドロップダウンリストで [ISO] を選択した場合にのみ表示されます。 プロファイルの作成時または作成後にイメージをマッピングできます。サーバでアップグレードを開始するためには、ISO イメージのマッピングが必須です。サーバでイメージをマッピングしていない場合にファームウェアをアップグレードしようとすると、イメージがマッピングされていないことを通知するエラー メッセージが表示されます。このシナリオでのイメージのマッピングについては、ホスト イメージのマッピングおよびマップ解除（179 ページ）を参照してください。

フィールド	説明
[既存のすべてのイメージを削除（Delete All Existing Images）] チェックボックス	ファームウェア アップグレード対象として選択されたサーバの Cisco IMC で使用可能なダウンロード済みイメージをすべて削除します。
[ダウンロード後にアップグレードを実行（Run Upgrade After Download）] チェックボックス	ファームウェア ファイルのダウンロード後すぐにアップグレード プロセスを開始する場合は、このチェックボックスをオンにします。 アップグレード プロセスを後で手動で開始する場合は、このチェックボックスをオンにしないでください。後でこのプロセスを実行するには、ホストイメージアップグレードの手動での実行 （177 ページ）を参照してください。 **重要** [ファイル タイプ（File Type）] ドロップダウンリストで [ISO] を選択した場合、およびこのチェックボックスをオンにした場合、続行するには、[ダウンロード後のマッピング（Map After Download）] チェックボックスもオンにする必要があります。これら両方のチェックボックスをオンにすると、ファームウェア ファイルがダウンロードされ、Cisco IMC にマッピングされます。

ステップ 5 [送信（Submit）] をクリックします。

次のタスク

プロファイルが作成されたら、このプロファイルを実行するサーバを選択する必要があります。詳細については、ホスト イメージ プロファイルの適用 （176 ページ）を参照してください。

プロファイルの作成後に実行できるその他の操作の一部を次に示します。

- プロファイルの編集または削除
- プロファイルのステータス情報の表示
- アップグレード プロセスの開始（プロファイルの作成中に指定しなかった場合）
- イメージのダウンロード（プロファイルの作成中にダウンロードしなかった場合）
- ダウンロードしたイメージの削除

ホスト イメージ プロファイルの適用

ホスト イメージ マッピング プロファイルの作成後に、次の目的に使用するサーバを選択できます。

- Cisco IMC にイメージをダウンロードするためにプロファイルを実行できる。
- ファームウェア アップグレードを即時に開始する必要がある（プロファイルの作成時に [ダウンロード後にアップグレードを実行（Run Upgrade After Download）] チェックボックスをオンにしている場合）。

（注） ホスト イメージ プロファイルを適用していない場合は、[ステータスの表示（View Status）] オプションを選択すると空白のレポートが生成されます。また、プロファイルを適用していない場合や、ホストイメージプロファイルの適用アクションが進行中の場合には、ファームウェア アップグレードを開始できません。

始める前に

システムでホスト イメージ マッピング プロファイルを作成している必要があります。

手順

ステップ 1 **[システム（Systems）] > [ファームウェア管理（Firmware Management）]** を選択します。

ステップ 2 [ファームウェア管理（Firmware Management）] ページで、[ホスト イメージ マッピング（Host Image Mapping）] クリックします。

ステップ 3 テーブルからプロファイルを選択し、[適用（Apply）] をクリックします。

あるいは、プロファイルを選択して、[その他の操作（More Actions）] ドロップダウンリストから [適用（Apply）] を選択できます。

ステップ 4 [プロファイルの適用（Apply Profile）] 画面で [選択（Select）] をクリックし、ファームウェア イメージを適用する必要があるサーバを選択します。

複数のサーバを選択できます。サーバのリストには、プロファイルの作成時に選択したサーバ プラットフォームに基づいてサーバが表示されます。

ステップ 5 [選択（Select）] をクリックして [プロファイルの適用（Apply Profile）] 画面に戻ります。

ステップ 6 [送信（Submit）] をクリックします。

ファームウェア イメージのダウンロード

サーバの Cisco IMC でファームウェア イメージをダウンロードするには、次の手順を実行します。

始める前に

ファームウェア イメージをダウンロードするための Cisco.com プロファイルを作成している必要があります。

- ファームウェア イメージをダウンロードするための Cisco.com プロファイルを作成しています。
- プロファイルの作成時に [今すぐダウンロード（Download Now）] チェックボックスをオフにしています。

手順

ステップ 1 **[システム（Systems）] > [ファームウェア管理（Firmware Management）]** を選択します。

ステップ 2 [ファームウェア管理（Firmware Management）] ページで、[ホスト イメージ マッピング（Host Image Mapping）] クリックします。

ステップ 3 プロファイルのリストから CCO プロファイルを選択します。

ステップ 4 [その他の操作（More Actions）] ドロップダウンリストから [イメージのダウンロード（Download Image）] を選択します。

ステップ 5 [イメージのダウンロード（Download Image）] 画面に表示される情報を確認し、[ダウンロード（Download）] をクリックします。

プロファイルに指定されているファームウェア イメージが、設定したクレデンシャルを使用して Cisco.com からダウンロードされます。

次のタスク

ダウンロードしたイメージは後で削除できます。詳細については、ダウンロードイメージの削除 （178 ページ）を参照してください。

ホスト イメージ アップグレードの手動での実行

ホスト イメージ マッピング プロファイルの作成時に [ダウンロード後にアップグレードを実行（Run Upgrade After Download）] チェックボックスをオンにしていない場合、次の手順に従ってアップグレード プロセスを手動で実行します。

始める前に

システムでホスト イメージ マッピング プロファイルを作成している必要があります。

手順

ステップ 1 **[システム（Systems）] > [ファームウェア管理（Firmware Management）]** を選択します。

ステップ 2 [ファームウェア管理（Firmware Management）] ページで、[ホスト イメージ マッピング（Host Image Mapping）] クリックします。

ステップ 3 [アップグレードの実行（Run Upgrade）] を選択します。

ステップ 4 [ホスト イメージのアップグレード（Upgrade Host Image）] 画面で、次を含む必須フィールドに入力します。

フィールド	説明
[プロファイルの選択（Select Profile）] ドロップダウンリスト	プロファイルを選択します。 プロファイルを選択したら、プロファイルの詳細が画面に表示されます。
[サーバ（Servers）] フィールド	[選択（Select）] をクリックし、アップグレードを実行する必要があるサーバを選択します。
[後でスケジュール（Schedule Later）] チェックボックス	このチェックボックスをオンにして、後でサーバをアップグレードするための既存のスケジュールを選択するか、または [+] をクリックして新しいスケジュールを作成します。 新しいスケジュールの作成の詳細については、スケジュールの作成（183 ページ）を参照してください。

ステップ 5 [送信（Submit）] をクリックします。

ダウンロード イメージの削除

Cisco.com プロファイルの作成時に、プロファイル作成後すぐにファームウェア イメージをダウンロードすることを選択するか、または後でダウンロードすることができます。ダウンロードしたイメージは、Cisco IMC Supervisor から削除できます。このオプションは、Cisco.com プロファイルを使用してダウンロードしたイメージでのみ使用可能です。

手順

ステップ 1 **[システム（Systems）] > [ファームウェア管理（Firmware Management）]** を選択します。

ステップ 2 [ファームウェア管理（Firmware Management）] ページで、[ホスト イメージ マッピング（Host Image Mapping）] クリックします。

ステップ 3 作成したプロファイルのリストから CCO プロファイルを選択します。

ステップ 4 [その他の操作（More Actions）] ドロップダウンリストから [イメージの削除（Delete Image）] を選択します。

ステップ 5 [イメージの削除（Delete Image(s)）] 画面で、[削除（Delete）] をクリックします。

ホスト イメージのマッピングおよびマップ解除

特定の Cisco IMC サーバでホストイメージをマッピングまたはマップ解除するには、次の手順を実行します。ISO ホストイメージだけをマッピングおよびマップ解除できます。その他のホスト イメージ（BIOS、CIMC など）は、この画面で削除のみ実行できます。

始める前に

システムでホスト イメージ マッピング プロファイルを作成している必要があります。

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [ラック グループ（Rack Groups）] を展開し、サーバが含まれているラック グループを選択します。

ステップ 3 選択したラック グループのページで、[ラック サーバ（Rack Servers）] をクリックします。

ステップ 4 リストでサーバをダブルクリックしてその詳細を確認するか、リストでサーバを選択し、右端の下矢印をクリックして [詳細の表示（View Details）] を選択します。

（注） リストからサーバを選択するまでは、右端に下向き矢印は表示されません。

ステップ 5 [ホスト イメージ（Host Images）] タブを選択します。

Cisco IMC サーバで使用可能なすべてのイメージのリストが画面に表示されます。

ステップ 6 ISO ホスト イメージを選択し、[イメージのマッピング（Map Image）]、[イメージのマップ解除（Unmap Image）]、[イメージの削除（Delete Image）] のいずれかを選択します。

BIOS イメージと CIMC イメージの場合、この画面では [イメージの削除（Delete Image）] だけを選択できます。

ホスト プロファイル イメージのステータス詳細の表示

始める前に

システムでホスト イメージ マッピング プロファイルを作成している必要があります。

手順

ステップ 1 **[システム（Systems）] > [ファームウェア管理（Firmware Management）]** を選択します。

ステップ 2 [ファームウェア管理（Firmware Management）] ページで、[ホスト イメージ マッピング（Host Image Mapping）] クリックします。

ステップ 3 テーブルからプロファイルを選択し、[その他の操作（More Actions）] ドロップダウンリストから [ステータス詳細の表示（View Status Details）] を選択します。

テーブルからプロファイルを選択し、右クリックして [ステータス詳細の表示（View Status Details）] を選択することもできます。

[ホストイメージマッピングプロファイルのステータスを表示します（View Host Image Mapping Profile Status）] 画面に次の情報が表示されます。

- プロファイル名
- サーバの IP アドレス
- ダウンロード ステータス
- アップグレードステータス

アップロードプロファイルおよびCisco.comプロファイルのステータス情報が表示されます。

（注） ファームウェアをアップグレードするために BIOS ファイルを選択している場合は、そのサーバの Cisco IMC に変更が反映されるまで 3 ～ 4 分待つ必要があります。

ホスト イメージ マッピング プロファイルの削除

手順

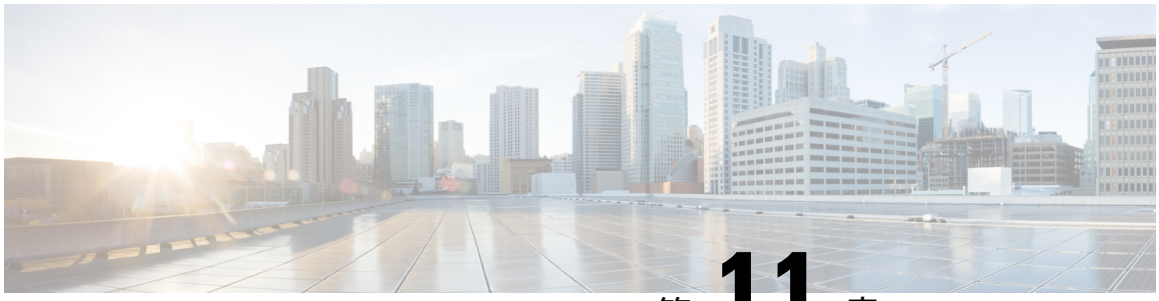
ステップ 1 **[システム（Systems）] > [ファームウェア管理（Firmware Management）]** を選択します。

ステップ 2 [ファームウェア管理（Firmware Management）] ページで、[ホスト イメージ マッピング（Host Image Mapping）] クリックします。

ステップ 3 テーブルからプロファイルを選択し、[プロファイルの削除（Delete Profile）] をクリックします。

ステップ 4 [プロファイルの削除（Delete Profile）] 画面で、[削除（Delete）] をクリックします。

プロファイルがシステムから削除されます。



第 11 章

Cisco IMC Supervisor パッチの更新

この章は次のトピックで構成されています。

Cisco IMC Supervisor パッチの更新の概要

自動パッチ更新通知は Cisco IMC Supervisorで使用できます。Cisco IMC Supervisor は、シスコの自動ソフトウェア配布（ASD）サービスを使用して、cisco.com で使用可能な新しいパッチ更新の有無を定期的に（14 日ごとに）確認します。現在のリリース以降のパッチ更新があれば、Cisco IMC Supervisor更新マネージャーによってパッチが Cisco IMC Supervisor 内の場所にダウンロードされます。たとえば、[場所（Location）] に **/opt/infra/uploads/external/downloads/imcs/<*filename.zip*>** と表示される場合は、パッチ URL に **file:////opt/infra/uploads/external/downloads/imcs/<filename.zip>** ftp コマンドを使用できます。その後、Shell Admin に移動して、パッチを適用できます。パッチ適用の詳細については、『Cisco IMC Supervisor Shell Guide』の「*Applying a Patch to Cisco IMC Supervisor*」を参照してください。[今すぐ更新を確認（Check For Updates Now）] オプションを使用して、新しいバージョンが使用可能か手動で確認することもできます。

（注） 現在のリリースの新しいパッチ更新のみが通知されます。Cisco IMC Supervisorベースの更新は OVF ファイルには適用されません。

Cisco IMC Supervisor パッチ更新の確認

Cisco IMC Supervisor に新しいパッチ更新の有無について定期的に（14 日ごとに）チェックを実行させるには、サポート クレデンシャルとその他の詳細を入力する必要があります。Cisco IMC Supervisorはこれらの詳細を使用して、Cisco ASD のバックエンド サービスと通信し、新しい更新について問い合わせを行います。パッチの新しいバージョンは、Cisco IMC Supervisor アプライアンスに自動的にダウンロードされます。

手順

ステップ 1 **[管理（Administration）] > [IMCS の更新（Update IMCS）]** を選択します。

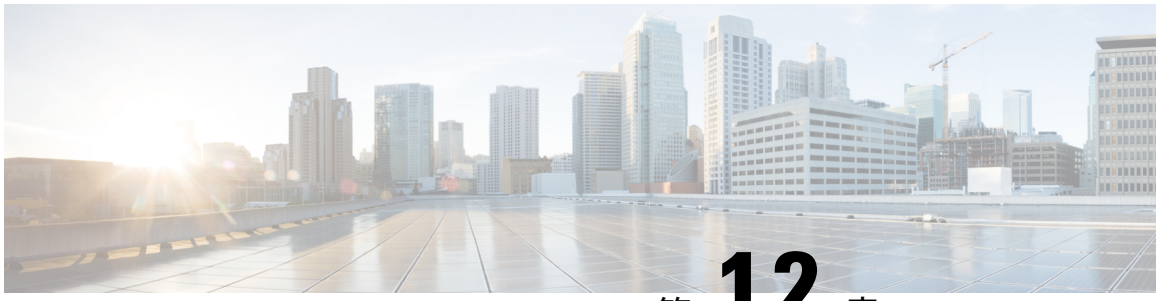
ステップ 2 [IMCS の更新（Update IMCS）] ページで [今すぐ更新を確認（Check For Updates Now）] を使用して、Cisco IMC Supervisorの更新を確認します。

ステップ 3 [送信（Submit）] をクリックします。
レポートに最新の更新が表示されます。

ステップ 4 [レポートのエクスポート（Export Report）] アイコンをクリックして、レポートを PDF、CSV、または XLS 形式でエクスポートします。

ステップ 5 [レポートの生成（Generate Report）] をクリックして、レポートを生成します。

ステップ 6 [ダウンロード（Download））] をクリックしてレポートをダウンロードするか、[閉じる（Close）] をクリックします。



第 12 章

スケジュールの管理

この章は次のトピックで構成されています。

スケジュール管理の概要

スケジュールを定義することで、特定のタスクを異なるタイミングで実行するために保留できます。たとえば、ファームウェアのアップデート、サーバ検出、ポリシーおよびプロファイルの適用などのタスクを、事前定義の時刻または事前定義の頻度で実行するようにスケジュールできます。サーバの作業負荷が低いオフピーク時にタスクをスケジュールできます。

スケジュールの作成

新しいスケジュールを作成するときに、この手順を実行します。

手順

ステップ 1 **[ポリシー（Policies）] > [スケジュールの管理（Manage Schedules）]** を選択します。

ステップ 2 [スケジュールの管理（Manage Schedules）] ページで [追加（Add）] をクリックします。

ステップ 3 [スケジュールの作成（Create Schedule）] ダイアログボックスで、次の情報を入力します。

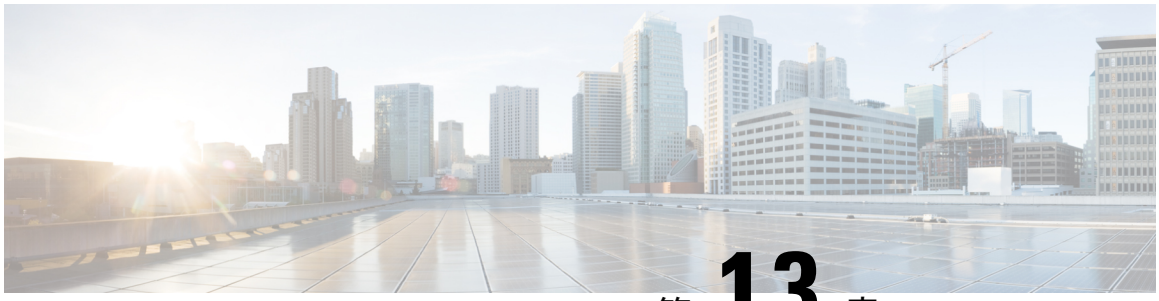
フィールド	説明
[スケジュール名（Schedule Name）] フィールド	スケジュール タスクの名前を入力します。

フィールド	説明
[スケジュールの有効化（Enable Schedule）] チェック ボックス	スケジュールを有効にするには、このチェック ボックスをオンにします。スケジュールを有効または無効にすることで（[有効（Enable）] または [無効（Disable）] オプションを使用）、スケジュールに関連付けられたタスクの実行を有効または無効にすることができます。
[スケジュール タイプ（Scheduler Type）] ラジオボタン	スケジュールの実行を 1 回限りにするか、繰り返すかを選択します。 [1 回限り（One Time）] のスケジュールを選択する場合は、日付、時刻、午前、午後のオプション ボタンを選択します。 （注） スケジュールの時刻はアプライアンスの時刻に基づいています。ただし、タイム ゾーンはローカル クライアント ブラウザに基づきます。 [繰り返し（Recurring）] のスケジュールを選択した場合は、ドロップダウンリストから、日付（0 ～ 30 日）、時間、分を選択します。

ステップ 4 [送信（Submit）] をクリックします。

次のタスク

- 既存のスケジュールを選択して、変更または削除したり、スケジュール済みのタスクを表示したりできます。[スケジュール済みのタスクの表示（View Scheduled Tasks）] には、ファームウェアのアップグレード、自動検出の実行、ハードウェア ポリシーの適用 （142 ページ）またはハードウェア プロファイルの適用 （148 ページ）を行う場合に、スケジュールに関連付けられたファームウェアのアップグレード、自動検出、ポリシーおよびプロファイルの適用の各タスクのステータスを確認できるレポートが表示されます。
- スケジュールに関連付けられているタスク（複数可）を選択し、[スケジュール済みタスクの削除（Remove Scheduled Tasks）] オプションを使用して、スケジュールとの関連を解除できます。



第 13 章

サーバ診断の実行

この章は次のトピックで構成されています。

サーバ診断の概要

サーバ診断は、UCS サーバ設定ユーティリティ（UCS-SCU）から使用できます。診断ツールを使用して、シスコ サーバのハードウェアの問題を診断し、さまざまなサーバ コンポーネントに対してテストを実行し、ハードウェアの問題を見つけたり、テスト結果を表形式で分析することができます。

UCS-SCU イメージをダウンロードおよび設定し、リモート ロケーションに保存する必要があります。

（注） UCS-SCU イメージを使用して診断テストを実行すると、サーバが UCS-SCU イメージで再起動されるので、サーバが一時的に使用できなくなります。

Cisco IMC Supervisor では、サーバが存在するさまざまな地理的場所にまたがる複数の診断イメージを設定できます。診断では、サーバとその場所にあるイメージの間で低遅延ネットワーク促進されるため、高速に実行されます。

どのラック サーバで診断を実行する場合でも、そのサーバは設定した場所でホストされている UCS-SCU イメージでリブートされます。診断の表形式のレポートには、診断を実行した各サーバに関する診断のステータスが表示されます。また、サーバの詳細、レポートが生成された日時、診断ステータスなども表示されます。単一または複数のサーバに関する診断レポートを削除したり、ダウンロードしたりできます。

（注） サーバ診断を実行するには、scpuser パスワードを設定する必要があります。scpuser パスワードを設定するには、SCP ユーザの設定 （38 ページ）を参照してください。

サーバ設定ユーティリティ イメージの場所の設定

UCS-SCU イメージの場所を設定および保存するには、次の手順を実行します。

手順

ステップ 1 **[システム（Systems）]** > **[サーバ診断（Server Diagnostics）]** を選択します。

ステップ 2 [SCU イメージ プロファイル（SCU Image Profiles）] をクリックします。

ステップ 3 [サーバ診断（Server Diagnostics）] ページで [+] をクリックします。

ステップ 4 [SCU イメージの場所の設定（Configure SCU Image Location）] ページで次のフィールドに入力します。

フィールド	説明
[プロファイル名（Profile Name）] フィールド	プロファイルの記述名。
[ISO 共有タイプ（ISO Share Type）] ドロップダウンリスト	[ネットワーク ファイル システム（NFS）（Network File System (NFS)）]、[Common Internet File System（CIFS）]、[ワールド ワイド ウェブ（WWW）（World Wide Web (WWW)）]、[LOCAL] のいずれかの共有タイプを選択します。
[LOCAL] を選択する場合	
[SCU イメージ（SCU Image）] フィールド	SCUイメージファイルを参照、選択、およびアップロードします。
[NFS]、[CIFS]、または [WWW (HTTP/HTTPS)] を選択する場合	
[ISO 共有 IP（ISO Share IP）] フィールド	ISO 共有 IP アドレスを入力します。
[ISO 共有パス（ISO Share Path）] フィールド	ISO 共有パスを入力します。
[ユーザ名（Username）] フィールド	ISO 共有ログインのユーザ名を入力します。
[パスワード（Password）] フィールド	IISO 共有ログインのパスワードを入力します。

ステップ 5 [保存（Save）] をクリックします。

診断の実行

サーバまたはサーバ グループの診断を実行するには、次の手順を実行します。

（注） 3.0(3e) より古いバージョンの Cisco IMC が稼働しているサーバのローカル SCU イメージ プロファイルを使用して診断を実行する場合は、Cisco IMC Supervisor で HTTP を有効にする必要があります。Cisco IMC Supervisor Shell Admin コンソールで HTTP を有効または無効にする方法については、『Cisco IMC Supervisor Shell Guide, Release 2.2』を参照してください。

手順

ステップ 1 **[システム（Systems）] > [サーバ診断（Server Diagnostics）]** を選択します。

ステップ 2 [診断の実行（Run Diagnostics）] をクリックします。

ステップ 3 [診断の実行（Run Diagnostics）] ページで、次のフィールドに入力します。

フィールド	説明
[プロファイルの選択（Select Profile）] ドロップダウンリスト	ドロップダウンリストから既存のプロファイルを選択します。
[選択（Choose）] ドロップダウンリスト	ドロップダウンリストのサーバまたはサーバ グループに対して診断を実行するかどうかを選択します。
[サーバ（Server(s)）] または [サーバ グループ（Server Group(s)）] ドロップダウンリスト	診断を実行するサーバまたはサーバ グループを選択します。

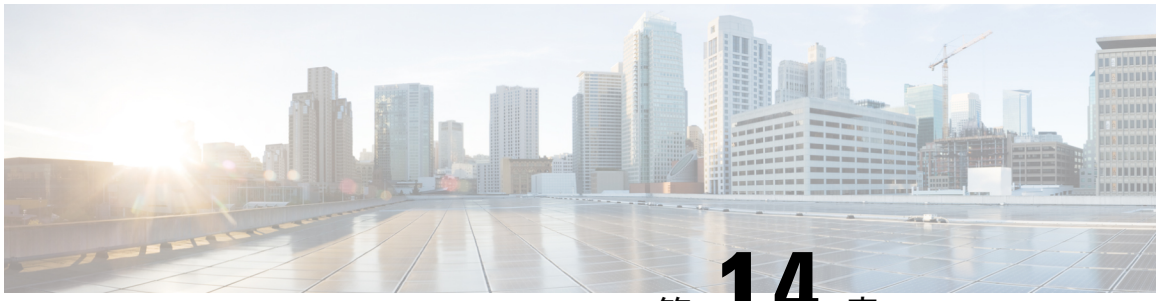
ステップ 4 [選択（Select）] をクリックし、[選択（Select）] ダイアログボックスからサーバまたはサーバ グループを選択します。

ステップ 5 [選択（Select）] をクリックします。
選択したサーバまたはサーバ グループは、[サーバ（Server(s)）] または [サーバ グループ（Server Group(s)）] フィールドの横に表示されます。

ステップ 6 [送信（Submit）] をクリックします。

（注） 1 つ以上のサーバに対して次の操作を実行できます。

- レポートを表示するには、サーバを選択して、[レポートの表示（View Report）] をクリックします。
- レポートを削除するには、1つ以上のサーバを選択して、[レポートの削除（Delete Report）] をクリックします。
- レポートをダウンロードするには、1つ以上のサーバを選択して、[レポートのダウンロード（Download Report）] をクリックします。診断レポートをダウンロードするために複数のサーバを選択した場合は、すべてのレポートを含む zip ファイルがダウンロードされます。
- 診断操作がすでに実行中であるサーバは選択できません。そのサーバで別の診断を開始するには、診断操作が完了するまで待ちます。
- 診断が完了するまでには 40 分程度かかります。これは、サーバに存在するコンポーネントの数に応じて異なります。



第 14 章

Smart Call Home： Cisco IMC Supervisor

この章は次のトピックで構成されています。

Smart Call Home の概要

Cisco Smart Call Home は一部の Cisco デバイスに組み込まれている自動サポート機能であり、該当デバイスの継続的なモニタリング、予防的診断、アラート、および修復の推奨を行います。Smart Call Home を使用すると、問題を迅速に特定して解決し、可用性と運用効率を向上させることができます。この機能は、Cisco IMC Supervisorが管理するハードウェアの有効なサポート契約がある場合に利用できます。有効な場合、Smart Call Home は、Cisco Technical Assistance Center（TAC）のエンジニア、シスコ サポート コミュニティ、および開発者との対話を通じてシスコが特定した一連の障害を検索します。Smart Call Home では、ユーザがエスカレートして報告すべき問題や障害に気付くまで待たずに、障害を事前に特定して診断します。

Cisco IMC Supervisor により管理されるサーバ タスク（**グループ ラック サーバ インベントリ**、**ラック サーバ障害**、**ヘルス システム**など）は定期的に実行され、関連情報を Smart Call Home バックエンドに送信します。バックエンドはこのデータを処理し、問題が確認された場合は、問題解決のために TAC でケースが自動的に登録されます。

Cisco IMC Supervisor ユーザ インターフェイスを使用して Smart Call Home を設定できます。詳細については、Smart Call Home の設定 （189 ページ）を参照してください。

Smart Call Home の設定

Smart Call Home を設定するには、次の手順を実行します。

手順

ステップ 1 **[管理（Administration）] > [システム（System）]** を選択します。

ステップ 2 [システム（System）] ページで [Smart Call Home] をクリックします。

ステップ 3 収集された障害が Smart Call Home のバックエンドに転送されるように、[Smart Call Home の有効化（Enable Smart Call Home）] チェックボックスをオンにします。

（注） デフォルトでは、Smart Call Home は無効です。

ステップ 4 [連絡先の電子メール（Contact Email）] に、連絡先の電子メール アドレスを入力します。

（注） このフィールドには、一度に 1 つの連絡先電子メールを入力できます。

ステップ 5 デフォルトでは、Smart Call Home バックエンドの [宛先 URL（Destination URL）] が設定されます。

（注）
- デフォルト URL を変更しないことを推奨します。
- [プロキシ設定（Proxy Configuration）] チェックボックスはデフォルトでオンになっています。Smart Call Home は、すでに設定されているプロキシの詳細を使用します。プロキシ設定 （40 ページ）を参照してください。

ステップ 6 （オプション）サーバのインベントリの詳細を送信するには、[グループ インベントリを今すぐ送信（Send Group Inventory Now）] チェックボックスをオンにします。管理対象サーバごとに 1 つのインベントリ メッセージが Smart Call Home バックエンドに送信されます。これは、TAC チームによる問題解決のための追加情報として使用されることがあります。

ステップ 7 [保存（Save）] をクリックします。

（注）
- 管理対象サーバで発生した障害はバックエンドに送信されます。各種障害コードとその重大度については、障害コード （190ページ）を参照してください。Smart Call Home へのログインとさまざまなタスクの実行については、Cisco Smart Call Home Community で情報を参照してください。
- URL https://tools.cisco.com/its/service/oddce/services/DDCEService が Cisco IMC Supervisor アプライアンスから到達可能であることを確認します。

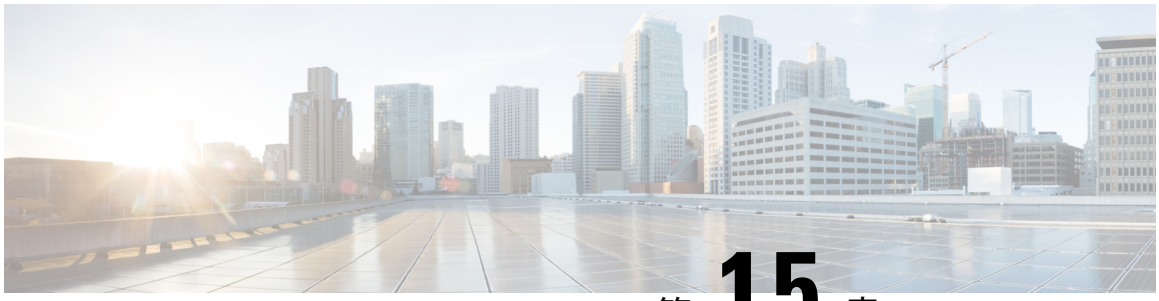
障害コード

Smart Call Home の障害コード

Cisco IMC Supervisor が Smart Call Home のバックエンドに送信するエラー メッセージのリストを次に示します。

障害コード	障害名	メッセージ	重大度	サービス リクエストの作成
F0174	fltProcessorUnitInoperable	Processor [id] on [Serverid] operability: [operability]	深刻 | メジャー	Y
F0177	fltProcessorUnitThermalThresholdNonRecoverable	Processor [id] on [serverid] temperature:[thermal]	深刻	Y
F0181	fltStorageLocalDiskInoperable	Local disk [id] on [serverid] operability: [operability]	メジャー | 警告	Y
F0185	fltMemoryUnitInoperable	DIMM [location] on [serverid] operability: [operability]	メジャー	Y
F0188	fltMemoryUnitThermalThresholdNonRecoverable	DIMM [location] on [serverid] temperature: [thermal]	深刻	N
F0379	fltEquipmentIOCardThermalProblem	IOCard [location] on server [id] operState: [operState]	メジャー	N
F0385	fltEquipmentPsuThermalThresholdNonRecoverable	Power supply [id] in [serverid] temperature: [thermal]	深刻	Y
F0389	fltEquipmentPsuVoltageThresholdCritical	Power supply [id] in [serverid] voltage: [voltage]	メジャー	N
F0391	fltEquipmentPsuVoltageThresholdNonRecoverable	Power supply [id] in [serverid] voltage: [voltage]	深刻	Y
F0407	fltEquipmentPsuIdentity	Power supply [id] on [serverid] has a malformed FRU	深刻	N
F0411	fltEquipmentChassisThermalThresholdNonRecoverable	Thermal condition on [serverid] cause: [thermalStateQualifier]	深刻	N
F0424	fltComputeBoardCmosVoltageThresholdCritical	CMOS battery voltage on [serverid] is [cmosVoltage]	メジャー	N

障害コード	障害名	メッセージ	重大度	サービス リクエストの作成
F0425	fltComputeBoardCmosVoltageThresholdNonRecoverable	CMOS battery voltage on [serverid] is [cmosVoltage]	深刻	Y
F0531	fltStorageRaidBatteryInoperable	RAID Battery on [serverid] operability: [operability]	メジャー	Y
F0868	fltComputeBoardPowerFail	Motherboard of [serverid] power: [power]	深刻	N
F0997	fltStorageRaidBatteryDegraded	Raid battery [id] on [serverid] operability: [operability]	メジャー	N
F1004	fltStorageControllerInoperable	Storage Controller [id] operability: [operability]	深刻	N
F1007	fltStorageVirtualDriveInoperable	Virtual drive [id] on [serverid] operability: [operability]	深刻	N



第 15 章

Cisco UCS S3260 高密度ストレージ ラック サーバの管理

この章は次のトピックで構成されています。

Cisco UCS S3260 高密度ストレージ ラック サーバについて

Cisco UCS S3260 は、デュアル サーバ ノードをサポートする高密度ストレージ ラック サーバです。ビッグ データ、クラウド、オブジェクト ストレージ、コンテンツ配信などの環境で使用される大規模データ セットに対応して最適化できます。これは、Cisco UCS C シリーズ ラックマウント サーバ製品ファミリに属しています。

Cisco UCS S3260 高密度ストレージ ラック サーバは、Cisco Unified Computing System と Cisco IMC Supervisor の統合の一部としてスタンドアロン環境で動作するように設計されています。Cisco UCS S3260 高密度ストレージ ラック サーバには、次の機能が含まれています。

- 高速かつ可用性構成可能なディスク アレイ（RAID）および Just a Bunch Of Disks（JBOD）を活用した、エンタープライズクラスの冗長化構成に対応
- Web ベース アクセス、管理可能なインターフェイス（Cisco Integrated Management Controller）
- サーバ ノードの交換やアップグレード時にデータ移行が不要
- サーバ シャーシの奥行きが短い設計

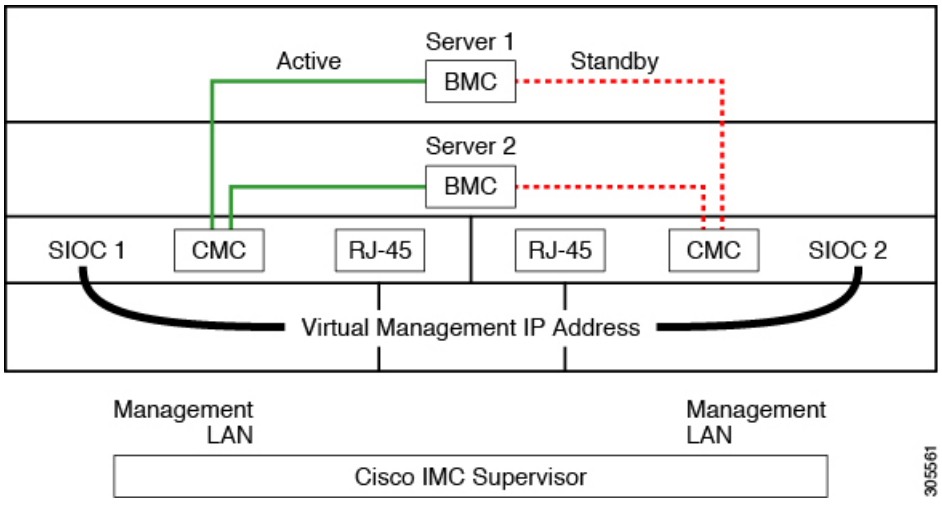
Cisco UCS S3260 高密度ストレージ ラック サーバの詳細については、Cisco UCS S3260 Rack Serverを参照してください。

Cisco UCS S3260 高密度ストレージ ラック サーバのアーキテクチャの概要

アーキテクチャの概要

Cisco UCS S3260 は、シスコのブレード テクノロジーに関する専門知識を活かしたモジュール型サーバアーキテクチャを採用しており、システム内のコンピュートまたはネットワーク ノードをアップグレードする場合でも、別のシステムにデータを移行することなくアップグレードできます。次の機能を備えています。

- 1 つのシャーシにサーバ ノードを 2 台搭載
- サーバ ノードあたり最大 24 のコンピューティング コア
- 最大 60 ドライブ スロット、サーバ ノードごとに HDD だけでなく、最大 14 の SSD ドライブと 2 つの SSD SATA ブート ドライブが搭載でき、様々なストレージ構成に対応
- サーバ ノードあたり最大 512 GB のメモリ（2 台合計 1 テラバイト [TB]）
- 12 Gbps のダイレクト接続 SCSI （SAS）ドライブのサポート
- Cisco VIC 1300 シリーズのチップを内蔵したシステム I/O コントローラ、デュアルポート 40 Gbps
- ツール不要なサーバ ノード、システム I/O コントローラ、使いやすいラッチ構造、ホットスワップおよびホットプラグ可能なコンポーネントで実現する高い信頼性、可用性、有用性（RAS）の機能



このシステムは、シャーシ管理コントローラ（CMC）を使用してサーバ ノードを管理します。各システム I/O コントローラ（SIOC）モジュールには、内蔵型 CMC が組み込まれています。

2 つの SIOC を使用する場合、2 つの CMC がアクティブ/スタンバイ構成で機能します。Cisco IMC インターフェイスでログインしている SIOC 内の CMC がアクティブ CMC になります。アクティブ CMC を使用して、両方のサーバ ノードの BMC を管理できます。

Cisco IMC インターフェイスを使用してサーバ ノードの BMC を管理するためにシステムに接続する場合、SIOC 上の管理ポート（RJ-45）に物理的に接続することになります。Cisco IMC インターフェイスにログインするときは、その SIOC 内の CMC に割り当てられている仮想的な管理 IP アドレスを使用します。

すべてのユーザ インターフェイスは、アクティブ CMC でのみ動作します。設定の変更は、アクティブ CMC とスタンバイ CMC の間で自動的に同期されます。

システムの電源を再投入すると、デフォルトで SIOC 1 内の CMC がアクティブ CMC になります。次のいずれかの条件が発生すると、アクティブ CMC はスタンバイ CMC にフェールオーバーします。

- アクティブ CMC のリブートまたは障害が発生した場合。
- アクティブ CMC を持つ SIOC が取り外された場合。
- アクティブ CMC でネットワーク接続が失われた場合。

S3260 ラック サーバの設定については、『Cisco UCS S3260Rack Server Specification Sheet』を参照してください。

Cisco IMC Supervisor と Cisco UCS S3260 高密度ストレージ ラック サーバ

Cisco IMC Supervisor により管理される高密度ストレージ ラック サーバでは、C シリーズ ラック サーバのすべての機能がサポートされます。また追加のレポートが用意されています。これらの機能と概念については、次に示すセクションで詳しく説明します。

- 概要：Cisco UCS S3260 のアーキテクチャと、Cisco IMC Supervisor により Cisco UCS S3260 が管理される際の接続について詳しく説明します。
- ラック アカウントの追加：Cisco UCS 3260 シャーシ ラック アカウントの追加について詳しく説明します。
- シャーシの管理：高密度ストレージ ラック シャーシの管理について詳しく説明します。
- ポリシーとプロファイル：Cisco UCS 3260 シャーシに関連するポリシーとプロファイルについて詳しく説明します。
- ファームウェアのアップグレード：シャーシファームウェア パッケージと、ファームウェアを手動で更新できる Cisco UCS S3260 のエンドポイントについて詳しく説明します。
- Cisco UCS S3260 ラック サーバの詳細の表示：PSU、VIC アダプタ、シャーシの概要、SAS エクスパンダなどの詳細情報を表示します。

ラック アカウントの追加

ラック アカウントを追加するために、[サーバ IP（Server IP）] フィールドに仮想的な管理 IP を指定できるようになりました。ラック アカウントの追加の詳細については、ラック アカウントの追加 （63 ページ）を参照してください。[ラック サーバ（Rack Servers）] タブからのインベントリ収集後に、Cisco UCS S3260 ラック サーバが管理するサーバを確認できます。

（注） CMC 1 または CMC 2 の IP アドレスを追加すると、エラーが発生します。

Cisco UCS S3260 ラック サーバの管理

シャーシ管理コントローラの再起動

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [ラック グループ（Rack Groups）] ページで、[シャーシ（Chassis）] をクリックします。

ステップ 3 [CMC の再起動（Reboot CMC）] をクリックします。

ステップ 4 [シャーシ管理コントローラの再起動（Reboot Chassis Management Controller）] ウィンドウで、[CMC1] または [CMC2] のいずれかを選択します。

ステップ 5 [送信（Submit）] をクリックします。
選択したシャーシが再起動します。

Cisco UCS S3260 ラック サーバのアセットのタグ付け

アセット タグは、サーバのユーザ定義タグです。[アセット タグ（Asset Tag）] オプションを使用し、Cisco IMC Supervisorで Cisco IMC サーバ プロパティを追加できます。

ラック サーバとシャーシの両方でアセットをタグ付けできます。ラック マウント サーバのアセットにタグを付けるには、ラック マウント サーバのアセットのタグ付け （86 ページ）を参照してください。シャーシのアセットにタグを付けるには、次の手順を実行します。

始める前に

サーバはすでに、ラック アカウントとしてラック グループに追加されています。

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [ラック グループ（Rack Groups）] ページで、[シャーシ（Chassis）] をクリックします。

（注） また、[インベントリと障害のステータス（Inventory and Fault Status）] ペインの [ラック グループ（Rack Groups）] でサブ グループを選択することもできます。

ステップ 3 シャーシのリストから、タグを付けるシャーシを選択します。

ステップ 4 [その他の操作（More Actions）] ドロップダウンリストから [アセット タグ（Asset Tag）] を選択します。

（注） リストからサーバを選択するまでは、[アセット タグ（Asset Tag）] オプションは表示されません。

ステップ 5 [送信（Submit）] をクリックします。

（注） [アセット タグ（Asset Tag）] オプションは、Cisco IMCリリース 3.0.(1c) 以降でのみ使用可能です。これよりも古いバージョンのプラットフォームでは、[ラック グループ（Rack Groups）] ページの [アセット タグ（Asset Tag）] カラムは空白になります。

Cisco UCS C3260 ラック サーバのフロント ロケータ LED の設定

サーバ ロケータ LED を使用すると、データセンター内の多数のサーバ間で特定のサーバを識別できます。選択したシャーシのフロント ロケータ LED をオンまたはオフにするには、次の手順を実行します。

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [ラック グループ（Rack Groups）] ページで、[シャーシ（Chassis）] をクリックします。

ステップ 3 [フロント ロケータ LED（Front Locator LED）] をクリックします。

ステップ 4 [選択したシャーシのフロント ロケータ LED の点灯/消灯（Turn the Front Locator LED for selected chassis on/off）] ドロップダウンリストから、[オン（ON）] または [オフ（OFF）] を選択します。

ステップ 5 [送信（Submit）] をクリックします。

Cisco UCS S3260 ラック サーバのタグの管理

タグは、オブジェクト（リソース グループ、Cisco UCS S3260 高密度ストレージ ラック サーバ、ラックマウントサーバなど）にラベルを割り当てる場合に使用されます。タグは、ラックの位置、担当サポート グループ、目的、またはオペレーティング システムなどの情報を提供するために使用できます。Cisco UCS S3260 高密度ストレージ ラック サーバまたはラックマウント サーバのタグの追加と変更については、ラック マウント サーバのタグの管理 （93 ページ）を参照してください。

（注） サーバのタグを管理できるのは、サーバがラック グループ内にラック アカウントとして含まれている場合だけです。

Cisco UCS S3260 ラック サーバのタグの追加

タグは、オブジェクト（リソース グループ、ラック サーバなど）にラベルを割り当てる場合に使用されます。タグは、ラックの位置、担当サポートグループ、目的、またはオペレーティング システムなどの情報を提供するために使用できます。Cisco UCS S3260 ラック サーバにタグを追加するには、次の手順を実行します。

始める前に

サーバはすでに、ラック アカウントとしてラック グループに追加されています。

（注） 複数のラック サーバを選択することもできます。

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [タグの追加（Add Tags）] をクリックします。

（注） リストからサーバを選択するまでは、[タグの追加（Add Tags）] ボタンは表示されません。

ステップ 3 ドロップダウンリストから [タグ名（Tag Name）] を選択します。

ステップ 4 ドロップダウンリストから [タグ値（Tag Value）] を選択します。

ステップ 5 プラス アイコンをクリックして新しいタグを作成します。タグの作成については、Cisco UCS S3260 ラック サーバのタグの管理 （198 ページ）を参照してください。

（注）　タグの詳細を編集、削除、および表示することもできます。

ポリシーとプロファイル

Cisco IMC Supervisor に追加された新しい **Cisco UCS S3260** オプションでは、Cisco UCS S3260 シャーシのポリシーとプロファイルを作成し、シャーシ情報を追加できます。

新しいシャーシ ポリシーはユーザ管理ポリシーと呼ばれ、既存のラックマウント サーバ ポリシーは本書ではコンピューティング ノード ポリシーと呼ばれます。区別されているユーザ管理ポリシーとコンピューティング ノードポリシーの一覧は、[ハードウェア ポリシー（Hardware Policies）] テーブルで確認できます。ユーザ管理ポリシーのサーバ プラットフォームは [Cisco UCS S3260] と表示され、コンピューティング ノード ポリシーのサーバ プラットフォームは [Cisco UCS S3260 を除くすべての C シリーズと E シリーズ（All C-Series and E-Series except Cisco UCS S3260）]と表示されます。

ポリシーおよびプロファイルのレポートには、ポリシーが Cisco UCS S3260 であるかどうかを示す [サーバ プラットフォーム（Server Platform）] カラムがあります。ユーザ管理ポリシーまたはコンピューティング ノード ポリシーに関係のないシャーシ ポリシーは [Cisco UCS S3260] と表示されます。その他の C シリーズおよび E シリーズのプラットフォーム、または Cisco UCS S3260 以外のポリシーは、[Cisco UCS S3260 を除くすべての C シリーズと E シリーズ（All C-Series and E-Series except Cisco UCS S3260）] と表示されます。

Cisco UCS S3260 シャーシ プロファイルまたはラックマウント サービス プロファイルのいずれかを作成できます。コンピューティング ノード ポリシーを選択すると、ポリシーを適用するサーバ ノードを選択できます。

ポリシーの適用

作成したポリシーを適用するには、Cisco UCS 3260 ラックサーバおよびラックマウント サーバのリストからサーバを選択します。選択したサーバ プラットフォームに基づいて、Cisco UCS S3260 シャーシまたはラックマウント サーバのいずれかを選択できます。ポリシーの作成と適用については、ハードウェアポリシー （104 ページ）を参照してください。

ユーザ管理ポリシーとコンピューティング ノード ポリシーを次に示します。

ユーザ管理ポリシー	コンピューティング ノード ポリシー
ユーザ	BIOS
SNMP	高精度のブート順序
LDAP	RAID
NTP	KVM
ネットワーク セキュリティ	vMedia
SSH	VIC

ユーザ管理ポリシー	コンピューティング ノード ポリシー
NTP	Serial over LAN

（注）
- IPMI Over LAN およびネットワーク ポリシーには、Cisco UCS 3260 ラックサーバの BMC と CMC の両方の設定詳細が含まれています。
- ゾーン分割ポリシーは、Cisco UCS 3260 ラックサーバにのみ適用されます。したがって UI の [Cisco UCS S3260] チェックボックスがオンになっています。
- レガシー ブート順序ポリシーと Flex Flash ポリシーは Cisco UCS S3260 ラック サーバでは使用できません。

プロファイルの適用

作成した Cisco UCS S3260 プロファイルを適用するには、Cisco UCS 3260 ラック サーバおよびラックマウント サーバを選択します。Cisco UCS S3260 シャーシだけを選択できます。プロファイルには Cisco UCS S3260 ポリシーだけを追加できます。コンピューティング ノード ポリシーの場合、ポリシーを適用する際に、[ポリシーの適用対象（Apply Policy To）] フィールドを選択し、ポリシーの適用対象サーバ ノードを選択できます。プロファイルの作成と適用については、ハードウェアプロファイル （144 ページ）を参照してください。

ファームウェアのアップグレード

Cisco IMC Supervisor ファームウェアのアップグレードはサーバ レベルで実行できます。ただし、サーバのアップグレード時に、そのサーバに関連付けられているシャーシ コンポーネントおよびハード ディスク ドライブ コンポーネントもアップグレードされます。サーバをアップグレードする場合、シャーシとディスク ドライブのファームウェアが自動的に更新されます。ファームウェアのアップグレードについては、ファームウェアのアップグレード（163ページ）を参照してください。

（注）一度に 1 つのサーバ ノードだけをアップグレードできます。

Cisco UCS S3260 高密度ストレージ ラック サーバの詳細の表示

Cisco UCS S3260 高密度ストレージ ラック サーバの詳細（PSU、VIC アダプタ、シャーシの概要、SAS エクスパンダなど）を表示するには、次の手順を実行します。

始める前に

サーバがラック アカウントとしてラック グループに追加されていることを確認します。

手順

ステップ 1 **[システム（Systems）] > [インベントリと障害のステータス（Inventory and Fault Status）]** を選択します。

ステップ 2 [ラック グループ（Rack Groups）] を展開し、Cisco UCS S3260 高密度ストレージ ラック サーバが含まれているラック グループを選択します。

ステップ 3 [ラック グループ（Rack Groups）] ページで、[シャーシ（Chassis）] をクリックします。

ステップ 4 リストで Cisco UCS S3260 高密度ストレージ ラック サーバをダブルクリックして詳細を表示するか、またはリストで Cisco UCS S3260 高密度ストレージ ラック サーバをクリックして [詳細の表示（View Details）] を選択します。

（注） リストで Cisco UCS S3260 高密度ストレージ ラック サーバを選択するまでは、[詳細の表示（View Details）] オプションは表示されません。

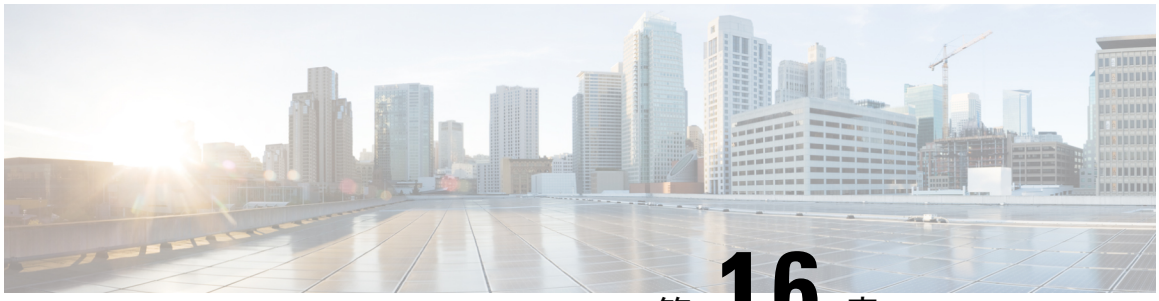
Cisco UCS S3260 高密度ストレージ ラック サーバに関する次の詳細が表示されます。

タブ	説明
PSUs	サーバで使用されている電源モジュールの詳細。 （注） Cisco UCS S3260 高密度ストレージ ラック サーバには適用されません。
VICアダプタ	サーバで使用されている VIC アダプタの詳細。 リストされている VIC アダプタのいずれかを選択して [詳細の表示（View Details）] をクリックすると、[外部イーサネット インターフェイス（External Ethernet Interfaces）] と [VM FEX（VM FEXs）] の情報が表示されます。
通信	HTTP、HTTPS、SSH、IPMI Over LAN、NTP、SNMP などのプロトコルに関する情報。
リモート プレゼンス	VKVM、Serial Over LAN、および vMedia の詳細。
障害	サーバで記録された障害の詳細。

タブ	説明
ユーザ数	**デフォルト グループ**のユーザに関する詳細。ユーザ ポリシーおよびパスワードの有効期限ポリシーの作成時に設定した強力なパスワード ポリシーとパスワード有効期限の詳細も確認できます。ユーザ ポリシー （134 ページ）およびパスワードの有効期限ポリシー （125 ページ）を参照してください。 （注） • Cisco UCS S3260 高密度ストレージ ラック サーバには適用されません。 • シャーシ レベルで**ユーザ**を表示できますが、サーバ レベルでは表示できません。
Cisco IMC ログ	サーバの Cisco IMC ログの詳細。 （注） Cisco UCS S3260 高密度ストレージ ラック サーバには適用されません。
システム イベント ログ	サーバ ログの詳細。 （注） Cisco UCS S3260 高密度ストレージ ラック サーバには適用されません。
障害履歴	サーバで発生した障害の履歴情報。
テクニカル サポート	ファイル名、宛先タイプ、アップロードのステータスなどのテクニカル サポート ログ ファイルに関する詳細は、[テクニカル サポート（Tech Support）] テーブルに表示されます。 リモート サーバまたはローカルの Cisco IMC Supervisorアプライアンスへテクニカル サポート ログ ファイルをエクスポートするオプションがあります。エクスポートの詳細については、リモート サーバへのテクニカル サポート データのエクスポート （97 ページ）を参照してください。 （注） Cisco UCS S3260 高密度ストレージ ラック サーバには適用されません。
関連付けられているハードウェア プロファイル	ハードウェア プロファイルに関連付けられているポリシーの詳細。
シャーシ要約	CMC 1 ネットワーク、共通、NIC などのプロパティの概要。
ラック サーバ	ホスト名、IP アドレス、接続ステータスなどのラック サーバの詳細。
システムIOコントローラ	IP アドレス、MAC アドレス、ファームウェア バージョンなどの詳細。

タブ	説明
SAS エクスパンダ	ID、SAS 名、ファームウェア バージョンなどの詳細。
ゾーン分割	ヘルス、プレゼンス、所有権、サイズなどの詳細。

ステップ 5 右端の [戻る（Back）] ボタンをクリックして前のウィンドウに戻ります。



第 16 章

サポート情報の表示

この章は次のトピックで構成されています。

サポート情報

Cisco IMC Supervisor は、基本的なシステム情報と、高度なシステム情報を提供し、ログの表示およびダウンロードをサポートします。また、デバッグ ロギングを記録し、API のログをダウンロードできます。

サポート情報の表示

Cisco IMC Supervisor のサポート情報を表示するには、次の手順を使用します。

始める前に

ポップアップ ブロッカーが Web ブラウザで無効になっていることを確認します。

手順

ステップ 1 **[管理（Administration）] > [サポート情報（Support Information）]** を選択します。

ステップ 2 [サポート情報（Support Information）] ウィンドウでは、次の情報を確認できます。

表 *2:* システム情報（基本）

フィールド	説明
[サポート情報（Support Information）] ドロップダウンリスト	基本情報を表示するには、[システム情報（基本）（System Information (Basic)）] を選択して [送信（Submit）] をクリックします。

サポート情報の表示

表 *3:* システム情報（詳細）

フィールド	説明
[サポート情報（Support Information）] ドロップダウンリスト	詳細情報（プロセッサ、メモリ、ディスク情報など）を表示するには、[システム情報（詳細）（System Information (Advanced)）] を選択し、[送信（Submit）] をクリックします。

表 *4 : View Logs*

フィールド	説明
[サポート情報（Support Information）] ドロップダウンリスト	[ログの表示（Show log）] を選択します。
[ログの表示（Show Log）] ドロップダウンリスト	表示するログタイプを選択して、[ログの表示（Show Logs）] をクリックします。

表 *5:* すべてのログをダウンロード

フィールド	説明
[サポート情報（Support Information）] ドロップダウンリスト	[すべてのログをダウンロード（Download All Logs）] を選択して [ダウンロード（Download）] をクリックします。

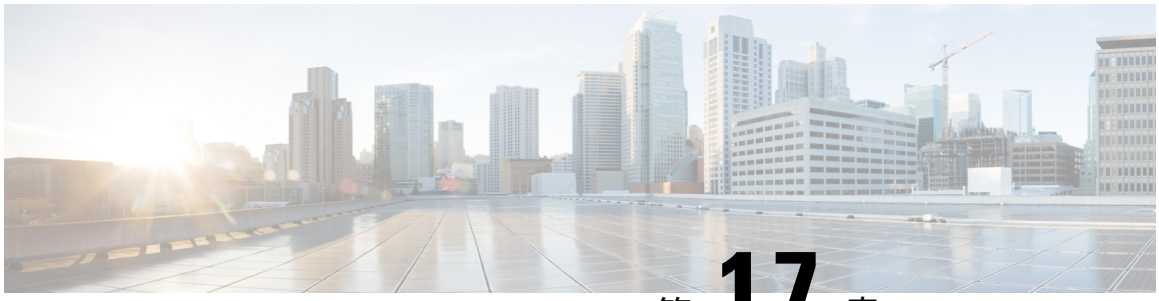
表 *6:* デバッグ ログのダウンロード

フィールド	説明
[サポート情報（Support Information）] ドロップダウンリスト	1. [デバッグ ロギング（Debug Logging）] を選択して [デバッグ ロギングの開始（Start Debug Logging）] をクリックします。 2. 停止してログデータをダウンロードするには、[デバッグ ロギングの停止（Stop Debug Logging）] をクリックして、デバッグのダウンロード リンクをクリックします。

表 *7*: *API* ロギング

フィールド	説明
[サポート情報（Support Information）] ドロップダウンリスト	**1.** [API ロギング（API Logging）] を選択して [API ロギングの開始（Start API Logging）] をクリックします。 **2.** 停止してログ データをダウンロードするには、[API ロギングの停止（Stop API Logging）] をクリックして、[API デバッグ ログのダウンロード（download API debug logs）] リンクをクリックします。

サポート情報の表示



第 17 章

頻繁に実行するタスクおよび手順

この章は次のトピックで構成されています。

頻繁に実行する手順

この項では、Cisco IMC Supervisorで頻繁に実行する手順をすばやく確認できます。参照先は、詳細な手順が説明されている本マニュアルの各項にリンクしています。

手順	参考資料
ログイン方法 Cisco IMC Supervisor	起動 Cisco IMC Supervisor （16 ページ）
ライセンスのアップグレード方法	ライセンスの更新 （17 ページ）
ログイン ユーザを追加する方法 Cisco IMC Supervisor	ユーザ アカウントの作成 （47 ページ）
ラック グループの追加方法	ラック グループの追加 （62 ページ）
ラック アカウントの作成方法	ラック アカウントの追加 （63 ページ）

その他の手順

以降のセクションでは、Cisco IMC Supervisorを使用して実行するさまざまな手順について説明します。

ダッシュボード ビューの有効化

Cisco IMC Supervisor メニュー バーでダッシュボード ビューを有効にするには、次の手順を実行します。

手順

ステップ 1 アプリケーションへのログインに使用したユーザ名をクリックします。ユーザ名は、アプリケーション ヘッダーの右端に表示されています。

ステップ 2 [ユーザ情報（User Information）] ウィンドウで [ダッシュ ボード（Dashboard）] をクリックします。

ステップ 3 [ダッシュボードの有効化（最上位メニュー）（Enable Dashboard（in the top level menu））] チェックボックスをオンにして、ダッシュボードを有効にします。

ステップ 4 [適用（Apply）] をクリックして、ウィンドウを閉じます。

（注） メニュー バーに [ダッシュ ボード（Dashboard）] タブが表示されます。

追加ダッシュボードの作成

始める前に

ユーザインターフェイスで[ダッシュボード（Dashboard）]を有効にしている必要があります。

手順

ステップ 1 Cisco IMC Supervisor ユーザ インターフェイスにログインします。

デフォルトの [ダッシュボード（Dashboard）] 画面が表示されます。

ステップ 2 [+] アイコンをクリックして新しいダッシュ ボードを作成します。

ステップ 3 ダッシュボードの名前を入力します。

ステップ 4 ダッシュボードのレポートを自動更新するには、[自動更新（Automatic Refresh）] を [オン（ON）] にします。

ステップ 5 [間隔（Interval）] を分単位で設定します。ダッシュボードのレポートは、ここで設定した間隔に基づいて更新されます。

ステップ 6 ダッシュボード ウィジェットの [ウィジェット サイズ（Widget Size）] を設定します。

ステップ 7 [送信（Submit）] をクリックします。

ダッシュボードの自動更新の有効化

ダッシュボードに追加したレポートの自動更新を有効にするには、次の手順を実行します。更新間隔も定義できます。

手順

ステップ 1 メニュー バーから [ダッシュボード（Dashboard）] を選択します。

ステップ 2 [ダッシュボード（Dashboard）] パネルで、[自動更新（Automatic Refresh）] オプションの横にある [オフ（OFF）] をクリックします。
[自動更新（Automatic Refresh）] オプションが [オン（ON）] に変わり、[間隔（Interval）] スライド バーが表示されます。

ステップ 3 [間隔（Interval）] を使用して、更新間隔を設定します。

（注） 更新間隔は 5 分単位で最大 60 分まで設定できます。

ダッシュボードへの要約レポートの追加

すぐにアクセスできるように要約レポートをダッシュボードに追加するには、次の手順を実行します。

（注） ダッシュボードには、要約レポートのみを追加できます。

手順

ステップ 1 ダッシュボードに追加する要約レポートを参照します。

ステップ 2 レポート パネルの右上隅にある下矢印をクリックします。

ステップ 3 [ダッシュボードに追加（Add to Dashboard）] をクリックします。

（注） 要約レポートがダッシュボード ビューに対応している場合にのみ、[ダッシュボードに追加（Add to Dashboard）] オプションが選択可能になります。

ステップ 4 メニュー バーから [ダッシュボード（Dashboard）] を選択し、レポートがダッシュボードに表示されることを確認します。

ダッシュボードの削除

デフォルト ダッシュボードは削除できません。

手順

ステップ 1 Cisco IMC Supervisor ユーザ インターフェイスにログインします。

デフォルトの [ダッシュボード（Dashboard）] 画面が表示されます。

ステップ 2 作成したダッシュ ボードのリストを表示するドロップダウンリストをクリックします。

ステップ 3 ダッシュ ボード名の横に表示される **X** マークをクリックします。

ステップ 4 ダッシュボードを削除することを確認します。

ダッシュ ボードが削除されたことを確認するメッセージが表示されます。

お気に入りへのメニューまたはタブの追加

[お気に入り（Favorites）] メニューにメニュー オプションまたはタブを追加するには、次の手順を実行します。

手順

ステップ 1 [お気に入り（Favorites）] メニューに追加するメニューまたはタブに移動します。

ステップ 2 [お気に入り（Favorites）] をクリックします。

（注） [お気に入り（Favorites）] ボタンは、これに対応しているメニューまたはタブのみに表示されます。

ステップ 3 [お気に入りレポート（Favorite Report）] ダイアログボックスで、[メニュー ラベル（Menu Label）] フィールドを編集できます。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 メニューバーで [お気に入り（Favorites）] を選択し、新しいメニューが表示されることを確認します。

お気に入り

Cisco IMC Supervisor では、表形式レポートを表示する画面をお気に入りとしてマークできます。メニューバーで [お気に入り（Favorites）] を選択すると、お気に入りとして指定した画面が一覧表示され、これらの画面にすばやくアクセスできます。

レポート テーブル ビューのカスタマイズ

レポート テーブルのフィールドを追加または削除するには、次の手順を実行します。

始める前に

テーブルのカスタマイズに対応しているウィンドウでは、ページの右端に [テーブル ビューのカスタマイズ（Customize Table View）] アイコンが表示されます。

手順

ステップ 1 ページの右端で [テーブル ビューのカスタマイズ（Customize Table View）] アイコンを見つけてクリックします。

ステップ 2 [レポート テーブルのカスタマイズ（Customize Report Table）] ダイアログボックスでは、次の操作が可能です。

- テーブル レポートのフィールドを表示するには、そのフィールドの横のチェックボックスをオンにします。
- テーブル レポートからフィールドを削除するには、そのフィールドの横のチェックボックスをオフにします。
- デフォルトのテーブル ビューにリセットするには、[デフォルトにリセット（Reset to Default）] をクリックします。

ステップ 3 [保存（Save）] をクリックします。

レポートのフィルタリング

ユーザ定義の条件に基づいてデータをフィルタリングするには、次の手順を実行します。

始める前に

データのフィルタリングに対応しているウィンドウでは、ページの右端に [高度な検索フィルタを追加（Add Advanced Filter）] アイコンが表示されます。

手順

ステップ 1 ページの右端で [高度な検索フィルタを追加（Add Advanced Filter）] アイコンを見つけてクリックします。
アイコンをクリックするたびに、レポート テーブルの上部にフィルタ条件が追加されます。

ステップ 2 [一致条件（Match Condition）] ドロップダウンリストで、必要に応じて [すべての条件に一致（Match All Conditions）] または [いずれかの条件に一致（Match Any Condition）] を選択します。

ステップ 3 [列内を検索（Search in Column）] ドロップダウンリストで、データをフィルタリングするためのフィールドを選択します。

ステップ 4 [テキスト（Text）] フィールドに、データをフィルタリングするための値を入力します。

ステップ 5 複数のフィルタ条件がある場合は、すべての条件に対してステップ 3 とステップ 4 を繰り返します。

ステップ 6 [検索] をクリックします。

レポートのエクスポート

PDF、CSV、XLS 形式でレポート データをエクスポートするには、次の手順を実行します。

始める前に

レポート データのエクスポートに対応しているウィンドウでは、ページの右端に [レポートのエクスポート（Export Report）] アイコンが表示されます。

手順

ステップ 1 ページの右端で [レポートのエクスポート（Export Report）] アイコンを見つけてクリックします。

ステップ 2 [レポートのエクスポート（Export Report）] ダイアログボックスで、次の手順を実行します。

1. [レポート形式の選択（Select Report Format）] ドロップダウンリストから、[PDF]、[CSV]、または [XLS] を選択します。
2. [レポート作成（Generate Report）] をクリックします。
3. レポートが生成されたら、[ダウンロード（Download）] をクリックします。

選択した形式のレポートが新しいウィンドウに生成されます。

ステップ 3 [レポートのエクスポート] ダイアログボックスで **[閉じる]** をクリックします。

システム情報の表示

[システム情報（System Information）] 画面には次の情報が表示されます。

- プライマリ ノード
- サービス ノード
- DB ノード
- システム メモリ
- システム ディスク

この画面では、画面に表示されているデータを更新するか、画面に表示されるレポートの数を編集できます。

サイト マップ

[サイト マップ（Site Map）] オプションを使用すると、Cisco IMC Supervisor ユーザ インターフェイスで使用可能な主要なオプションをすべて確認できます。この画面から、オプションを

選択して、関連画面に直接移動できます。たとえば、サイドペインで**[システム（Systems）]**>**[ファームウェア管理（Firmware Management）]** を選択する代わりに、[サイト マップ（Site Map）] 画面の [システム（Systems）] で [ファームウェア管理（Firmware Management）] を選択できます。