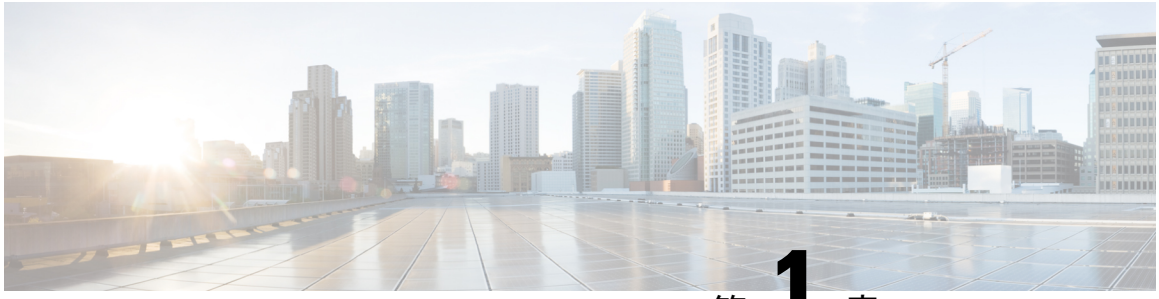
Cisco IMC Supervisor ラックマウントサーバ リリース 2.3 管理ガイド

初版：2021 年 3 月 17 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。

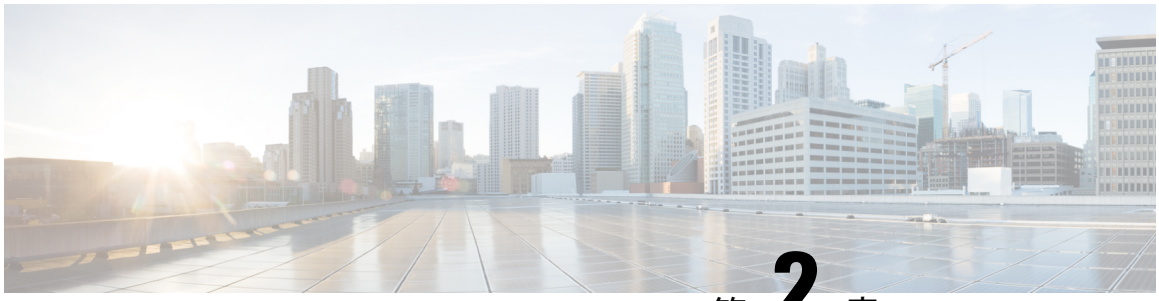
このリリースの新規情報および変更情報

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 *2.3* の新機能と変更された動作

機能	説明	参照先
LDAP 統合	セキュリティ PSB の一般的なバージョンは TLS：1.2 以降です。	LDAP 統合の規則と制限事項
高精度のブート順序ポリシーの機能拡張	高精度ブート順序ポリシーには、HTTP ブート デバイス タイプのサポートが含まれています。	高精度のブート順序ポリシー （121 ページ）
RAID ポリシーの機能拡張	RAID ポリシーには、仮想ドライブ ストリップ サイズを指定するオプションが含まれています。	RAID ポリシー （123 ページ）
SNMP ポリシー	暗号化方式 DES を使用する SNMP ユーザーは、CIMC バージョン 4.1（3b）および Cisco IMC Supervisor バージョン 2.3 ではサポートされません。	SNMP ポリシー （127 ページ）

このリリースの新規情報および変更情報



第 2 章

概要

この章は、次の内容で構成されています。

About Cisco IMC Supervisor

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 を使用して次のタスクを実行できます。

- サーバの論理的なグループ化とグループごとのサマリーの表示
- 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の管理
- 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
- ネットワーク構成ポリシーよる 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
- さまざまな地理的場所にまたが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 基本ライセンスのあと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 アドバンスド版ライセンス。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、エンドユーザーが 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。50 個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の場合も行われますが、新しいサーバの追加は行えません。たとえば、評価時に約 100 台のサーバを追加し、購入しているのが 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、高度な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。

いずれのライセンスも、入手してインストールするため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 サイトで製品アクセス 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 ソフトウェア ライセンスの Web サイトに移動します。

ステップ 2 [Product License Registration] ページに転送されたら、トレーニングを受けるか、[Continue to Product License Registration] をクリックして続行してください。

ステップ 3 [Product License Registration] ページで、[Get New Licenses from a PAK or Token] をクリックします。

ステップ 4 [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 [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、[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	組織名。
Site Contact Name	サイトの連絡先の名前。
Street Address	組織の番地。
City/Town	市区町村名。
[State/Province]	都道府県名。
[Zip/Postal Code]	郵便番号。
国	国名。

ステップ 7 [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 ファイルが電子メールに添付されて、ユーザ指定の電子メール アドレスに送信されます。

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 **[Default Group (デフォルト グループ)]** 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 アカウントを追加したり、新しいラック グループを作成し、そのグループにラック アカウントを追加したりできます。ただし、このデフォルトのラック 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、デフォルト グループまたは作成したグループへのラック 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、複数のサーバにわたって設定の一貫性と反復可能性を確保するうえで役立ちます。包括的なポリシーセットを定義して使用すると、多数のサーバに類似する設定を適用できるので、一貫性、制御、予測可能性、自動化が促進されます。

プロファイル

複数のポリシーを組み合わせて、ハードウェア プロファイルが形成されます。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。これにより、複数のサーバにわたって設定の一貫性と反復可能性が確保されます。プロファイルを定義して使用すると、類似する設定が多数のサーバに適用されるため、一貫性、制御、予測可能性、自動化が促進されます。

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、ユーザー 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

以前のリリースでは、メインメニューバーを使用して画面にアクセスできました。このリリース以降、すべてのナビゲーション オプションは、水平メイン メニュー バーではなく、サイドバーから使用できるようになりました。そのため、ユーザインターフェイスにメインメニューバーは表示されなくなりました。マウスを使用してカーソルをサイド ナビゲーション バーのオプションの上に合わせ、メニュー オプションのいずれかをクリックします。

ユーザ インターフェイスのラベルの廃止

ユーザ インターフェイスに、[追加（Add）]、[編集（Edit）]、[削除（Delete）]、[エクスポート（Export）]、[フィルタ（Filter）]などのアクションのラベルが表示されなくなりました。これらのアクションはアイコンのみで表示されます。マウスを使用してカーソルをアイコンの上に合わせると、そのアイコンを使用して実行できるアクションがラベルに表示されます。

ダッシュボードを使用した詳細レポートへのアクセス

ダッシュボードが有効になっている場合は、これが Cisco IMC Supervisor にログインしたときに最初に表示される画面になります。通常はこのダッシュボードを使用して重要なレポートや頻繁にアクセスするレポートのウィジェットを追加します。**ダッシュボード**に表示されたレポートをクリックすると、より詳細な情報が表示されるユーザインターフェイスの画面にすぐにアクセスできるようになりました。「ダッシュボード ビューの有効化 （203 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 （204 ページ）およびダッシュボードの削除 （205 ページ）を参照してください。

表形式レポートの機能強化

次に、ユーザインターフェイスで使用できる表形式レポートで強化された機能のいくつかを示します。

- 右クリックによる他のオプションの表示

  行を選択した後でマウスを右クリックすると、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）] オプションが使用できます。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、表形式レポートの結果を特定の基準で絞り込むことができます。この [フィルタ（Filter）] オプションは複数のページにまたがっていない表形式レポートで使用できます。複数の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を絞り込みます。

- [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た表形式レポートをお気に入りとして追加できます。お気に入りとしてレポートを追加すると、[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。

- 列のサイズ変更

  表形式レポートに表示された列は、最後の列を含めて、すべてサイズを変更できます。列を展開した後、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。

- データがない場合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は、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

使用できる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。画面上でタブを閉じると、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表示されなくなります。そのタブを画面に戻すには、画面の右端に表示されている下向きの矢印をクリックします。使用可能ではあるものの非表示になっているタブのドロップダウン リストが表示されます。復元するタブを選択します。

（注） 2 個以上のタブが画面にあるときにのみ、タブを削除または復元できます。この機能は、インターフェイスの画面に表示されるタブが 1 個のみの場合は使用できません。

レポート機能の強化

次に、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を示します。

- 円グラフと棒グラフの導入

  円グラフまたは棒グラフを個々にPDF、CSV、またはXLSの形式でエクスポートしたり、**ダッシュボード** に追加できます。

- [他のレポート（More Reports）] オプションの可用性

  [More Reports (その他のレポート)] オプションを使用して、障害、サーバの状態、ファームウェア バージョン、サーバ モデル、電源状態、サーバ接続状態のレポートを生成できます。

ランディング ページ（Landing Page）

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、どのように表示を設定しているか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すると統合ビューが表示されます。

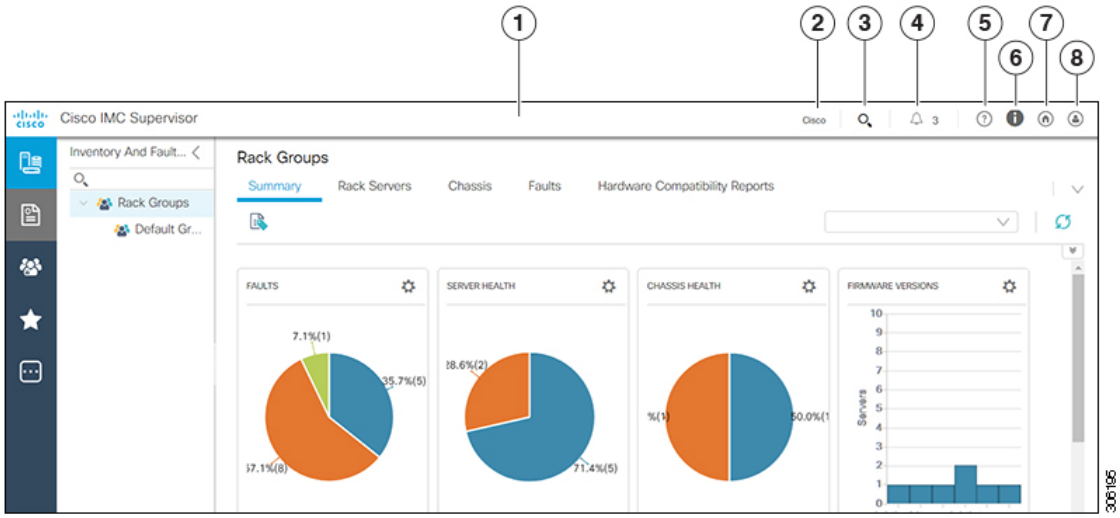
次に、ランディング ページで利用可能な要素を示します。

- 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 ナビゲーション バーが画面の上部に表示されなくなりました。画面左側の垂直メニューとして利用できるようになっています。

（注） このメニューにスクロールバーはありません。使用可能なスペースに収まる数のオプションのみが表示されます。一部のオプションは、画面を最小化したり、または拡大すると表示されないことがあります。使用可能なオプションをすべて表示するには、[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	Header	メニューなどの頻繁にアクセスする要素が含まれています。ヘッダーは常に表示されています。
2	Link	ソフトウェアの仕様に関する情報にアクセスできるシスコの Web サイトへのリンクが提供されています。
3	[Search] アイコン	ポータルで特定のレポートを検索して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	ログに記録されている診断システム メッセージの数を表示します。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）] 画面が表示されます。

番号	名前	説明
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 システムにリンクしています。
6	[バージョン情報（About）] アイコン	ソフトウェアについての情報と、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 ページに戻ります。
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または無効化、ユーザインターフェイスのクラシック ビューへのアクセス、およびログアウトができます。

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（Refresh）]**	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）**	[Favorites] 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。
	**Add**	[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。
	**Edit**	[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。
	**Customize Table**	[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。

アイコン	ラベル	説明
	**エクスポート レポート**	[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
	**Expand**	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。
	**Collapse**	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。
	**Add Advanced Filter**	ページに追加のフィルタリング パラメータを提供します。
	**Search Field**	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受け入れます。

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、ファイル内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接続の設定

デフォルトでは、Cisco IMC Supervisor ユーザー 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、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には、次の手順を実行する必要があります。

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 ファイルを次のように変更します。

a) 既存の 8080 ポート コネクタの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 8080 ポート コネクタのタグとして次を追加します。

```
<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 ファイルに <security-constraint> タグをコメントします。

```
<!--
<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>
-->
```

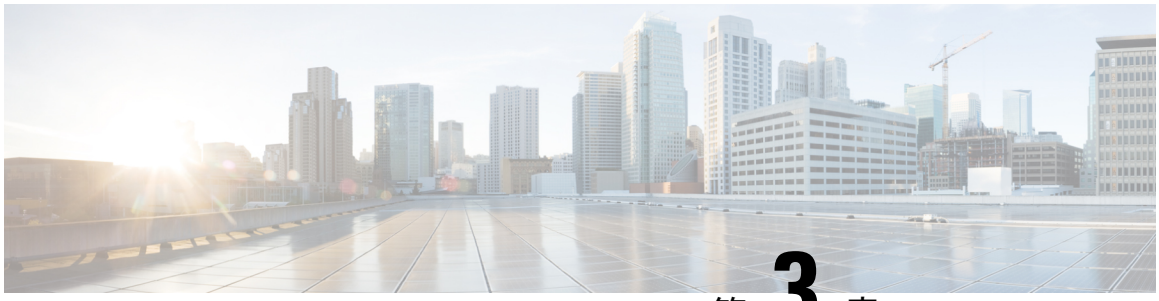
ステップ 4 サービスを再起動します。

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。

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 モードと非セキュア モードの両方でユーザ インターフェイスを起動できます。



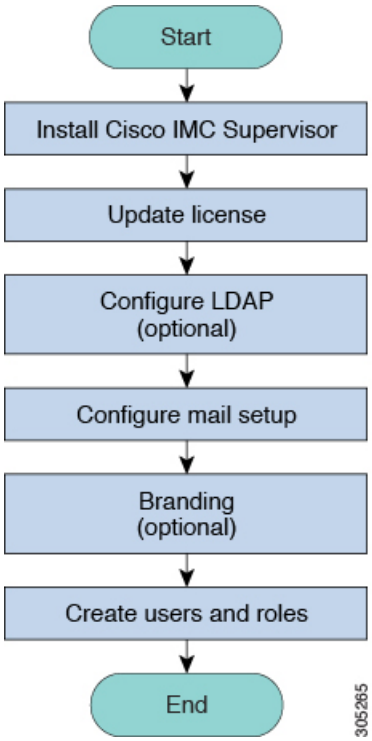
第 3 章

使用する前に

この章は、次の内容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。



Cisco IMC Supervisor の起動

Cisco IMC Supervisorは正常に正しく設定されたIPアドレスで、インストールする必要があります。

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。

- [User Name]：**admin**
- [Password]：**admin**

ログイン後、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 ビューを表示します。

ライセンス タスク

[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率を確認できます。次のライセンス手順は、**[Administration]** > **[License]** メニューから使用できます。

タブ	説明
ライセンス キー	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。このタブを使用してライセンスを交換および移行することもできます。新しいバージョンの Cisco IMC Supervisor が使用可能な場合は、ライセンスを更新できます。
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。
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。
Deactivated Licenses	このタブには、非アクティブ化されたライセンスの一覧が表示されます。

ライセンスの更新

Cisco IMC Supervisor の使用を始める前にライセンスを更新するには、次の手順を実行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 キーを要求し、登録する必要があります。Cisco IMC Supervisor をインストール後、ライセンスが検証され、Cisco IMC Supervisor の使用を開始できます。

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 **[Administration]** > **[License]** の順に選択します。

ステップ 2 [License] ページで、[License Keys] を選択します。

ステップ 3 [License Keys] ページで、[Update License] をクリックします。

ステップ 4 [Update License] 画面で、次のいずれかを実行します。

- **.lic** ファイルをアップロードするには、[Browse] をクリックして **.lic** ファイルを探して選択し、[Upload] をクリックします。
- ライセンス キーの場合は、[Enter License Text] 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 [License Text] 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 [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。

ライセンスの交換

この手順を使用すると、システム内のライセンスを交換することができます。このアクションによって、システム上のその他すべて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 **[Administration]** > **[License]** の順に選択します。

ステップ 2 [License] ページで、[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 **[Upload License (ライセンスのアップロード)]** 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 **[Select a File (ファイルを選択)]** 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 [Submit] をクリックします。`

すべての既存のライセンスが新しいライセンスに交換されます。

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
- ライセンス価格
- Expiry Date
- 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 **[Administration]** > **[License]** の順に選択します。
ステップ 2 [License] ページで、[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 ユーザー 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 **[Administration]** > **[License]** の順に選択します。
ステップ 2 [License] ページで、[License Keys] を選択します。
ステップ 3 **[License Keys (ライセンス キー)]**ページで **[Migrate License (ライセンスの移行)]** をクリックします。
ステップ 4 **[Upload License (ライセンスのアップロード)]** 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 **[Select a File (ファイルを選択)]** 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

ライセンス監査を実行するには、次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 **[Administration]** > **[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） [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 **[Administration]** > **[Users and Groups]** の順に選択します。

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

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

ステップ 6 **[Add Entry to Access Profiles (アクセス プロファイルへのエントリの追加)]**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
[Name] フィールド	プロファイル名。
[Description] フィールド	プロファイルの説明です。
[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。
[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。
[Show Resources From All Other Groups the User Has Access] チェックボックス	ユーザがアクセスできるか、属する他のグループすべてのリソースを表示できるようにするには、このチェックボックスをオンにします。
[Shared Groups] フィールド	[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。
[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 [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

システムのユーザとして、ユーザアカウントに対して複数のプロファイルがある場合、特定のプロファイルを使用してシステムにログインできます。

手順

ステップ 1 **[Cisco IMC Supervisor login (Cisco IMC Supervisor ログイン)]** ページの **[Username (ユーザー名)]** 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 [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。

Default Profile

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、右上隅に表示されているユーザ名をクリックします。

ユーザ名は [logout] オプションの左側に表示されます。

ステップ 2 **[User Information (ユーザー情報)]** ページで、**[Access Profiles (アクセス プロファイル)]** 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、[Set as Default Profile] をクリックします。

（注） プロファイルは、追加または編集されている間、デフォルトとしても設定できます。

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（VID）認証を設定できます。

名前	説明
[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 **[Administration]** > **[Users and Groups]** の順に選択します。

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

ステップ3 [Authentication Preferences] ドロップダウン リストから、次のオプションのいずれかを選択できます。

- **[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 （28 ページ）を参照してください。

- [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 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、[Browse] をクリックします。
証明書を見つけて選択し、[Upload] をクリックします。

b) [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。次の項では、これらの手順の実行方法について説明します。

LDAP 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。

手動または自動で新しい組織単位（OU）が LDAP ディレクトリに追加され、同期プロセスが実行されると、直近に追加された 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。

[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、[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

（注） セキュリティ PSB の推奨バージョンは TLS：1.2 以上です。

既存の機能をアップグレードおよび中断しない場合は、service.properties を手動で更新し、古いバージョンに設定する必要があります。service.properties ファイルのパスは **/resources/properties/service.properties** です。サポートされているバージョン Cisco IMC Supervisor リリース 2.3 の **ldap.ssl.socket.protocols** の TLSv1.2 および TLSv1.3 です。

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 [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 [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。
- ユーザは複数のユーザ グループに属することができます。ただし、ユーザが属しているグループ リストで最初に表示されているグループは、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 [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、指定された LDAP グループが取得されてシステムに追加されると共に、ネストされたグループがあれば併せて追加されます。

- 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、[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、指定したフィルタに一致するすべてのユーザと、それらのユーザが属するグループが取得され、システムに追加されます。
- 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。プロファイル名とともにユーザ プリンシパル名を使用しての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 [Local] 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 ディレクトリに作成されると、最初に同期された LDAP ディレクトリのユーザの詳細が表示されます。もう一方の LDAP ディレクトリからのユーザの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 外部ユーザーは、完全なドメイン名をユーザー名と共に指定して 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 など。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 同期プロセスの後に、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 に同期させると、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 に同期します。

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 **[Administration]** > **[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 **[Add LDAP Configurations (LDAP 設定の追加)]** 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。
[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。
[Server] フィールド	サーバのホスト名または IP アドレス。
[Enable SSL] チェックボックス	LDAP サーバへのセキュアな接続をイネーブルにします。
[Port] フィールド	ポート番号 SSL の場合は 636 に、非セキュア モードの場合は389 に自動的に設定されます。
[Domain Name] フィールド	LDAP ユーザのドメイン名。
[Username] フィールド	LDAP ユーザの名前を入力します。
[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。
[Synchronization Freqency] 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

フィールド	説明
	• 4 • 12 • 24

ステップ 4 [Next] をクリックします。

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

（注） Cisco IMC Supervisor ユーザー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です）。システム同期更新タスクが 24 時間ごとに実行され、検索基準に基づいて LDAP ユーザが同期更新されます。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 （33 ページ）を参照してください。

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

選択済みの検索条件が、[Search Base] フィールドの横に表示されます。

ステップ 7 [LDAP Search Base] ダイアログボックスで [Next] をクリックします。

ステップ 8 [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するには、[+] をクリックします。

ステップ 9 [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。

これらのフィルタを編集または削除することができます。また、上/下矢印を使ってフィルタを移動すると、優先順位を設定できます。

ステップ 11 [LDAP User Role Filter] ダイアログボックスで、[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。
- 結果の数を制限し、グループおよびユーザに対する 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 [Local First, fallback to LDAP] に設定しておく必要があります。

手順

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

ステップ 2 [Add] をクリックします。

ステップ 3 **[LDAP Server Configuration (LDAP サーバ設定)]** 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。
[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
[Server] フィールド	LDAP サーバの IP アドレスまたはホスト名。
[Enable SSL] チェックボックス	LDAP サーバへのセキュアな接続をイネーブルにします。
[Port] フィールド	ポート番号 SSL の場合は 636 に、非セキュア モードの場合は389 に自動的に設定されます。
[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。

名前	説明
[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てください。 **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。
[Password] フィールド	ユーザのパスワード。
[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 [Next] をクリックします。

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

ステップ 7 [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
[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。
[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ユーザがすべて取得されて、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。

名前	説明
[Add Entry to User Filters] または [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）	
[Attribute Name] ドロップダウン リスト	[Group Name] または [User Name] を選択します。
[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。 • **次に等しい** • **開始（Starts with）**
[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 [Next] をクリックします。

ステップ 9 [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 [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
[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。
[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。 • **等しい** • **開始（Starts with）**
[Attribute Value] フィールド	このフィールドで値を指定します [Operator] フィールドと [Attribute Value] フィールドの値に一致するすべてのユーザが、[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。

名前	説明
[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。デフォルトで使用可能だったロールを選択するか、またはシステムで作成された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 • オペレーター • システム管理者

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 [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、最初の行に指定したフィルタが処理されます。

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 に認証設定を設定していない場合は、認証設定を変更するように求めるプロンプトが表示されます。「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 サーバの概要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 **[Administration]** > **[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 [View] をクリックします。

[View LDAP Account Information] 画面には、LDAP アカウントの概要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 **[Administration]** > **[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 [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 [Test LDAP Connectivity] ダイアログボックスで、[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 **[Administration]** > **[LDAP Integration]** を選択します。

ステップ 2 [Search BaseDN] をクリックします。

（注） Cisco IMC Supervisor ユーザー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です）。

ステップ 3 [LDAP Search Base] ダイアログボックスの [Select] をクリックします。

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

ステップ 5 [LDAP Search Base] ダイアログボックスの [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 **[Administration]** > **[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 **[Manual LDAP Sync (手動 LDAP 同期)]** ページで、次のフィールドに入力します。

名前	説明
[Basic Search] チェックボックス	組織単位で基本検索をイネーブルにします。
[Advanced Search] チェックボックス	詳細検索をイネーブルにします。

（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、[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、[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、[Advanced Filtering Options] ペインで、[User Filters] と [Group Filters] の属性名を追加または編集します。

ステップ 7 [Next] をクリックします。

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

名前	説明
[LDAP Groups] フィールド	ユーザが同期する必要がある LDAP グループ。
[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。

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

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 **[Administration]** > **[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 [User and Group Tasks] を展開し、[LDAPSyncTask] を選択します。
ステップ 4 **[Run Now (今すぐ実行)]** をクリックします。
ステップ 5 **[Submit (送信)]** をクリックします。
ステップ 6 （任意）[Manage Task] をクリックして、同期プロセス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 Integration] ページで、LDAP アカウントを選択し、[Results] をクリックして同期プロセスの概要を表示します。

LDAP サーバの詳細の変更

設定済みの LDAP サーバに対し変更できるのは次の詳細情報のみです。

- ポート番号と SSL 設定
- ユーザ名とパスワード
- 同期頻度
- 検索ベース DN の選択内容
- 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 **[Administration]** > **[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 **[Modify]** をクリックします。
ステップ 4 **[LDAP Server Configuration (LDAP サーバ設定)]** ページで、次のフィールドを編集します。

名前	説明
[Enable SSL] チェックボックス	LDAP サーバへのセキュアな接続をイネーブルにします。
[Port] フィールド	ポート番号 SSL の場合は 636 に、非セキュア モードの場合は389 に自動的に設定されます。

名前	説明
[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てください。 **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。
[Password] フィールド	ユーザのパスワード。
[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 [Next] をクリックします。

ステップ 6 [LDAP Search Base] エントリを編集し、[Next] をクリックします。

ステップ 7 [User Filters] および [Group Filters] テーブルで必要な属性を選択して編集し、[Next] をクリックします。

ステップ 8 [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、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 [Domain Users] として設定されます。**[Manage Profiles (プロファイルの管理)]** オプションを使用して、ユーザーのグループ 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 では特定のユーザー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 **[Administration]** > **[Users and Groups]** の順に選択します。

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 [Group Membership] をクリックします。

[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 **[Administration]** > **[Users and Groups]** の順に選択します。

ステップ 2 **[LDAP Integration (LDAP 統合)]** 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 [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 [Delete] をクリックします。

これにより、Cisco IMC Supervisor 内の 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数によって、この削除プロセスが完了するまでに数分かかる場合があります。この間、LDAP アカウントが Cisco IMC Supervisor に表示され続ける場合があります。[Refresh] をクリックして、アカウントが削除されたことを確認します。

SFTP ユーザー パスワードの設定

SFTP ユーザーは、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、SFTP 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。SFTP ユーザー 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。

SFTP ユーザー 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 **[Administration]** > **[Users and Groups]** の順に選択します。
ステップ 2 **[SFTP ユーザー設定（SFTP 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。

[Mail Setup] 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 （74 ページ） を参照してください。

手順

ステップ 1 **[Administration]** > **[System]** を選択します。
ステップ 2 **[Mail Setup (電子メール設定)]** をクリックします。
ステップ 3 **[Mail Setup (電子メール設定)]** ページで、次のフィールドに入力します。

フィールド	説明
[Outgoing Email Server (SMTP)]	サーバの IP アドレスまたはドメイン名。
[Outgoing SMTP Port]	SMTP サーバのポート番号。
[Outgoing SMTP User]	（オプション）SMTP 認証で使用する送信 SMTP ユーザ ID。
[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。
[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。
[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 のユーザ クレデンシャルの設定とプロキシ設定

Cisco ユーザー クレデンシャルおよびプロキシの詳細はは、**[Administration (管理)]** > **[System (システム)]** から設定できます。Cisco.com のユーザ クレデンシャルとプロキシ クレデンシャルは、アプリケーション全体の設定です。これらのクレデンシャルは、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 のユーザ名とパスワードを設定する場合は、次の手順を実行します。

手順

ステップ 1 **[Administration]** > **[System]** を選択します。

ステップ 2 [System] ページで、[Cisco.com User Configuration] をクリックします。

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

フィールド	説明
[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。
[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 **[Administration]** > **[System]** を選択します。

ステップ 2 [System] ページで、[Proxy Configuration] をクリックします。

ステップ 3 次の項目を入力してプロキシを設定します。

フィールド	説明
[Enable Proxy Configuration] チェックボックス	（任意）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。 • [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。 • [Port] フィールド：プロキシ設定用のポートを入力します。
[プロキシ認証の有効化（Enable Proxy Authentication）] チェックボックス	（任意）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化し、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。 • [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 **[Administration]** > **[Integration]** の順に選択します。

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

ステップ 3 [CMDB 統合設定（CMDB Integration Setup）] 画面で、次を含む必須フィールドに値を入力します

名前	説明
[FTP サーバにエクスポート（Export to FTP Server）] 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。

名前	説明
[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（FTP Password）] フィールド	FTP ユーザ パスワード。
[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（Test FTP）] 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。

ブランド表示

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 **[Administration]** > **[Users and Groups]** の順に選択します。

ステップ 2 **[Login Page Branding (ログイン ページ ブランディング)]** をクリックします。

ステップ 3 [Add] をクリックします。

ステップ 4 **[Domain Branding (ドメイン ブランディング)]** ページで、次のフィールドに入力します。

フィールド	説明
[Domain Name] フィールド	ブランディング用のドメイン名。たとえば、imcs.xxxx.com のようになります。 （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 のようになります。
[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.** [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.** [Open] をクリックします。

ステップ 5 [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。

[User Interface Settings] 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。

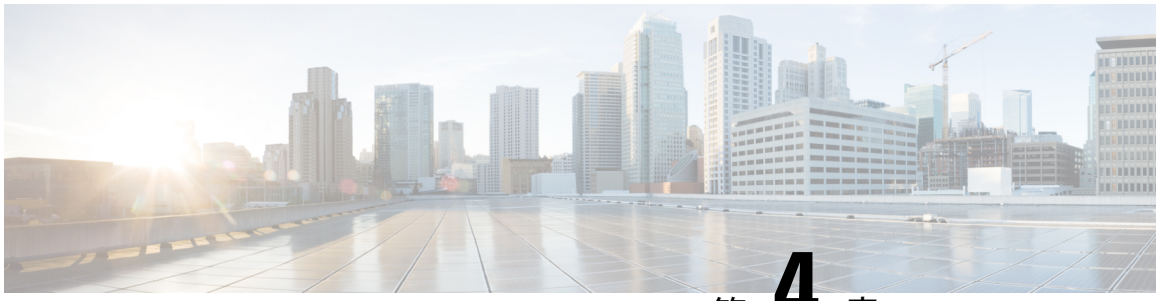
手順

ステップ 1 **[Administration]** > **[User Interface Settings]** を選択します。

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

フィールド	説明
[Hide Entire Header] チェックボックス	このチェックボックスを使用して、ヘッダーを有効または無効にします。
[Product Name] フィールド	ヘッダーのメイン タイトル。
[Product Name 2nd Line] フィールド	ヘッダーのサブタイトル。
[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 [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	
[Custom Link 1 Lable] 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。
[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。
[Custom Link 2 Lable] 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。
[Custom Link 2 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	
[Custom Link 1 Lable] 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。
[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。
[Custom Link 2 Lable] 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。
[Custom Link 2 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、次の内容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ー ロールをデフォルトでサポートしています。

- [System Admin]：ユーザの追加を含む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ー ロールまたはカスタム定義のユーザー ロールをユーザに割り当てることができます。後で、割り当て済みのロールの情報を確認することもできます。次の割り当てを行うことができます。
  - システムのカスタム 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、既存のユーザにロールを割り当てます。

    新しいユーザ ロールの作成時に、そのロールを管理者またはオペレータのロール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 ロールの作成の詳細については、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の変更手順は、ユーザ ロールの作成時の手順と同じです。

- [Group Admin]：すべての権限を持つユーザ。システム定義のユーザー グループ **[Default Group (デフォルト グループ)]** 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。ユーザは複数のユーザ 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、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。
- [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Operatorに割り当てられます。

メニュー設定	ユーザ権限
システム： • インベントリと障害のステータス • 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 • 書き込み：物理コンピューティング • 読み取り：システム管理者 • 読み取り：ユーザ • 読み取り：タグ ライブラリの読み取り • 書き込み：タグ ライブラリの書き込み • 読み取り：オーケストレーション • 書き込み：オーケストレーション
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： • ユーザとグループ • 統合	

（注） [SCP User Configuration]、[Authentication Preferences]、および [Password Policy] などのレポートは、[Users and Groups] の下で Operator ロールに対して有効になります。

ユーザ アカウントの作成

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

手順

ステップ 1 **[Administration]** > **[Users and Groups]** の順に選択します。

ステップ 2 [Users] をクリックします。

ステップ 3 [Add] をクリックします。

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

フィールド	説明
[User Role] ドロップダウン リスト	[Group Admin]、[Operator]、または [System Admin] を選択します。
[User Group] ドロップダウン リスト	ユーザがアクセスできるようにするグループを選択します。すでに使用可能なグループを選択することも、新しいグループを追加することもできます。 （注） このフィールドは、ユーザ ロールとして [Group Admin] を選択している場合にのみ表示されます。
[Login Name] フィールド	ユーザのログイン名。
[Password] フィールド	ユーザのパスワード。ユーザに対して Lightweight Directory Access Protocol（LDAP）認証が設定されている場合、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。
[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。
[User Contact Email（ユーザの連絡先電子メール）] フィールド	電子メール アドレス。
[First Name] フィールド	（オプション）ユーザの名。
[Last Name] フィールド	（オプション）ユーザの姓。
[Phone] フィールド	（オプション）ユーザの電話番号。

フィールド	説明
[Address] フィールド	（オプション）ユーザの物理アドレス。

ステップ 5 [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 **[Administration]** > **[Users and Groups]** の順に選択します。

ステップ 2 **[Current Online Users (現在のオンライン ユーザー)]** 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、すべてのユーザーの最近のログイン履歴を確認できます。システムは、すべてのログイン試行に関する次の情報を記録します。

- Login Name
- Remote Address
- クライアントの詳細
- クライアント タイプ
- Authentication Status
- 注
- アクセス日

手順

ステップ 1 **[Administration]** > **[Users and Groups]** の順に選択します。

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

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

手順

ステップ 1 **[Administration]** > **[Users and Groups]** の順に選択します。

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値を入力します

名前	説明
[ユーザあたりのセッションの最大数（Maximum 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 の範囲内の数を入力してください。 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 [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 **[GroupAdmin (グループ管理者)]** と **[Operator (オペレータ)]** 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 **Operator** ロールを必要に応じて変更できます。同様に、次の手順のように新しいロールを作成し、それらのロールにユーザを割り当てることもできます。

手順

ステップ 1 **[Administration]** > **[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 [Add] をクリックします。

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

フィールド	説明
[User Role] フィールド	ユーザ ロールの記述名。
[Role Type] ドロップダウン リスト	[Admin] を選択します。
[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 [Next] をクリックします。

ステップ 6 [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横のチェックボックスをオンにします。

ステップ 7 [Next] をクリックします。

ステップ 8 [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、操作の横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 ロールを編集、複製、削除することもできます。

ユーザ グループのブランディング

ユーザー 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 **[Administration]** > **[Users and Groups]** の順に選択します。

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

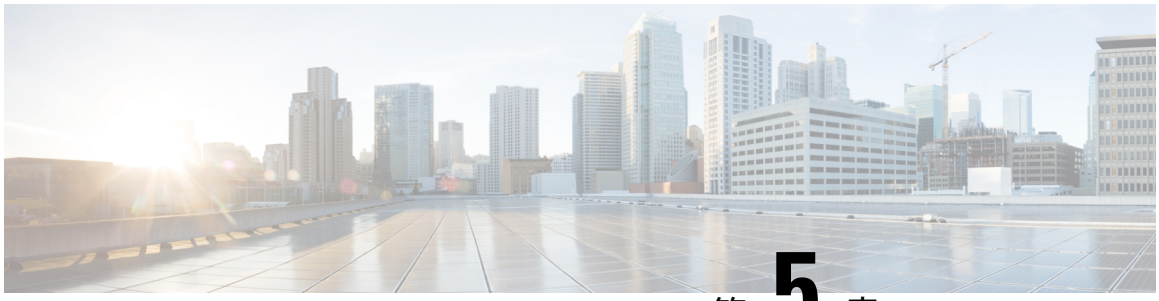
ステップ 3 ユーザ グループを選択します。

ステップ 4 [Branding] をクリックします。

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

フィールド	説明
[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。
[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のヘッダー セクションに表示されます。
[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。
[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。



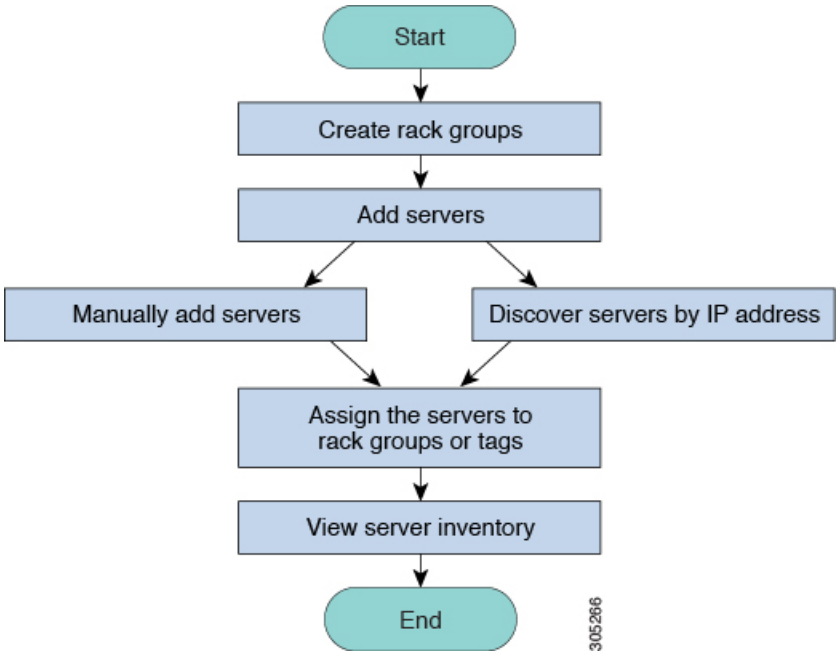
第 5 章

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、次の内容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。手動でのサーバの追加、またはサーバの検出ができます。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リングとタギング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 グループ下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。必要に合わせ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入れ替えることができます。たとえば、Windows、Linux などという名前のラック グループがある場合に、オペレーティング システムのタグ名の下にそ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。次の項では、自動検出プロファイルの設定、自動検出の実行、および自動検出されたサーバのインポートなどのトピックについて取り上げます。

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 **[Systems]** > **[Physical Accounts]** を選択します。

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

ステップ 3 [Add] をクリックします。

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

フィールド	説明
[Profile Name] フィールド	プロファイルの記述名。
[Search Criteria] ドロップダウン リスト	ドロップダウン リストから [IP Address Range]、[Subnet Mask Range]、[IP Address CSV File]、または [IP Address List] を選択します。
[Starting IP] フィールド	有効な IP アドレス
[Ending IP] フィールド	有効な IP アドレス
[Use Credential Policy] チェックボックスがオンの場合	
[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（100 ページ）を参照してください。
[Use Credential Policy] チェックボックスがオフの場合	
[User Name] フィールド	サーバのログイン名。
[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。
[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。
[Port] フィールド	ポート番号を入力します。

フィールド	説明
以下のフィールドは、[Search Criteria] で [IP Address Range]、[Subnet Mask Range]、および [IP Address List] を選択した場合のみ使用できます。 （注） [IP Address CSV File] を選択した場合、これらのフィールドは CSV ファイルに次の形式で指定できます。サンプルの csv ファイルは、[File Template] をクリックすると使用できます。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）<*description*> • （オプション）<*location*> • （オプション）<*contact*> • （オプション）<*rack group*> • （オプション）<*tag name:tag value*>;<*tag name:tag value*> （注） • Rack Group と 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任意です。CSV ファイルに Rack Group の値を指定しない場合、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、[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。	
[Description] フィールド	サーバの説明を入力します。
[Contact] フィールド	サーバの連絡先の詳細を入力します。
[Location] フィールド	サーバのアドレスを入力します。
[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 [Submit] をクリックします。`

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

自動検出の実行

システムでラックマウント 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 **[Systems]** > **[Physical Accounts]** を選択します。

ステップ 2 [Discover Devices] をクリックします。

ステップ 3 [Discover] をクリックします。

ステップ 4 [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
[Select Profile] ドロップダウン リスト	[Select] をクリックして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。
[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。スケジュール作成の詳細については、スケジュールの作成（179 ページ） を参照してください。 **[Policies]** > **[Manage Schedules]** の順に移動して、スケジュールを選択し、[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 [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。
[Schedule(s)] ドロップダウン リスト	[Schedule Later] チェックボックスを選択した場合、作成したスケジュールをドロップダウンリストから選択できます。 （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 **[Systems]** > **[Physical Accounts]** を選択します。

ステップ 2 [Discover Devices] をクリックします。

ステップ 3 [Import] をクリックします。

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

フィールド	説明
[Select Device(s)] フィールド	[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 ステータス**がインポートされると、ステータスがインポートされ、そのラック アカウントはインポート用に表示されません。
[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つことなく、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 **[Systems]** > **[Physical Accounts]** を選択します。

ステップ 2 [Discover Devices] をクリックします。

ステップ 3 [Discovered Devices] テーブルでデバイスを選択します。

ステップ 4 [Set Properties] をクリックします。

ステップ 5 **[Set Properties (プロパティの設定)]** ページで、次のフィールドに入力します。

フィールド	説明
[Description] フィールド	サーバの説明を入力します。
[Contact] フィールド	サーバの連絡先の詳細を入力します。
[Location] フィールド	サーバのアドレスを入力します。
[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。デフォルトでは、システム定義のグループ [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 **[Systems]** > **[Physical Accounts]** を選択します。

ステップ 2 [Add] をクリックします。

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

フィールド	説明
[Group Name] フィールド	ラック グループの記述名。
[Description] フィールド	（任意）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 **[Systems]** > **[Physical Accounts]** を選択します。

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

ステップ 3 [Add] をクリックします。

ステップ 4 **[Create Account (アカウントの作成)]** 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。
[Server IP or Hostname (サーバ IP/ホスト名)] 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。
[Description] フィールド	（オプション）ラック アカウントの説明。
[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た場合は、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。
[Use Credential Policy] チェックボックスがオンの場合	
[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。
[Use Credential Policy] チェックボックスがオフの場合	
[User Name] フィールド	ラックマウント サーバのログイン ID。
[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。
[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。
[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。
[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 （59 ページ） を参照してください。

フィールド	説明
[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。
[Location] フィールド	（オプション）アカウントの場所。

ステップ 5 [Submit] をクリックします。

（注）
- ラック アカウントを作成するための前のコマンドが完了するのを待つことなく、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することができます。インベントリ収集、障害ヘルス収集、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 （63 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 **[Systems]** > **[Physical Accounts]** を選択します。
ステップ 2 **[Rack Accounts (ラックアカウント)]** 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 [Inventory] をクリックします。

ステップ 5 **[Collect Inventory for Account(s) (アカウントのインベントリ収集)]**ページで、**[Rack Group (ラック グループ)]** または **[Rack Account (ラック アカウント)]** 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 サーバを選択するには [Select] をクリックします。

ステップ 7 [Select] ダイアログボックスでサーバを選択して、[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に掛けるには、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

[Rack Accounts] で、ラック アカウントまたはサーバを作成しておきます。

手順

ステップ 1 **[Systems]** > **[Physical Accounts]** を選択します。

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

ステップ 3 サーバの一覧が表示されます。

ステップ 4 1 つ以上のサーバを選択して、[Assign Rack Group] をクリックします。

ステップ 5 **[Assign Rack Groups (ラック グループの割り当て)]** 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、[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 **[Systems]** > **[Physical Accounts]** を選択します。

ステップ 2 **[Rack Accounts (ラックアカウント)]** 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。

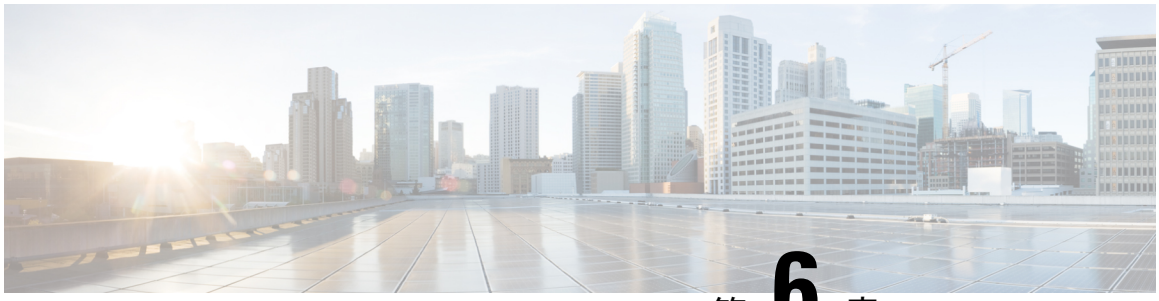
ステップ 4 [Test Connection] をクリックします。

（注） リストから少なくとも 1 つのラック アカウントを選択するまで、[Test Connection] ボタンは表示されません。

ステップ 5 [Test Connection] ダイアログボックスで、[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 [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、次の内容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） **[Rack Groups (ラック グループ)]** 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 **[Systems]** > **[Inventory and Fault Status]** を選択します。

ステップ 2 **[Rack Groups (ラック グループ)]** 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、[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 **[View Details (詳細の表示)]** 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を表示できます。

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装置の詳細。 （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 Adapters]	サーバで使用されている PCI アダプタの詳細。
[VIC Adapters]	サーバで使用されている VIC アダプタの詳細。 リストにある任意の VIC アダプタを選択して [View Details] をクリックすると、[External Ethernet Interfaces] や [VM FEXs] など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。 リストされている任意のネットワーク アダプタを選択して [View Details] をクリックすると、[External Ethernet Interfaces] の情報が表示されます。
[Storage Adapters]	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 **[View Details (詳細の表示)]** をクリックすると、**[Controller Info (コントローラ情報)]**、**[Physical Drives (物理ドライブ)]**、**[Virtual Drives (仮想ドライブ)]** などの情報が表示されます。「SSD のスマート情報の表示 （68 ページ）」を参照してください。
[FlexFlash Adapters]	サーバで使用されている FlexFlash アダプタの詳細。 リストにある任意の FlexFlash アダプタを選択して [View Details] をクリックすると、[Controller Info] や [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 **[Systems (システム)]** > **[Physical Accounts (物理アカウント)]** > **[Rack Accounts (ラック アカウント)]**> **[Inventory (インベントリ)]** 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
コミュニケーション	HTTP、HTTPS、SSH、IPMI Over LAN、NTP、SNMP などのプロトコルの情報。
[Remote Presence]	vKVM、Serial over LAN、vMedia の詳細。
障害（**Fault**）	サーバで記録された障害の詳細。
Users	**デフォルト グループ**のユーザーに関する詳細。ユーザー 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（129 ページ）およびパスワードの有効期限ポリシー（120 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 設定とブート順序に関する詳細。 サーバを選択して、[View BIOS Settings]、[View Boot Settings]、または [View Boot Order] をクリックしてください。
障害履歴	サーバで発生した障害の履歴情報。
[Tech Support]	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、[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（93 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、**[Map Image (イメージのマッピング)]**、**[Unmap Image (イメージのマップ解除)]**、または **[Delete Image (イメージの削除)]** 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。
[Associated Hardware Profiles]	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 [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 **[Systems]** > **[Inventory and Fault Status]** を選択します。

ステップ 2 **[Rack Groups (ラック グループ)]** 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、[Rack Servers] をクリックします。

（注） また、[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 [Rack Server (ラック サーバ)] ページで **[Storage Adapters (ストレージ アダプタ)]** 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、**[Controller Info (コントローラ情報)]** 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**
- **SMART エラーでの SSD へのコピーバックの有効化**

ステップ 7 SSD ドライブをダブルクリックし、**[Physical Drives (物理ドライブ)]** 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、**[View Smart Information (スマート情報の表示)]** 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
[Power Cycle Count (電源の再投入回数)] フィールド	製造された時点からドライブの電源が再投入された回数。
[Power on Hours] フィールド	ドライブが「電源オン」モードにある時間の合計数。
[Percentage Life Left] フィールド	ソリッドステートドライブ（SSD）に残っている書き込みサイクル数。たとえば、SSD がライフタイム中に 100 の書き込みサイクルに対応でき、15 の書き込みを完了している場合、ドライブの残りのライフのパーセンテージは85%です。各パーセンテージ範囲は、異なる色で表されます。たとえば、75%～100%の場合は緑色、1～25%の場合は赤色です。 （注） **[Controller Info (コントローラ情報)]** の下の **[SSD - Percentage Life Left (SD - 残量 (パーセンテージ))]** に、SSD の棒グラフが追加されます。
[Wear Status in Days] フィールド	SSD が書き込みサイクルを実行した日数。 SSD ベンダーによって、SSD での 1 日あたりの有限書き込み数が提示されます。その数に基づいて、SSD が動作し続ける総年数を計算できます。
[Operating Temperature] フィールド	選択した SSD が選択時点で動作しているドライブの現在の温度。
[Percentage Reserved Capacity Consumed (消費された予約済みの容量の割合)]フィールド	SSD によって消費された総容量 (そのために予約されている割合のうちの)。
[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） [Storage Adapter (ストレージ アダプタ)] ページで **[Controller Info (コントローラ情報)]** をクリックし、**[Percentage LIFE LEFT (残量パーセンテージ)]**、**[Enable Copy back on SMART (SMART でのコピーバックの有効化)]**、**[Enable Copy back to SSD on SMART Error (SMART エラーでの SSD へのコピーバックの有効化)]** 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 キーはユーザーが指定するか、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 （70 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

[Controller Info (コントローラ情報)]、**[Physical Drives (物理ドライブ)]**、および **[Virtual Drives (仮想ドライブ)]** 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 **[Systems]** > **[Inventory and Fault Status]** を選択します。

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

ステップ 3 **[Rack Servers (ラック サーバ)]** 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 [Rack Server (ラック サーバ)] ページで、**[Storage Adapters (ストレージ アダプタ)]** 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、**[View Details (詳細の表示)]**をクリックします。

ステップ 7 [Storage Adapter (ストレージ アダプタ)] ページで **[Controller Info (コントローラ情報)]** 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
[Power Cycle Count] フィールド	製造された時点からドライブの電源が再投入された回数。
[Power on Hours (電源オンの時間数)] フィールド	ドライブが「電源オン」モードにある時間の合計数。
[Percentage Life Left (残りのライフのパーセンテージ)] フィールド	ソリッド ステート ドライブ（SSD）に残っている書き込みサイクル数。たとえば、SSD がライフタイム中に 100 の書き込みサイクルに対応でき、15の書き込みを完了している場合、ドライブの残りのライフのパーセンテージは 85% です。各パーセンテージ範囲は、異なる色で表されます。たとえば、75% ～ 100% の場合は緑色、1 ～ 25% の場合は赤色です。 （注） **[Controller Info (コントローラ情報)]** の下の **[SSD - Percentage Life Left (SD - 残量 (パーセンテージ))]** に、SSD の棒グラフが追加されます。
[Wear Status in Days] フィールド	SSD が書き込みサイクルを実行した日数。 SSD ベンダーによって、SSD での 1 日あたりの有限書き込み数が提示されます。その数に基づいて、SSD が動作し続ける総年数を計算できます。
[Operating Temperature (動作温度)] フィールド	選択した SSD が選択時点で動作しているドライブの現在の温度。

タブ	説明
[Percentage Reserved Capacity Consumed (消費された予約済みの容量の割合)]フィールド	SSD によって消費された総容量（そのために予約されている割合のうちの）。
[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 [Storage Adapter (ストレージ アダプタ)] ページで **[Physical Drives (物理ドライブ)]**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 [Storage Adapter (ストレージ アダプタ)] ページで **[Virtuall Drives (仮想ドライブ)]** 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 **[Systems]** > **[Inventory and Fault Status]** を選択します。

ステップ 2 [Rack Groups (ラック グループ)] ページで、**[Faults (障害)]** 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 **[View Details (詳細の表示)]** 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を表示できます。

タブ	説明
説明	問題の原因の要約。
推奨事項	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 グループのサマリー レポート

[Inventory and Fault Status for Rack Groups (インベントリと障害のステータス)] ページには、ラック グループのリストが表示されます。**[Rack Groups (ラック グループ)]** 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 **[Summary (要約)]** レポートが表示されます。

- [Faults]：選択されたラック グループに対し、全体の障害の数を表します。障害の数は、[Critical]、[Major]、[Warnings]、[Minor]、[Info] などの重大度に基づいて分類されます。
- [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、[Good]、[Memory Test In Progress]、[Moderate Fault]、[Severe Fault] などの状態のいずれかになります。

（注） [Moderate Fault] と [Severe Fault] は、重大度が [Major] および [Critical] となっている障害とそれぞれ相互に関連します。しかし、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、上記の障害の重要度対して、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。

- **[Chassis Health (シャーシの状態)]**：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]、[メモリ テストが進行中です]、[中程度の障害]、[重大な障害] などの状態のいずれかになります。
- [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全体的な数を表します。
- [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全体的な数を表します。
- [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全体的な数を表します。電源の状態は [On] または [Off] のいずれかです。
- [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全体的な数を表します。接続ステータスは [Success] または [Failed] のいずれかです。
- **[Overview (概要)]**：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、アラートの指定した条件に一致する障害が一致すると、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 **[Administration]** > **[System]** を選択します。

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

（注） [Email Alert Rules] テーブルには、電子メール アラートのルール名、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。

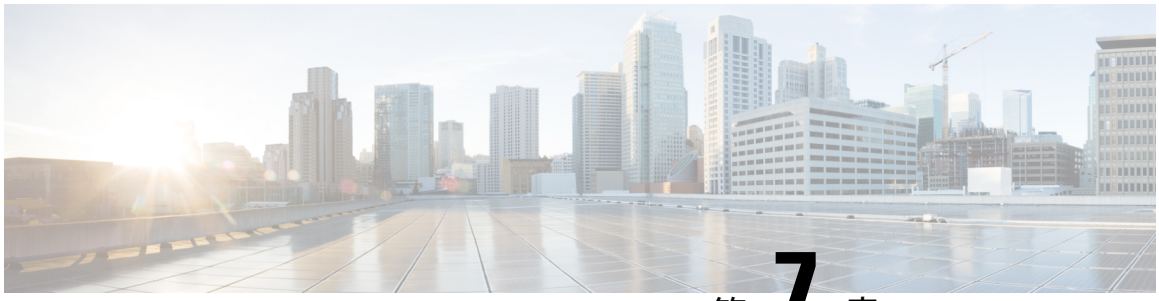
ステップ 3 [Add] をクリックします。

ステップ 4 **[Add Email Alert Rule (電子メール アラート ルールの追加)]** 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）]	ルールの一意の名前を入力します。
[Alert Scope]	いずれか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 アラートを受信するには、[System] を選択します。指定されたラック グループに含まれ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、[ServerGroup] を選択します。指定された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、**[Server (サーバ)]** を選択します。
サーバ グループ	アラート レベルで [ServerGroup] を選択した場合、このオプションが表示されます。 **1.** [Select] をクリックします。 **2.** [Select] ダイアログボックスで 1 つ以上のラック サーバ グループにチェックマークを付けて、[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。

フィールド	説明
サーバ	アラート レベルで [Server] を選択した場合、このオプションが表示されます。 **1.** [Select] をクリックします。 **2.** [Select] ダイアログボックスで 1 つ以上のサーバにチェックマークを付けて、[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名が、このフィールドの横にリストされます。
[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。複数の電子メール アドレスをカンマで区切って入力できます。
Severity	[Email Addresses] フィールドに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.** **[Select... (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にチェックマークを付けて、[Select] をクリックします。 （注） 選択した値が [Select...] ボタンの横に表示されます。
[Enable Alert] 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。
[Send alert for all fault every 24 hours (24 時間ごとにすべての障害に関するアラートを送信する)] チェックボックス	24 時間ごとに電子メールアラートを送信するには、このチェックボックスをオンにします。この電子メールアラートには、設定されている電子メール アラート ルールに基づいて、アクティブおよびオープンなすべての障害が含まれます。

（注）
- 電子メール アラートのルールを修正と削除ができます。[Edit] および [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。[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、[Delete] をクリックして、削除することを確認します。
- 複数のルールを同時に選択して [Delete] をクリックすると、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 [Alert Level] フィールドを変更することはできませんが、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、次の内容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） **[Rack Groups (ラック グループ)]** 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 **[Systems]** > **[Inventory and Fault Status]** を選択します。

ステップ 2 **[Rack Groups (ラック グループ)]** 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、[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 **[View Details (詳細の表示)]** 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を表示できます。

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装置の詳細。 （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 Adapters]	サーバで使用されている PCI アダプタの詳細。
[VIC Adapters]	サーバで使用されている VIC アダプタの詳細。 リストにある任意の VIC アダプタを選択して [View Details] をクリックすると、[External Ethernet Interfaces] や [VM FEXs] など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。 リストされている任意のネットワーク アダプタを選択して [View Details] をクリックすると、[External Ethernet Interfaces] の情報が表示されます。
[Storage Adapters]	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 **[View Details (詳細の表示)]** をクリックすると、**[Controller Info (コントローラ情報)]**、**[Physical Drives (物理ドライブ)]**、**[Virtual Drives (仮想ドライブ)]** などの情報が表示されます。「SSD のスマート情報の表示 （68 ページ）」を参照してください。

タブ	説明
[FlexFlash Adapters]	サーバで使用されている FlexFlash アダプタの詳細。 リストにある任意の FlexFlash アダプタを選択して [View Details] をクリックすると、[Controller Info] や [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 **[Systems (システム)]** > **[Physical Accounts (物理アカウント)]** > **[Rack Accounts (ラック アカウント)]**> **[Inventory (インベントリ)]** 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。
コミュニケーション	HTTP、HTTPS、SSH、IPMI Over LAN、NTP、SNMP などのプロトコルの情報。
[Remote Presence]	vKVM、Serial over LAN、vMedia の詳細。
障害（Fault）	サーバで記録された障害の詳細。
Users	**デフォルト グループ**のユーザーに関する詳細。ユーザー 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（129 ページ）およびパスワードの有効期限ポリシー（120 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 設定とブート順序に関する詳細。 サーバを選択して、[View BIOS Settings]、[View Boot Settings]、または [View Boot Order] をクリックしてください。

タブ	説明
障害履歴	サーバで発生した障害の履歴情報。
[Tech Support]	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、[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 （93 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、**[Map Image (イメージのマッピング)]**、**[Unmap Image (イメージのマップ解除)]**、または **[Delete Image (イメージの削除)]** 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。
[Associated Hardware Profiles]	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 [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 **[Systems]** > **[Inventory and Fault Status]** を選択します。

ステップ 2 [Rack Groups (ラック グループ)] ページで、**[Faults (障害)]** 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 **[View Details (詳細の表示)]** 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を表示できます。

タブ	説明
説明	問題の原因の要約。
推奨事項	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 **[Systems]** > **[Inventory and Fault Status]** を選択します。

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

（注） [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、[Rack Servers] をクリックします。

（注） また、[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 **[Power On (電源オン)]** をクリックします。**[More Actions (その他の操作)]** ドロップダウン リストから **[Power OFF (電源オフ)]** 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。また、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、サーバのユーザー定義タグです。**[Asset Tag (アセット タグ)]**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 （192 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 **[Systems]** > **[Inventory and Fault Status]** を選択します。

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

（注） また、**[Inventory and Fault Status (インベントリと障害のステータス)]** ペインの **[Rack Groups (ラック グループ)]**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 **[More Actions (その他の操作)]**ドロップダウン リストから **[Asset Tag (アセット タグ)]** 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） **[Asset Tag (アセット タグ)]** 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、**[Rack Groups (ラック グループ)]** ページの **[Asset Tag (アセット タグ)]** 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 **[Systems]** > **[Inventory and Fault Status]** を選択します。

ステップ 2 **[Inventory and Fault Status (インベントリおよび障害ステータス)]** ペインで、**[Rack Groups (ラック グループ)]** をせん。

（注） [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、[Rack Servers] をクリックします。

（注） また、[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 **[More Actions (その他の操作)]** ドロップダウン リストから、**[Shut Down (シャット ダウン)]** 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 **[Systems]** > **[Inventory and Fault Status]** を選択します。

ステップ 2 **[Inventory and Fault Status (インベントリおよび障害ステータス)]** ペインで、**[Rack Groups (ラック グループ)]** をせん。

（注） [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、[Rack Servers] をクリックします。

（注） また、[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 **[More Actions (その他の操作)]** ドロップダウン リストから、**[Hard Reset (ハード リセット)]** 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 **[Systems]** > **[Inventory and Fault Status]** を選択します。

ステップ 2 **[Inventory and Fault Status (インベントリおよび障害ステータス)]** ペインで、**[Rack Groups (ラック グループ)]** をせん。

（注） [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、[Rack Servers] をクリックします。

（注） また、[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 **[More Actions (その他の操作)]** ドロップダウン リストから、**[Power Cycle (電源の再投入)]** 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。

（注） 4.1(1c) 以降のファームウェアを実行している C シリーズ M4 または C シリーズ M5 サーバの KVM コンソールを起動するには、明示的な認証が必要です。

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 **[Systems]** > **[Inventory and Fault Status]** を選択します。

ステップ 2 **[Inventory and Fault Status (インベントリおよび障害ステータス)]** ペインで、**[Rack Groups (ラック グループ)]** をせん。

（注） [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、[Rack Servers] をクリックします。

（注） また、[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 **[More Actions (その他の操作)]** ドロップダウンリストから **[KVM Console (KVM コンソール)]**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 台選択できます。

ステップ 6 [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 Console] が別ウィンドウで開きます。

（注） 別のウィンドウで開く `launcher.jsp` ファイルに、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ているか確認することもできます。

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 **[Systems]** > **[Inventory and Fault Status]** を選択します。

ステップ 2 **[Inventory and Fault Status (インベントリおよび障害ステータス)]** ペインで、**[Rack Groups (ラック グループ)]** をせん。

（注） [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、[Rack Servers] をクリックします。

（注） また、[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 **[More Actions (その他の操作)]** ドロップダウン リストから **[Launch GUI (GUI の起動)]** 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 **[Submit (送信)]** 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/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 **[Systems]** > **[Inventory and Fault Status]** を選択します。

ステップ 2 **[Inventory and Fault Status (インベントリおよび障害ステータス)]** ペインで、**[Rack Groups (ラック グループ)]** をせん。

（注） [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、[Rack Servers] をクリックします。

（注） また、[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 **[More Actions (その他の操作)]** ドロップダウン リストから、**[Locator LED (ロケータ 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 [Turn] ドロップダウン リストから、[ON] または [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ことで、サーバの分類に役立ちます。これによって、必要なサーバの検索、表示、比較がしやすくなります。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 **[Systems]** > **[Inventory and Fault Status]** を選択します。

ステップ 2 **[Inventory and Fault Status (インベントリおよび障害ステータス)]** ペインで、**[Rack Groups (ラック グループ)]** をせん。

（注） [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、[Rack Servers] をクリックします。

（注） また、[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 **[More Actions (その他の操作)]** ドロップダウンリストから **[Set Label (ラベルの設定)]** 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

タギングは、リソース グループまたはラック サーバなどのオブジェクトにラベルを割り当てるために使用されます。タグは、ラックの位置、担当サポート グループ、目的、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 **[Systems]** > **[Inventory and Fault Status]** を選択します。

ステップ 2 [Inventory and Fault Status (インベントリと障害のステータス)] ペインで **[Rack Groups (ラック グループ)]**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 **[Rack Servers (ラック サーバ)]** または **[Chassis (シャーシ)]** をクリックします。

（注） **[Rack Groups (ラック グループ)]** 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、[Manage Tags] テーブルにエントリを追加します。

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

フィールド	説明
[Tag Name]	

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 [Submit] をクリックするか、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.** [Create Tag] ウィンドウで、次の手順を実行します。 **1.** [Name] フィールドに、タグを記述する名前を入力します。 **2.** [Description] フィールドに、タグの説明を入力します。 **3.** [Type] フィールドで、ドロップダウン リストから文字列または整数を選択します。 **4.** [Possible Tag Values] フィールドで、可能なタグ値を入力します。 **5.** [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.** [Add Entry to Entities] ウィンドウで、[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。 • [Administration] カテゴリの場合、ユーザ用のタグ エンティティが作成されます。 （注） シャーシのタグを追加することもできます。シャーシのタグの追加方法の詳細については、Cisco UCS S3260 ラック サーバのタグの追加 （194 ページ）を参照してください。 **4.** [Rack Servers] または [Chassis] チェック

フィールド	説明
	ボックスをオンにします。 5. [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 **[Manage Tags (タグの管理)]** 画面でタグを選択し、**[Edit (編集)]** 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 [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

タギングは、リソース グループまたはラック サーバなどのオブジェクトにラベルを割り当てるために使用されます。タグは、ラックの位置、担当サポート グループ、目的、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 **[Systems]** > **[Inventory and Fault Status]** を選択します。

ステップ 2 **[Inventory and Fault Status (インベントリおよび障害ステータス)]** ペインで、**[Rack Groups (ラック グループ)]** をせん。

（注） [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、[Rack Servers] をクリックします。

（注） また、[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 [その他のアクション（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 [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 [Tag Value] を選択します。

ステップ 7 [+] 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 （88 ページ）を参照してください。

（注） また、タグの詳細を複製、編集、削除、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 **[Systems]** > **[Inventory and Fault Status]** を選択します。

ステップ 2 **[Inventory and Fault Status (インベントリおよび障害ステータス)]** ペインで、**[Rack Groups (ラック グループ)]** をせん。

（注） [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、[Rack Servers] をクリックします。

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

名前	説明
[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。
[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 ファイルを保存する必要のあるサーバの IP アドレスまたはホスト名。[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。
Username	システムがリモート サーバへのログインに使用する必要のあるユーザ名。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。
Password	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 [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、[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、[Download] をクリックします。*<hostname>_<timestamp>*. 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 **[Systems]** > **[Inventory and Fault Status]** を選択します。

ステップ 2 **[Inventory and Fault Status (インベントリおよび障害ステータス)]** ペインで、**[Rack Groups (ラック グループ)]** をせん。

（注） [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、[Rack Servers] をクリックします。

（注） また、[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 **[View Details (詳細の表示)]** を選択します。

ステップ 5 [System Event Log] をクリックします。

ステップ 6 [Clear IMC SEL Log] をクリックします。

ステップ 7 （任意） **[Clear IMC SEL Logs (IMC SEL ログのクリア)]** 画面で、**[Delete historical logs from Cisco IMC Supervisor (Cisco IMC Supervisor から履歴ログを削除する)]** 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 Supervisor GUI 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 **[Administration]** > **[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、[Manage Task] をクリックします。

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

フィールド	説明
[Task Execution] ドロップダウン リスト	（オプション）[Enable] または [Disable] を選択します。
[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**
[スケジュール タイプ] 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。次のいずれかのオプションを使用できます。 • **[遅延の固定]**：1 つのタスクの実行を完了し、次のタスクの実行の開始までの時間を意味します。 • **[固定レート]**：連続のタスクの実行時間を意味します。1つのタスクの実行に遅延が発生した場合、または 1 つのタスクを実行する時間がスケジュールされた時間より長くかかった場合、後続のタスクの実行が遅延します。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、同時に実行されません。

フィールド	説明
[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。 **[遅延の固定]** 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、次のタスクの実行の開始する間の時間間隔を示します（時間）。 **[Fixed Rate (固定レート)]** 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）。
[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] 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**
[Start Time] 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。
[頻度（Frequency）] 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。 • **毎時** • **[毎日(Daily)]** • **[毎週（Weekly）]** • **[月 1 回(Monthly)]** （注） このフィールドは、**[繰り返しタイプ]** ドロップダウン リストから **[無期限]** を選択した場合にのみ表示されます。
[頻度の間隔（Frequency Interval）] ドロップダウン リスト	ドロップダウンリストから頻度間隔を選択します。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。

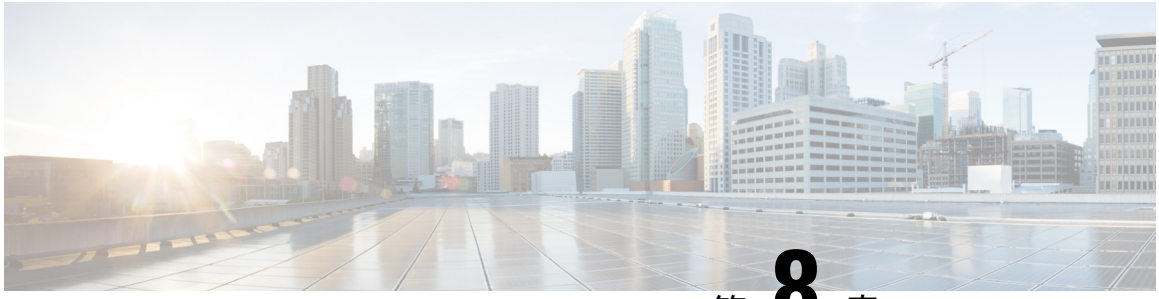
タスクの実行

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 **[Administration]** > **[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 **[Run Now (今すぐ実行)]** 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、次の内容で構成されています。

クレデンシャル ポリシー

ポリシーは、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ルールのセットから成ります。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 で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、新しいポリシーをクレデンシャル タイプのデフォルトのポリシーとして割り当てるか、または個々のアプリケーションに割り当てることができます。

[Credential Policies] ページには、次の詳細が表示されます。

フィールド	説明
[Policy Name]	ポリシーのユーザ定義名。
[Description]	ポリシーのユーザ定義の簡単な説明。
[Username]	シスコ ユーザ名。
[Protocol]	ポリシーが準拠するプロトコル。
[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 ポリシーの作成の詳細については、クレデンシャル ポリシーの作成 （100 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 **[Policies]** > **[Manage Policies and Profiles]** を選択します。

ステップ 2 [Manage Policies and Profiles] ページで、[Credential Policies] をクリックします。

ステップ 3 [Add] をクリックします。

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

フィールド	説明
[Policy Name] フィールド	ポリシーの記述名。
[Description] フィールド	（オプション）ポリシーの説明。
[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。
[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。
[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。
[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メカニズムです。ポリシーは、複数のサーバにわたって設定の一貫性と反復可能性を確保するうえで役立ちます。包括的なポリシー セットを定義して使用すると、多数のサーバに類似する設定を適用できるので、一貫性、制御、予測可能性、自動化が促進されます。

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 （101 ページ）を参照してください。
    2. サーバ上の既存の設定からポリシーを作成します。サーバ上の既存の設定からポリシーを作成する方法の詳細については、既存の設定からのポリシーの作成 （136 ページ）を参照してください。
2. サーバでポリシーを適用します。ポリシーの適用方法の詳細については、ハードウェア ポリシーの適用 （138 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. Edit
    2. 削除
    3. Clone
    4. また、特定のポリシーにマップされるサーバのリストを表示できます。これらのタスクの実行方法の詳細については、ハードウェア ポリシーでの一般タスク （139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、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方法の詳細については、ハードウェア プロファイルの適用 （143 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 **[Policies]** > **[Manage Policies and Profiles]** を選択します。

ステップ 2 [Manage Policies and Profiles] ページで、[Hardware Policies] をクリックします。

ステップ 3 [Add] をクリックします。

ステップ 4 [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』に記載されています。各ポリシー タイプごとに、このマニュアル内の各セクションがリストされています。

（注） ポリシー作成用の 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ています。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。

Policy Type	『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』内のセクション
BIOS ポリシー （103 ページ）	*BIOS* の設定
ディスク グループ ポリシー （104 ページ）	ストレージ アダプタの管理
FlexFlash ポリシー （105 ページ）	*Flexible Flash* コントローラの管理
IPMI Over LAN ポリシー （110 ページ）	*IPMI* の設定
LDAP ポリシー （112 ページ）	*LDAP* サーバの設定
レガシー ブート順序ポリシー （113 ページ）	サーバのブート順
ネットワーク構成ポリシー （114 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 （118 ページ）	ネットワーク セキュリティの設定
NTP ポリシー （119 ページ）	ネットワーク タイム プロトコル設定の設定
パスワードの有効期限ポリシー （120 ページ）	パスワードの有効期限切れ
高精度のブート順序ポリシー （121 ページ）	高精度ブート順の設定
電力復元ポリシー （122 ページ）	電力復元ポリシーの設定
RAID ポリシー （123 ページ）	ストレージ アダプタの管理
Serial over LAN ポリシー （126 ページ）	*Serial over LAN* の設定
SNMP ポリシー （127 ページ）	*SNMP* の設定
SSH ポリシー （128 ページ）	*SSH* の設定

Policy Type	『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』内のセクション
ユーザ ポリシー （129 ページ）	ローカル ユーザの設定
VIC アダプタ ポリシー （132 ページ）	*VIC* アダプタのプロパティの表示
仮想 KVM ポリシー （131 ページ）	仮想 *KVM* の設定
vMedia ポリシー （134 ページ）	仮想メディアの設定
ゾーン分割ポリシー （135 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 （138 ページ）」を参照してください。

BIOS ポリシー

BIOS ポリシーは、サーバの BIOS 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 ポリシーを指定した場合、ポリシーの値がサーバに設定されている値に置き換わります。

BIOS の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 BIOS Settings*」を参照してください。

手順

ステップ 1 [Hardware Policies] を選択したら、[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 [Add] 画面で、ドロップダウン リストから [BIOS Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力します。

また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[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 （136 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用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て [Next] をクリックします。

ステップ 5 [Main] 画面で、主要な BIOS プロパティ（[Boot Option Retry]、[Post Error Pause]、および [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。[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 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 [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 [Next] をクリックします。

ステップ 7 [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 [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は、ディスク グループと呼ばれます。

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。このポリシーは、仮想ドライブに使用される 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。その場合、それらの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。1 つの RAID ポリシー内の複数の異なる仮想ドライブに関連付けられるディスク グループ ポリシーが使用するいずれかの物理ディスクを、別のディスク グループポリシーで繰り返し使用することはありません。RAIDポリシーの詳細については、RAID ポリシー （123 ページ）を参照してください。

さまざまなディスク グループ 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。

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 [Hardware Policies] を選択したら、[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 [Add] 画面で、ドロップダウン リストから [Disk Group Policy] を選択して [Submit] をクリックします。

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

ステップ 4 [Virtual Drive Configuration] 画面で、[RAID Level] ドロップダウン リストから RAID レベルを選択し、[Next] をクリックします。

ステップ 5 [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、[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。
- サーバの現在の設定からRAIDポリシーが作成されるときに、ディスク グループ ポリシーもまたサーバ設定から自動的に作成されます。

FlexFlash ポリシー

FlexFlash ポリシーを使用して、SD カードを設定して有効に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「*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 [Hardware Policies] を選択したら、[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 [Add] 画面で、ドロップダウン リストから [FlexFlash Policy] を選択して [Submit] をクリックします。

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

また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[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 （136 ページ）を参照してください。

ステップ 4 [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
[Firmware Mode] ペイン	次のファームウェア動作モードのいずれかを選択します。 • [Mirror Mode]：このモードはミラー設定で、C220 M4 および C240 M4 サーバでのみ使用できます。 • [Util Mode]：このモードでは、4 つのパーティションを持つ 1 つのカードと、単一パーティションを持つ 1 つ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。 • [Not Applicable]：ファームウェアの動作モードが選択されません。[Not Applicable] を選択した場合はステップ 5 に進みます。このモードは、C220 M3、C240 M3、C22、C24、C460 M4 サーバでのみ使用できます。
[Mirror] オプション ボタン	[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 [Erase Virtual Drive] チェックボックスをオンにして仮想ドライブを削除します。

フィールド	説明
[Util] オプション ボタン	[Enable Virtual Drive] チェックボックスをオンにして仮想ドライブ（[SCU]、[Hypervisor]、[Drivers]、[HUU]、および [User Partition]）を有効にするか、または [Erase Virtual Drive] チェックボックスをオンにして仮想ドライブを削除します。 （注） 複数の仮想ドライブを選択できます。
[Not Applicable] ラジオ ボタン	[Enable Virtual Drive] チェックボックスをオンにして仮想ドライブ（[SCU]、[HV]、[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。 • [Erase Virtual Drive] チェックボックスは使用できません。
[Partition Name] フィールド（[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。
[Non Util Card Partition Name] フィールド	2枚目のカードの単一パーティションに割り当てる名前（存在する場合）。 （注） このオプションは、util モードの場合にのみ使用できます。
[Select Primary Card]（ミラー モードで使用可能）または [Select Util Card]（Util モードで使用可能） ドロップダウン リスト	SD カードが配置されているスロット [Slot 1] または [Slot 2] を選択するか、または SD カードがサーバに 1 枚しかない場合は [None] を選択します。 （注） [None] は [Select Util Card] オプションでのみ使用できます。
[Auto Sync] チェックボックス	選択したスロットで使用可能な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
[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可される読み取りエラーの数。読み取りエラーの数がカード上のこのしきい値を超えると、カードが正常でないとマークされます。 読み取りエラーのしきい値を指定するには、1～255 の整数を入力します。検出されたエラー数に関係なく、カードがディセーブルにならないように指定するには、0（ゼロ）を入力します。
[Slot-1 Write 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可される書き込みエラーの数。書き込みエラーの数がカード上のこのしきい値を超えると、カードが正常でないとマークされます。 書き込みエラーのしきい値を指定するには、1～255 の整数を入力します。検出されたエラー数に関係なく、カードがディセーブルにならないように指定するには、0（ゼロ）を入力します。
[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可される読み取りエラーの数。読み取りエラーの数がカード上のこのしきい値を超えると、カードが正常でないとマークされます。 読み取りエラーのしきい値を指定するには、1～255 の整数を入力します。検出されたエラー数に関係なく、カードがディセーブル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、util モードの場合にのみ使用できます。ミラーモードの場合は、スロット 1 の読み取り/書き込みしきい値がスロット 2 にも適用されます。

フィールド	説明
[Slot-2 Write 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可される書き込みエラーの数。書き込みエラーの数がカード上のこのしきい値を超えると、カードが正常でないとマークされます。 書き込みエラーのしきい値を指定するには、1～255 の整数を入力します。検出されたエラー数に関係なく、カードがディセーブル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、util モードの場合にのみ使用できます。ミラーモードの場合は、スロット 1 の読み取り/書き込みしきい値がスロット 2 にも適用されます。

ステップ 5 ステップ 4 の [Details] ペインで [Not Applicable] を選択した場合は、次のフィールドに値を入力します。

フィールド	説明
[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 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 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 Read Error Threshold] フィールド	Cisco FlexFlash カードへのアクセス中に許可される読み取りエラーの数。読み取りエラーの数がカード上のこのしきい値を超えると、カードが正常でないとマークされます。 読み取りエラーのしきい値を指定するには、1～255 の整数を入力します。検出されたエラー数に関係なく、カードがディセーブル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 Write Error Threshold] フィールド	Cisco FlexFlash カードへのアクセス中に許可される書き込みエラーの数。書き込みエラーの数がカード上のこのしきい値を超えると、カードが正常でないとマークされます。 Cisco FlexFlash カードへのアクセス中に許可される書き込みエラーの数。書き込みエラーの数がカード上のこのしきい値を超えると、カードが正常でないとマークされます。
[Clear Errors] チェックボックス	オンにした場合、[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 [Submit] をクリックします。

また、[Hardware Policies] テーブルから既存の FlexFlash ポリシーを選択し、ユーザ インターフェイスで該当するオプションを選択することで、適用ステータスの削除、編集、複製、適用、表示が行えます。

（注） FlexFlash ポリシーの適用は、次のように 2 つのステップからなるプロセスです。

1. サーバの設定がデフォルトに設定されます。
2. 新しいポリシーの設定が適用されます。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。Cisco IMC を IPMI メッセージで管理するには、IPMI over LAN ポリシーを設定します。

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 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 [Hardware Policies] を選択したら、[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 [Add] 画面で、ドロップダウン リストから [IPMI Over LAN Policy] を選択して [Submit] をクリックします。

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

また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[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 （136 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) [Main] 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。

オプション	説明
[Enable IPMI Over LAN]	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。
[Privilege Level Limit]	ドロップダウン リストから特権レベルを選択します。
Encryption Key	このフィールドにキーを入力します。

（注） 暗号キーに含まれる 16 進数文字の数は偶数でなければならず、長さの合計が 40 文字を超えてはなりません。40 文字未満が指定されている場合、キーの長さが 40 になるまでゼロが埋め込まれます。

b) [Next] をクリックします。

c) [Confirm] 画面で、[Submit] をクリックします。
[Hardware Policies] ページの [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 Cisco UCS S3260 サーバ用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て [Next] をクリックします。

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

ステップ 7 [Next] をクリックします。

ステップ 8 [BMC Settings] 画面で、必要に応じて、BMC 1 と BMC 2 の両方の [Enable IPMI Over LAN] チェックボックスをオンにします。

ステップ 9 [Confirm] 画面で、[Submit] をクリックします。

You can see the Cisco UCS S3260 Dense Storage Rack Server listed in the Server Platform column in the **[Hardware Policies (ハードウェア ポリシー)]** ページの [Server Platform (サーバ プラットフォーム)] 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。

さまざまな LDAP プロパティの設定の詳細については、*Cisco UCS C* シリーズ サーバの統合管理コントローラ *GUI* の構成ガイド（*Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*） の「Configuring LDAP Server」の項を参照してください。

手順

ステップ 1 [Hardware Policies] を選択したら、[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 [Add] 画面で、ドロップダウン リストから [LDAP Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力します。

また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[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 （136 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用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て [Next] をクリックします。

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

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

ステップ 7 [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 [Add Entry to LDAP Groups] 画面で、グループの詳細を入力し、[Submit] をクリックします。

（注）
- サーバに設定されている既存の LDAP ロール グループはすべて削除され、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、サーバ上の既存のロール グループは単純に削除されます。
- **[Nested Group Search Depth (検索するグループのネスト レベル)]** 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ブート順序設定のグループを含む、1 つ以上のレガシーブート順序ポリシーを作成することができます。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。また、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 （121 ページ）」を参照してください。

さまざまなサーバブート順序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「*Server Boot Order*」の項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 ラック サーバでは使用できません。

手順

ステップ 1 [Hardware Policies] を選択したら、[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 [Add] 画面で、ドロップダウン リストから [Legacy Boot Order Policy] を選択して [Submit] をクリックします。

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

また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[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 （136 ページ）を参照してください。

ステップ 4 [Main] 画面で [+] をクリックして、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リストされます。

[Select Devices] テーブルで、既存のデバイスを選択して [x] をクリックするとデバイスが削除されます。エントリの順序を変更するには、上/下矢印アイコンを使用します。テーブルのエントリの順序により、ブート順序が決まります。

同じデバイス タイプをさらに追加することはできません。

ステップ 5 [Add Entry to Select Devices] 画面で [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。より高い 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てください。

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 ドメイン
- IPv4 および IPv6 用の DNS サーバ
- VLAN コンフィギュレーション

各種のネットワーク設定プロパティに関する詳細は、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』の「*Configuring 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 [Hardware Policies] を選択したら、[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 [Add] ダイアログボックスで、ドロップダウン リストから [Network Configuration Policy] を選択して [Submit] をクリックします。

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

また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[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 （136 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) [Main] 画面で、次のフィールドに入力します。

フィールド	説明
[Common Properties]	
[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
[Use Dynamic DNS] チェックボックスをオンにした場合	
[**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。
[Obtain DNS Server Addresses from DHCP] チェックボックスをオフにした場合	
[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。
[Obtain DNS Server Addresses from DHCP] チェックボックスをオフにした場合	
[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 Properties]	
[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。
[Enable VLAN] チェックボックスをオンにした場合	
[VLAN ID] フィールド	VLAN ID。
[Priority] フィールド	VLAN でのこのシステムのプライオリティ。

b) [Next] をクリックします。
c) [Confirm] 画面で、[Submit] をクリックします。

[Hardware Policies] ページの [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 Cisco UCS S3260 サーバ用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て [Next] をクリックします。

ステップ 6 [Main] 画面で、次のフィールドに入力します。

フィールド	説明
[Common Properties]	
[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
[Use Dynamic DNS] チェックボックスをオンにした場合	
[**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、[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。
[Obtain DNS Server Addresses from DHCP] チェックボックスをオフにした場合	
[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	
[Enable IPv6] チェックボックス	オンにすると、[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、[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、Cisco IMC Supervisor は DNS サーバ アドレスを DHCP から取得します。
[Use DHCP] チェックボックスをオフにした場合	

フィールド	説明
[Management IP Address] フィールド	管理 IP アドレスを入力します。
[**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。
[Gateway] フィールド	ゲートウェイの IP アドレスを入力します。
[Obtain DNS Server Addresses from DHCP] チェックボックスをオフにした場合	
[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 Properties]	
[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。
[Enable VLAN] チェックボックスをオンにした場合	
[VLAN ID] フィールド	VLAN ID。
[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 [Next] をクリックします。

ステップ 8 [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 Address] フィールド	IPv4 の IP アドレス。
[IPv6 Address] フィールド	IPv6 の IP アドレス。

ステップ 9 [Next] をクリックします。

ステップ 10 [BMC 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。
[IPv4 Address] フィールド	IPv4 の IP アドレス。
[IPv6 Address] フィールド	IPv6 の IP アドレス。

ステップ 11 [Next] をクリックします。

ステップ 12 [Confirm] 画面で、[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 を使用している場合、サーバの管理 IP アドレスに DHCP を使用するために（このポリシーが適用される）ラック サーバも設定されます。

ネットワーク セキュリティ ポリシー

Cisco IMC Supervisor 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 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 IP プロパティのグループを含む、1 つ以上のネットワーク 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ときに 4 つの IP フィルタリング プロパティを設定できます。IP フィルタリングでは、選択した一連の IP がサーバにアクセスできます。4 つのフィルタ フィールドのいずれも、単一の IP アドレスまたはハイフンで区切った IP アドレス範囲を入力できます。IP アドレスは、IPv4 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 [Hardware Policies] を選択したら、[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 [Add] 画面で、ドロップダウン リストから [Network Security] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力します。

また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[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 （136 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用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て [Next] をクリックします。

ステップ 5 [IP Blocking] ウィンドウで、IP をブロックするために [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 [Next] をクリックします。

ステップ 7 [IP Filtering] 画面で、[Enable IP Filtering] チェックボックスをオンにして IP を有効にし、IP アドレスを 1 つまたは範囲で入力します。

（注） [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 が管理するサーバが NTP サーバと時刻を同期するように設定できます。デフォルトでは NTP サーバは Cisco IMC Supervisor で動作しません。NTP サービスを有効にして設定する必要があります。その際、NTP サーバとして動作する少なくとも 1 台、最大 4 台のサーバの IP/DNS アドレスを指定します。NTP サービスを有効にすると、Cisco IMC Supervisor は設定された NTP サーバと管理されているサーバで時刻を同期します。

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 Network Time 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 [Hardware Policies] を選択したら、[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 [Add] 画面で、ドロップダウン リストから [NTP Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力します。

また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[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 （136 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用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て [Next] をクリックします。

ステップ 5 [Main] 画面で、[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 [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

パスワードの有効期限を設定することができ、その期限を過ぎるとパスワードは期限切れになります。管理者として、この時間を日数で設定できます。この設定は、すべてのユーザに共通です。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 [Hardware Policies] を選択したら、[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 [Add] 画面で、ドロップダウン リストから [Password Expiration Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力します。

ステップ 4 [Main] 画面で、次のフィールドに入力します。

フィールド	説明
[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。 [Password Expiry Duration]：パスワードが期限切れになる日数を設定します。
[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発生数を設定します。
[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。
[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 [Submit] をクリックします。

（注）
- 既存のポリシーを選択し、[Properties] または [Delete] をクリックして、[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

高精度の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。

さまざまなブート順序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 Precision Boot Order*」の項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以上を実行しているサーバに対して作成できます。2.x より前のバージョンを実行しているサーバの場合、代わりにレガシー ブート順序ポリシーを設定する必要があります。

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 [Hardware Policies] を選択したら、[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 [Add] ウィンドウで、ドロップダウン リストから [Precision Boot Order Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力します。

また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[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 （136 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用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て [Next] をクリックします。

ステップ 5 [Main] ウィンドウで、[UEFI Secure Boot] チェックボックスをオンにするか、[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 [+] をクリックして、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リストされます。

また、[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。エントリの順序を変更するには、上/下矢印アイコンを使用します。テーブルのエントリの順序により、ブート順序が決まります。

（注） **HTTP ブート**は、CIMC バージョン4.1（3b）からサポートされます。

ステップ 7 [Add Entry to Select Devices] ページで、[Submit] をクリックします。

ステップ 8 サーバが一回起動する必要があるデバイスを設定するには、[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 [One Time Boot Device] ドロップダウン リストからデバイスを選択します。

（注） [Configure One Time Boot 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ときは、[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

C シリーズまたは E シリーズ サーバに設定されている電力復元ポリシーの値を変更し、この際にサーバの Cisco IMC にログインする必要がないようにする場合に、このポリシーを作成します。

（注） ENCS サーバでこのポリシーを作成することはできません。

手順

ステップ 1 [Hardware Policies] を選択したら、[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 **[Add (追加)]** 画面で、ドロップダウンリストから **[Power Restore Policy (電力復元ポリシー)]** を選択して **[Submit (送信)]** をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力します。

また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[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 （136 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用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て [Next] をクリックします。

ステップ 5 **[Power Restore Policy (電力復元ポリシー)]** から設定を選択します。

次のいずれかのオプションを使用できます。

- **Power Off**
- **電源オン**

  このオプションを選択すると、**[Power Delay Type (電源遅延タイプ)]** フィールドが表示されます。このオプションを使用できるのは Cisco UCS C シリーズ サーバだけです。

- **最後の状態の復元**

ステップ 6 **[Power Delay Type (電源遅延タイプ)]** ドロップダウン リストから値を選択します。

次のいずれかのオプションを使用できます。

- **固定**: このオプションを選択すると、**[Power Delay Value (電源遅延値)]** フィールドが表示されます。
- **ランダム**: このオプションを選択した場合、**[Power Delay Value (電力遅延値)]** フィールドは表示されません。

ステップ 7 **[Power Delay value (電力遅延値)]** フィールドに 0 ~ 240 秒の値を指定します。

ステップ 8 [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 （138 ページ）を参照してください。

RAID ポリシー

RAID ポリシーを使用すると、サーバ上に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 ポリシー内のそれぞれの仮想ドライブは、1 つのディスク 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 ポリシーを使用すると、特定の仮想ドライブに使われるディスクを選択し、設定することができます。

RAID ポリシーは、以下の環境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。

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「*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 [Hardware Policies] を選択したら、[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 [Add] ウィンドウで、ドロップダウン リストから [RAID Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力します。

また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[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 （136 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用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て [Next] をクリックします。

ステップ 5 [Drive Security] ウィンドウで、[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。

重要 **[サーバの現在の設定からポリシーを作成する (Create policy from current configuration of the server)]** チェック ボックスをオンにして、セキュリティ キー ID などのセキュリティ プロパティがサーバに関連付けられているすべてのコントローラ スロットに共通している場合にのみ、ポリシーのドライブ セキュリティ プロパティが取得されます。セキュリティ キー ID がサーバ内のすべてのコントローラで共通でない場合は、ドライブセキュリティ設定の取得に失敗し、その後RAIDポリシーは作成されません。

ステップ 6 [Enable Drive Security] または [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 [Enable Drive Security] を選択し、次のフィールドに入力します。

フィールド	説明
[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。
[Security Key] フィールド	セキュリティ キーを入力します。
[Security Key Identifier] フィールド	セキュリティ キー識別子を入力します。
[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。
[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 [Virtual Drive Configuration] ダイアログボックスで [+] 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。

サーバ上のすべてのコントローラ スロットの仮想ドライブと、それらの仮想ドライブ上の対応するディスク グループ ポリシーが取得され、ユーザー インターフェイスに表示されます。

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。[Add Entry to Virtual Drives] ページで、次のように入力します。

フィールド	説明
[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。 [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	各ストライプのサイズ（KB 単位）。 M2 RAID コントローラは 32K と 64K のみをサポートします。他の RAID コントローラは、64k、128k、256k、612k、および 1024k をサポートします。
[Disk Group Policy] ドロップダウン リスト	[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、または [+] 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 ディスクを指定します。ディスク グループ ポリシー（104 ページ）を参照してください。 （注） 2 つの仮想ドライブが作成されて同じディスク グループ ポリシーに関連付けられた場合、それらは同じ仮想ドライブ 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。
[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。
[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。
[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。

フィールド	説明
[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。
[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。
[Boot Drive] チェックボックス	ブート ドライブとして作成する仮想ドライブを設定します。 （注） 複数のブート ドライブを設定することはできません。
[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。
[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 [Submit] をクリックします。
作成した仮想ドライブは [Virtual Drives] テーブルで確認できます。

ステップ 11 [Delete existing Virtual Drives] チェックボックスをオンにして、サーバ上の既存のすべての仮想ドライブを削除します。

このチェックボックスを選択した場合、ポリシーの適用時に、サーバ上の既存のすべての仮想ドライブが削除されます。この結果、既存のデータが失われることがあります。

ステップ 12 [Next] をクリックします。

ステップ 13 [Physical Drive Configuration] ページで、次のように入力します。

ステップ 14 [Configure Unused Disks] チェックボックスをオンにし、未使用ディスクを [Unconfigured Good] または [JBOD] 状態に設定するオプションを選択します。

（注） [Unconfigured Good] を選択すると、[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、[Enable Secure Drive] チェックボックスが表示されます。

ステップ 15 物理ドライブ上のすべてのデータを削除する場合は [Clear Secure Drive] チェックボックスをオンにし、セキュア ドライブを有効にする場合は [Enable Secure Drive] チェックボックスをオンにします。

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。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 Serial over LAN 属性のグループを含む、1 つ以上の Serial over LAN ポリシーを作成できます。

さまざまな Serial over LAN 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 [Hardware Policies] を選択したら、[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 [Add] 画面で、ドロップダウン リストから [Serial Over LAN Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力します。

また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[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 （136 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用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て [Next] をクリックします。

ステップ 5 [Main] ウィンドウで、[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 Port] 値と [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。

さまざまな SNMP 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 SNMP*」の項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 [Hardware Policies] を選択したら、[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 [Add] 画面で、ドロップダウン リストから [SNMP Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力します。

また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[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 （136 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用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て [Next] をクリックします。

ステップ 5 [SNMP Users] ウィンドウで [+] をクリックして SNMP ユーザを追加し、ユーザの詳細情報を入力します。[+] アイコンを使用して、最大で 15 SNMP ユーザを追加することができます。

既存の SNMP エントリを選択すると、そのエントリを編集またはテーブルから削除できます。

（注） **DES** プライバシー タイプは、CIMC バージョン 4.1（3b）および Cisco IMC Supervisor バージョン 2.3 ではサポートされていません。

ステップ 6 [Next] をクリックします。

ステップ 7 [SNMP Traps] ウィンドウで [+] をクリックして SNMP トラップを追加し、トラップの詳細情報を入力します。[+] アイコンを使用して、最大で 15 個の SNMP トラップを追加することができます。

既存の SNMP エントリを選択すると、そのエントリを編集またはテーブルから削除できます。

ステップ 8 [Next] をクリックします。

ステップ 9 [SNMP Settings] ウィンドウで、SNMP プロパティを設定します。

ステップ 10 [Submit] をクリックします。

（注）
- サーバで以前に設定されていた既存の [SNMP Users] または [SNMP Traps] が削除され、ポリシーで設定したユーザやトラップに置き換わります。ポリシーにユーザやトラップをまだ追加していない場合は、サーバ上の既存のユーザまたはトラップが削除されますが、置き換わりません。
- 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 サーバは、SSH クライアントがセキュアな暗号化された接続を行えるようにします。SSH クライアントは、SSH プロトコルで動作し、デバイスの認証および暗号化を提供するアプリ

ケーションです。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SSHプロパティのグループを含む、1 つ以上の SSH ポリシーを作成することができます。

さまざまな SSH 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 SSH*」の項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 [Hardware Policies] を選択したら、[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 [Add] ウィンドウで、ドロップダウン リストから [SSH Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力します。

また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[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 （136 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用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て [Next] をクリックします。

ステップ 5 [Main] ウィンドウで [Enable SSH] チェックボックスをオンにして、SSH プロパティを入力するか、または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 ポリシーを使用して、ローカル ユーザの設定を自動化できます。1 つのサーバまたはサーバのグループに設定される必要のあるローカル ユーザ リストを含む、1 つ以上のユーザ ポリシーを作成することができます。

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 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 [Hardware Policies] を選択したら、[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 [Add] ウィンドウで、ドロップダウン リストから [User Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力します。

また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[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 （136 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用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て [Next] をクリックします。

ステップ 5 [Main] ウィンドウで、サーバに設定する必要があるユーザを [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適用する場合は、[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) 以上を実行してい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 [Add Entry to Users] 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
Username	ユーザの名前をフィールドに入力します。
ロール（Role）	読み取り専用、管理などのユーザ ロールをドロップダウン リストから選択します。
[Enable User Account]	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（New Password）]	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 [Submit] をクリックします。

ステップ 10 パスワードの有効期限ポリシーを適用するには、[Add Password Expiration Policy] チェックボックスをオンにします。

（注） パスワードの有効期限ポリシーを個別に適用できません。

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（120 ページ）を参照してください。

ステップ 12 [Submit] をクリックします。

また、[Main] ウィンドウの [Users] テーブルで既存のユーザを選択し、[Edit] または [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）
- [Users]テーブルの最初のユーザは、管理ユーザです。この管理ユーザを削除することはできませんが、パスワードは変更できます。
- 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ー エントリが作成されています。CIMC 2.0(8d) 以上を実行しているサーバにポリシーを適用する場合、ブランク ユーザ エントリは作成されません。（以前のポリシーにより適用された）既存のダミー ユーザ エントリはクリアされます。
- Cisco IMC Supervisor の管理に使用されるアカウントが、ポリシーのユーザー 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。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仮想 KVM プロパティのグループを含む、1 つ以上の KVM ポリシーを作成することができます。

さまざまな KVM 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*」の項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 [Hardware Policies] を選択したら、[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 [Add] ウィンドウで、ドロップダウン リストから [Virtual KVM Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力します。

また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[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 （136 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用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て [Next] をクリックします。

ステップ 5 [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 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

さまざまな VIC アダプタ プロパティの設定の詳細については、Cisco UCS C シリーズ サーバの統合管理コントローラ GUI の構成ガイド（Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide） の「*Viewing VIC Adapter Properties*」の項を参照してください。

手順

ステップ 1 [Hardware Policies] を選択したら、[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 [Add] 画面で、ドロップダウン リストから [VIC Adapter Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力します。

また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[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 （136 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用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て [Next] をクリックします。

ステップ 5 [Main] 画面で [+] をクリックして、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 アダプタにエントリを追加 (Add Entry TO VIC Adapters)]** 画面で、次のアダプタの詳細を編集するか、確認することができます。

- **PCI スロット選択**：アダプタを使用可能な PCI スロットまたは特定の PCI スロットに装着するかを指定します。[任意 (Any)] を選択すると、**[PCI スロット (PCI Slot)]** フィールドは表示されません。
- **PCI スロット**：アダプタが装着されている PCI スロット。
- **説明**：アダプタの説明
- **FIP モード**：FCoE Initialization PROTOCOL (FIP) モードを有効にするか無効にするかを指定します。
- **LLDP の設定**：オンにすると、Link Layer Discovery Protocol（LLDP）によってすべての Data Center Bridging Capability Exchange プロトコル（DCBX）機能が有効になります。これには、FCoE、プライオリティ ベースのフロー制御も含まれます。18-06-2020 18:12
- **Vntag モード**：VNTAG モードを有効にするか無効にするかを指定します。
- **ポート チャネル**：ポートチャネルを **[有効 (Enabled)]**、**[無効 (Disabled)]**、または **[適用されない (Not Applicable)]** 状態に設定します。Cisco VIC 1455 および 1457 アダプタの場合、

ポート チャネルはデフォルトで **[有効 (Enabled)]** に設定されています。ポート チャネル設定をサポートしていないアダプタの場合、このフィールドは **[適用されない (Not Applicable)]** に設定されます。vNICs と Vnics は、このフィールドで選択されたポート チャネルの状態に基づいて、デフォルトで設定されます。ポートチャネルの状態を変更すると、既存の設定が最新の設定に上書きされます。**[ポート チャネル (Port Channel)]** フィールドが **[有効 (Enabled)]** または **[適用しない (Not Applicable)]** に設定されている場合、デフォルトで少なくとも 2 個の vNIC (eth0 と Eth1) と 2 個の vHBA (fc0 と fc1) が設定されます。**[ポート チャネル (Port Channel)]** フィールドが **[無効 (Disabled)]** に設定されている場合、最低 4 個の vNIC (eth0、eth1、eth2、および eth3) と 4 個の vhba (fc0、fc1、fc2、および fc3) がデフォルトで設定されます。ただし、これらのアダプタに追加の vHBA または vNIC を作成できます。

- **外部イーサネット インターフェイス**: Cisco VIC 1455、Cisco VIC 1457、Cisco VIC 1495、Cisco VIC 1497 アダプタの管理前方誤り訂正 (FEC) モードを設定します。デフォルトでは、4 個のポートがあり、削除することはできません。ただし、[管理 FEC (Admin FEC)] モードで設定されたポート数は、選択したアダプタに基づきます。たとえば、Cisco VIC 1497 アダプタでは 2 ポートのみです。したがって、[管理 FEC (Admin FEC)] モードは最初の 2 ポート (ポート 0 およびポート 1) でのみ設定されており、残りのポート (ポート 2 およびポート 3) は無視されます。

  既存のポリシーでは、このフィールドは **[自動（Auto）]** に設定されています。しかし、値を **cl91**、**cl74**、**Off** に変更できます。アダプタ モデルが [管理 FEC (Admin FEC)] モードをサポートしていない場合、これらの値は無視されます。

  （注） **cl74**オプションは、Cisco VIC 1495 および Cisco VIC 1497 アダプタではサポートされていません。

- **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のみが可能であり、削除はできません。また、usNIC プロパティでもこれらのプロパティを使用できます。**[ポート チャネル (Port Channel)]** フィールドが **[有効 (Enabled)]** または **[適用しない (Not Applicable)]** に設定されている場合、デフォルトでは 2 個以上の vNIC (eth0 と eth1) が設定され、アップリンク ポートは 0 および 1 となります。**[ポート チャネル (Port Channel)]** フィールドが **[無効 (Disabled)]** に設定されている場合、デフォルトで 0 ~ 3 のアップリンク ポートを使用して、最低 4 個の vNIC、eth0、eth1、eth2、および eth3 が設定されます。ただし、これらのアダプタに追加の vNIC を作成できます。

- **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のみが可能であり、削除はできません。**[ポート チャネル (Port Channel)]** フィールドが **[有効 (Enabled)]** または **[適用しない (Not Applicable)]** に設定されている場合、デフォルトで少なくとも 2 個の vHBA (fc0 と fc1) が設定されます。**[ポート チャネル (Port Channel)]** フィールドが **[無効 (Disabled)]** に設定されている場合、最低 4 個の vHBA、fc0、fc1、fc2、および fc3 がデフォルトで設定されます。ただし、これらのアダプタに追加の vHBA を作成できます。

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。1 つのサーバまたはサーバ セットのニーズに適合する、さまざまな OS イメージ用の vMedia マッピングを含む 1 つ以上の vMedia ポリシーを作成することができます。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。

さまざまな vMedia 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 Virtual Media*」の項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 [Hardware Policies] を選択したら、[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 [Add] 画面で、ドロップダウン リストから [vMedia Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力します。

また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[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 （136 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用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て [Next] をクリックします。

ステップ 5 [Main] ウィンドウで、[Enable vMedia] チェックボックスをオンにして vMedia を有効にし、[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 [Next] をクリックします。

ステップ 7 [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 [Next] をクリックします。

ステップ 9 **[Add HDD vMedia Mapping (HDD vMedia マッピングの追加)** 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 **[Low Power USB State (低電力 USB 状態)]** を設定することはできません。
- vMedia ポリシーを適用すると、ポリシーに vMedia マッピングが含まれない場合でも、それまでサーバに設定されていた既存の 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）ドライブのダイナミック ストレージをサポートしています。このダイナミック ストレージのサポートは、CMC の SAS Fabric Manager によって提供されます。ダイナミック ストレージは次のオプションをサポートしています。

- サーバ 1 およびサーバ 2 への物理ディスクの割り当て
- シャーシ幅ホット 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 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
- 選択した物理ドライブを割り当てるコントローラ スロットを選択できます。

ディスク グループの各種プロパティの設定の詳細については、『Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide for S3260 Servers』の「*Dynamic Storage*」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 [Hardware Policies] を選択したら、[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 [Add] 画面で、ドロップダウン リストから [Zoning Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力します。

また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[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 （136 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 **[Zoning (ゾーニング)]** ウィンドウで **[+]** をクリックして、サーバ上に設定するローカル ディスクを追加します。

ステップ 5 **[Add Entry to Local Disks (エントリをローカル ディスクに追加)]**ウィンドウで、ローカル ディスクが存在する **[Slot Number (スロット番号)]** を入力します。

ステップ 6 **[Ownership (所有権)]** ドロップダウンリストから、ローカル ディスクの所有権を特定のサーバに割り当てます。

ステップ 7 **[Choose controller (コントローラの選択)]** チェックボックスをオンにして、サーバ内の特定のコントローラにローカル ディスクを割り当てます。

ローカル ディスクのコントローラ スロットの選択は必須ではありません。特定のコントローラ スロットを選択しない場合、ゾーン分割ポリシーは、選択したサーバで使用可能な最初のコントローラ スロットに適用されます。

ステップ 8 **[Controller (コントローラ)]**ドロップダウンリストから、サーバの特定のコントローラ名を選択します。

ステップ 9 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、[Force] チェックボックスをオンにします。

ステップ 10 [送信（Submit）] をクリックします。

ステップ 11 ポリシーを設定するには、**[Zoning (ゾーン分割)]** ページで、**[Modify Physical Drive Power Policy (物理ドライブ電源ポリシーの変更)]** チェックボックスをオンにします。

ステップ 12 [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 13 [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

すでに設定済みのサーバを使用してポリシーを作成することもできます。サーバ上の既存の設定を再使用すると、類似する設定を作成するのに必要な時間と労力を軽減できます。

（注） サーバの現在の設定からポリシーを作成するときには、サーバからパスワードフィールドが取得されません。

サーバの現在の設定からポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [Hardware Policies] を選択したら、[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 [Create policy from current configuration of the server] チェックボックスをオンにして、[Next] をクリックします。

ステップ 3 **[Server Details (サーバの詳細)]** 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 S3260 サーバのポリシーを作成している場合は、手順 5 に進みます。

a) [Enter Server Details Manually] チェックボックスをオンにして、次のフィールドに入力します。

1. [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 [Use Credential Policy] チェックボックスをオンにして [Credential Policy] ドロップダウン リストからポリシーを選択するか、[Credential Policy] ドロップダウン リストの横にある [+] をクリックし、[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. [User Name] フィールドにサーバ ログイン名を入力します。
4. [Password] フィールドにサーバ ログイン パスワードを入力します。
5. [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. [Port] フィールドに、選択したプロトコルに関連付けられるポート番号を入力します。

b) [Select] をクリックして、設定の取得元となるサーバを選択します。

ステップ 4 [Next] をクリックします。

[Main] 画面に進みます。ポリシーの作成を続けます。

ステップ 5 Cisco UCS S3260 サーバの場合は、[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、[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。このポリシーは E シリーズ サーバでのみ作成できます。

ステップ 6 [Server Details] 画面で [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 [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 [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 [Use Credential Policy] チェックボックスをオンにして [Credential Policy] ドロップダウン リストからポリシーを選択するか、[Credential Policy] ド

ロップダウン リストの横にある [+] をクリックし、[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. [User Name] フィールドにサーバ ログイン名を入力します。
4. [Password] フィールドにサーバ ログイン パスワードを入力します。
5. [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. [Port] フィールドに、選択したプロトコルに関連付けられるポート番号を入力します。

ステップ 7 [Server Node 1] または [Server Node 2] のオプション ボタンを選択します。

ステップ 8 [Next] をクリックします。

[Main] 画面に進みます。ポリシーの作成を続けます。

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 **[Policies]** > **[Manage Policies and Profiles]** を選択します。

ステップ 2 [Manage Policies and Profiles] ページで、[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 上部にある利用可能なオプションから、[Apply] をクリックします。
[Apply Policy] 画面で、ポリシーを適用する [Chassis] または [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 [Select] をクリックして、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） **[Select (選択)]** で、C シリーズ サーバ (Cisco UCS 3260 サーバを除く)、E シリーズ サーバ、ENCS サーバなどのすべてのサーバが表示されます。電源ポリシーを適用している場合、ENCS サーバはグレー表示され、これらのサーバを選択することはできません。Cisco UCS 3260 サーバの電源ポリシーを作成している場合は、[Select (選択)] をクリックすると、Cisco UCS 3260 サーバのみが表示されます。他のサーバは表示されません。

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（195 ページ）を参照してください。

ステップ 6 ポリシー タスクの適用を後でスケジュールするには、[Schedule Later] チェックボックスをオンにします。

ステップ 7 [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、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（179 ページ）を参照してください。

（注） [Policies] > [Manage Schedules] の順に移動して、スケジュールを選択し、[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 [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 [Submit] をクリックします。

指定したサーバセットにポリシーを適用するプロセスが開始します。ポリシーの種類、およびポリシーが適用されるサーバへのネットワーク接続に応じて、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 ポリシーでの一般タスク

既存のポリシーのサーバマッピング詳細を編集、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 **[Policies]** > **[Manage Policies and Profiles]** を選択します。

ステップ 2 [Manage Policies and Profiles] ページで、[Hardware Policies] をクリックします。

ステップ 3 [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。オプションで次の手順を実行することができます。

a) （任意） ポリシーを削除するには、[Delete] をクリックします。[Delete Policy] ダイアログボックスで [Select] をクリックし、削除するポリシーを選択します。[Select] および [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、エラーになります。

b) （任意） ポリシーを変更するには、[Properties] をクリックし、必要に応じてプロパティを変更します。

ポリシー名を変更するときには、すでに存在する名前を指定しないでください。

c) （任意） ポリシーを複製するには、[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） [View Details] をクリックすると、すでに適用したポリシーのステータス、およびポリシーが適用されたサーバ IP アドレスが表示されます。ポリシーが正常に適用されない場合、[Status Message] 列にエラー メッセージが表示されます。

ステップ 4 サーバまたはサーバ グループにポリシーを適用するには、[Apply] をクリックします。プロファイルを適用する方法の詳細については、ハードウェア ポリシーの適用 （138 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

複数のポリシーを組み合わせて、ハードウェア プロファイルが形成されます。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。これにより、複数のサーバにわたって設定の一貫性と反復可能性が確保されます。プロファイルを定義して使用すると、類似する設定が多数のサーバに適用されるため、一貫性、制御、予測可能性、自動化が促進されます。

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 （141 ページ）を参照してください。
    2. サーバ上の既存の設定からプロファイルを作成します。サーバ上の既存の設定からプロファイルを作成する方法の詳細については、既存の設定からのプロファイルの作成 （141 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。プロファイルを適用する方法の詳細については、ハードウェア プロファイルの適用 （143 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. Edit
    2. 削除
    3. Clone

    また、特定のプロファイルにマップされるサーバのリストを表示して、このプロファイルに関連付けられているポリシーの詳細を表示することもできます。これらのタスクの実行方法の詳細については、ハードウェア プロファイルでの一般タスク （144 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 **[Policies]** > **[Manage Policies and Profiles]** を選択します。

ステップ 2 [Manage Policies and Profiles] ページで、[Hardware Profiles] をクリックします。

ステップ 3 [Add] をクリックします。

ステップ 4 [Hardware Profile] 画面で、作成するプロファイルの名前を [Profile Name] フィールドに入力します。

既存のサーバ構成を使用する場合は、[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。これにより、[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」を参照してください。

ステップ 5 Cisco UCS S3260 サーバ用のプロファイルの場合は、[Cisco UCS S3260] チェックボックスをオンにして [Next] をクリックします。

ステップ 6 [Profile Entities] ウィンドウで [+] をクリックして、プロファイル エントリを追加します。

[Delete] アイコンをクリックして、既存のエントリを削除することもできます。

ステップ 7 [Add Entry to Profile Name] ウィンドウで、[Policy Type] を選択します。

ステップ 8 作成済みのポリシーの名前が一覧表示される [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。

[Policy Name] の横にある [+] をクリックすると、選択したポリシー タイプに基づき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 （101 ページ）」を参照してください

ステップ 9 [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 [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、選択されたプロファイルにマップされるサーバを表示したりできます。ハードウェア プロファイルでの一般タスク （144 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

すでに設定済みの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。サーバ上の既存の設定を再使用すると、類似する設定を作成するのに必要な時間と労力を軽減できます。

（注） サーバの現在の設定からプロファイルを作成するときには、サーバからパスワードフィールドが取得されません。

サーバの現在の設定からプロファイルを作成するには、次の手順を実行します。

手順

ステップ 1 **[Policies]** > **[Manage Policies and Profiles]** を選択します。

ステップ 2 [Manage Policies and Profiles] ページで、[Hardware Profiles] をクリックします。

ステップ 3 [Add] をクリックします。

ステップ 4 プロファイルの名前を [Name] フィールドに入力します。

ステップ 5 [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) [Enter Server Details Manually] チェックボックスをオンにして、次のフィールドに入力します。

1. [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 [Use Credential Policy] チェックボックスをオンにして [Credential Policy] ドロップダウン リストからポリシーを選択するか、[Credential Policy] ドロップダウン リストの横にある [+] をクリックし、[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. [User Name] フィールドにサーバ ログイン名を入力します。
4. [Password] フィールドにサーバ ログイン パスワードを入力します。
5. [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. [Port] フィールドに、選択したプロトコルに関連付けられるポート番号を入力します。
7. [Select] をクリックし、ポリシーを選択して [Select] をクリックします。

b) [Select] をクリックして、設定の取得元となるサーバを選択します。

c) [Select] をクリックし、ポリシーを選択して、[Select] をクリックします。

ステップ 6 [Next] をクリックします。

ステップ 7 [Profile Entities] ウィンドウで [+] をクリックして、プロファイル名にエントリを追加します。

[Profile Name] テーブルから既存のエントリを削除するには、[x] をクリックします。

ステップ 8 [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て、[Next] をクリックします。

a) [Enter Server Details Manually] チェックボックスをオンにして、次のフィールドに入力します。

1. Cisco UCS S3260 プラットフォームの [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 [Use Credential Policy] チェックボックスをオンにして [Credential Policy] ドロップダウン リストからポリシーを選択するか、[Credential Policy] ドロップダウン リストの横にある [+] をクリックし、[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. [User Name] フィールドにサーバ ログイン名を入力します。
4. [Password] フィールドにサーバ ログイン パスワードを入力します。
5. [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. [Port] フィールドに、選択したプロトコルに関連付けられるポート番号を入力します。
7. [Select] をクリックし、ポリシーを選択して [Select] をクリックします。

b) [Select] をクリックして、設定の取得元となるサーバを選択します。
c) [Select] をクリックし、サーバから作成するポリシーを選択して、[Select] をクリックします。

ステップ 10 [Next] をクリックします。

ステップ 11 [Profile Entities] ウィンドウで [+] をクリックして、プロファイル名にエントリを追加します。

[Profile Name] テーブルから既存のエントリを削除するには、[x] をクリックします。

（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、[Apply Policy To] フィールドでサーバ ノードを指定する必要があります。例、[Server-1]、[Server-2]、および [Both]。管理ポリシーの場合、このフィールドは関係ありません。

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 **[Policies]** > **[Manage Policies and Profiles]** を選択します。

ステップ 2 [Manage Policies and Profiles] ページで、[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、[Apply] をクリックします。

[Apply Profile] 画面で、プロファイルの適用先として [Chassis]（Cisco UCS S3260 タイプのプロファイルに適用可能）または [Server(s)] を選択できます。これらのオプションを選択したサーバ プラットフォームに基づいて表示されます。

ステップ 4 [Apply Profile] ダイアログボックスで、[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 タスクの適用を後でスケジュールするには、[Schedule Later] チェックボックスをオンにします。

ステップ 6 [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、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（179 ページ）を参照してください。

（注） [Policies] > [Manage Schedules] の順に移動して、スケジュールを選択し、[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 [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 [Submit] をクリックします。

指定したサーバ セットにプロファイルを適用するプロセスが開始します。プロファイルの種類、およびプロファイルが適用されるサーバへのネットワーク接続に応じて、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 プロファイルでの一般タスク

既存のプロファイルのサーバマッピング詳細を編集、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 **[Policies]** > **[Manage Policies and Profiles]** を選択します。

ステップ 2 [Manage Policies and Profiles] ページで、[Hardware Profiles] をクリックします。

ステップ 3 [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、[Delete] をクリックします。[Delete Profile] ダイアログボックスの [Select] をクリックし、1 つ以上のプロファイルを選択して、[Select] をクリックします。[送信（Submit）] をクリックするとプロファイルが削除されます。

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、[Edit] をクリックして、必要に応じてプロパティを変更します。

プロファイル名を変更するときには、すでに存在する名前を指定しないでください。

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、[Clone] をクリックします。
d) （任意） サーバまたはサーバ グループにプロファイルを適用するには、[Apply] をクリックします。ハードウェア プロファイルの適用 （143 ページ）を参照してください。
e) （任意）[View Details] をクリックすると、すでに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が適用されたサーバ 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ない場合、[Status Message] 列にエラー メッセージが表示されます。

ステップ 4 状況に応じて [Submit] または [Close] をクリックします。

タグ ライブラリ

オブジェクトにラベルを割り当てる場合にタグ付けを行います。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を付けることを決定できます。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のタイプのアカウントにタグを適用することもできます。

[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
Name	タグ ライブラリのユーザ定義名。
[Description]	タグ ライブラリのユーザ定義の簡単な説明。
[Type]	文字列または整数。
[Possible Tag Values]	ユーザ定義のタグ値。
[Applies To]	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 **[Policies]** > **[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 **[Create Tag (タグの作成)]** 画面で、**[Tag Details (タグの詳細)]** の次のフィールドに入力します。

フィールド	説明
[Name] フィールド	タグの記述名。

フィールド	説明
[Description] フィールド	（オプション）タグの説明。
[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。
[Possible Tag Values] フィールド	タグに使用できる値。

ステップ 4 [Next] をクリックします。

ステップ 5 [Applicability Rules] ペインで、次の手順を実行します。

名前	説明
[Taggable Entities] フィールド	タグを適用する必要がある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、以下を実行します。 **1.** [+] アイコンをクリックします。 **2.** [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.** [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

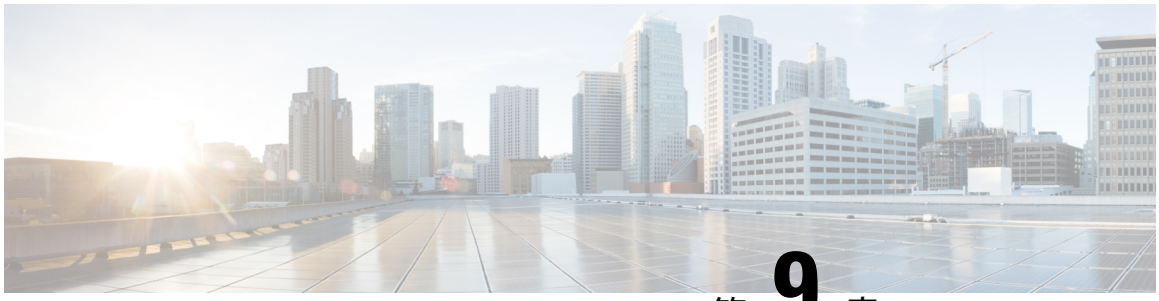
[REST API Browser (REST API ブラウザ)] 画面には、Cisco IMC Supervisor で提供されておりユーザーが使用できる API のリストが表示されます。API は次のグループに分類されます。

- ファームウェア管理のタスク
- 一般的な作業
- 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
- サーバー タスク
- ユーザー 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 **[Favorites (お気に入り)]** に追加する
- **[Search (検索)]** または **[Advanced Filter (高度なフィルタ)]** 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、次の内容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、Cisco 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 （39 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 **[Systems]** > **[Inventory and Fault Status]** を選択します。

ステップ 2 **[Rack Servers (ラック サーバ)]** でラック サーバを選択するか、**[Rack Groups (ラック グループ)]** 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 **[Manage OS Tag For HCR (HCR の OS タグを管理)]**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 **[Operating System Vendor (オペレーティング システムのベンダー)]** を選択します。

ステップ 5 ドロップダウンリストから **[Operating System Version (オペレーティング システムのバージョン)]** 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、**[Administration (管理)]** > **[System (システム)]** > **[System Tasks (システム タスク)]** 画面にある **[Synchronize Hardware Compatibility Reports (ハードウェア互換性レポートの同期)]** 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 **[Delete OS Tag For HCR (HCR の OS タグを削除)]** 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 （39 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 （150ページ）」を参照してください。

手順

ステップ 1 **[Policies]** > **[Hardware Compatibility Report]** の順に選択します。

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 **[Select Profile (プロファイルの選択)]** フィールドにプロファイル名を入力します。

ステップ 4 **[Choose Server (サーバの選択)]** 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 [検証（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。
[Hardware Compatibility Report (ハードウェア互換性レポート)] 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、**[Hardware Compatibility Report (ハードウェア互換性レポート)]**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、**[Delete (削除)]**、**[Edit (編集)]**、**[Synchronize HCL Report(s) (HCL レポートを同期)]**、または **[View Status Details (ステータス詳細の表示)]** 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。コンプライアンスは次のいずれかの状態になります。

- 完全に準拠: 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: 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: 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。
- エラーまたは決定不能] 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

[Synchronize Hardware Compatibility Reports (ハードウェア互換性レポートの同期)] 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 （39 ページ）」を参照してください。

手順

ステップ 1 **[Administration]** > **[System]** を選択します。

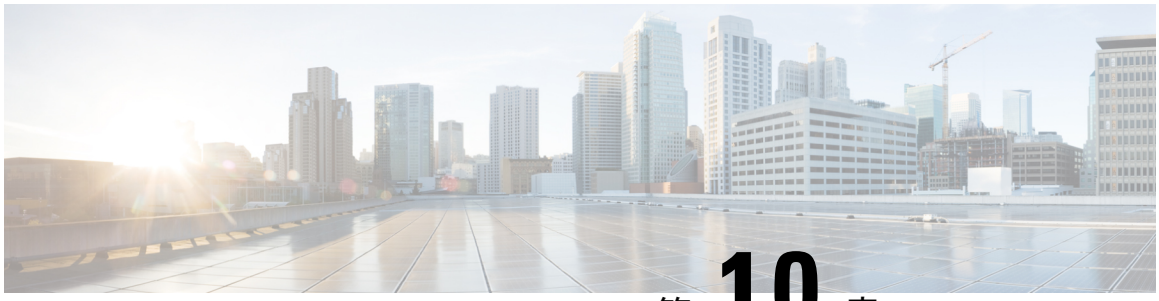
ステップ 2 **[System (システム)]** ページで、**[System Tasks (システム タスク)]** をクリックします。

ステップ 3 **[Rack Server Tasks (ラック サーバ タスク)]** を展開し、**[Synchronize Hardware Compatibility Reports (ハードウェア互換性レポートの同期)]** を選択します。

ステップ 4 **[Run Now (今すぐ実行)]** をクリックします。

ステップ 5 **[Submit (送信)]** をクリックします。

（注） [Hardware Compatibility Report (ハードウェア互換性レポート)] ページからレポートを手動で同期するには、**[Synchronize HCL Report (HCL レポートを同期)]** 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、次の内容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。

Cisco 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 ファームウェア イメージをダウンロードするには、cisco.com アカウントへの契約アクセスの関連付けを行う必要があります。

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。E シリーズ サーバでこのタスクを実行することはできません。E シリーズ サーバにファームウェア イメージを追加するには、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（155 ページ） を参照してください。

（注） Cisco IMC Supervisor バージョン 2.2(0.3) 以降、**イメージ - ローカル**、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 **[Systems]** > **[Firmware Management]** を選択します。

ステップ 2 [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 **[Add Firmware Image - Local (ファームウェアイメージの追加 - ローカル)]** 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	プロファイルを記述する一意の名前を入力します。
[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。 少なくとも 1 つのサーバを管理するプラットフォームだけがここにリストされます。
[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。
[Download Now] チェックボックス	プロファイルの追加後、ただちに .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。そうでない場合は、[Download Image] をクリックして、後でイメージをダウンロードすることができます。
[Graceful Timeout (グレースフル タイムアウト)] 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。
[Timeout (in mins) (タイムアウト（分）)] 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。
[Force Shutdown Server (サーバの強制シャットダウン)] チェックボックス	**[（Graceful Timeout (in mins) (グレースフル タイムアウト（分）)]** 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。

フィールド	説明
[Allow Downloads for Images having Software Advisory (ソフトウェアアドバイザリを含むイメージのダウンロードを許可します)] チェックボックス	ソフトウェア アドバイザリが関連付けられている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。
ライセンス契約に同意する	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。[Terms and Conditions] リンクをクリックすると、エンド ユーザ ライセンス契約書を確認できます。 （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。
- [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になるファームウェア プロファイルの場合は、[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、[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、この手順に従います。

（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 **[Systems]** > **[Firmware Management]** を選択します。

ステップ 2 **[Upload (アップロード)]**を選択してイメージを追加します。

ステップ 3 **[Upload Firmware Image - Local (ファームウェアイメージのアップロード - ローカル)]**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	プロファイルを記述する一意の名前を入力します。
[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、**[Select a File (ファイルを選択)]**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。
[Graceful Timeout (グレースフル タイムアウト)]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。
[Timeout (in mins) (タイムアウト（分）)] 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。
[Force Shutdown Server (サーバの強制シャットダウン)]チェックボックス	**[（Graceful Timeout (in mins) (グレースフル タイムアウト（分）)]** 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。
- [Delete Profile] オプションを使用すると、プロファイルに関連付けられたイメージを削除できます。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提供することで、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 **[Systems]** > **[Firmware Management]** を選択します。

ステップ 2 **[Firmware Management (ファームウェア管理)]** ページで **[Images - Network (イメージ - ネットワーク)]**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 **[Add Firmware Image - Network (ファームウェアイメージの追加 - ネットワーク)]** 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	プロファイルを記述する一意の名前。プロファイル名は固有である必要があります。
[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。 少なくとも 1 つのサーバを管理するプラットフォームだけがここにリストされます。
[Mount Type] ドロップダウン リスト	[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。
[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。

フィールド	説明
[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。
[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。
[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。
[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。
[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。
[Mount Options] ドロップダウン リスト（CIFS サーバ タイプの場合のみ）	[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。
[Graceful Timeout (グレースフル タイムアウト)] 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。
[Timeout (in mins) (タイムアウト（分）)] 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。
[Force Shutdown Server (サーバの強制シャットダウン)] チェックボックス	**[（Graceful Timeout (in mins) (グレースフル タイムアウト（分）)]** 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) より前のバージョンの Cisco IMC を実行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 （39 ページ）およびプロキシ設定 （39 ページ）を参照してください。

手順

ステップ 1 **[Systems]** > **[Firmware Management]** を選択します。

ステップ 2 **[Firmware Management (ファームウェア管理)]** 画面で **[Firmware Upgrades (ファームウェア アップグレード)]** をクリックします

ステップ 3 [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のアップデート 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、サーバがリブートして元のホスト OS が起動します。

ステップ 4 [OK] をクリックして確定します。

ステップ 5 [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
[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。
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。
[Image Version]	
[Image Path]	
[Server (サーバ)] 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。
[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。[+]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。スケジュール作成の詳細については、スケジュールの作成 （179 ページ） を参照してください。**[Policies]** > **[Manage Schedules]** の順に移動してスケジュールを選択し、[View Scheduled Tasks] をクリックしてスケジュールされたタスクとその進行状況を確認できます。また、スケジュールされたタスクを選択し、[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 [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（161 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 （164 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 （161 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 **[Systems]** > **[Firmware Management]** を選択します。

ステップ 2 **[Firmware Management (ファームウェア管理)]** ページで、**[Host Image Mapping (ホスト イメージ マッピング)]** クリックします。

ステップ 3 **[Network Profile (ネットワーク プロファイル)]** 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 **[Create Host Image Mapping Profile - Network (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)]** 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。

[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。
[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。
[File Type (ファイル タイプ)]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**
[File Name] フィールド	ファイルの名前を入力します。
[User name] フィールド	ユーザ名。 （注） このフィールドは、**[Download Image From (イメージのダウンロード元)]** ドロップダウンリストで **[FTP Server (FTP サーバ)]** または **[FTPS Server (FTPS サーバ)]** を選択した場合にのみ表示されます。

[Password] フィールド	ユーザのパスワード。 （注） このフィールドは、**[Download Image From (イメージのダウンロード元)]** ドロップダウンリストで **[FTP Server (FTP サーバ)]** または **[FTPS Server (FTPS サーバ)]** を選択した場合にのみ表示されます。
[Map After Download (ダウンロード後のマッピング)] 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、**[File Type (ファイル タイプ)]** 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（170 ページ）を参照してください。
[Delete All Existing Images (既存のすべてのイメージを削除)] 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。

[Run Upgrade After Download (ダウンロード後にアップグレードを実行)] 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 （169 ページ） を参照してください。 **重要** **[File Type (ファイル タイプ)]** 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、**[Map After Download (ダウンロード後のマッピング)]** 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 （167 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 **[Systems]** > **[Firmware Management]** を選択します。

ステップ 2 **[Firmware Management (ファームウェア管理)]** ページで、**[Host Image Mapping (ホスト イメージ マッピング)]** クリックします。

ステップ 3 **[Upload Proifle (プロファイルのアップロード)]**を選択します。

ステップ 4 **[Create Host Image Mapping Profile - Upload (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)]** 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	プロファイルを記述する一意の名前。プロファイル名は固有である必要があります。
[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。
[File Type (ファイル タイプ)]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
[File Name] フィールド	**[Select a File (ファイルを選択)]** 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
[Map After Download (ダウンロード後のマッピング)] 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、**[File Type (ファイル タイプ)]** 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（170 ページ）を参照してください。
[Delete All Existing Images (既存のすべてのイメージを削除)]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。
[Run Upgrade After Download (ダウンロード後にアップグレードを実行)] 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 （169 ページ） を参照してください。 重要 **[File Type (ファイル タイプ)]** 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、**[Map After Download (ダウンロード後のマッピング)]** 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 （167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 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 **[Run Upgrade After Download (ダウンロード後にアップグレードを実行)]** 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、**[View Status (ステータスの表示)]** 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 **[Systems]** > **[Firmware Management]** を選択します。

ステップ 2 **[Firmware Management (ファームウェア管理)]** ページで、**[Host Image Mapping (ホスト イメージ マッピング)]** 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、**[Apply (適用)]**をクリックします。

あるいは、プロファイルを選択して、**[More Actions (その他の操作)]**ドロップダウン リストから **[Apply (適用)]** を選択できます。

ステップ 4 **[Apply Profile (プロファイルの適用)]** 画面で **[Select (選択)]**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 **[Select (選択)]** をクリックし、**[Apply Profile (プロファイルの適用)]** 画面に戻ります。

ステップ 6 **[Schedule Later (後でスケジュール)]** チェックボックスをオンにして、このプロセスを完了する必要がある日付と時刻を選択します。

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できます。

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（179ページ）を参照してください。

ステップ 7 [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 [Download Now (今すぐダウンロード)] チェックボックスをオフにしています。

手順

ステップ 1 **[Systems]** > **[Firmware Management]** を選択します。

ステップ 2 **[Firmware Management (ファームウェア管理)]** ページで、**[Host Image Mapping (ホスト イメージ マッピング)]** 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 **[More Actions (その他の操作)]** ドロップダウン リストから **[Download Image (イメージのダウンロード)]** を選択します。

ステップ 5 **[Download Image (イメージのダウンロード)]**画面に表示される情報を確認し、**[Download (ダウンロード)]** 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 （170 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 **[Run Upgrade After Download (ダウンロード後にアップグレードを実行)]** 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 **[Systems]** > **[Firmware Management]** を選択します。

ステップ 2 **[Firmware Management (ファームウェア管理)]** ページで、**[Host Image Mapping (ホスト イメージ マッピング)]** クリックします。

ステップ 3 **[Run Upgrade (アップグレードの実行)]**を選択します。

ステップ 4 **[Upgrade Host Image (ホスト イメージのアップグレード)]** 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
[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。
[Servers] フィールド	**[Select (選択)]** 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。

フィールド	説明
[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（179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 **[Systems]** > **[Firmware Management]** を選択します。

ステップ 2 **[Firmware Management (ファームウェア管理)]** ページで、**[Host Image Mapping (ホスト イメージ マッピング)]** 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 **[More Actions (その他の操作)]** ドロップダウン リストから **[Delete Image (イメージの削除)]** を選択します。

ステップ 5 **[Delete Image(s) (イメージの削除)]** 画面で、**[Delete (削除)]** 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 **[Systems]** > **[Inventory and Fault Status]** を選択します。

ステップ 2 **[Rack Groups (ラック グループ)]**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、[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 **[View Details (詳細の表示)]** 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 **[Host Images (ホスト イメージ)]**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、**[Map Image (イメージのマッピング)]**、**[Unmap Image (イメージのマップ解除)]**、**[Delete Image (イメージの削除)]** 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 **[Delete Image (イメージの削除)]**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 **[Systems]** > **[Firmware Management]** を選択します。

ステップ 2 **[Firmware Management (ファームウェア管理)]** ページで、**[Host Image Mapping (ホスト イメージ マッピング)]** 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、**[More Actions (その他の操作)]**ドロップダウン リストから **[View Status Details (ステータス詳細の表示)]**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 **[View Status Details (ステータス詳細の表示)]** を選択することもできます。

[View Host Image Mapping Profile Status (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)] 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 **[Systems]** > **[Firmware Management]** を選択します。

ステップ2 **[Firmware Management (ファームウェア管理)]** ページで、**[Host Image Mapping (ホスト イメージ マッピング)]** 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、**[Delete Profile (プロファイルの削除)]** をクリックします。

ステップ4 **[Delete Profile (プロファイルの削除)]** 画面で、**[Delete (削除)]** 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。

SD カードからのファームウェア アップグレード

管理者は、Miscro SDカードまたはFlexFlashカードにISOイメージをダウンロードすることにより、ラック サーバにファームウェアのアップグレードを実行できるようになりました。ユーザー インターフェイスには次のオプションが用意されており、これらのファームウェア アップグレードを実行できます。

- **[Download Image (イメージのダウンロード)]**: 特定のサーバのファームウェア イメージをダウンロードするには、このオプションを使用します。イメージのダウンロード後すぐにファームウェア アップグレードを開始するように選択することもできます。「SD カードへのファームウェア イメージのダウンロード （173 ページ）」を参照してください。
- **[Run Upgrade (アップグレードの実行)]**: イメージのダウンロード後、後の時点でファームウェア アップグレードを開始するには、このオプションを使用します。「SD カードからファームウェア アップグレードの実行 （174 ページ）」を参照してください。
- [Delete Status Messages (ステータス メッセージの削除)]: ユーザー インターフェイスからすべてのファームウェア アップグレード関連のステータス メッセージを削除するには、こ

のオプションを使用します。「イメージのダウンロードメッセージの削除（175ページ）」を参照してください。

これらのオプションを使用するには、最初にシステムでラック アカウントを作成してから、システムでローカル イメージ プロファイルまたはネットワーク イメージ プロファイルのいずれかを作成する必要があります。これらのプロファイルの作成の詳細については、ローカル サーバへのイメージの追加（153ページ）およびネットワーク サーバからのイメージの追加（157ページ）を参照してください。

SD カードへのファームウェア イメージのダウンロード

始める前に

- ラック アカウントがシステムに追加されます。
- ローカルおよびネットワークのイメージ プロファイルがシステムに作成されます。
- Cisco UCS M4 サーバで、FlexFlash コントローラが、ミラー モードではなく Util モードで設定されていることを確認します。コントローラがミラーモードに設定されている場合、ISO ファイルを SD カードにダウンロードすることはできません。FlexFlash ポリシーを使用して、Util モードでコントローラを設定します。

手順

ステップ 1 **[Systems]** > **[Firmware Management]** を選択します。

ステップ 2 **[Firmware Upgrades - SD (ファームウェア アップグレード - SD)]** を選択します。

ステップ 3 **[Download Image (イメージのダウンロード)]** を選択します。

ステップ 4 **[Upgrade Host Image (ホスト イメージのダウンロード)]** 画面で、次を含む必須フィールドに入力します。

フィールド名	説明
[Download Image From] ドロップダウン リスト	イメージをダウンロードするためにローカル プロファイルを使用するか、ネットワーク プロファイルを使用するか選択します。
[Select Profile] ドロップダウン リスト	プロファイルをリストから選択します。このドロップダウン リストには、M4 および M5 サーバのみのプロファイルが表示されます。

フィールド名	説明
[Run Upgrade After Download (ダウンロード後にアップグレードを実行)] チェックボックス	イメージがダウンロードされた後、ファームウェア アップグレード プロセスが開始する必要がある場合、このチェックボックスをオンにします。 デフォルトでは、このチェックボックスはオフになっています。
[Servers] フィールド	**[Select (選択)]** をクリックして、ファームウェア アップグレード プロセスをオンにするサーバのチェックボックスをオンにします。 **[Select (選択)]** をクリックして、**[Download Image (イメージのダウンロード)]** 画面に戻ります。

ステップ 5 [送信（Submit）] をクリックします。

選択したサーバにファームウェア イメージがダウンロードされます。

次のタスク

サーバでファームウェア アップグレードが開始されます。「SD カードからファームウェア アップグレードの実行 （174 ページ）」を参照してください。

SD カードからファームウェア アップグレードの実行

始める前に

[Download Image (イメージのダウンロード)] オプションを使用してこのファームウェア イメージをダウンロードしました。「SD カードへのファームウェア イメージのダウンロード （173 ページ）」を参照してください。

手順

ステップ 1 **[Systems]** > **[Firmware Management]** を選択します。

ステップ 2 **[Firmware Upgrades - SD (ファームウェア アップグレード - SD)]** を選択します。

ステップ 3 [Run Upgrade] をクリックします。

ステップ 4 **[Select (選択)]** をクリックして、ファームウェア アップグレード プロセスをオンにするサーバのチェックボックスをオンにします。

ステップ 5 [選択 (Select)] をクリックします。

ステップ 6 [提出 (Submit)] をクリックします。`

ファームウェアのアップグレード プロセスは、選択したサーバで開始されます。**[Images -SD (イメージ-SD)]** 画面からアップグレードの進行状況を確認できます。ステータスが **[Upgrade status (アップグレード ステータス)]** 列に表示されます。

イメージのダウンロード メッセージの削除

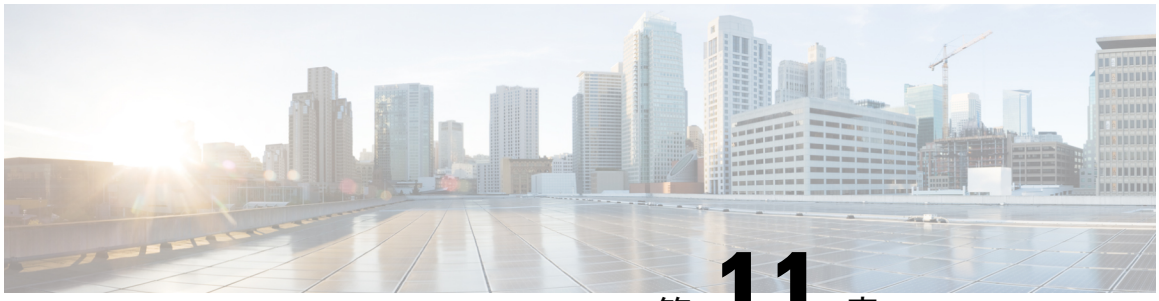
手順

ステップ 1 **[Systems]** > **[Firmware Management]** を選択します。

ステップ 2 **[Firmware Upgrades - SD (ファームウェア アップグレード - SD)]** を選択します。

ステップ 3 リストからプロファイルを選択し、**[Delete Status (ステータスの削除)]** をクリックします。

ステップ 4 **[Delete Image Download Messages（イメージ ダウンロード メッセージの削除)]** 画面で、**[Delete (削除)]** をクリックします。



第 11 章

Cisco IMC Supervisor パッチの更新

この章は、次の内容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、Cisco 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、[Location] に **/opt/infra/uploads/external/downloads/imcs/<*filename.zip*>** と表示されている場合は、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、署名済みパッチを適用できます。署名済みパッチの適用に関する詳細については、『Cisco IMC Supervisor Shell ガイド』の「署名済みパッチを *Cisco IMC Supervisor* に適用する」の項を参照してください。[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 **[Administration]** > **[Update IMCS]** を選択します。

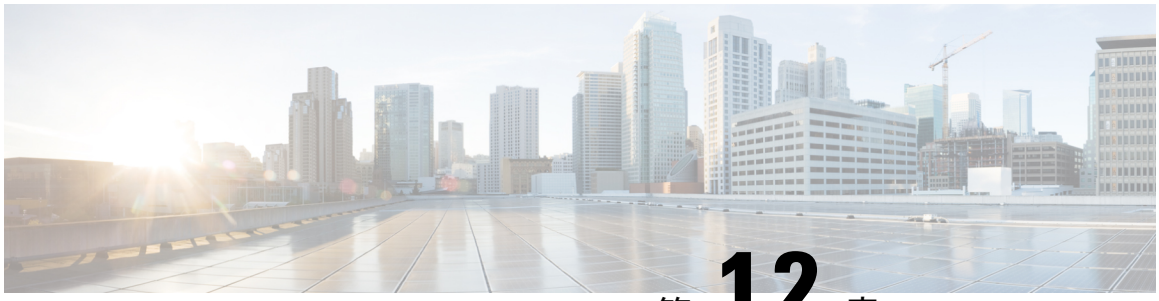
ステップ 2 [Update IMCS (IMCS の更新)] ページで **[Check For Updates Now (今すぐ更新を確認)]** を使用して、Cisco IMC Supervisor の更新を確認します。

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 [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 **[Generate Report (レポートの生成)]** をクリックして、レポートを生成します。

ステップ 6 [Download] をクリックしてレポートをダウンロードするか、または [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、次の内容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発生するように保留することができます。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に定義した時刻または事前に定義した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には、次の手順を実行します。

手順

ステップ 1 **[Policies]** > **[Manage Schedules]** を選択します。

ステップ 2 **[Manage Schedules (スケジュールの管理)]** ページで、**[Add (追加)]** をクリックします。

ステップ 3 [Create Schedule] ダイアログボックスで、次の情報を入力します。

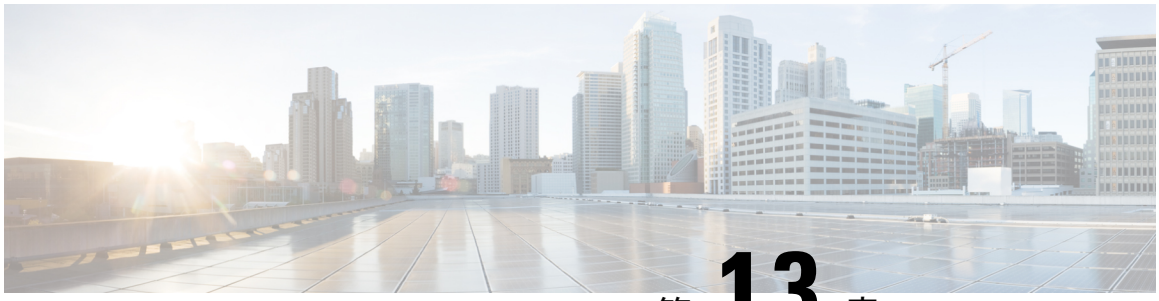
フィールド	説明
[Schedule Name (スケジュール名)] フィールド	スケジュール タスクの名前を入力します。

フィールド	説明
[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により（[Enable] または [Disable] オプションを使用）、スケジュールに関連付けられているタスクの実行を有効または無効にできます。
[Scheduler Type] オプション ボタン	1 回限りのスケジュールか、繰り返しのスケジュール間隔を選択します。 [One Time] スケジュールを選択した場合は、日付、時刻、および AM または PM 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。 [Recurring] スケジュールを選択した場合は、日数（0 ～ 30 日）、時間と分数をドロップダウン リストから選択します。

ステップ 4 [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、スケジュール済みタスクの変更、削除、確認ができます。[View Scheduled Tasks] には、ファームウェアのアップグレード、自動検出のステータスを確認できるレポートが表示されます。また、「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 （138 ページ）、または ハードウェア プロファイルの適用 （143 ページ） で、スケジュールに関連付けられた適用ポリシーやプロファイル タスクのステータスを確認できるレポートも表示されます。
- 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、[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、次の内容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。これとしてずっと早く実行する診断は、その場所内のサーバとイメージの間の低遅延ネットワークが容易になります。

任意のラック サーバで診断を実行すると、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、SFTPユーザーパスワードを設定する必要があります。SFTPユーザー パスワードを設定するには、SFTP ユーザー パスワードの設定 （37 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して保存するには、次の手順を実行します。

手順

ステップ 1 **[Systems]** > **[Server Diagnostics]** を選択します。

ステップ 2 [SCU Image Profiles] をクリックします。

ステップ 3 [Server Diagnostics (サーバ診断)] ページで、**[+]** をクリックします。

ステップ 4 **[Configure SCU Image Location (SCU イメージの場所の設定)]** 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 Share Type] ドロップダウンリスト	[Network File System (NFS)]、[Common Internet File System (CIFS)]、[World Wide Web (WWW)]、または [LOCAL] 共有タイプを選択します。
[LOCAL] を選択する場合	
[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 Share IP] フィールド	ISO 共有 IP アドレスを入力します。
[ISO Share Path] フィールド	ISO 共有パスを入力します。
[Username] フィールド	ISO 共有ログイン ユーザ名を入力します。
[Password] フィールド	ISO 共有ログイン 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 **[Systems]** > **[Server Diagnostics]** を選択します。

ステップ 2 [Run Diagnostics] をクリックします。

ステップ 3 **[Run Diagnostics (診断の実行)]** ページで、次のフィールドに入力します。

フィールド	説明
[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。
[Choose] ドロップダウン リスト	ドロップダウン リストから、診断をサーバで実行するかサーバ グループで実行するかを選択します。
[Server(s)] または [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。

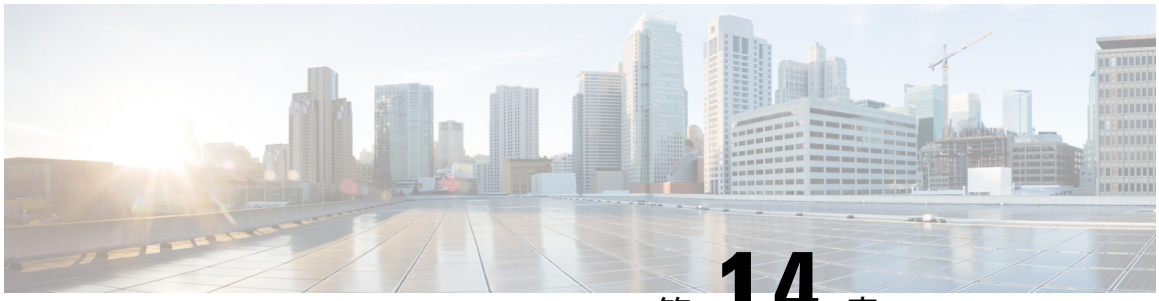
ステップ 4 [Select] をクリックし、[Select] ダイアログボックスからサーバまたはサーバ グループを選択します。

ステップ 5 [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、[Server(s)] または [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） サーバもしくは複数のサーバ上で次のアクションを実行できます。

- レポートを表示するには、サーバを選択して、[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、[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、[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。
- すでに診断操作を実行しているサーバは選択できません。そのサーバで別の診断をトリガーするには、診断操作が完了するまで待ちます。
- 診断が終了するまでに約 40 分かかる場合があります。これは、サーバに存在するコンポーネントの数によって異なります。



第 14 章

Smart Call Home: Cisco IMC Supervisor

この章は、次の内容で構成されています。

Smart Call Home の概要

Cisco Smart Call Home は、選択されたシスコ デバイスで継続的なモニタリング、プロアクティブな診断、アラート、修復案を提供する自動サポート機能です。Smart Call Home は、問題を迅速に特定および解決し、高可用性と業務の効率化の向上を実現するために役立ちます。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 が、シスコが Cisco Technical Assistance Center（TAC）のエンジニアやシスコ サポート コミュニティおよび開発者とやりとりして識別した特定の障害について確認します。ユーザが問題または障害に気づいてエスカレーションや報告するのを待つのではなく、Smart Call Home が障害を事前に特定し、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 を使用して自動的にケースが上げられます。

Cisco IMC Supervisor ユーザー 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 （185 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 **[Administration]** > **[System]** を選択します。

ステップ 2 **[System (システム)]** 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、[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 は無効になっています。

ステップ 4 [Contact Email] アドレスを入力します。

（注） このフィールドに一度に入力できる連絡先電子メールは 1 つだけです。

ステップ 5 Smart Call Home のバックエンドの [Destination URL] はデフォルトで設定されます。

（注）
- デフォルトの URL は変更しないことを推奨します。
- **[Proxy Configuration (プロキシ設定)]** 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 （39 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、[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 の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 **[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 （186 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	Severity	サービス リクエストの作成
F0174	fltProcessorUnitInoperable	Processor [id] on [serverId] operability: [operability]	critical|major	Y
F0177	fltProcessorUnitThermalThresholdNonRecoverable	Processor [id] on [serverid] temperature:[thermal]	critical	Y
F0181	fltStorageLocalDiskInoperable	Local disk [id] on [serverid] operability: [operability]	major| warning	Y
F0185	fltMemoryUnitInoperable	DIMM [location] on [serverid] operability: [operability]	major	Y
F0188	fltMemoryUnitThermalThresholdNonRecoverable	DIMM [location] on [serverid] temperature: [thermal]	critical	N
F0379	fltEquipmentIOCardThermalProblem	IOCard [location] on server [id] operState: [operState]	major	N
F0385	fltEquipmentPsuThermalThresholdNonRecoverable	Power supply [id] in [serverid] temperature: [thermal]	critical	Y
F0389	fltEquipmentPsuVoltageThresholdCritical	Power supply [id] in [serverid] voltage: [voltage]	major	N
F0391	fltEquipmentPsuVoltageThresholdNonRecoverable	Power supply [id] in [serverid] voltage: [voltage]	critical	Y
F0407	fltEquipmentPsuIdentity	Power supply [id] on [serverid] has a malformed FRU	critical	N
F0411	fltEquipmentChassisThermalThresholdNonRecoverable	Thermal condition on [serverid] cause: [thermalStateQualifier]	critical	N
F0424	fltComputeBoardCmosVoltageThresholdCritical	CMOS battery voltage on [serverid] is [cmosVoltage]	major	N

障害コード	障害名	メッセージ	Severity	サービス リクエストの作成
F0425	fltComputeBoardCmosVoltageThresholdNonRecoverable	CMOS battery voltage on [serverid] is [cmosVoltage]	critical	Y
F0531	fltStorageRaidBatteryInoperable	RAID Battery on [serverid] operability: [operability]	major	Y
F0868	fltComputeBoardPowerFail	Motherboard of [serverid] power: [power]	critical	N
F0997	fltStorageRaidBatteryDegraded	Raid battery [id] on [serverid] operability: [operability]	major	N
F1004	fltStorageControllerInoperable	Storage Controller [id] operability: [operability]	critical	N
F1007	fltStorageVirtualDriveInoperable	Virtual drive [id] on [serverid] operability: [operability]	critical	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、次の内容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。また、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 デリバリなどの環境で使用される大規模データセット用に 1 つのサーバを最適化することもできます。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。

- 冗長ディスク アレイ（RAID）および Just a Bunch Of Disks（JBOD）の全機能とのエンタープライズクラスの冗長性
- スタンドアロンの管理インターフェイス（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
- 奥行きが深いラックが不要

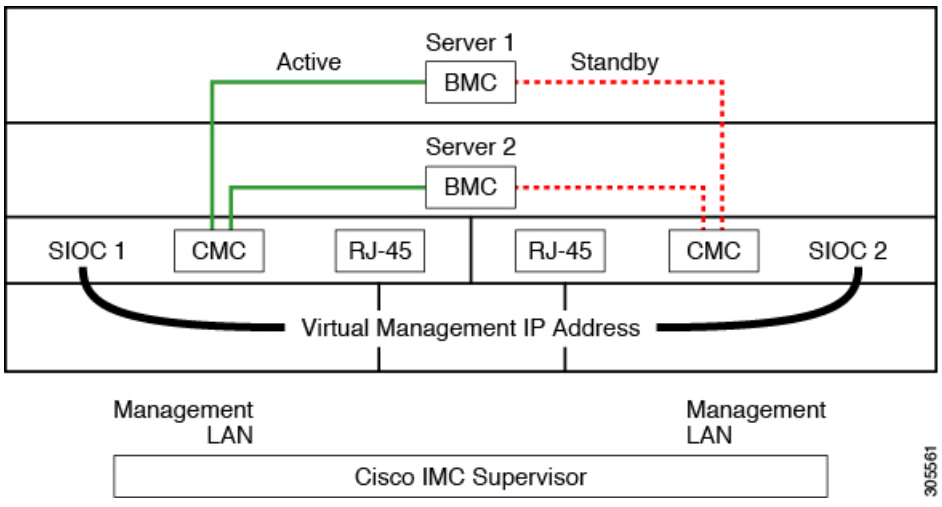
Cisco UCS S3260 高密度ストレージ ラック サーバの詳細については、『Cisco UCS S3260 Rack Server』を参照してください。

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、Cisco 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。

- デュアル サーバ ノード
- サーバ ノードあたり最大 24 のコンピューティング コア
- サーバ ノードあたり最大 60 台の混合ドライブ（Large Form Factor（LFF）と最大 14 台のソリッド ステート ディスク（SSD）ドライブ、および 2 台の SSD SATA ブート ドライブ）
- サーバ ノードあたり最大 512 GB のメモリ（合計 1 テラバイト [TB]）
- 12 Gbps の Serial Attached SCSI（SAS）ドライブのサポート
- デュアルポート 40 Gbps をサポートする、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
- 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。構成の変更は、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のスーパーバイザ マネージド高密度ストレージ ラック サーバはCシリーズ ラック サーバとともになるすべての機能をサポートします。また、これらの機能に追加のレポートを提供し、概念は、次の項で詳細述べられます。

- 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—説明し、Cisco UCS 3260シャーシ ラック アカウントの追加についての詳細情報が表示されます。
- シャーシの管理—説明し、高密度ストレージ ラック シャーシの構文に関する詳細情報が表示されます。
- ポリシーとプロファイル—説明し、Cisco UCSの詳細情報が3260シャーシ ポリシーと関連プロファイル提供します。
- 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、[Server IP] フィールドに仮想的な管理 IP を指定することができます。ラック アカウントの詳細については、ラック アカウントの追加 （60 ページ）を参照してください。**[Rack Servers (ラック サーバ)]** 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 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 **[Systems]** > **[Inventory and Fault Status]** を選択します。

ステップ 2 [Rack Groups] ページで、[Chassis] をクリックします。

ステップ 3 [Reboot CMC] をクリックします。

ステップ 4 **[Reboot Chassis Management Controller (シャーシ管理コントローラの再起動)]** 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、サーバのユーザー定義タグです。**[Asset Tag (アセット タグ)]**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 （82 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 **[Systems]** > **[Inventory and Fault Status]** を選択します。

ステップ 2 [Rack Groups] ページで、[Chassis] をクリックします。

（注） また、**[Inventory and Fault Status (インベントリと障害のステータス)]** ペインの **[Rack Groups (ラック グループ)]**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 **[More Actions (その他の操作)]**ドロップダウン リストから **[Asset Tag (アセット タグ)]** を選択します。

（注） リストからサーバを選択するまでは、**[Asset Tag (アセット タグ)]** 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） **[Asset Tag (アセット タグ)]** 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、**[Rack Groups (ラック グループ)]** ページの **[Asset Tag (アセット タグ)]** 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前面ロケータ LED を点灯または消灯するには、次の手順を実行します。

手順

ステップ 1 **[Systems]** > **[Inventory and Fault Status]** を選択します。

ステップ 2 [Rack Groups] ページで、[Chassis] をクリックします。

ステップ 3 [Front Locator LED] をクリックします。

ステップ 4 [Turn the Front Locator LED for selected chassis on/off] ドロップダウンリストから、[ON] または [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 （88 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

タギングは、リソース グループまたはラック サーバなどのオブジェクトにラベルを割り当てるために使用されます。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 **[Systems]** > **[Inventory and Fault Status]** を選択します。

ステップ 2 [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、[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 [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 [Tag Value] を選択します。

ステップ 5 [+] 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 （194 ページ）を参照してください。

（注） また、タグの詳細を編集、削除、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 には、シャーシ情報を追加できる Cisco UCS S3260 シャーシのポリシーとプロファイルを作成するための新しい [Cisco UCS S3260] オプションとがあります。

本書では、これらの新しいシャーシ ポリシーはユーザ管理ポリシーと呼び、既存のラック マウント サーバ ポリシーはコンピューティング ノード ポリシーと呼びます。差別化された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、[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]、コンピューティング ノード ポリシーは [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 **[Server Platform (サーバ プラットフォーム)]** カラムがあります。シャーシ ポリシーは、ユーザ管理ポリシーやコンピューティング ノード ポリシーに関係なく [Cisco UCS S3260] と表示されます。他の C シリーズや E シリーズのプラットフォームまたは Cisco UCS S3260 以外のポリシーの場合、[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 サーバ プロファイルを作成できます。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 サーバとラックマウント サーバのリストから選択します。選択したサーバ プラットフォームに基づき、Cisco UCS S3260 シャーシまたはラックマウント サーバを選択できます。ポリシーの作成および適用の詳細については、ハードウェア ポリシー （100 ページ）を参照してください。

次のポリシーは、ユーザ管理ポリシーとコンピューティング ノード ポリシーです。

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	Precision Boot Order
LDAP	RAID
NTP	KVM
ネットワーク セキュリティ	vmedia
SSH	VIC
NTP	Serial Over LAN

（注）

- Cisco UCS 3260 ラック サーバの場合、IPMI Over LAN およびネットワーク ポリシーには、BMC と CMC の両方の構成の詳細が混在しています。
- ゾーン分割ポリシーは、Cisco UCS 3260 ラック サーバにのみ適用可能なため、UI の [Cisco UCS S3260] チェック ボックスはオンになっています。
- レガシー ブート順序および Flex Flash のポリシーは、Cisco UCS 3260 ラック サーバには適用できません。

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 サーバのリストから選択します。Cisco UCS S3260 シャーシのみ選択でき、Cisco UCS S3260 ポリシーのみプロファイルに追加できます。コンピューティング ノード ポリシーの場合は、**[Apply Policy To (ポリシーの割り当て先)]** フィールドを選択して、プロファイル適用時にポリシーを適用する必要があるサーバ ノードを示すことができます。プロファイルの作成および適用の詳細については、ハードウェア プロファイル （140 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の詳細については、ファームウェアのアップグレード （159 ページ）を参照してください。

（注）

一度に 1 つのサーバ ノードのみアップグレードできます。

Viewing Cisco UCS S3260 Dense Storage Rack Server Details

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 **[Systems]** > **[Inventory and Fault Status]** を選択します。

ステップ 2 **[Rack Groups (ラック グループ)]**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 [Rack Groups] ページで、[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 **[View Details (詳細の表示)]** を選択します。

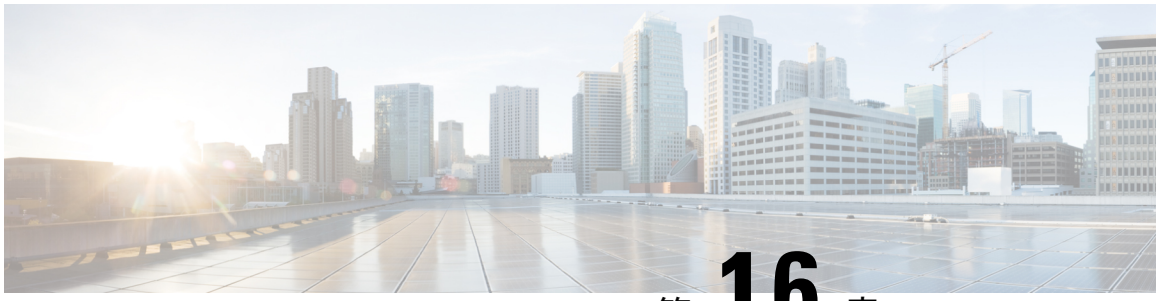
（注） リストで Cisco UCS S3260 高密度ストレージ ラック サーバを選択するまでは、**[View Details (詳細の表示)]** オプションは表示されません。

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装置の詳細。 （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 Adapters]	サーバで使用されている VIC アダプタの詳細。 リストにある任意の VIC アダプタを選択して [View Details] をクリックすると、[External Ethernet Interfaces] や [VM FEXs] などの情報が表示されます。
コミュニケーション	HTTP、HTTPS、SSH、IPMI Over LAN、NTP、SNMP などのプロトコルの情報。
[Remote Presence]	vKVM、Serial over LAN、vMedia の詳細。
障害（Fault）	サーバで記録された障害の詳細。
Users	**デフォルト グループ**のユーザーに関する詳細。ユーザー 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（129 ページ）およびパスワードの有効期限ポリシー（120 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**ユーザー**を表示できますが、サーバ レベルでは表示できません。

タブ	説明
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。
[Tech Support]	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、[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 （93 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。
[Associated Hardware Profiles]	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。
[Chassis Summary]	CMC 1 ネットワーク、共通、NIC などのプロパティの要約。
[Rack Servers]	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。
[System IO Controller]	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。
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。
ゾーニング	状態、プレゼンス、所有権、サイズなどの詳細。

ステップ 5 右端の [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、次の内容で構成されています。

サポート情報

Cisco IMC Supervisor 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、録音したデバッグを記録し、APIのログをダウンロードします。

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 **[Administration]** > **[Support Information]** を選択します。

ステップ 2 [Support Information] ウィンドウで、次の情報を表示できます。

表 *2:* システム情報（基本）

フィールド	説明
[Support Information] ドロップダウン リスト	基本情報を表示するには、[System Information (Basic)] を選択して [Submit] をクリックします。

表 *3:* システム情報（詳細）

フィールド	説明
[Support Information] ドロップダウン リスト	プロセッサ、メモリ、ディスク情報などの詳細情報を表示するには、[System Information (Advanced)] を選択して [Submit] をクリックします。

表 *4: View Logs*

フィールド	説明
[Support Information] ドロップダウン リスト	[Show log] を選択します。
[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、[Show Logs] をクリックします。

表 *5:* すべてのログのダウンロード

フィールド	説明
[Support Information] ドロップダウン リスト	[Download All Logs] を選択して [Download] をクリックします。

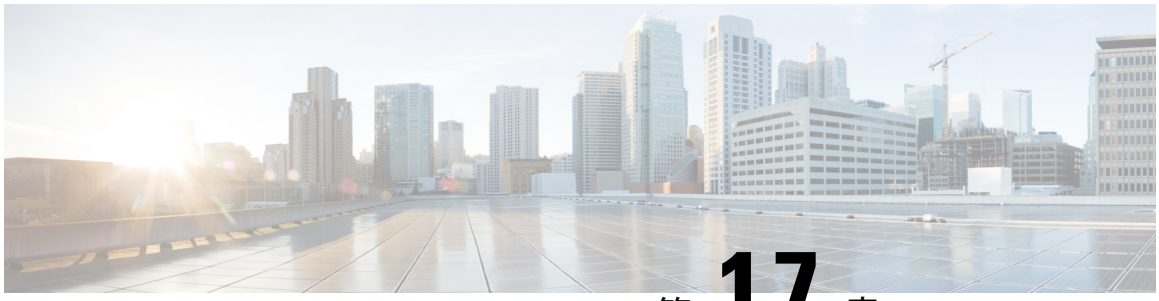
表 *6:* デバッグ ログのダウンロード

フィールド	説明
[Support Information] ドロップダウン リスト	**1.** [Debug Logging] を選択して [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、[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
[Support Information] ドロップダウン リスト	**1.** [API Logging] を選択して [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、[Stop API Logging] をクリックして、API デバッグ ログのダウンロード 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、次の内容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にすばやくアクセスできます。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	参照先
へのログイン方法 Cisco IMC Supervisor	Cisco IMC Supervisor の起動 （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）
にログイン 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 （59 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 （60 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 アプリケーションにログインしている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 ヘッダーの右端にあります。

ステップ 2 [User Information] ウィンドウで [Dashboard] をクリックします。

ステップ 3 [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 [Apply] をクリックし、ウィンドウを閉じます。

（注） メニュー バーに [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）] を有効にしておく必要があります。

手順

ステップ 1 Cisco IMC Supervisor ユーザー 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、**[Automatic Refresh (自動更新)]** を **[ON (オン)]** にします。

ステップ 5 **[Interval (間隔)]** 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 **[Widget Size (ウィジェット サイズ)]**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。更新率も定義できます。

手順

ステップ 1 メニュー バーから [Dashboard] を選択します。

ステップ 2 [Dashboard] パネルで、[Automatic Refresh] オプションの横にある [OFF] をクリックします。[Automatic Refresh] オプションが [ON] に変わり、[Interval] スライド バーが表示されます。

ステップ 3 [Interval] を使用して、更新率を設定します。

（注） 更新率は 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サマリー レポートの追加

すぐにアクセスできるようにサマリー 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） サマリー レポートのみをダッシュボードに追加できます。

手順

ステップ 1 ダッシュボードに追加するサマリー 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向き矢印をクリックします。

ステップ 3 [Add to Dashboard] をクリックします。

（注） サマリー 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、[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 [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

デフォルトの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 ユーザー 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 ドロップダウン リストをクリックし、作成したダッシュボードのリストを表示します。
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。

[Favorites] へのメニューまたはタブの追加

[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 [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 [Favorite] をクリックします。

（注） [Favorite] 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 [Favorite Report] ダイアログボックスで、[Menu Label] フィールドを編集できます。
ステップ 4 **[Save]** をクリックします。
ステップ 5 メニュー バーで [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 **[Favorites (お気に入り)]** 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 [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 [Customize Table View] アイコンを見つけてクリックします。

ステップ 2 [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、[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 [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 [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 [Match Condition] ドロップダウン リストで、必要に応じて [Match All Conditions] または [Match Any Condition] を選択します。

ステップ 3 [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 [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（Search）] 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 [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 [Export Report] アイコンを見つけてクリックします。

ステップ 2 [Export Report] ダイアログボックスで、次の手順を実行します。

1. [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. [Generate Report] をクリックします。
3. レポートが生成されたら、**[Download (ダウンロード)]** 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 [Export Report] ダイアログボックスで [Close] をクリックします。

システム情報の表示

[System Information (システム情報)] 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

[Site Map (サイト マップ)] オプションを使用すると、Cisco IMC Supervisor ユーザー 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 **[Firmware Management (ファームウェア管理)]**を選択できます。