Cisco IMC Supervisor ラックマウント サーバ管理ガイド、リリース 2.0

初版：2016 年 03 月 18 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/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

はじめに

ここでは、次の項について説明します。

対象読者

このマニュアルは、 または を使用し、以下の少なくとも 1 つの分野において責任と専門知識を持つデータセンター管理者を主に対象としています。

- サーバ管理
- ストレージ管理
- ネットワーク管理
- ネットワーク セキュリティ
- 仮想化および仮想マシン

表記法

テキストのタイプ	説明
GUI 要素	タブの見出し、領域名、フィールドのラベルのようなGUI要素は、[GUI 要素] のように示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトルのようなメイン タイトルは、[メイン タイトル] のように示しています。

テキストのタイプ	説明
マニュアルのタイトル	マニュアルのタイトルは、イタリック体（*italic*）で示しています。
TUI 要素	テキストベースのユーザ インターフェイスでは、システムによって表示されるテキストは、courier フォントで示しています。
システム出力	システムが表示するターミナル セッションおよび情報は、courier フォントで示しています。
CLI コマンド	CLI コマンドのキーワードは、ボールド体（**bold**）で示しています。 CLI コマンド内の変数は、イタリック体（*italic*）で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。stringの前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ヒント　「問題解決に役立つ情報」です。ヒントには、トラブルシューティングや操作方法ではなく、ワンポイントアドバイスと同様に知っておくと役立つ情報が記述される場合もあります。

ワンポイント アドバイス　「時間の節約に役立つ操作」です。ここに紹介している方法で作業を行うと、時間を短縮できます。

警告　安全上の重要事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。

これらの注意事項を保管しておいてください。

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォームよりご連絡ください。ご協力をよろしくお願いいたします。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、毎月更新される『What's New in Cisco Product Documentation』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

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 *2.0* の新機能と変更された動作

機能	説明	参照先
タスクのスケジューリングのサポート	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。ファームウェアのアップデートやサーバ検出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。	スケジュール管理の概要，（125 ページ）．
FlexFlash ポリシーの概要	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。	FlexFlash ポリシー，（85 ページ）．

このリリースの新規情報および変更情報

機能	説明	参照先
Smart Call Home のサポート	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、および修復の提案を提供する自動サポート機能です。 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、Cisco IMC Supervisor が管理するサーバ タスクは、定期的に実行され、関連情報を Smart Call Home の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。	Smart Call Home の概要，（131 ページ）.
サーバ診断の実行	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。	サーバ診断の概要，（127 ページ）.

このリリースの新規情報および変更情報

機能	説明	参照先
パッチ リリースの自動通知	Cisco IMC Supervisor は、Cisco.com で利用される新しいパッチ リリースの有無を定期的に（14 日ごとに）確認します。設定を行うと、新しいバージョンがあれば通知されます。より高いバージョンが使用可能な場合は、[Diagnostic System Messages] ダイアログボックスに、Cisco IMC Supervisor の新しいバージョンが見つかったことを示すメッセージが表示されます。 更新設定を行っていない場合は、右上隅のログイン名の横に通知バブルが表示されます。[Diagnostic System Messages] ダイアログボックスに、設定が行われていないことを示すメッセージが表示されます。	Cisco IMC Supervisor パッチの更新の概要, （121 ページ）.
グループ共有ポリシーの作成のサポート	作成したポリシーをユーザ グループと共有できるようになりました。	グループ共有ポリシーの追加, （41 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
- サーバを検出、モニタ、管理し、ファームウェア アップグレードをプログラムで実行するためにノースバウンド REST API を提供します。
- 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

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 Advanced ライセンス。ポリシーやプロファイルの追加、編集、および削除は基本ライセンスで行えますが、サーバへのポリシーまたはプロファイルの適用には Advanced ライセンスが必要です。ポリシーを適用する際にこのライセンスがないとエラーが発生します。
- デフォルトの組み込み Cisco IMC Supervisor 評価ライセンス。評価ライセンスは、エンドユーザが Cisco IMC Supervisor をインストールし、すべてのサービスを初めて起動するときに自動的に生成されます。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 60 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。

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, （7 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, （15 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，（15 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。

はじめる前に

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
Organization Name	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。
Country	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） 初めてログインすると、Cisco IMC Supervisor によって [Default Group] というタイトルのラック グループが提供されます。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 に追加することができます。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。

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
	Refresh	ページ上の報告されたデータを更新します。
	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。
	Export Report	[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

アイコン	ラベル	説明
	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。

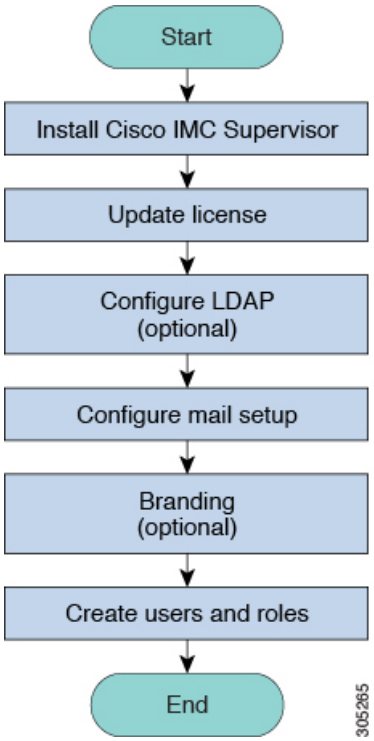
第 3 章

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 にログインするには、次の手順を実行します。

はじめる前に

- 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 のインストール中に IP アドレスを確実に設定します。

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

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
License Keys	このタブには、Cisco IMC Supervisor で使用されるライセンスの詳細が表示されます。このタブを使用してライセンスをアップグレード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、ライセンスをアップグレードできます。
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。
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。

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，（6 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。

はじめる前に

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 メニュー バーで、[Administration] > [License] を選択します。

ステップ 2 [License Keys] タブを選択します。

ステップ 3 [Update License] をクリックします。

ステップ 4 [Update License] ダイアログボックスで、次のいずれかの操作を実行します。

- .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 [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。

はじめる前に

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, （15 ページ） を参照してください。

手順

ステップ 1 メニュー バーで、[Administration] > [License] を選択します。
ステップ 2 [License Utilization] タブをクリックします。
ステップ 3 [Run License Audit] をクリックします。
ステップ 4 [ライセンス監査の実行] ダイアログボックスで、[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。
ステップ 5 確認ダイアログボックスで、[OK] をクリックします。

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 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 メニュー バーから、[Administration] > [Users and Groups] の順に選択します。

ステップ 2 [Authentication Preferences] タブを選択します。

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, （20 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 [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 統合の規則と制限事項

ユーザの同期規則

- 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 [External] 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。
- これらの LDAP ディレクトリが同期された後、LDAP 外部ユーザは、完全なドメイン名と共にユーザ名を指定して 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。

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） LDAP 同期プロセスの後には、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てください。

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 メニュー バーから、[Administration] > [Users and Groups] の順に選択します。

ステップ 2 [LDAP Integration] タブを選択します。

ステップ 3 LDAP 設定を追加するには [+] をクリックします。

ステップ 4 [Add LDAP Configurations] 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。

フィールド	説明
[Account Name] フィールド	LDAP アカウント名。

フィールド	説明
[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てい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 • 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] ダイアログボックスで [Select] をクリックして、表示されるテーブルから、OU に基づいてユーザを検索するための検索条件を選択します。

（注） Cisco IMC Supervisor ではユーザのみがサポートされ、グループはサポートされません。[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，（25 ページ）を参照してください。

ステップ 7 [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 8 [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 9 [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 10 [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 11 [Submit] をクリックします。

ステップ 12 [Submit Result] ダイアログボックスで、[OK] 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 13 [LDAP User Role Filter] ダイアログボックスで、[Submit] をクリックします。

ステップ 14 [Submit Result] ダイアログボックスで、[OK] 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 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。
- 結果を絞り込み、グループおよびユーザに LDAP ロール フィルタを指定する、グループ フィルタまたはユーザ フィルタ。

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

はじめる前に

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 メニュー バーで、[Administration] > [Users and Groups] の順に選択します。

ステップ 2 [LDAP Integration] タブを選択します。

ステップ 3 [Add] をクリックします。

ステップ 4 [LDAP Server Configuration] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[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。
[User Name] 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。

名前	説明
[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 5 [Next] をクリックします。

ステップ 6 [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。
Cisco IMC Supervisor で使用可能なすべての組織単位（OU）がこのリストに表示されます。

ステップ 7 [Next] をクリックします。

ステップ 8 [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 フィルタに属するユーザがすべて取得され、システムに追加されます。ただし、選択したグループのユーザが他のグループにも属している場合は、このフィールドで選択されていない限り、それらのグループは取得されず、システムへの追加もされません。
[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。

名前	説明
[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。 • Equals to • 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 9 [Next] をクリックします。

ステップ 10 [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 11 [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	次のいずれかを指定できます。 • Equal to • 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。
[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。 以下は、Cisco IMC Supervisor でデフォルトで使用可能なロールです。 • Group Admin • Operator • System Admin

ステップ 12 [Submit] をクリックします。

ステップ 13 [OK] 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。

[Login Users] タブでユーザのユーザ 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。

次の作業

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。認証設定の変更の詳細については、認証の環境設定, （17 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 メニュー バーから、[Administration] > [Users and Groups] の順に選択します。

ステップ 2 [LDAP Integration] タブを選択します。

ステップ 3 表から LDAP アカウント名を選択します。

ステップ 4 [View] をクリックします。
[View LDAP Account Information] ダイアログボックスに、LDAP アカウントのサマリー情報が表示されます。

ステップ 5 [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 メニュー バーから、[Administration] > [Users and Groups] の順に選択します。
ステップ 2 [LDAP Integration] タブを選択します。
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 [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 5 [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 メニュー バーから、[Administration] > [Users and Groups] の順に選択します。
ステップ 2 [LDAP Integration] タブをクリックして、LDAP アカウントを選択します。
ステップ 3 [Search BaseDN] をクリックします。
（注） Cisco IMC Supervisor ではユーザのみがサポートされ、グループはサポートされません。[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 4 [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 5 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 6 [LDAP Search Base] ダイアログボックスの [Submit] をクリックします。
ステップ 7 [Submit Result] ダイアログボックスで、[OK] 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 メニュー バーから、[Administration] > [Users and Groups] の順に選択します。

ステップ 2 [LDAP Integration] タブをクリックして、LDAP アカウントを選択します。

ステップ 3 [Request Manual LDAP Sync] をクリックします。

ステップ 4 [Manual LDAP Sync] 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
[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 に存在している場合、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 5 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 6 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 7 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 8 [Next] をクリックします。

ステップ 9 [Select Users and Groups] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[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 10 [Submit] をクリックします。

ステップ 11 [Submit Result] ダイアログボックスで、[OK] をクリックし、LDAP サーバを同期します。
メニュー バーから [Administration] > [Users and Groups] を選択し、[Users] タブをクリックすると、同期されたユーザが表示されます。

LDAP 同期結果の表示

LDAP の同期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 メニュー バーから、[Administration] > [Users and Groups] の順に選択します。
ステップ 2 [LDAP Integration] タブをクリックして、LDAP アカウントを選択します。
ステップ 3 [Results] をクリックします。
ステップ 4 [License Status] タブをクリックして、Cisco IMC Supervisor ライセンスの有効性を確認します。
ステップ 5 [LDAP Integration] タブをクリックして、LDAP 同期の開始および終了の時刻、同期のステータス、ステータスの詳細メッセージなどの詳細を確認します。

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
- 検索ベース DN の選択内容

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 メニュー バーから、[Administration] > [Users and Groups] の順に選択します。
ステップ 2 [LDAP Integration] タブをクリックして、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 [Modify LDAP Server Configuration] ダイアログボックスで、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
[User Name] 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。

ステップ 5 [Next] をクリックします。

ステップ 6 [LDAP Search Base] ダイアログボックスで、[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。

ステップ 7 [Next] をクリックします。

ステップ 8 [Configure User and Group Filters] ペインで、[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ます。

ステップ 9 [Next] をクリックします。

ステップ 10 [LDAP User Role Filter] ダイアログボックスで、テーブル エントリの追加/編集/削除操作をクリックするか、上矢印と下矢印を使ってエントリを移動します。

ステップ 11 それぞれのダイアログボックスで [Submit] をクリックします。

ステップ 12 [Submit Result] ダイアログボックスで、[OK] をクリックします。

ステップ 13 [LDAP User Role Filter] ダイアログボックスで、[Submit] をクリックします。

ステップ 14 [Submit Result] ダイアログボックスで、[OK] 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 メニュー バーから、[Administration] > [Users and Groups] の順に選択します。
ステップ 2 [LDAP Integration] タブを選択します。
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。
ステップ 6 [OK] 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。

SCP ユーザの設定

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

手順

ステップ 1 メニュー バーから、[Administration] > [Users and Groups] の順に選択します。
ステップ 2 [SCP User Configuration] タブをクリックします。
ステップ 3 [Password] フィールドに scp ユーザ パスワードを入力します。
ステップ 4 [Submit] をクリックします。
ステップ 5 [Submit Result] ダイアログボックスで、[OK] 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, （57 ページ） を参照してください。

手順

ステップ 1 メニュー バーで、[Administration] > [System] を選択します。

ステップ 2 [Mail Setup] タブをクリックします。

ステップ 3 [Mail Setup] ペインで、次のフィールドに値を入力します。

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。
Server IP Address	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 [Save] をクリックします。

ステップ 5 確認ダイアログボックスで、[OK] 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 メニュー バーから、[Administration] > [Users and Groups] の順に選択します。

ステップ 2 [Login Page Branding] タブをクリックします。

ステップ 3 [Add] をクリックします。

ステップ 4 [Domain Branding] ダイアログボックスで、次の手順を実行します。

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

この手順を使用して、Cisco IMC Supervisor アプリケーションをカスタマイズすることができます。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 メニュー バーで、[Administration] > [User Interface Settings] を選択します。

ステップ 2 [User Interface Settings] ウィンドウで、次の手順を実行します。

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 [Save] をクリックします。

ステップ 4 確認ダイアログボックスで、[OK] をクリックします。

第 4 章

ユーザとユーザ ロールの作成

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 ロールをデフォルトでサポートしています。

- [System Admin]：ユーザを追加する権限を持つユーザ。Cisco IMC Supervisor では、管理者として、システムによって提供されたユーザ ロールもしくはカスタム定義されたユーザ ロールを、ユーザに割り当てることができます。また、ユーザに割り当てられているロールに関する情報を後で確認することができます。ユーザ ロールを使用して、次のタスクを実行できます。
  - システム内でカスタム ユーザ ロールを作成し、このロールを持つユーザを作成するか、既存のユーザにロールを割り当てる。

    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。ユーザの作成の詳細については ユーザの作成，（36 ページ） を参照し、ユーザ ロールの作成については ユーザ ロールの追加，（37 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]：システム定義されたユーザ グループ [Default Group] は、Cisco IMC Supervisor でデフォルトで使用可能です。グループ管理者として、ユーザ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割り当てることができます。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。

ユーザの作成

新しいユーザを作成するには、次の手順を実行します。

（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 メニュー バーから、[Administration] > [Users and Groups] の順に選択します。

ステップ 2 [Users] タブをクリックします。

ステップ 3 [Add] をクリックします。

ステップ 4 [Add User] ダイアログボックスで、次の手順を実行します。

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。

フィールド	説明
[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] 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。
[Address] フィールド	（オプション）ユーザの住所。

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 メニュー バーから、[Administration] > [Users and Groups] の順に選択します。

ステップ 2 [Current Online Users] タブをクリックします。
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 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 ロールと Operator ロールを使用できます。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、それにユーザを割り当てることもできます。

手順

ステップ 1 メニュー バーで、[Administration] > [System] を選択します。

ステップ 2 [User Roles] タブをクリックします。

ステップ 3 [Add] をクリックします。

ステップ 4 [Add User Role] ダイアログボックスの [User Role] ペインで、次の手順を実行します。

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 [Submit] をクリックします。

ステップ 10 確認ダイアログボックスで、[OK] 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 グループの追加

新しいユーザ グループを追加する場合は、次の手順を実行します。

手順

ステップ 1 メニュー バーから、[Administration] > [Users and Groups] の順に選択します。

ステップ 2 [User Group] タブをクリックします。

ステップ 3 [Add] をクリックします。

ステップ 4 [Add User Group] 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
[Name] フィールド	ユーザ グループの名前。
[Description] フィールド	（オプション）ユーザ グループの説明。
[Code] フィールド	（オプション）グループの短い名前またはコード名。
[Cost Center] フィールド	（オプション）コストセンターの名前または番号（必要な場合）。この名前または番号は、グループが関連付けられているコストセンターを表します。
[Contact Email] フィールド	この電子メールは、必要に応じてサービス リクエストおよびリクエスト承認のステータスをグループ所有者に通知する目的で使用されます。
[First Name] フィールド	（オプション）担当者の名。
[Last Name] フィールド	（オプション）担当者の姓。
[Phone] フィールド	（オプション）担当者の電話番号。
[Address] フィールド	（オプション）担当者の住所。
[Group Share Policy] ドロップダウン リスト	（オプション）このグループのユーザのグループ共有ポリシーを選択します。 このドロップダウン リストは、グループ共有ポリシーを作成した場合にのみ表示されます。
[Allow Resource Assignment To Users] チェックボックス	（オプション）オンにすると、このグループのユーザは、そのユーザに割り当てられたリソースを持つことができ、これらのリソースを所有できます。また、これらのユーザは、グループに属するリソースを確認できます。しかし、ユーザ間でリソースを共有することはできません。

ステップ 5 [Add] をクリックします。

ステップ 6 [OK] をクリックします。

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

ユーザ グループのブランディング

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

手順

ステップ 1 メニュー バーから、[Administration] > [Users and Groups] の順に選択します。

ステップ 2 [User Group] タブをクリックします。

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] ダイアログボックスで、次の手順を実行します。

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 [Submit] をクリックします。

ステップ 7 [Submit Result] ダイアログボックスで [OK] をクリックします。

グループ共有ポリシー

グループの共有ポリシーは、リソースのユーザと、ユーザが他のユーザと共有可能なものを、より詳細に制御できるようにします。このポリシーを使用すると、ユーザは、自分に現在割り当てられているリソースのみを表示可能にするか、またはそのユーザが属するすべてのグループに割り当てられているリソースを表示可能にすることができます。

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

グループ共有ポリシーの追加

ポリシーを追加して、ユーザ グループと共有するには、次の手順を実行します。

手順

ステップ 1 メニュー バーから、[Administration] > [Users and Groups] の順に選択します。

ステップ 2 [Group Share Policy] タブをクリックします。

ステップ 3 [Add] をクリックします。

ステップ 4 [Add Group Share Policy] 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。

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

ステップ 5 [Submit] をクリックします。

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

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

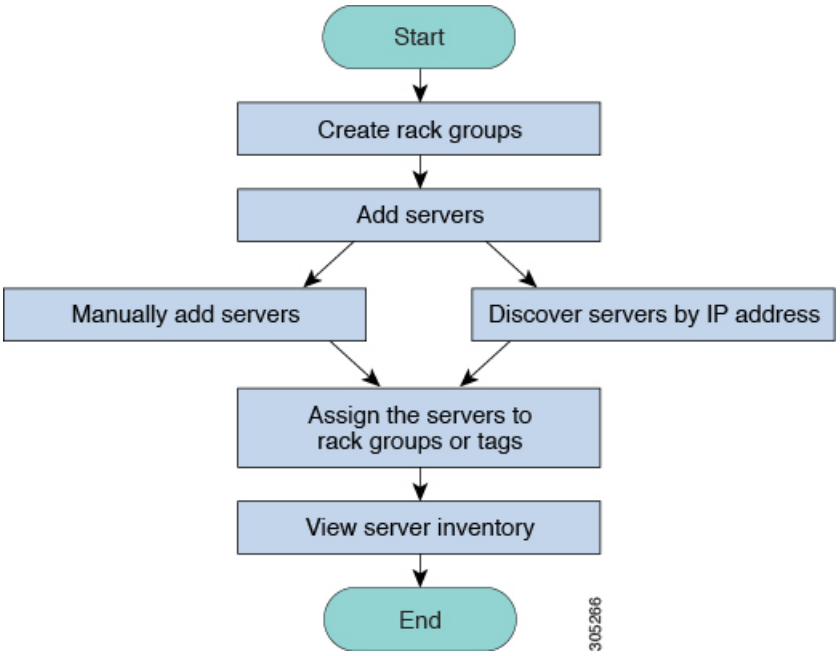
第 5 章

サーバ検出、ラック グループ、およびラック アカウントの管理

この章は、次の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に関する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、事前設定が一切されていないため、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。手動で追加するか、またはIPアドレスによって検出することで、これらのサーバをCisco IMC Supervisorに導入できます。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に加わ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 メニュー バーで、[Systems] > [Physical Accounts] を選択します。

ステップ 2 [Discovery Profiles] タブをクリックします。

ステップ 3 [Add] をクリックします。

ステップ 4 [Add Discovery Profile] 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
[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, （80 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
[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。

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） 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

システムが自動的にラックマウント サーバを検出して Cisco IMC Supervisor にインポートするようにするには、次の手順を実行します。

はじめる前に

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 メニュー バーで、[Systems] > [Physical Accounts] を選択します。

ステップ 2 [Discovered Devices] タブをクリックします。

ステップ 3 [Discover] をクリックします。

ステップ 4 [Discover Devices] ダイアログボックスで、次のフィールドに入力します。[Select Profile] ドロップダウン リストからプロファイルを選択します。

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, （125 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ている場合、このスケジュールには、ユーザが作成したスケジュールがリストから選択されます。 （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 [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。

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。

はじめる前に

- 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 メニュー バーで、[Systems] > [Physical Accounts] を選択します。

ステップ 2 [Discovered Devices] タブをクリックします。

ステップ 3 [Import] をクリックします。

ステップ 4 [Import Discovered Devices] 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
[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。
Description	ユーザの説明を入力します。
Contact	ユーザの連絡先の詳細を入力します。
Location	ユーザ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 ラック グループを選択した場合は [Submit] をクリックし、ラック グループの作成を選択した場合は [Create] 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） 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。

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。

はじめる前に

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, （15 ページ） を参照してください。

手順

ステップ 1 メニュー バーで、[Systems] > [Physical Accounts] を選択します。
デフォルトでは、[Rack Group] タブが選択されます。

ステップ 2 [Add] をクリックします。

ステップ 3 [Create Rack Group] 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。

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 [Create] をクリックします。

ステップ 5 [Submit Result] ダイアログボックスで、[OK] をクリックします。

次の作業

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

Cisco IMC Supervisor のラック グループのいずれかにラックマウント サーバを追加できます。アカウントを追加すると、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。

はじめる前に

- 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, （15 ページ） を参照してください。
- ラック グループが存在します。

（注） システムによって提供されたデフォルト 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 を有効にし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 メニュー バーで、[System] > [Physical Accounts] を選択します。

ステップ 2 [Rack Accounts] タブをクリックします。

ステップ 3 [Add] をクリックします。

ステップ 4 [Create Account] 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。

フィールド	説明
[Account Name] フィールド	ラック アカウントの記述名。
[Server IP] フィールド	ラックマウント サーバの IP アドレス。
[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	

フィールド	説明
[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, （48 ページ） を参照してください。
[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。

次の作業

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, （52 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。

はじめる前に

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 メニュー バーで、[Systems] > [Physical Accounts] を選択します。

ステップ 2 [Rack Accounts] タブをクリックします。

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)] ダイアログボックスで、[Rack Group] または [Rack Account] を選択して、ドロップダウン リストからサーバを選択します。

ステップ 6 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 [Submit] をクリックします。

ステップ 9 確認ダイアログボックスで、[OK] 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。

はじめる前に

[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 メニュー バーで、[Systems] > [Physical Accounts] を選択します。
ステップ 2 [Rack Accounts] タブをクリックします。
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] ダイアログボックスで、サーバの割り当て先となるラック 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 [Submit] をクリックします。
ステップ 7 確認ダイアログボックスで、[OK] 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 メニュー バーで、[Systems] > [Physical Accounts] を選択します。
ステップ 2 [Rack Accounts] タブをクリックします。
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。
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。
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

サーバで使用されているメモリ、CPU、PSU などのラック マウント サーバの詳細を表示するには、次の手順を実行します。

（注） また、左側のペインで [Rack Groups] をクリックして、この手順を実行することもできます。

はじめる前に

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 メニュー バーで、[Systems] > [Inventory and Fault Status] を選択します。

ステップ 2 左側のペインで、[Rack Groups] を展開し、サーバを含むラック グループを選択します。

ステップ 3 右側のペインで、[Rack Servers] タブを選択します。

ステップ 4 リストのサーバをダブルクリックして詳細を表示するか、リストのサーバをクリックし、右端の下向き矢印をクリックして [View Details] を選択します。

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

ラックマウント サーバに関する次の詳細を表示できます。

タブ	説明
Summary	ラック アカウントの概要。
CPUs	サーバで使用されている CPU の詳細。
Memory	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。
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。 リストされている任意の VIC アダプタを選択して [View Details] をクリックすると、[External Ethernet Interfaces] 、[VM FEXs] などの情報が表示されます。
Network Adapters	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。 リストされている任意のストレージ アダプタを選択して [View Details] をクリックすると、[Controller Info] 、[Physical Drives] などの情報が表示されます。
FlexFlash Adapters	サーバで使用されている FlexFlash アダプタの詳細。 リストされている任意の FlexFlash アダプタを選択して [View Details] をクリックすると、[Controller Info] 、[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する場合、FlexFlash 詳細情報をレポートに表示するには [Systems] > [Physical Accounts] > [Rack Accounts] > [Inventory] に移動してインベントリを実行するか、定期的なインベントリが実行されるのを待つ必要があります。
Communication	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。
Faults	サーバで記録された障害の詳細。
Users	ユーザの詳細。

タブ	説明
Cisco IMC Log	サーバの Cisco IMC ログの詳細。
System Event Log	サーバ ログの詳細。
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。
Fault History	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、 Cisco IMC Supervisor アプライアンス、ローカル ディレクトリに、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使用できます。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, （74 ページ） を参照してください。
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。

はじめる前に

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 メニュー バーで、[Systems] > [Inventory and Fault Status] を選択します。

ステップ 2 左側のペインで [Rack Groups] を選択します。

ステップ 3 右側のペインで、[Faults] タブを選択します。

ステップ 4 リストのサーバをダブルクリックして詳細を表示するか、リストのサーバをクリックし、右端の下向き矢印をクリックして [View Details] を選択します。

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

ラックマウント サーバに関する次の詳細を表示できます。

タブ	説明
Explanation	問題の原因の要約。
Recommendation	問題を解決する手順。

ステップ 5 [Fault Details] ウィンドウで [Close] をクリックすると、前のウィンドウに戻ります。

ラック グループのサマリー レポート

[Inventory and Fault Status for Rack Groups] ページは、左右 2 つのセクションに分かれています。左側のペインにはラック グループのリストが表示されます。[Rack Groups] の見出しがデフォルト グループを含む左側のペインで選択されている場合、サマリー レポートは、次のレポートが表示される右側のペインで使用することができます。

- [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。

- [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。

サーバ障害に関する電子メール アラート ルールの追加

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

手順

ステップ 1 メニュー バーで、[Administration] > [System] を選択します。

ステップ 2 [Email Alert Rules] タブをクリックします。

（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] ダイアログボックスで、次の手順を実行します。

フィールド	説明
[Name]	ルールの一意の名前を入力します。
[Alert Scope]	任意のサーバで検出された新しい障害に関するすべてのシステム レベルのアラートを受信するには [System] を選択します。特定のラック グループの一部であるサーバで検出された新しい障害に関する電子メール アラートを受信するには [ServerGroup] を選択します。特定のサーバで検出された新しい障害に関する電子メール アラートを受信するには [Server] を選択します。

フィールド	説明
[Server Groups]	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。
[Servers]	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...] 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。
[Rule Enabled] チェックボックス	このチェックボックスをオンにして、設定された電子メール アドレスへの電子メール アラートを有効にします。

（注）
- 電子メール アラート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

サーバで使用されているメモリ、CPU、PSU などのラック マウント サーバの詳細を表示するには、次の手順を実行します。

（注） また、左側のペインで [Rack Groups] をクリックして、この手順を実行することもできます。

はじめる前に

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 メニュー バーで、[Systems] > [Inventory and Fault Status] を選択します。

ステップ 2 左側のペインで、[Rack Groups] を展開し、サーバを含むラック グループを選択します。

ステップ 3 右側のペインで、[Rack Servers] タブを選択します。

ステップ 4 リストのサーバをダブルクリックして詳細を表示するか、リストのサーバをクリックし、右端の下向き矢印をクリックして [View Details] を選択します。

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

ラックマウント サーバに関する次の詳細を表示できます。

タブ	説明
Summary	ラック アカウントの概要。
CPUs	サーバで使用されている CPU の詳細。
Memory	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。
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。 リストされている任意の VIC アダプタを選択して [View Details] をクリックすると、[External Ethernet Interfaces] 、[VM FEXs] などの情報が表示されます。
Network Adapters	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。 リストされている任意のストレージ アダプタを選択して [View Details] をクリックすると、[Controller Info] 、[Physical Drives] などの情報が表示されます。

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。 リストされている任意の FlexFlash アダプタを選択して [View Details] をクリックすると、[Controller Info] 、[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する場合、FlexFlash 詳細情報をレポートに表示するには [Systems] > [Physical Accounts] > [Rack Accounts] > [Inventory] に移動してインベントリを実行するか、定期的なインベントリが実行されるのを待つ必要があります。
Communication	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。
Faults	サーバで記録された障害の詳細。
Users	ユーザの詳細。
Cisco IMC Log	サーバの Cisco IMC ログの詳細。
System Event Log	サーバ ログの詳細。
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。
Fault History	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、 Cisco IMC Supervisor アプライアンス、ローカル ディレクトリに、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使用できます。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, （74 ページ） を参照してください。
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。

はじめる前に

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 メニュー バーで、[Systems] > [Inventory and Fault Status] を選択します。

ステップ 2 左側のペインで [Rack Groups] を選択します。

ステップ 3 右側のペインで、[Faults] タブを選択します。

ステップ 4 リストのサーバをダブルクリックして詳細を表示するか、リストのサーバをクリックし、右端の下向き矢印をクリックして [View Details] を選択します。

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

ラックマウント サーバに関する次の詳細を表示できます。

タブ	説明
Explanation	問題の原因の要約。
Recommendation	問題を解決する手順。

ステップ 5 [Fault Details] ウィンドウで [Close] をクリックすると、前のウィンドウに戻ります。

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。

はじめる前に

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 メニュー バーで、[Systems] > [Inventory and Fault Status] を選択します。

ステップ 2 左側のペインで [Rack Groups] を選択します。

ステップ 3 右側のペインで、[Rack Servers] タブを選択します。

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] または [Power OFF] をクリックするか、右クリックしてオプションを選択します。

（注） リストからサーバを選択するまでは、[Power On] および [Power Off] ボタンは表示されません。

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。

はじめる前に

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 メニュー バーで、[Systems] > [Inventory and Fault Status] を選択します。

ステップ 2 左側のペインで [Rack Groups] を選択します。

ステップ 3 右側のペインで、[Rack Servers] タブを選択します。

ステップ 4 リストからサーバを選択します。

ステップ 5 [Shut Down] をクリックするか、右クリックしてオプションを選択します。

（注） リストからサーバを選択するまでは、[Shut Down] ボタンは表示されません。また、右端にある下矢印を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。

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。

はじめる前に

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 メニュー バーで、[Systems] > [Inventory and Fault Status] を選択します。

ステップ 2 左側のペインで [Rack Groups] を選択します。

ステップ 3 右側のペインで、[Rack Servers] タブを選択します。

ステップ 4 リストからサーバを選択します。

ステップ 5 [Hard Reset] 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、[Hard Reset] ボタンは表示されません。また、右端にある下矢印を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。

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。

はじめる前に

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 メニュー バーで、[Systems] > [Inventory and Fault Status] を選択します。
ステップ 2 左側のペインで [Rack Groups] を選択します。
ステップ 3 右側のペインで、[Rack Servers] タブを選択します。
ステップ 4 リストからサーバを選択します。
ステップ 5 [Power Cycle] 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、[Power Cycle] ボタンは表示されません。また、右端にある下矢印を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。

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。

はじめる前に

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 メニュー バーで、[Systems] > [Inventory and Fault Status] を選択します。
ステップ 2 左側のペインで [Rack Groups] を選択します。
ステップ 3 右側のペインで、[Rack Servers] タブを選択します。
ステップ 4 リストからサーバを選択します。
ステップ 5 [KVM Console] 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、[KVM Console] ボタンは表示されません。
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。

必要な Java ランタイム環境（JRE）がインストールされていない場合は、ダイアログボックスの [More Info] をクリックし、画面の手順に従って JRE をダウンロードしてインストールします。

ラックマウント サーバの GUI の起動

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

はじめる前に

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 メニュー バーで、[Systems] > [Inventory and Fault Status] を選択します。
ステップ 2 左側のペインで [Rack Groups] を選択します。
ステップ 3 右側のペインで、[Rack Servers] タブを選択します。
ステップ 4 リストからサーバを選択します。
ステップ 5 [Launch GUI] 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、[Launch GUI] ボタンは表示されません。
ステップ 6 [Launch GUI] ダイアログボックスで、[Submit] をクリックします。
サーバの GUI が別のブラウザで起動します。

ラックマウント サーバのロケータ LED の設定

サーバ ロケータ LED を使用すると、データセンター内の多数のサーバ間で特定のサーバを識別できます。LED をオン/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。

はじめる前に

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 メニュー バーで、[Systems] > [Inventory and Fault Status] を選択します。
ステップ 2 左側のペインで [Rack Groups] を選択します。
ステップ 3 右側のペインで、[Rack Servers] タブを選択します。
ステップ 4 リストからサーバを選択します。
ステップ 5 [Locator LED] 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、[Locator LED] ボタンは表示されません。

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 [Submit] をクリックします。

ステップ 8 [Submit Result] ダイアログボックスで、[OK] 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。

はじめる前に

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 メニュー バーで、[Systems] > [Inventory and Fault Status] を選択します。

ステップ 2 左側のペインで [Rack Groups] を選択します。

ステップ 3 右側のペインで、[Rack Servers] タブを選択します。

ステップ 4 リストからサーバを選択します。

ステップ 5 [Set Label] 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、[Set Label] ボタンは表示されません。

ステップ 6 新しいラベルを入力します。

ステップ 7 [Submit] をクリックします。

ステップ 8 [Submit Result] ダイアログボックスで、[OK] 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、またはオペレーティング システムなどの情報を提供するために使用できます。タグを追加または変更するには、次の手順を実行します。

はじめる前に

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 メニュー バーで、[Systems] > [Inventory and Fault Status] を選択します。

ステップ 2 左側のペインで、[Rack Groups] を展開し、サーバを含むラック グループを選択します。

ステップ 3 右側のペインで、[Rack Servers] タブを選択します。

ステップ 4 [Manage 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、[Manage Tags] ボタンは表示されません。

ステップ 5 新しいタグを追加するには、プラス アイコンをクリックします。

ステップ 6 [Add Entry to Tag] ダイアログボックスで、次のように入力します。

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。 **a** [Name] フィールドに、タグを記述する名前を入力します。 **b** [Description] フィールドに、タグの説明を入力します。 **c** [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。 **d** [Possible Tag Values] フィールドで、可能なタグ値を入力します。 **e** [Next] をクリックします。 **f** [+]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。 **4** 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。 **5** [Submit] をクリックします。 （注） タグは、タグ付け可能なエンティティの設定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

フィールド	説明
	クします。
Tag Value	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 [Submit] をクリックします。

ステップ 8 [Submit Result] ダイアログボックスで、[OK] をクリックします。

ステップ 9 [Manage Tags] ダイアログボックスでタグを選択し、[Edit] アイコンをクリックしてタグを編集できます。

ステップ 10 タグ名とタグ値を選択して、タグを変更します。

ステップ 11 [Submit] をクリックします。

ステップ 12 [Submit Result] ダイアログボックスで、[OK] 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。

はじめる前に

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 メニュー バーで、[Systems] > [Inventory and Fault Status] を選択します。

ステップ 2 左側のペインで、[Rack Groups] を展開し、サーバを含むラック グループを選択します。

ステップ 3 右側のペインで、[Rack Servers] タブを選択します。

ステップ 4 [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 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, （69 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。

手順

ステップ 1 メニュー バーで、[Systems] > [Inventory and Fault Status] を選択します。

ステップ 2 左側のペインで [Rack Groups] を選択します。

ステップ 3 右側のペインで、[Rack Servers] タブを選択します。

ステップ 4 リストのサーバをダブルクリックして詳細を表示するか、リストのサーバをクリックし、右端の下向き矢印をクリックして [View Details] を選択します。

ステップ 5 [Tech Support] タブをクリックします。

ステップ 6 [Upload Logs] をクリックします。

ステップ 7 [Upload Technical Logs] 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
[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。 • TFTP • FTP • SFTP • SCP
[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。

名前	説明
[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 メニュー バーで、[Systems] > [Inventory and Fault Status] を選択します。

ステップ 2 左側のペインで [Rack Groups] を選択します。

ステップ 3 右側のペインで、[Rack Servers] タブを選択します。

ステップ 4 リストのサーバをダブルクリックして詳細を表示するか、リストのサーバをクリックし、右端の下向き矢印をクリックして [View Details] を選択します。

ステップ 5 [System Event Log] タブをクリックします。

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] ダイアログボックスで、[Delete historical logs from Cisco IMC Supervisor] チェックボックスをオンにします。
このオプションを選択すると、Cisco IMC 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 [Submit] をクリックします。

システム タスクの管理

[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 メニュー バーで、[Administration] > [System] を選択します。

ステップ 2 [System Tasks] タブをクリックします。

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] ダイアログボックスで、次の手順を実行します。

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
[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。

ステップ 5 [Submit] をクリックします。

ステップ 6 [OK] 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 メニュー バーで、[Administration] > [System] を選択します。

ステップ 2 [System Tasks] タブをクリックします。

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] 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 [OK] 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, （80 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 メニュー バーで、[Policies] > [Manage Policies] > [Credential Policies] 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 [Add Credential Policy] 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。

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 4 [Submit] をクリックします。

ステップ 5 確認ダイアログボックスで、[OK] をクリックします。
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。

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 内に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に示します。

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。
   a. 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, （81 ページ）を参照してください。
   b. 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, （105 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, （106 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。
   a. Edit
   b. Delete
   c. Clone
   d. 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, （107 ページ）を参照してください。
   e. 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, （111 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 メニュー バーで、[Policies] > [Manage Policies and Profiles] を選択します。

ステップ 2 [Hardware Policies] タブを選択します。

ステップ 3 [Add] をクリックします。

ステップ 4 [Add Policy] ダイアログボックスで、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、以下の表に示されているポリシー タイプを選んでください。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。

ポリシー タイプ	『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』内のセクション
BIOS ポリシー, （83 ページ）	*BIOS* の設定
ディスク グループ ポリシー, （84 ページ）	ストレージ アダプタの管理
FlexFlash ポリシー, （85 ページ）	*Flexible Flash* コントローラの管理
IPMI Over LAN ポリシー, （89 ページ）	*IPMI* の設定
LDAP ポリシー, （90 ページ）	*LDAP* サーバの設定
レガシー ブート順序ポリシー, （91 ページ）	サーバのブート順
ネットワーク構成ポリシー, （92 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, （94 ページ）	ネットワーク セキュリティの設定
NTP ポリシー, （95 ページ）	ネットワーク タイム プロトコル設定の設定
高精度のブート順序ポリシー, （96 ページ）	高精度ブート順の設定
RAID ポリシー, （97 ページ）	ストレージ アダプタの管理
Serial over LAN ポリシー, （98 ページ）	*Serial over LAN* の設定
SNMP ポリシー, （99 ページ）	*SNMP* の設定
SSH ポリシー, （100 ページ）	*SSH* の設定
ユーザ ポリシー, （101 ページ）	ローカル ユーザの設定

ポリシー タイプ	『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』内のセクション
VIC アダプタ ポリシー, （103 ページ）	*VIC* アダプタのプロパティの表示
仮想 KVM ポリシー, （102 ページ）	仮想 *KVM* の設定
vMedia ポリシー, （104 ページ）	仮想メディアの設定

次の作業

サーバに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, （106 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 ポリシーを作成することができます。あるサーバの BIOS ポリシーを指定しない場合、BIOS 設定は現状のまま、つまり、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 Cisco IMC を使って設定された値のセットになります。BIOS ポリシーを指定した場合、サーバで設定済みの値が、ポリシーで指定された値に置き換わります。

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

BIOS 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] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、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 [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] 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のタスクの実行については、既存の設定からのポリシーの作成, （105 ページ）を参照してください。

（注） Cisco IMC Supervisor のプロパティまたは属性のうち、特定の Cisco IMC バージョンを実行するサーバに該当しないものがある場合、それらは適用できません。プロパティが Cisco IMC サーバで利用可能でない場合、そのプロパティ フィールドには [Platform-Default] として表示されます。

ステップ 4 [Main] ダイアログボックスで、主要な BIOS プロパティ（[Boot Option Retry]、[Post Error Pause]、[TPM Support] ドロップダウン リストなど）の値を選択します。

ステップ 5 [Advanced] ダイアログボックスで、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 6 [Server Management] ダイアログボックスで、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。

ステップ 7 [Submit Result] ダイアログボックスで、[OK] をクリックします。

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, （97 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] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、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 [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] ダイアログボックスで、仮想ドライブ プロパティを選択して [Next] をクリックします。

ステップ 5 [Local Disk Configuration] ダイアログボックスで、[+] 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。

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

ステップ 7 [Main] ダイアログボックスで [Submit] をクリックします。

ステップ 8 [Submit Result] ダイアログボックスで、[OK] 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] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、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 [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] 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のタスクの実行については、既存の設定からのポリシーの作成, （105 ページ）を参照してください。

ステップ 4 [Configure Cards] 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。

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。
[Partition Name] フィールド	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。

ステップ 7 [Submit Result] ダイアログボックスで、[OK] 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. ポリシーの新しい設定が適用されます。したがって、この手順で失敗すると、ポリシーを適用する前に既存の設定が失われます。

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] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、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 [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] 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のタスクの実行については、既存の設定からのポリシーの作成, （105 ページ）を参照してください。

ステップ 4 [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。

ステップ 5 [Submit] をクリックします。

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

LDAP ポリシー

Cisco C シリーズと E シリーズのサーバは LDAP をサポートし、Cisco IMC Supervisor は LDAP ポリシーを使用してサーバでの LDAP 設定をサポートします。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 LDAP 設定のグループを含む、1 つ以上の LDAP ポリシーを作成することができます。

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-Series Servers Integrated Management Controller GUI Configuration Guide*』の「*Configuring LDAP Server*」の項を参照してください。

LDAP 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] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、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 [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] 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のタスクの実行については、既存の設定からのポリシーの作成, （105 ページ）を参照してください。

ステップ 4 [Main] ダイアログボックスで、LDAP プロパティを入力します。

ステップ 5 [Next] をクリックします。

ステップ 6 [LDAP Servers] ダイアログボックスで、LDAP サーバの詳細を入力します。

ステップ 7 [Next] をクリックします。

ステップ 8 [Group Authorization] ダイアログボックス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 9 [Add Entry to LDAP Groups] ダイアログボックスで、グループの詳細を入力します。

ステップ 10 [Submit] をクリックします。

ステップ 11 [Submit Result] ダイアログボックスで、[OK] をクリックします。

ステップ 12 [Group Authorization] ダイアログボックスで [Submit] をクリックします。

ステップ 13 [Submit Result] ダイアログボックスで、[OK] をクリックします。

（注）
- 設定済みの LDAP ロール グループがサーバに存在する場合、それらはすべて削除され、ポリシーで設定したロール グループに置き換わります。ポリシーにロール グループをまだ追加していない場合、サーバ上の既存のロール グループは削除されますが、置換されません。
- [Nested Group Search Depth] は、Cisco IMC バージョン 2.0(4c) 以上にのみ適用できます。2.0(4c) より前のバージョンの Cisco IMC を実行しているサーバには、ポリシーを使っ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。高精度ブート順序の詳細については、 高精度のブート順序ポリシー, （96 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。

レガシー 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] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、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 [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] 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のタスクの実行については、既存の設定からのポリシーの作成, （105 ページ）を参照してください。

ステップ 4 [Main] ダイアログボックスで [+] 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] ダイアログボックスで [Submit] をクリックします。

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

ステップ 7 [Main] ダイアログボックスで [Submit] をクリックします。

ステップ 8 [Submit Result] ダイアログボックスで、[OK] をクリックします。

（注） このポリシーは、2.0 より前のバージョンの Cisco IMC にのみ適用できます。それ以降のバージョンの Cisco IMC を実行するサーバに対して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、ダイナミック DNS、IPv4、IPv6、VLAN などの各種プロパティを使用して、ネットワーク構成ポリシーを作成できます。

さまざまなネットワーク構成プロパティの設定の詳細については、『*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。

はじめる前に

手順

ステップ 1 [Hardware Policies] ページで、[Add] をクリックします。このページに移動する方法の詳細については、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] 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のタスクの実行については、既存の設定からのポリシーの作成, （105 ページ）を参照してください。

ステップ 4 [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。

フィールド	説明
共通のプロパティ	
[Use Dynamic DNS] チェックボックス	ダイナミック DNS は、Cisco IMC Supervisor から 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。
IPv4 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。
[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 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。
[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。

フィールド	説明
VLAN プロパティ	
[Enable VLAN] チェックボックス	オンにすると、仮想 LAN に接続されます。

ステップ 5 [Submit] をクリックします。

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

ネットワーク セキュリティ ポリシー

Cisco IMC Supervisor は、ネットワーク セキュリティとして IP ブロッキングを使用します。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。

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] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、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 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] 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のタスクの実行については、既存の設定からのポリシーの作成, （105 ページ）を参照してください。

ステップ 4 [Main] ダイアログボックスで、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 5 [Submit] をクリックします。

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

NTP ポリシー

NTP サービスを使用すると、NTP サーバとの間で時刻を同期するよう、Cisco IMC Supervisor によって管理されるサーバを設定できます。デフォルトでは、Cisco IMC Supervisor では NTP サーバが動作しません。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、管理対象サーバと設定済み NTP サーバとの間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] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、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 [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] 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のタスクの実行については、既存の設定からのポリシーの作成, （105 ページ）を参照してください。

ステップ 4 [Main] ダイアログボックスで、[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 5 [Submit] をクリックします。

ステップ 6 [Submit Result] ダイアログボックスで、[OK] 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。

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、ブート順序とブート モードの変更、各デバイス タイプの下への複数のデバイスの追加、ブート順序の並び替え、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用に作成できます。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] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、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 [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] 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のタスクの実行については、既存の設定からのポリシーの作成, （105 ページ）を参照してください。

ステップ 4 [Main] ダイアログボックスで、[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 5 [+] 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。

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

ステップ 7 [Submit Result] ダイアログボックスで、[OK] をクリックします。

ステップ 8 [Main] ダイアログボックスで [Submit] をクリックします。

ステップ 9 [Submit Result] ダイアログボックスで、[OK] をクリックします。

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) 以上。
- 単一のストレージ コントローラを含むサーバ。複数のストレージ コントローラを含むサーバでは、RAID ポリシーは最初のスロットのストレージ コントローラにのみ適用されます。

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 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] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、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 [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] 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のタスクの実行については、既存の設定からのポリシーの作成, （105 ページ）を参照してください。

ステップ 4 [Main] ダイアログボックスで [+] をクリックすると、サーバ上に設定する仮想ドライブを [Virtual Drives] リストに追加できます。

ステップ 5 [Add Entry to Virtual Drives] ダイアログボックスで、仮想ドライブの詳細を入力または選択します。ドロップダウン リストから既存のディスク グループ ポリシーを選択して編集するか、新しいディスク グループ ポリシーを追加してローカルディスクを指定することができます。ディスク グループ ポリシーを作成するには、ディスク グループ ポリシー, （84 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。

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

ステップ 7 [Submit Result] ダイアログボックスで、[OK] をクリックします。

ステップ 8 サーバ上の既存のすべての仮想ドライブを削除するには、[Erase existing Virtual Drives] チェックボックスをオンにします。
このチェックボックスを選択した場合、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。その結果、既存のデータは消失します。

ステップ 9 残りのディスクを JBOD として設定するには、[Configure remaining disks as JBOD] チェックボックスをオンにします。
このオプションは、JBOD をサポートするストレージ コントローラにのみ適用できます。仮想ドライブやホット スペアに使用されないディスクは、JBOD として設定されます。

ステップ 10 [Main] ダイアログボックスで [Submit] をクリックします。

ステップ 11 [Submit Result] ダイアログボックスで、[OK] 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。Cisco IMC Supervisor を使用してホスト コンソールに到達するには、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] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、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 [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] 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のタスクの実行については、既存の設定からのポリシーの作成, （105 ページ）を参照してください。

ステップ 4 [Main] ダイアログボックスで、[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 5 [Submit] をクリックします。

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

SNMP ポリシー

Cisco IMC Supervisor は Simple Network Management Protocol（SNMP）の設定をサポートし、管理対象サーバから SNMP トラップによって障害とアラートの情報を送信するための設定が可能です。

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] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、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 [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] 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のタスクの実行については、既存の設定からのポリシーの作成, （105 ページ）を参照してください。

ステップ 4 [SNMP Users] ダイアログボックスで [+] 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。

ステップ 5 [Next] をクリックします。

ステップ 6 [SNMP Traps] ダイアログボックスで [+] 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 7 [Next] をクリックします。

ステップ 8 [SNMP Settings] ダイアログボックスで、SNMP プロパティを設定します。

ステップ 9 [Submit] をクリックします。

ステップ 10 [Submit Result] ダイアログボックスで、[OK] 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 サーバでは [SNMP Port] を設定できません。チェックボックスを使用して、そのようなサーバは除外する必要があります。
- Cisco IMC バージョン 2.x を実行している E シリーズ サーバでは [SNMP Port] を設定できません。チェックボックスを使用して、そのようなサーバは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] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、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 [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] 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のタスクの実行については、既存の設定からのポリシーの作成, （105 ページ）を参照してください。

ステップ 4 [Main] ダイアログボックスで [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 5 [Submit] をクリックします。

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

ユーザ ポリシー

ユーザ ポリシーは、ローカル ユーザの設定を自動化します。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。

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 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] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、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 [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] 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のタスクの実行については、既存の設定からのポリシーの作成, （105 ページ）を参照してください。

ステップ 4 [Main] ダイアログボックスで、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 5 [+] をクリックして、ユーザを追加します。

ステップ 6 [Add Entry to Users] ダイアログボックスで、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。
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。
Enabled	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。

フィールド	説明
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。
Confirm New Password	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 7 [Submit] をクリックします。

ステップ 8 [Submit Result] ダイアログボックスで、[OK] をクリックします。
また、[Main] ダイアログボックスの [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。
- ユーザ ポリシーを適用すると、Cisco IMC Supervisor 内のユーザ エントリが、作成したユーザ エントリに置き換わります。Cisco IMC 内の空白のエントリは Cisco IMC Supervisor のデフォルト ユーザに置き換えられます。デフォルト ユーザ ロールは常に読み取り専用であり、ユーザは無効になっています。
- Cisco IMC Supervisor の管理に使用されるアカウントは、ポリシーのユーザ リストから決して削除しないでください。削除した場合、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] ページで、[Add] をクリックします。

このページに移動する方法の詳細については、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 [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] 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のタスクの実行については、既存の設定からのポリシーの作成, （105 ページ）を参照してください。

ステップ 4 [Enable vKVM] チェックボックスをオンにします。

ステップ 5 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 6 [Submit] をクリックします。

ステップ 7 [Submit Result] ダイアログボックスで、[OK] をクリックします。

VIC アダプタ ポリシー

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「*Viewing VIC Adapter Properties*」の項を参照してください。

VIC アダプタ 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] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、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 [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] 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のタスクの実行については、既存の設定からのポリシーの作成, （105 ページ）を参照してください。

ステップ 4 [Main] ダイアログボックスで [+] 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 5 [Add Entry to VIC Adapters] ダイアログボックスで、アダプタの詳細を入力または選択します。

- [vNIC]：デフォルト プロパティは eth0 および eth1 です。これらのプロパティは編集のみが可能であり、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。
- [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。

ステップ 6 [Submit] をクリックします。

ステップ 7 [Submit Result] ダイアログボックスで、[OK] をクリックします。

ステップ 8 [Main] ダイアログボックスで [Submit] をクリックします。

ステップ 9 [Submit Result] ダイアログボックスで、[OK] 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、最大で 2 つの vMedia マッピングを設定できます。1 つは（CDD を介した）ISO ファイル用、もう 1 つは（HDD を介した）IMG ファイル用です。

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] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、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 [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] 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のタスクの実行については、既存の設定からのポリシーの作成, （105 ページ）を参照してください。

ステップ 4 [Main] ダイアログボックスで、[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 5 [Next] をクリックします。

ステップ 6 [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 7 [Next] をクリックします。

ステップ 8 [Add HDD vMedia Mapping] チェックボックスをオンにして、HDD マッピングの詳細を入力します。

ステップ 9 [Submit] をクリックします。

ステップ 10 [Submit Result] ダイアログボックスで、[OK] をクリックします。

（注）
- 現在、Cisco IMC Supervisor では [Low Power USB State] を設定できません。
- 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。

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] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、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] ダイアログボックスで、[Create policy from current configuration of the server] チェックボックスをオンにします。次の 2 つの方法でサーバの詳細を使用できます。

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。

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] ダイアログボックスに進みます。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 メニュー バーで、[Policies] > [Manage Policies] を選択します。

ステップ 2 [Hardware Policies] タブを選択します。

ステップ 3 左側のペインから、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。

ステップ 5 [Apply Policy] ダイアログボックスで、個別のサーバまたはラック サーバ グループ全体のどちらにポリシーを適用するかに応じて、ドロップダウン リスト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 6 [Select] をクリックして、ポリシーの適用対象となるサーバ グループまたはサーバを選択します。

ステップ 7 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 8 [Schedule] ドロップダウン リストから既存のスケジュールを選択するか、[+] をクリックして新しいスケジュールを作成します。スケジュール作成の詳細については、スケジュールの作成, （125 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 9 [Submit] をクリックします。

ステップ 10 [Submit Result] ダイアログボックスで、[OK] 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 メニュー バーで、[Policies] > [Manage Policies and Profiles] を選択します。

ステップ 2 [Hardware Policies] タブを選択します。

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, （106 ページ）を参照してください。

ステップ 5 状況に応じて [Submit] または [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。

次のワークフローは、Cisco IMC Supervisor でハードウェア プロファイルを使用する方法を示しています。

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。
   a. 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, （108 ページ）を参照してください。
   b. 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, （109 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, （111 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。
   a. Edit
   b. Delete
   c. 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, （111 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

ハードウェア 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 メニュー バーで、[Policies] > [Manage Policies and Profiles] を選択します。

ステップ 2 [Hardware Profiles] タブを選択します。

ステップ 3 [Add] をクリックします。

ステップ 4 [Hardware Profile] ダイアログボックスの [Profile Name] フィールドで、作成するプロファイルの名前を入力します。

ステップ 5 [Next] をクリックするか、[Create profile 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。
[Server Details] ウィンドウでタスクを実行するには、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 6 [Profile Entities] ダイアログボックスで [+] をクリックして、プロファイル エントリを追加します。また、編集アイコンや削除アイコンをクリックして、既存のエントリを編集および削除することもできます。

ステップ 7 [Add Entry to Profile Name] ダイアログボックスで、[Policy Type] を選択します。

ステップ 8 既に作成済みのポリシーの名前をリストする [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、既に選択したポリシー タイプに基づく新しいポリシーを作成できます。ポリシーの作成の詳細については、以下を参照してください。 ハードウェア ポリシーの作成, （81 ページ）

ステップ 9 [Submit] をクリックします。

ステップ 10 [Submit Result] 確認ダイアログボックスで、[OK] をクリックします。

ステップ 11 [Profile Entities] ダイアログボックスで [Submit] をクリックします。

ステップ 12 [Submit Result] 確認ダイアログボックスで、[OK] をクリックします。

次の作業

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することもできます。これらのタスクの実行については、以下を参照してください。
ハードウェア プロファイルでの一般タスク, （111 ページ）

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 メニュー バーで、[Policies] > [Manage Policies and Profiles] を選択します。

ステップ 2 [Hardware Profiles] タブを選択します。

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を使用できます。

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] ダイアログボックスで [+] 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 [Submit Result] ダイアログボックスで、[OK] 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 メニュー バーで、[Policies] > [Manage Policies and Profiles] を選択します。

ステップ 2 [Hardware Profiles] タブを選択します。

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。

ステップ 4 [Apply Profile] ダイアログボックスで、個別のサーバまたはラック サーバ グループ全体のどちらにプロファイルを適用するかに応じて、ドロップダウン リスト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] をクリックして、プロファイルの適用対象となるサーバ グループまたはサーバを選択します。

ステップ 6 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 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。スケジュール作成の詳細については、スケジュールの作成, （125 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。

ステップ 9 [Submit Result] 確認ダイアログボックスで、[OK] 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 メニュー バーで、[Policies] > [Manage Policies and Profiles] > [Hardware Profiles] を選択します。

ステップ 2 左側ペインの [Hardware Profile] を展開して、[Hardware Profiles] ページで、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。[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。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, （111 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 3 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 メニュー バーで、[Policies] > [Tag Library] を選択します。

ステップ 2 [Create] をクリックします。

ステップ 3 [Create Tag] ダイアログボックスで、[Tag Details] 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。
[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 • 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、タグ付け可能なエンティティの設定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 確認ダイアログボックスで、[OK] をクリックします。

ステップ 7 [Create Tag] ダイアログボックスで、[Submit] をクリックします。

ステップ 8 [OK] 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。

第 9 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。

シスコは、すべての Cisco IMC Supervisor コンポーネントをアップグレードするためのファームウェアのアップデートをまとめて提供します。ファームウェアのアップデートは、cisco.com からダウンロードできます。サーバが Cisco IMC Supervisor で管理されていない場合はアップグレードできません。E シリーズ 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。

手順

ステップ 1 メニュー バーで、[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] ダイアログボックスで、次の手順を実行します。

フィールド	説明
[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。

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。
[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設定を有効化し、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。
[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。 • [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。
[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。
[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。
[Accept License Agreement]	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 [Submit] をクリックします。

ステップ 5 [Submit Result] ダイアログボックスで、[OK] 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 イメージの詳細の変更や、イメージ プロファイルの削除をすることができます。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 システムに ISO イメージをアップロードするには、次の手順を実行します。

手順

ステップ 1 メニュー バーで、[Systems] > [Firmware Management] を選択します。

ステップ 2 [Images - Local] タブをクリックし、[Upload] をクリックしてイメージを追加します。

ステップ 3 [Upload Firmware Image - Local] 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
[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 Name] フィールド	ローカル ファイル システムでアップロードするファイルを検索して選択するには、[Browse] を選択します。

ステップ 4 [Upload] をクリックします。

ステップ 5 アップロードが完了したら、[File Upload] 確認ダイアログ ボックスで [OK] をクリックします。

ステップ 6 [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 メニュー バーで、[Systems] > [Firmware Management] を選択します。

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

フィールド	説明
[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。
[Server Type] ドロップダウン リスト	ネットワーク ファイル システム（NFS）、Common Internet File System（CIFS）またはHTTP/S 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。
[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。

フィールド	説明
[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。

ステップ 4 [Submit] をクリックします。

ステップ 5 [Submit Result] ダイアログボックスで、[OK] 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

ファームウェアをアップグレードする場合は次の手順を実行します。

はじめる前に

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。

手順

ステップ 1 メニュー バーで、[Systems] > [Firmware Management] を選択します。

ステップ 2 [Firmware Upgrades] タブをクリックします。

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更新ツールが起動すること、およびファームウェア更新の完了後にサーバがリブートして元のホスト OS が起動することが通知されます。

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] ダイアログボックスで、次の手順を実行します。

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。
[Server(s)] ボタン	[Select] をクリックして、リストからサーバを選択します。選択したプロファイルで設定されているプラットフォームに一致するサーバだけがリストに表示されます。
[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, （125 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 [Upgrade Firmware] ダイアログボックスで、[Submit] をクリックします。

ステップ 7 [OK] 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。

第 10 章

Cisco IMC Supervisor 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、シスコの自動ソフトウェア配布（ASD）サービスを使用して、cisco.com で使用可能な新しいパッチ更新の有無を定期的に（14 日ごとに）確認します。現在のリリース以降のパッチ更新があれば、Cisco IMC Supervisor 更新マネージャーによってパッチが Cisco IMC Supervisor 内の場所にダウンロードされます。その後、Shell Admin に移動して、パッチを適用できます。パッチの適用に関する詳細については、『*Cisco IMC Supervisor Shell Guide*』の「*Applying a Patch to Cisco IMC Supervisor*」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。

更新設定の実行

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。これらの詳細が Cisco IMC Supervisor によって使用され、Cisco ASD のバックエンド サービスと通信して、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。Cisco IMC Supervisor の新しいバージョンがあるときに通知されるように設定を行う必要があります。より高いバージョンが使用可能な場合は、

[Diagnostic System Messages] ダイアログボックスに、Cisco IMC Supervisor の新しいバージョンが見つかったことを示すメッセージが表示されます。更新設定を行うには、次の手順を実行します。

（注） 更新設定を行っていない場合は、右上隅のログイン名の横に通知バブルが表示されます。[Diagnostic System Messages] ダイアログボックスに、設定が行われていないことを示すメッセージが表示されます。

手順

ステップ 1 メニュー バーで、[Administration] > [Update IMCS] を選択します。
[IMCS Update Report] に、現在のバージョン、利用可能なアップグレード バージョン、アップグレード ステータス、ファイルがダウンロードされている場所などが表示されます。

ステップ 2 [Configure Update Settings] をクリックします。

ステップ 3 [Manage Update Settings] 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
[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。
[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設定を有効化し、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。
[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。 • [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 [Submit] をクリックします。

ステップ 5 [Submit Result] ダイアログボックスで、[OK] をクリックします。

（注） URL https://cloudsso.cisco.com.null と https://api.cisco.com/ 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。

第 11 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 メニュー バーで、[Policies] > [Manage Schedules] 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 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] 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。

ステップ 5 [Submit Result] ダイアログボックスで、[OK] をクリックします。

次の作業

- 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, （106 ページ）、またはハードウェア プロファイルの適用, （111 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 12 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。

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、scpuser パスワードを設定する必要があります。scpuser パスワードを設定するには、SCP ユーザの設定，（29 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 メニュー バーから、[Systems] > [Server Diagnostics] を選択します。

ステップ 2 [Configure SCU Image Location] をクリックします。

ステップ 3 [Configure SCU Image Location] 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
[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。
[ISO Share Type] ドロップダウン リスト	ネットワーク ファイル システム（NFS）、Common Internet File System（CIFS）または World Wide Web（WWW）の共有タイプを選択します。
[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 4 [Save] をクリックします。

ステップ 5 [Submit Result] ダイアログボックスで、[OK] 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。

手順

ステップ 1 メニュー バーから、[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] 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
[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 [Submit] をクリックします。

ステップ 7 [Submit Result] ダイアログボックスで、[OK] 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 13 章

Cisco IMC Supervisor 向け Smart Call Home

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 によって管理されているハードウェアに有効なサポート契約があれば使用できます。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。

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、Cisco IMC Supervisor が管理するサーバ タスクは、定期的に実行され、関連情報を Smart Call Home の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 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，（131 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 メニュー バーから、[Administration] > [System] > [Smart Call Home] の順に選択します。

ステップ 2 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 3 [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 4 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。

ステップ 5 （オプション）[Enable Proxy] チェックボックスをオンにし、次の情報を入力します。

a) [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。

b) [Host Name or IP Address] フィールド：プロキシ サーバのホスト名または IP アドレスを入力します。

c) [Port] フィールド：プロキシ設定用のポートを入力します。

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。

ステップ 8 [Submit Result] ダイアログボックスで、[OK] 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。さまざまな障害コードと重大度については、障害コード, （132 ページ） を参照してください。Smart Call Home にログインし、さまざまなタスクを実行する方法についての詳細は https://supportforums.cisco.com/community/4816/smart-call-home を参照してくあさい。Smart Call Home のバックエンドで受信したメッセージを表示する方法についての詳細は http://tools.cisco.com/sch/ 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

以下は、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です。

障害コード	障害名	メッセージ	重大度
F0868	fltComputeBoardPowerFail	Motherboard of [serverid] power: [power]	critical
F0424	fltComputeBoardCmosVoltageThresholdCritical	CMOS battery voltage on [serverid] is [cmosVoltage]	major
F0425	fltComputeBoardCmosVoltageThresholdNonRecoverable	CMOS battery voltage on [serverid] is [cmosVoltage]	critical
F0177	fltProcessorUnitThermalThresholdNonRecoverable	Processor [id] on [serverid] temperature:[thermal]	critical
F0379	fltEquipmentIOCardThermalProblem	IOCard [location] on server [id] operState: [operState]	major
F1004	fltStorageControllerInoperable	Storage Controller [id] operability: [operability]	critical
F0181	fltStorageLocalDiskInoperable	Local disk [id] on [serverid] operability: [operability]	major| warning
F1007	fltStorageVirtualDriveInoperable	Virtual drive [id] on [serverid] operability: [operability]	critical
F0531	fltStorageRaidBatteryInoperable	RAID Battery on [serverid] operability: [operability]	major
F0997	fltStorageRaidBatteryDegraded	Raid battery [id] on [serverid] operability: [operability]	major
F0185	fltMemoryUnitInoperable	DIMM [location] on [serverid] operability: [operability]	major
F0188	fltMemoryUnitThermalThresholdNonRecoverable	DIMM [location] on [serverid] temperature: [thermal]	critical

障害コード	障害名	メッセージ	重大度
F0385	fltEquipmentPsuThermalThresholdNonRecoverable	Power supply [id] in [serverid] temperature: [thermal]	critical
F0389	fltEquipmentPsuVoltageThresholdCritical	Power supply [id] in [serverid] voltage: [voltage]	major
F0391	fltEquipmentPsuVoltageThresholdNonRecoverable	Power supply [id] in [serverid] voltage: [voltage]	critical
F0407	fltEquipmentPsuIdentity	Power supply [id] on [serverid] has a malformed FRU	critical
F0411	fltEquipmentChassisThermalThresholdNonRecoverable	Thermal condition on [serverid] cause: [thermalStateQualifier]	critical
F0174	fltProcessorUnitInoperable	Processor [id] on [serverId] operability: [operability]	critical|major

第 14 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
Cisco IMC Supervisor へのログイン方法	Cisco IMC Supervisor の起動, （14 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, （15 ページ）
Cisco IMC Supervisor にログイン ユーザを追加する方法	ユーザの作成, （36 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, （48 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, （49 ページ）

その他の手順

次の項には、Cisco IMC Supervisor を使用して実行するさまざまな手順が含まれています。

ダッシュボード ビューの有効化

Cisco IMC Supervisor メニュー バーのダッシュボード 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。

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。

[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。

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。

はじめる前に

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 [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。

はじめる前に

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 ステップ 3 とステップ ステップ 4 を繰り返します。

ステップ 6 [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。

はじめる前に

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] 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。