概要

この章は、次の内容で構成されています。

About Cisco IMC Supervisor

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

Cisco IMC Supervisor を使用して次のタスクを実行できます。

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

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

ライセンスについて

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

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

重要

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

いずれのライセンスも、入手してインストールするためのプロセスは同じです。ライセンスを取得するには、次の手順を実行します。

1. Cisco IMC Supervisor をインストールする前に、Cisco IMC Supervisor ライセンス キーを生成し、証明書（製品アクセス キー）を要求します。
2. シスコのソフトウェア ライセンス サイトに製品アクセス キー（PAK）を登録します（製品アクセス キーの契約履行 （3 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」を参照してください。

製品アクセス キーの契約履行

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

始める前に

PAK 番号が必要です。

手順

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

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

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

ステップ 4 [Enter a Single PAK or TOKEN to Fulfill] フィールドに PAK 番号を入力します。

ステップ 5 [Fulfill Single PAK/TOKEN] をクリックします。

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

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

ステップ 7 [Issue Key] をクリックします。

ライセンス契約した機能が表示され、デジタル ライセンス契約書と zip 圧縮のライセンス ファイルが電子メールに添付されて、ユーザ指定の電子メール アドレスに送信されます。

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

ラック グループ

ラック グループとは、物理ラックマウント サーバの論理グループです。ラック グループは、C シリーズまたは E シリーズ（またはその両方）サーバの単一のコンバージド インフラスト

ラクチャ スタックを表します。必要に応じて、ラック グループを追加、変更、および削除することができます。

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

ラック アカウント

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

ポリシー

ポリシーは、Cisco IMC でのさまざまな属性設定を定義するための主要なメカニズムです。ポリシーは、複数のサーバにわたって設定の一貫性と反復可能性を確保するうえで役立ちます。包括的なポリシーセットを定義して使用すると、多数のサーバに類似する設定を適用できるので、一貫性、制御、予測可能性、自動化が促進されます。

プロファイル

複数のポリシーを組み合わせて、ハードウェア プロファイルが形成されます。たとえば、1つのラック ハードウェア プロファイル設定の詳細情報を複数のラックマウント サーバに適用することができます。いくつかの特定のラックマウント サーバにこのハードウェア プロファイルを関連付けることができます。これにより、複数のサーバにわたって設定の一貫性と反復可能性が確保されます。プロファイルを定義して使用すると、類似する設定が多数のサーバに適用されるため、一貫性、制御、予測可能性、自動化が促進されます。

Cisco IMC Supervisor ユーザ インターフェイス

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

ナビゲーションの変更

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

ユーザ インターフェイスのラベルの廃止

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

ダッシュボードを使用した詳細レポートへのアクセス

ダッシュボードが有効になっている場合は、これが Cisco IMC Supervisor にログインしたときに最初に表示される画面になります。通常はこのダッシュボードを使用して重要なレポートや頻繁にアクセスするレポートのウィジェットを追加します。**ダッシュボード**に表示されたレポートをクリックすると、より詳細な情報が表示されるユーザインターフェイスの画面にすぐにアクセスできるようになりました。「ダッシュボード ビューの有効化」を参照してください。さらに、複数のダッシュボードを作成したり、必要がなくなった場合はそれらを削除することができます。追加ダッシュボードの作成およびダッシュボードの削除を参照してください。

表形式レポートの機能強化

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

- 右クリックによる他のオプションの表示

  行を選択した後でマウスを右クリックすると、選択した行に関連するオプションのリストが表示されます。

- フィルタおよび検索

  Cisco IMC Supervisor インターフェイスの表形式レポートで [フィルタ（Filter）] オプション、または [検索（Search）] オプションが使用できます。表形式レポートの任意のページで [フィルタ（Filter）] オプションを使用すると、表形式レポートの結果を特定の基準で絞り込むことができます。この [フィルタ（Filter）] オプションは複数のページにまたがっていない表形式レポートで使用できます。複数のページにまたがる表形式レポートの場合は、[検索（Search）] オプションを使用して検索結果を絞り込みます。

- [お気に入り（Favorites）] メニューへの表形式レポートの追加

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

- 列のサイズ変更

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

- データがない場合に表示される情報メッセージ

  レポートに表示する情報がない場合は、次のメッセージが表示されます。

  データがありません

タブの削除と復元

使用できるタブが複数ある画面では、その画面に表示するタブの数を選択できます。画面上でタブを閉じると、そのタブはユーザインターフェイスに表示されるタブの行に表示されなくなります。そのタブを画面に戻すには、画面の右端に表示されている下向きの矢印をクリックします。使用可能ではあるものの非表示になっているタブのドロップダウン リストが表示されます。復元するタブを選択します。

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

レポート機能の強化

次に、ユーザ インターフェイスで使用できる、強化されたレポート機能の一部を示します。

- 円グラフと棒グラフの導入

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

- [他のレポート（More Reports）] オプションの可用性

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

ランディング ページ（Landing Page）

Cisco IMC Supervisor の管理者ポータルにログインすると、ランディング ページが開きます。ランディングページに表示される要素は、どのように表示を設定しているかによって異なります。デフォルトでは、ポータルにログインすると統合ビューが表示されます。

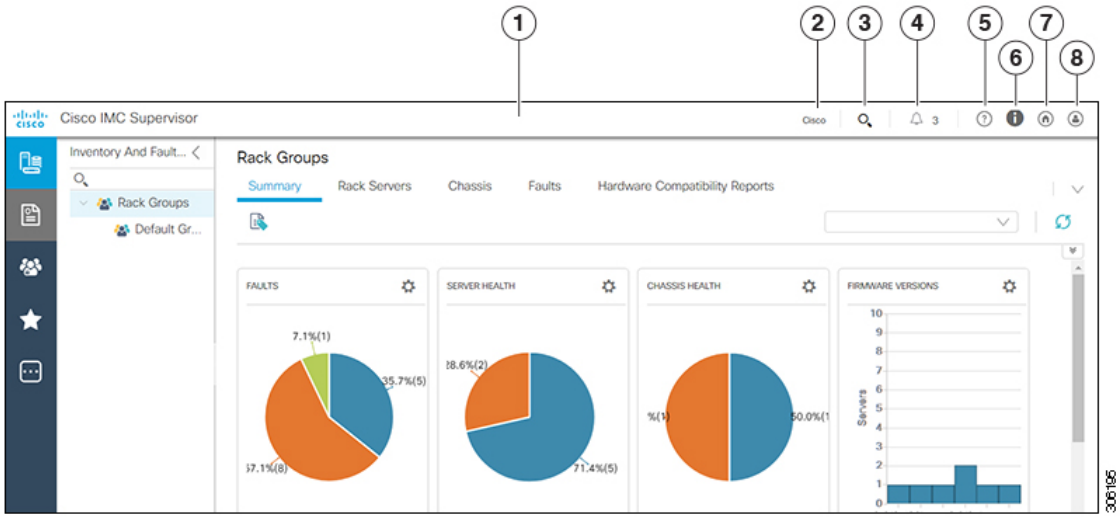
次に、ランディング ページで利用可能な要素を示します。

- ヘッダー：画面の上部に表示されます。

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

（注） このメニューにスクロールバーはありません。使用可能なスペースに収まる数のオプションのみが表示されます。一部のオプションは、画面を最小化したり、または拡大すると表示されないことがあります。使用可能なオプションをすべて表示するには、[サイトマップ（Site Map）] をクリックします。

図 *1*：新しいユーザ インターフェイス



番号	名前	説明
1	Header	メニューなどの頻繁にアクセスする要素が含まれています。ヘッダーは常に表示されています。
2	Link	ソフトウェアの仕様に関する情報にアクセスできるシスコの Web サイトへのリンクが提供されています。
3	[Search] アイコン	ポータルで特定のレポートを検索してそのレポートに直接移動できます。
4	[診断システム メッセージ（Diagnostic System Messages）] アイコン	ログに記録されている診断システム メッセージの数を表示します。このリンクをクリックすると、詳細情報を表示できる [診断システム メッセージ（Diagnostic System Messages）] 画面が表示されます。

番号	名前	説明
5	[ヘルプ（Help）] アイコン	管理者ポータルのオンライン ヘルプ システムにリンクしています。
6	[バージョン情報（About）] アイコン	ソフトウェアについての情報と、現在インストールされているバージョンが表示されます。
7	[ホーム（Home）] アイコン	ユーザ インターフェイスの任意の場所からランディング ページに戻ります。
8	[ユーザ（User）] アイコン	プロファイルの編集、ダッシュボードの有効化または無効化、ユーザインターフェイスのクラシック ビューへのアクセス、およびログアウトができます。

共通のユーザ インターフェイス オプション

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

アイコン	ラベル	説明
	**[更新（Refresh）]**	ページ上の報告されたデータを更新します。
	**お気に入り（Favorite）**	[Favorites] メニューにページを追加します。 このオプションを使用すると、頻繁にアクセスするページを簡単に表示できるようになります。
	**Add**	[Add] ダイアログ ボックスが表示されます。このダイアログボックスで新しいリソースを追加できます。
	**Edit**	[Edit] ダイアログ ボックスが表示されます。このダイアログボックスでリソースを編集できます。
	**Customize Table**	[Customize Report Table] ダイアログボックスが表示されます。このダイアログボックスで表示する列を選択できます。

アイコン	ラベル	説明
	**エクスポート レポート**	[Export Report] ダイアログ ボックスが表示されます。このダイアログ ボックスでレポートをシステムにダウンロードできます。 次のいずれかの形式でレポートを生成できます。 • PDF • CSV • XLS
	**Expand**	ページに表示されているすべてのフォルダを展開します。
	**Collapse**	ページに表示されているすべてのフォルダを折りたたみます。
	**Add Advanced Filter**	ページに追加のフィルタリング パラメータを提供します。
	**Search Field**	ページ上の特定のレコードをフィルタリングするためのキーワードを受け入れます。

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

システムへのセキュアな接続を設定するには、次の手順を実行します。

手順

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

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

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

ステップ 2 `web.xml` ファイルの次の行をアンコメントします。

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

これらの行は、ファイル内の任意の場所に追加できます。

ステップ 3 ユーザ インターフェイスを起動してシステムにログインします。

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

デフォルトでは、Cisco IMC Supervisor ユーザー インターフェイスはセキュア モードで起動します。セキュア モードをバイパスし、非セキュア モード（HTTP）でユーザ インターフェイスを起動するには、次の手順を実行する必要があります。

手順

ステップ 1 root としてログインします。

ステップ 2 /opt/infra/web_cloudmgr/apache-tomcat/conf/server.xml ファイルを次のように変更します。

a) 既存の 8080 ポート コネクタのタグをコメントアウトします。

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

b) 新しい 8080 ポート コネクタのタグとして次を追加します。

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

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

```
<!--
<security-constraint>
```

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

ステップ 4 サービスを再起動します。

ステップ 5 ユーザ インターフェイスを起動してシステムにログインします。

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

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

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