Cisco UCS Central Software HTML5 GUI ユーザ マニュアル リリース 1.3

初版：2015 年 04 月 06 日

最終更新：2015 年 05 月 06 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

この前書きは、次の項で構成されています。

対象読者

このガイドは、次の 1 つ以上に責任を持ち、専門知識を備えたデータセンター管理者を主な対象にしています。

- 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

表記法

テキストのタイプ	用途
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。
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。

テキストのタイプ	用途
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}	必ずいずれか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、このドキュメント以外の参照資料などを紹介しています。

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。

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。

ワンポイント アドバイス　時間を節約する方法です。 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。

Cisco UCS の関連ドキュメント

ドキュメント ロードマップ

すべての B シリーズ マニュアルの一覧については、http://www.cisco.com/go/unifiedcomputing/b-series-doc で入手できる『*Cisco UCS B-Series Servers Documentation Roadmap*』を参照してください。

すべての C シリーズ マニュアルの一覧については、http://www.cisco.com/go/unifiedcomputing/c-series-doc で入手できる『*Cisco UCS C-Series Servers Documentation Roadmap*』を参照してください。

管理用に UCS Manager と統合されたラック サーバに対してサポートされているファームウェアのバージョンとサポートされている UCS Manager のバージョンについては、『Release Bundle Contents for Cisco UCS Software』を参照してください。

その他のマニュアル リソース

ドキュメントの更新通知を受け取るには、Cisco UCS Docs on Twitter をフォローしてください。

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、HTMLmailto:ucs-docfeedback@cisco.com 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。

第 1 章

概要

この章は、次の内容で構成されています。

Cisco UCS Central の導入

Cisco UCS Central は、拡大する Cisco UCS 環境にスケーラブルな管理ソリューションを提供します。 Cisco UCS Central は、標準化、グローバル ポリシー、およびグローバル ID プールを通して、単一の管理ポイントからの複数の Cisco UCS ドメインの管理を簡略化します。 Cisco UCS Central は、単一の UCS ドメインのポリシー駆動型管理である Cisco UCS Manager を置き換えるものではありません。 代わりに、Cisco UCS Central は、世界中の複数の Cisco UCS Classic および Mini 管理ドメイン全体でのグローバル レベルの UCS ドメインの管理と監視に特化されています。

Cisco UCS Central を使用すれば、以下と組み合わせて、個別のまたはグループの Classic、Mini、または混合 Cisco UCS ドメインを管理できます。

- インフラストラクチャ全体の明確なビューと現在の情報技術基盤ライブラリ（ITIL）プロセスとのシンプルな統合のためのすべての Cisco UCS コンポーネントの集中管理されたインベントリ
- 自動スケジュールを通してグローバルにまたは選択的に、または、ビジネス ワークロード需要として適用可能な集中管理されたポリシー ベースのファームウェア アップグレード
- 識別子の競合を排除するためのグローバル ID プーリング
- Cisco UCS ドメインのグローバル管理とローカル管理の両方を有効にするグローバル管理ポリシー
- 高水準なデータセンター管理フレームワークに簡単に統合するための Cisco UCS Manager XML API に基づく XML API
- 登録された Cisco UCS ドメイン内のさまざまなエンド ポイントを管理するためのリモート管理

Cisco UCS Central では、API などの Cisco UCS Manager のローカル管理機能はいずれも削除または変更されていません。 このため、Cisco UCS Manager を Cisco UCS Central を導入する前と同様に使用し続けることも、既存のサードパーティー統合が従来どおりに動作し続けるようにすることもできます。

Cisco UCS Central の機能

次の表に、Cisco UCS Central の管理機能のリストと簡単な説明を示します。

機能	説明
インベントリの集中管理	Cisco UCS Central は、カスタマイズ可能な更新スケジュールを使用して、ドメイン別に整理された、すべての登録済み Cisco UCS コンポーネントのグローバルなインベントリを自動的に集計したり、XML インターフェイス経由のインベントリへの直接アクセスを使用して ITIL プロセスとのより簡単な統合を可能にしたりします。
障害サマリーの集中管理	Cisco UCS Central を使用すれば、グローバル障害サマリー パネル上で、ドメインと障害タイプ別に整理された障害サマリーを含む、すべての Cisco UCS インフラストラクチャのステータスを確認できます。 また、個別の Cisco UCS Manager ドメインのより細かい障害情報を表示して、より迅速な問題解決を図ることができます。 障害をドリル ダウンすると、シームレスに統一されたエクスペリエンスのコンテキスト内で UCS Manager が起動します。
ポリシー ベースのファームウェア アップグレードの集中管理	Cisco.com から Cisco UCS Central 内部のファームウェア ライブラリにファームウェア更新を自動的にダウンロードできます。 その後で、ビジネス要件に基づいて全体的または選択的に自動ファームウェア更新をスケジュールします。 ファームウェアを集中的に管理することによって、IT 標準の順守が保証され、リソースの再プロビジョニングがポイント アンド クリック操作で行えるようになります。
グローバル ID プール	Cisco UCS Central は、ID の競合を排除して、ソフトウェア ライセンスの移植性を保証します。 グローバル プールからのユニバーサル ユーザ ID（UUID）、MAC アドレス、IP アドレス、ワールドワイド名などのすべての ID の割り当てを集中管理したり、リアルタイム ID 使用状況サマリーを入手したりできます。 サーバ識別情報を集中管理することによって、世界中のあらゆる場所での Cisco UCS ドメイン間のサーバ識別子の移動や新しいサーバ上で動作する既存のワークロードのリブートが容易になります。

機能	説明
ドメイン グループ	Cisco UCS Central は、ドメイン グループとサブグループを作成するオプションを提供することで、ポリシー管理を容易にします。 ドメイン グループは、システムを地理的または組織的グループに分割するための Cisco UCS ドメインの恣意的なグループ分けです。 ドメイン グループごとに最大 5 レベルのドメイン サブ グループを割り当てることができます。 これにより、大量の Cisco UCS ドメインを管理しながら、ポリシー例外を管理できるようになります。 サブ グループごとに親ドメイン グループとの階層関係が構築されます。
グローバル管理ポリシー	Cisco UCS Central は、グローバル管理ポリシーを通してコンプライアンスとスタッフ効率の保証を支援します。 グローバル ポリシーは、ドメイン グループ レベルで定義され、日時やユーザ認証から機器の電力やシステム イベント ログ（SEL）ポリシーまで、インフラストラクチャ内のあらゆるものを管理できます。
グローバル サービス プロファイルとテンプレート	Cisco UCS Central のグローバル サービス プロファイルとテンプレートは、迅速で簡略化されたインフラストラクチャ展開を可能にし、会社全体での設定の一貫性を提供します。 この機能を使用すれば、ハイパーバイザが仮想化ワークロード モビリティを実現する方法と同じように、グローバル ベアメタル ワークロード モビリティを実現できます。
バックアップ	Cisco UCS Central は、登録された Cisco UCS ドメインと UCS Central 構成の設定情報を迅速かつ効率的にバックアップ可能な自動バックアップ ファシリティを提供します。
ハイ アベイラビリティ	すべての Cisco UCS ソリューションと同様に、Cisco UCS Central は単一障害点を排除するように設計されています。 Cisco UCS Central ソフトウェアのハイ アベイラビリティを利用すれば、組織は、アクティブな Cisco UCS Central が応答しない場合に自動的にフェールオーバーする、ハートビートを利用したアクティブ/スタンバイ モデルを使用して Cisco UCS Central を実行できます。

機能	説明
XML API	Cisco UCS Central は、Cisco UCS Manager と同様に、既存の管理フレームワークやオーケストレーション ツールとインターフェイスするための高度な業界標準 XML API を備えています。 Cisco UCS Central ソフトウェア用の XML API は、Cisco UCS Manager 用の XML API に似ており、上位マネージャとの統合を大幅に迅速化します。
Remote Management	Cisco UCS Central を使用すれば、1 つの管理ポイントから、登録された Cisco UCS ドメイン内のさまざまなエンドポイントを管理できます。 Cisco UCS Central GUI または CLI から、シャーシ、サーバ、ファブリック インターコネクト、およびファブリック エクステンダを管理できます。 また、Cisco UCS Central から、登録された UCS ドメインのテクニカル サポート ファイルにアクセスすることもできます。

Cisco UCS Central HTML 5 UI の概要

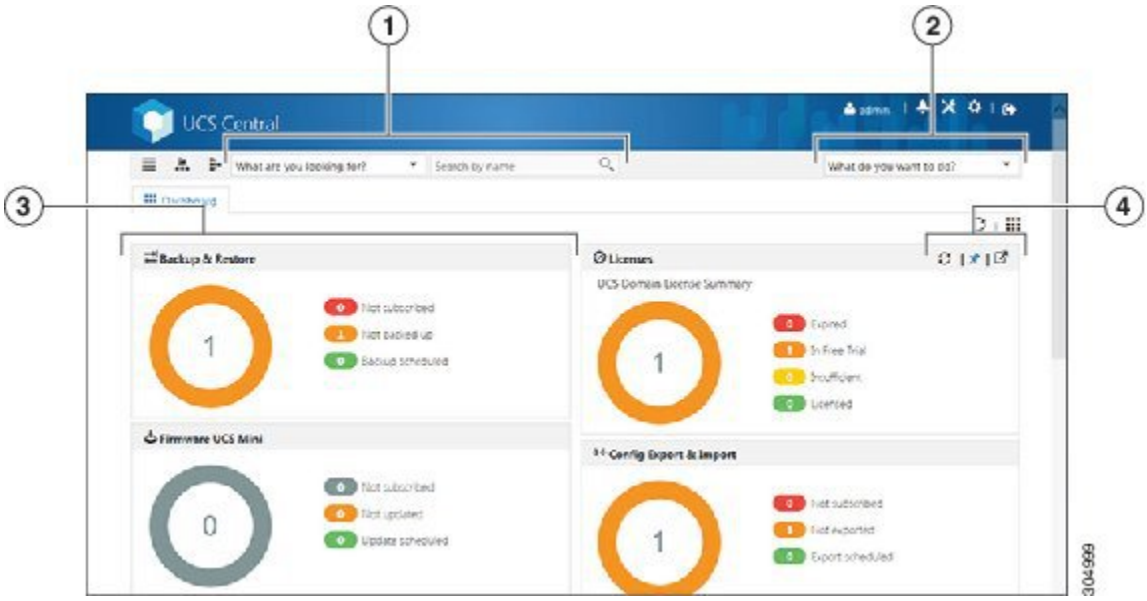
Cisco UCS Central HTML5 ベースのユーザ インターフェイスは、管理のための柔軟性とタスク ベースの操作性を提供します。

ダッシュボードには、システム内のコンポーネントの概要が表示されます。 頻繁に使用するコンポーネントを固定表示して、運用要件に合わせてダッシュボードをカスタマイズすることができます。 ダッシュボード上のオブジェクトをクリックすると、システム内の関連ページに移動できます。 このビデオの [Play] をクリックすれば、HTML 5 UI の簡単な説明を観ることができます。

HTML5 UI の使用

ダッシュボード

ダッシュボード ウィジェットを固定表示し、組織の要件に合わせてダッシュボードをカスタマイズできます。 基本的なダッシュボード構造を以下に示します。

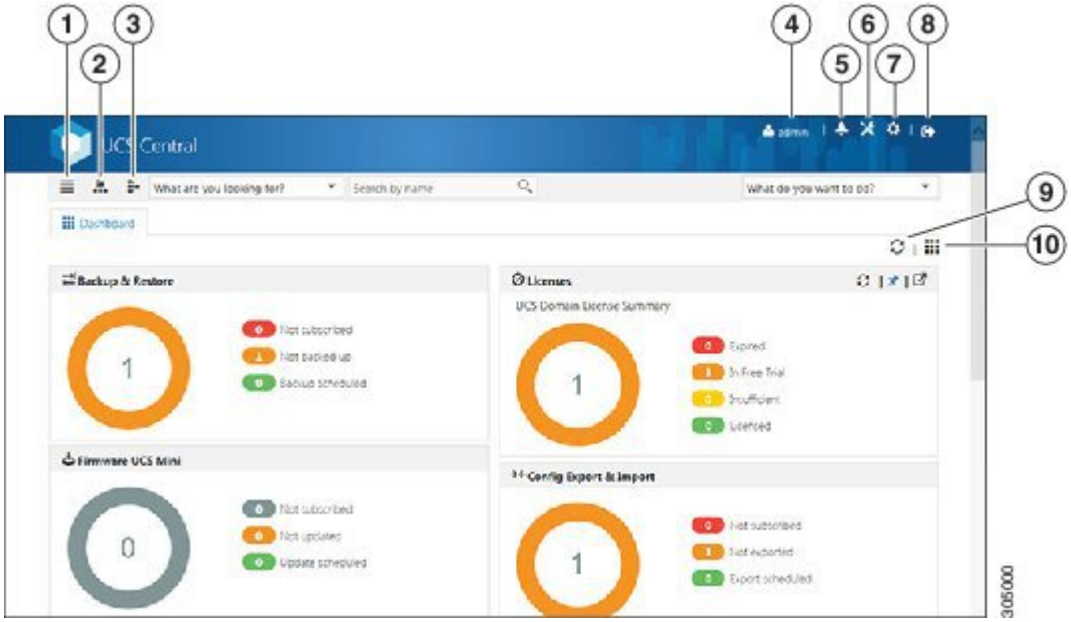


項目	説明
1	検索バー。 What are you looking for?。 次を実行できます。 • エンティティ タイプを選択して、システム内のエンティティを名前で検索します。 空の検索文字列はすべてのエンティティを返します。 • 必要に応じて場所とステータスで検索結果を絞り込みます。 • 検索結果内のエンティティをクリックすると、詳細が新しいページに表示されます。
2	アクション バー。 What do you want to do?。 ここでは、作成、スケジューリング、インストール、エクスポート、およびインポートを実行できます。 • ドロップダウンをクリックして使用可能なアクションを表示し、タスクを選択するか、フィールドにタスクを入力して、ダイアログ ボックスを開き、タスクを実行します。
3	ダッシュボード ウィジェット。 このダッシュボード上に任意のウィジェットを固定表示できます。 ウィジェット上にマウスを移動すると、ウィジェットのメニューバーで他のオプションが有効になります。

項目	説明
4	ダッシュボード上のウィジェット内に追加のオプションが表示されている場合は、次の操作を実行できます。 • この特定のウィジェットに表示された情報を更新する。 • ダッシュボードからこのウィジェットの固定表示を解除する。 • この操作に関する詳細ページを開く。

ナビゲーション アイコン

次のナビゲーション アイコンが製品のナビゲートと管理タスクの実行を支援します。



項目	説明
1	検索アイコン。 クリックすると、ドメイン、ファブリック インターコネクト、サーバ、シャーシ、FEX、vLAN、vSAN、サービスプロファイル、テンプレート、プール、ポリシー、IDユニバースなどのシステム内の物理的および論理的なインベントリ関連エンティティが表示されます。 これらのエンティティのいずれかをクリックすると、関連ページが開いて、詳細が表示されます。
2	組織アイコン。 クリックすると、システム内の組織ルートとその他のサブ組織が表示されます。 ルートまたはサブ組織をクリックすると、選択した組織の詳細ページを表示できます。

項目	説明
3	ドメイン グループ アイコン。 クリックすると、システム内のドメイン グループ ルートとその他のドメイン グループが表示されます。 ドメイン グループをクリックすると、詳細ページを表示できます。
4	ユーザ設定アイコン。 クリックすると、[User Settings] が開きます。 このページでは、[Change Password]、[Restore Dashboard Defaults]、および [Show First Launch Experience] を実行できます。
5	アラート アイコン。 クリックすると、[Pending Activities]、[System Faults]、[Domain Faults]、[Events]、[Audit Logs]、[Core Dumps]、[Sessions]、および [Internal Services] が表示され、そこに移動できます。
6	操作アイコン。 クリックすると、[Firmware]、[Backup & Restore]、[Export & Import]、[Licenses]、および [Tech Support] が表示され、そこに移動できます。
7	システム設定アイコン。 クリックすると、[System Profiles]、[System Policies]、[Users]、[Authentication]、および [SNMP] が表示され、そこに移動できます。
8	ログアウト アイコン。 クリックすると、アクティブな UCS Central セッションからログアウトします。
9	更新アイコン。 クリックすると、固定表示されたすべてのウィジェット内の情報が更新されます。 ウィジェットごとに、そのウィジェットのデータを更新するための個別の更新アイコンが付いています。
10	ダッシュボード ウィジェット ライブラリ アイコン。 クリックすると、使用可能なウィジェットが表示され、特定のウィジェットをクリックするとそれがダッシュボードに固定表示されます。

HTML5 UI の動作と設計変更

機能サポート

現在、UI で利用可能な次の機能は HTML5 UI でサポートされません。

- ポリシー インポート
- しきい値ポリシー

- 統計情報

設計に基づく動作の変更

- グローバル サービス プロファイルは、LAN または SAN 接続ポリシーを使用する初期または更新テンプレートを使用してしか作成することができません。 サービス プロファイルを作成する前に、グローバル サービス プロファイル テンプレートを作成する必要があります。
- 次のインライン オプションはサービス プロファイルで使用できません。
  - 手動 vNIC
  - iSCSI
  - vHBA
  - ブート ポリシー
  - スタティック ID

  既存のグローバル サービス プロファイルにこれらのオプションのいずれかが含まれている場合は、HTML5 UI でグローバル サービス プロファイルを編集できません。
- HTML5 UI で行われた iSCSI ブート パラメータに対する変更は、Flex UI で使用できなくなります。
- vNIC テンプレートは LAN 接続ポリシーでしか使用できません。
- vHBA テンプレートは SAN 接続ポリシーでしか使用できません。
- vNIC および vHBA 配置はインターフェイス配置と呼ばれるようになりました。
- 登録ポリシーはドメイン グループ資格ポリシーと呼ばれるようになりました。
- ID 範囲資格ポリシーは ID 範囲アクセス コントロール ポリシーと呼ばれるようになりました。
- ID 範囲アクセス コントロール ポリシー用として認定された IP アドレスは存在しません。
- サーバ プールを作成するときに、サーバ プール ポリシーを作成できます。 このポリシーを作成するサーバプール資格ポリシーを選択します。 サーバプールを割り当てるとき、グローバル サービス プロファイルでは追加のサーバ プール資格情報がサポートされません。
- 唯一のバックアップ オプションが全設定バックアップです。 論理設定やシステム設定などの他のバックアップ タイプはサポートされません。
- ローカル サービス プロファイルは、ドメイン グループの代わりに組織からホスト ファームウェア ポリシーを取得します。
- HTML 5 UI でインポートが失敗すると、メッセージにインポート失敗の原因が表示されます。 エラーを修正して、インポートの設定を再送信します。
- ローカル サービス プロファイル インベントリが表示されません。

- 現在、ローカル サービス プロファイルで使用され、ドメイン グループに属しているメンテナンス ポリシーとスケジュールは HTML5 UI で使用できません。

第 2 章

ライセンス管理

この章は、次の内容で構成されています。

ライセンスの管理

登録された Cisco UCS ドメインごとのドメイン ライセンスを使用すれば、Cisco UCS Central からドメインを管理することができます。 Cisco UCS Central GUI と CLI の両方を使用して Cisco UCS ドメイン ライセンスを管理することができます。

猶予期間

初めて Cisco UCS Central を使用する場合は、最大 120 日間の猶予期間に、無料で、最大 5 つの Cisco UCS ドメインを登録できます。 6 つ目のドメインを登録すると、新しく登録されたドメインに対して 120 日間の猶予期間が付与されます。 猶予期間の終了後は、Cisco UCS Central を使用してドメインを管理するためのアクティブ ドメイン ライセンスが必要です。 猶予期間は、Cisco UCS ドメインを登録した日からライセンスを取得してインストールする日までが換算されます。

登録された Cisco UCS ドメインの猶予期間の消化日数がシステムに保存されます。 システムからドメインの登録を解除しても、猶予期間はリセットされません。 たとえば、無料でドメインを登録して、猶予期間のうちの 40 日を消化してから、40 日後に登録を解除した場合は、そのドメインに関連付けられた 40 日間が記録されます。 この Cisco UCS ドメインを再度登録すると、そのドメインの猶予期間が再開され、40 日が消化済みであることが示されます。 猶予期間が終了する前にライセンスを取得してインストールする必要があります。 猶予期間が終了する前にライセンスを取得しなかった場合は、ライセンスを取得するためのリマインダとして複数のエラーが生成されます。 ライセンスの取得，（12 ページ） を参照してください。

ライセンス タイプ

2 つの使用可能なライセンス タイプを以下に示します。

- **初期ライセンス**：初期ライセンスには Cisco UCS Central の初期アクティベーション ライセンスと 5 つのドメイン ライセンスが含まれています。 初期ライセンスのインストール後に、

それをシステムから削除することはできません。 初期ライセンスのダウンロード タスクは削除できますが、初期ライセンスのインストール ステータスには影響しません。

- **ドメイン ライセンス**：6 つ以上のドメインを Cisco UCS Central に登録する予定の場合は、ドメイン ライセンスを購入する必要があります。 ドメイン ライセンスを取得してダウンロードしたら、Cisco UCS ドメイン を登録するときに、ドメインを選択して、ライセンスを割り当てることができます。

ライセンスの取得

シスコ ライセンス管理ポータルを使用して、Cisco UCS ドメイン のライセンスを取得できます。

（注）
- このプロセスは、このマニュアルのリリース後に変更される場合があります。次のステップのいずれかが当てはまらない場合は、シスコの担当者にライセンスの取得方法をお問い合わせください。
- 初期ライセンスを取得するには、ライセンス コードの L-UCS-CTR-INI= を使用します。
- ドメイン ライセンスを取得するには、ライセンス コードの L-UCS-CTR-LIC= を使用します。

はじめる前に

権利証明書またはその他の購入証明書から、製品認証キー（PAK）を取得します。

ステップ 1 メニュー バーで、[Tools] アイコンをクリックして、[Licenses] を選択します。

ステップ 2 [UCS Central GUID] をクリックして、GUID をコピーします。
GUID は、ライセンスを取得する Cisco UCS Central インスタンスごとに一意です。

ステップ 3 [Cisco SWIFT] をクリックして、ライセンス管理ポータルを開きます。

ステップ 4 ライセンス管理ポータルにログインして、[Continue to Product License Registratione] をクリックします。

ステップ 5 [Quickstart] ページで、[Enter a Single PAK or Token to fulfill] フィールドに PAK を入力して [Fulfill Single PAK/Token] をクリックします。

ステップ 6 [Assign SKUs to Devices] ページで、入力した PAK の横にある [Quantity Available] チェックボックスをオンにします。

ステップ 7 [GUID] フィールドに GUID を入力して、[Assign] をクリックします。

ステップ 8 [Next] をクリックします。

ステップ 9 [Review] ページで、電子メール アドレスを入力して、ユーザ ID を選択し、[License Agreement] チェックボックスをオンにします。

ステップ 10 [Get License] をクリックします。
シスコからライセンス zip ファイルが電子メールで送られてきます。 ライセンス ファイルは、指定された Cisco UCS ドメイン での使用だけを許可するようにデジタル署名されています。

注意 ライセンス ファイルを入手したら、ライセンス コードを改ざんしないでください。 一部でも手動で編集すると、改ざん防止機能が停止して、ライセンスが無効になります。

次の作業

ライセンス ファイルを解凍して、インストールします。

ライセンスのインストール

ライセンス ファイルは、ローカル ファイル システムまたはリモート ファイル システムからインストールできます。

はじめる前に

次の点を確認してください。

- シスコからライセンスを取得して、それをローカル システムまたはリモート ファイル システムに保存したかどうか。
- Cisco UCS ドメイン でこのタスクを実行するための管理権限。
- ライセンス ファイルをリモートの場所に保存する場合は、その場所が存在することを確認してください。 次の情報を準備しておく必要があります。
  - 絶対リモート パス。 たとえば、転送プロトコルが SCP の場合：
    `scp://user@<ip>/x/y/z`
  - リモート サーバのホスト名または IP アドレス
  - リモート サーバのユーザ名とパスワード

ステップ 1 メニュー バーで、[Operation] アイコンをクリックして、[Licenses] を選択します。

ステップ 2 [Licenses] メニュー バーで、[Install] アイコンをクリックします。
これにより、[Install License] ダイアログボックスが開きます。

ステップ 3 [License File Location] で、[Local] または [Remote] をクリックします。
ライセンス ファイルを保存した場所に応じて場所を選択します。

a) ライセンス ファイルがローカル システム上に存在する場合は、[File Name] を参照してファイルを選択します。
b) ライセンス ファイルがリモートの場所に存在する場合は、リモートの場所に関する必須情報を入力します。

ステップ 4 [Install] をクリックします。

正しいファイルを選択した場合は、ライセンスファイルがシステムにインストールされます。そうでない場合は、ダイアログボックスの最後にエラーメッセージが表示されます。正しいライセンス ファイルを選択してください。

第 3 章

ユーザ管理

この章は、次の内容で構成されています。

UCS Central ユーザー管理の管理

[Manage UCS Central Users Administration] ダイアログボックスでは、ユーザ、ロール、ロケール、およびパスワード プロファイルを設定できます

ステップ 1 [System Settings] アイコンから、[Users] を選択します。
これにより、[Manage UCS Central Users Administration] ダイアログボックスが開きます。

ステップ 2 設定するセクションのアイコンをクリックします。

- [Password Profile] セクションでは、[Manage UCS Central Password Profile] ダイアログボックスと同じタスクを実行できます。 詳細については、 UCS Central パスワード プロファイルの管理, （16 ページ）を参照してください。
- [Roles] セクションでは、[Manage UCS Central Roles] ダイアログボックスと同じタスクを実行できます。 詳細については、 UCS Central ロールの管理, （16 ページ）を参照してください。
- [Locales] セクションでは、[Manage UCS Central Locales] ダイアログボックスと同じタスクを実行できます。 詳細については、UCS Central ロケールの管理, （17 ページ）を参照してください。
- [Local Users] セクションでは、[Manage UCS Central Local Users] ダイアログボックスと同じタスクを実行できます。 詳細については、UCS Central ローカル ユーザの管理, （17 ページ）を参照してください。

- [Remote Users] セクションでは、[Manage UCS Central Remote Users] ダイアログボックスと同じタスクを実行できます。 詳細については、UCS Central リモート ユーザの管理, （18 ページ）を参照してください。

ステップ 3 セクションごとに必要なフィールドに値を入力します。

ステップ 4 [Save] をクリックします。

UCS Central パスワード プロファイルの管理

ステップ 1 タスク バーで、「Manage UCS Central Password Profile」と入力して、Enter キーを押します。
これにより、[Manage UCS Central Password Profile] ダイアログボックスが開きます。

ステップ 2 [Password Profile] で、[Password Strength Check] を有効にするかどうかを選択します。

ステップ 3 以前のパスワードが再利用できるようになるまでのパスワードの最小数を選択します。

ステップ 4 [Password Change During Interval] を有効にするかどうかを選択します。

ステップ 5 [Password Change Interval] を選択します。

ステップ 6 変更間隔期間のパスワードの最大数を選択します。
このフィールドは、[Password Change During Interval] が [Enabled] に設定されている場合にのみ表示されます。

ステップ 7 [Save] をクリックします。

関連トピック

UCS Central ロールの管理, （16 ページ）
UCS Central ロケールの管理, （17 ページ）
UCS Central ローカル ユーザの管理, （17 ページ）
UCS Central リモート ユーザの管理, （18 ページ）

UCS Central ロールの管理

ステップ 1 タスク バーで、「Manage UCS Central Roles」と入力して、Enter キーを押します。
これにより、[Manage UCS Central Locales Roles] ダイアログボックスが開きます。

ステップ 2 [Roles] で、[Add] をクリックして新しいロールを作成するか、既存のロールを選択します。
ステップ 3 ロールの [Network]、[Storage]、[Server]、および [Operations] の各特権を更新します。
ステップ 4 [Save] をクリックします。

関連トピック

UCS Central パスワード プロファイルの管理, （16 ページ）
UCS Central ロケールの管理, （17 ページ）
UCS Central ローカル ユーザの管理, （17 ページ）
UCS Central リモート ユーザの管理, （18 ページ）

UCS Central ロケールの管理

ステップ 1 タスク バーで、「Manage UCS Central Locales」と入力して、Enter キーを押します。
これにより、[Manage UCS Central Locales] ダイアログボックスが開きます。
ステップ 2 [Locales] で、[Add] をクリックして新しいロケールを追加するか、既存のロケールを選択します。
ステップ 3 [Organizations] または [Domain Groups] をロケールに割り当てます。
ステップ 4 [Save] をクリックします。

関連トピック

UCS Central パスワード プロファイルの管理, （16 ページ）
UCS Central ロールの管理, （16 ページ）
UCS Central ローカル ユーザの管理, （17 ページ）
UCS Central リモート ユーザの管理, （18 ページ）

UCS Central ローカル ユーザの管理

ステップ 1 タスク バーで、「Manage UCS Central Local Users」と入力して、Enter キーを押します。
これにより、[Manage UCS Central Local Users] ダイアログボックスが開きます。

ステップ 2 [Local Users] で、[Add] をクリックして新しいローカルユーザを作成するか、既存のユーザを選択します。
ステップ 3 [Basic] タブで、ユーザに関する必要な情報を入力します。
ステップ 4 [Roles] タブで、ユーザに割り当てるロールを追加または削除します。
ステップ 5 [Locales] タブで、ユーザに割り当てるロケールを追加または削除します。
ステップ 6 [SSH] タブで、[Authentication Type] を選択します。
ステップ 7 [Save] をクリックします。

関連トピック

UCS Central パスワード プロファイルの管理, （16 ページ）
UCS Central ロールの管理, （16 ページ）
UCS Central ロケールの管理, （17 ページ）
UCS Central リモート ユーザの管理, （18 ページ）

UCS Central リモート ユーザの管理

ステップ 1 タスク バーで、「Manage UCS Central Remote Users」と入力して、Enter キーを押します。
これにより、[Manage UCS Central Remote Users] ダイアログボックスが開きます。

ステップ 2 [Remote Users] で、リモート LDAP ユーザ、ロール、およびロケールを確認します。
（注） このセクションは読み取り専用です。

ステップ 3 ウィンドウを閉じる場合は [Cancel] をクリックし、他のセクションで行った変更を保存する場合は [Save] をクリックします。

関連トピック

UCS Central パスワード プロファイルの管理, （16 ページ）
UCS Central ロールの管理, （16 ページ）
UCS Central ロケールの管理, （17 ページ）
UCS Central ローカル ユーザの管理, （17 ページ）

ドメイン グループ ユーザの管理

ステップ 1 ルートの [Domain Group] ページに移動します。
ステップ 2 [Settings] アイコンをクリックして、[Users] を選択します。
ステップ 3 [Roles] で、ドメイン グループに関連付けるロールを追加または削除します。
ステップ 4 [Locales] で、ドメイン グループに関連付けるロケールを追加または削除します。
ステップ 5 [Save] をクリックします。

第 4 章

認証

この章は、次の内容で構成されています。

認証

Cisco UCS Central から、登録された UCS ドメインの認証用に LDAP、RADIUS、および TACACS+ を設定できます。

（注） リモート認証に使用できるのは、LDAP だけです。

リモート認証プロバイダーに関する注意事項および推奨事項

システムを、サポートされているリモート認証サービスのいずれかに設定する場合は、そのサービス用のプロバイダーを作成して、Cisco UCS Central がそのサービスと通信できるようにする必要があります。 また、ユーザ許可に影響する次のガイドラインに留意する必要があります。

リモート認証サービスのユーザ アカウント

ユーザ アカウントは、Cisco UCS Central にローカルに存在するか、またはリモート認証サーバに存在することができます。 リモート認証サービスを介してログインしているユーザの一時的なセッションは、Cisco UCS Central GUI または Cisco UCS Central CLI で表示できます。

リモート認証サービスのユーザ ロール

リモート認証サーバでユーザ アカウントを作成する場合は、ユーザが Cisco UCS Central で作業するために必要なロールをそれらのアカウントに含めること、およびそれらのロールの名前を Cisco UCS Central で使用される名前と一致させることが必要です。 ロール ポリシーによっては、ユーザがログインできない場合や読み取り専用権限しか付与されない場合があります。

ローカルおよびリモート ユーザ認証のサポート

Cisco UCS Central はリモート認証のために LDAP を使用しますが、このリリースでは RADIUS および TACACS+ 認証を除外します。 ただし、RADIUS、TACACS+、および LDAP 認証は、ローカルに管理される Cisco UCS ドメイン でサポートされています。

リモート認証プロバイダーのユーザ属性

ユーザがログインすると、Cisco UCS Central は次を実行します。

1. リモート認証サービスに問い合わせます。
2. ユーザを検証します。
3. ユーザが検証されると、そのユーザに割り当てられているロールとロケールをチェックします。

次の表に、Cisco UCS Central によってサポートされるリモート認証プロバイダーのユーザ属性要件の比較を示します。

表 *1*：リモート認証プロバイダーによるユーザ属性の比較

認証プロバイダー	カスタム属性	スキーマの拡張	属性 ID 要件
LDAP	任意	オプション。 次のいずれかを選択して実行できます。 • LDAP スキーマを拡張せず、要件を満たす既存の未使用の属性を設定します。 • LDAP スキーマを拡張して、CiscoAVPair などの一意の名前でカスタム属性を作成します。	シスコの LDAP の実装では、Unicode タイプの属性が必要です。 CiscoAVPair カスタム属性を作成する場合は、属性 ID として 1.3.6.1.4.1.9.287247.1 を使用します 次の項で、サンプル OID を示します。

LDAP ユーザ属性のサンプル OID

カスタム CiscoAVPair 属性のサンプル OID は、次のとおりです。

```
CN=CiscoAVPair,CN=Schema,
CN=Configuration,CN=X
objectClass: top
objectClass: attributeSchema
cn: CiscoAVPair
distinguishedName: CN=CiscoAVPair,CN=Schema,CN=Configuration,CN=X
instanceType: 0x4
uSNCreated: 26318654
attributeID: 1.3.6.1.4.1.9.287247.1
attributeSyntax: 2.5.5.12
isSingleValued: TRUE
showInAdvancedViewOnly: TRUE
adminDisplayName: CiscoAVPair
adminDescription: UCS User Authorization Field
oMSyntax: 64
lDAPDisplayName: CiscoAVPair
name: CiscoAVPair
objectCategory: CN=Attribute-Schema,CN=Schema,CN=Configuration,CN=X
```

LDAP プロバイダー

Cisco UCS Manager から LDAP ユーザを作成するのと同じ方法で、リモート ユーザを設定して、Cisco UCS Central からロールとロケールを割り当てることができます。 必ず、Cisco UCS Central Domain Group ルートから LDAP プロバイダーを作成する必要があります。

LDAP プロバイダー グループ マップ

最大 28 の LDAP プロバイダー グループ マップを定義して、Active Directory で Cisco UCS Central 内のネスティングがサポートされるレベルまでそれらのマップをネストすることができます。 プロバイダーをネスト グループに割り当てると、そのプロバイダーが別の LDAP グループのメン

バーであっても、親ネスト グループの認証メンバーになります。 認証中、プロバイダー グループ内のすべてのプロバイダーが順番に試行されます。 設定されたすべての LDAP サーバが使用または到達できない場合は、Cisco UCS Central が自動的にローカル ユーザ名とパスワードを使用するローカル認証方式にフォールバックします。

LDAP グループ マップ

すでに LDAP グループを使用して LDAP データベースへのアクセスを制限している組織では、Cisco UCS ドメインでグループ メンバーシップ情報を使用することによって、ログイン中の LDAP ユーザにロールまたはロケールを割り当てることができます。 これにより、Cisco UCS Central の展開時に LDAP ユーザ オブジェクトでロールまたはロケール情報を定義する必要がなくなります。

Cisco UCS Central は、ユーザ ロールとロケールをリモート ユーザに割り当てるときに LDAP グループ ルールを使用して LDAP グループを決定します。 ユーザがログインすると、Cisco UCS Central が LDAP グループ マップからそのユーザのロールとロケールに関する情報を取得します。 ロールとロケールの条件がポリシー内の情報と一致すると、Cisco UCS Central がアクセス権をユーザに付与します。

ロールとロケールの定義は Cisco UCS Central でローカルに設定され、LDAP ディレクトリに対する変更に基づいて自動的には更新されません。 LDAP ディレクトリ内の LDAP グループを削除または名前を変更した場合は、Cisco UCS Central でその変更を更新してください。

LDAP グループ マップは、次のロールとロケールの組み合わせのいずれかを含むように設定できます。

- ロールのみ
- ロケールのみ
- ロールとロケール

例：特定の場所にいるサーバ管理者のグループを表す LDAP グループに対する認証を設定する場合は、server-profile や server-equipment などのユーザ ロールをその LDAP グループに含めることができます。 特定の場所にいるサーバ管理者にアクセスを制限する場合は、特定のサイト名を含むロケールを指定できます。

（注） Cisco UCS Central には、すぐに使用可能なユーザ ロールが複数付属していますが、ロケールは付属していません。 そのため、LDAP プロバイダー グループをロケールにマッピングするカスタム ロケールを作成する必要があります。

ネストされた LDAP グループ

LDAP グループ マップで定義された別のグループ内でネストされた LDAP グループを検索できます。 この機能を使用する場合は、Cisco UCS Central でグループ マップ内にサブグループを作成する必要がありません。

（注） ネストされた LDAP の検索サポートは Microsoft Active Directory サーバに対してのみサポートされます。 サポートされているバージョンは Microsoft Windows 2003 SP3、Microsoft Windows 2008 R2、および Microsoft Windows 2012 です。

（注） MS-AD 内でネストされた LDAP グループを作成するときに、名前に特殊文字を使用する場合は、必ず、\\(と \\) を使用して文字を設定してください。 Cisco UCS Central CLI を使用して、ネストされた LDAP グループを作成する例を以下に示します。

create ldap-group CN=test1\\(\\),CN=Users,DC=ucsm,DC=qasam-lab,DC=in

LDAP ネスティング機能を使用して、LDAP グループを他のグループおよびネスト グループのメンバとして追加し、メンバ アカウントを統合してトラフィックの重複を減らすことができます。

LDAP グループが別のグループ内でネストされている場合は、デフォルトで、ユーザの権限が継承されます。 たとえば、Group_2 のメンバとして Group_1 を作成する場合、Group_1 のユーザは Group_2 のメンバと同じ権限が与えられます。 その結果、Group_1 のメンバになっているユーザを検索する場合は、Group_1 と Group_2 を別々に検索しなくても、LDAP グループ マップ内の Group_2 を選択するだけで済みます。

UCS Central 認証の管理

Cisco UCS Central は、ネイティブ認証に LDAP を使用しますが、RADIUS 認証と TACACS+ 認証は除きます。 ただし、Cisco UCS Central ドメイン グループ ルートからの RADIUS、TACACS+、または LDAP リモート認証が Cisco UCS ドメインに対してサポートされます。

認証ドメインを作成したら、必要に応じて、認証情報を編集できます。

ステップ 1 メニュー バーで、[Operations] アイコンをクリックして、[Authentication] を選択します。
これにより、[Manage Cisco UCS Central Authentication] ダイアログボックスが開きます。

ステップ 2 [LDAP] で、[Basic]、[Providers]、[Groups]、および [Group Maps] タブの該当するフィールドに値を入力します。

ステップ 3 [Authentication Domains] で、次の手順を実行します。

ステップ 4 [Native(Default)] をクリックして、次の情報を入力します。

a) [Default Behavior for Remote Users] を選択します。

b) [Web Session Refresh Period(Seconds)] と [Web Session Timeout(Seconds)] の値を入力します。
c) [Authentication] を [Enabled] にするか、[Disabled] にするかを選択します。
d) [Enabled] を選択した場合は、[Authentication Realm] を [Local] にするか、[LDAP] にするかを選択します。
e) [LDAP] を選択した場合は、[Provider Group] を選択します。

ステップ 5 [Console(Default)] をクリックして、次の情報を入力します。

a) [Authentication] を [Enabled] にするか、[Disabled] にするかを選択します。
b) [Enabled] を選択した場合は、[Authentication Realm] を [Local] にするか、[LDAP] にするかを選択します。
c) [LDAP] を選択した場合は、[Provider Group] を選択します。

ステップ 6 [Add] をクリックして、新しい認証ドメインを作成します。

a) 認証ドメインの名前を入力します。
この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）以外の特殊文字またはスペースを使用できません。

優先認証プロトコルとして RADIUS を使用しているシステムでは、認証ドメイン名がユーザ名の一部と見なされ、ローカルに作成されたユーザ名の 32 文字の制限が考慮されます。 Cisco UCS では書式設定用として 5 文字が予約されているため、ドメイン名とユーザー名で 27 文字を超えることができません。

b) [Web Session Refresh Period(Seconds)] に、選択した Cisco UCS Central ドメイン グループに含まれる Cisco UCS ドメインにアクセスしているユーザの更新要求間の最大許容時間を入力します。
この時間制限を超えると、Cisco UCS Central は Web セッションを非アクティブと見なしますが、そのセッションを終了することはありません。

60 ～ 172800 を指定します。 デフォルトは 600 秒です。

c) [Web Session Timeout(Seconds)] に、最後の更新要求後から CiscoCisco UCS Central で Web セッションが終了したと見なされるまでの最大経過時間を入力します。 この時間制限を超えると、Cisco UCS Central は自動的に Web セッションを終了します。
60 ～ 172800 を指定します。 デフォルトは 7200 秒です。

d) ドメイン内のユーザに適用される [Authentication Realm] を選択します。 次のいずれかになります。

- [LDAP]：ユーザを Cisco UCS Central で指定された LDAP サーバ上で定義する必要があります。
- [Local]：ユーザ アカウントを Cisco UCS Central または Cisco UCS ドメイン内でローカルに定義する必要があります。

e) [Realm] が LDAP に設定されている場合は、[Provider Group] ドロップダウン リストから関連するプロバイダー グループを選択できます。

ステップ 7 [Save（保存）] をクリックします。

UCS Central LDAP 設定の管理

ステップ 1 タスク バーで、「Create Domain Group」と入力して、Enter キーを押します。
これにより、[Create Domain Group] ダイアログボックスが開きます。

ステップ 2 [LDAP] で、必要に応じて次のセクションに値を入力します。

a) [Basic] タブで、[Database Conection Timeout]、[Filter]、[Attribute]、および [Base DN] の値を入力します。

b) [Providers] タブで、[Add] をクリックして、プロバイダーを追加し、[Basic] タブと [Group Rules] タブで必要な情報を入力します。

c) [Groups] タブで、[Add] をクリックして、プロバイダー グループを追加し、オプションで、それをプロバイダーに関連付けます。

d) [Group Maps] タブで、[Provider Group Map DN] を追加してから、オプションで、[Roles] と [Locales] を追加します。

ステップ 3 [Authentication Domains] で、新しいドメインを追加して、その値を更新します。

ステップ 4 [Save] をクリックします。

ドメイン グループ認証の管理

ステップ 1 タスク バーで、「Manage Domain Group Authentication」と入力して、Enter キーを押します。
これにより、[Manage Domain Group Authentication] ダイアログボックスが開きます。

ステップ 2 [LDAP] で、必要に応じて次のセクションに値を入力します。

a) [Basic] タブで、[Database Conection Timeout]、[Filter]、[Attribute]、および [Base DN] の値を入力します。

b) [Providers] タブで、[Add] をクリックして、プロバイダーを追加し、[Basic] タブと [Group Rules] タブで必要な情報を入力します。

c) [Groups] タブで、[Add] をクリックして、プロバイダー グループを追加し、オプションで、それをプロバイダーに関連付けます。

d) [Group Maps] タブで、[Provider Group Map DN] を追加してから、オプションで、[Roles] と [Locales] を追加します。

ステップ 3 [TACACS+] で、必要に応じて次のセクションに値を入力します。

a) [Basic] タブで、[Database Conection Timeout] と [Retry Count] の値を入力します。

b) [Providers] タブで、[Add] をクリックして、プロバイダーを追加し、必要な設定情報を入力します。
上矢印と下矢印を使用して、プロバイダーの順序を変更できます。

c) [Groups] タブで、[Add] をクリックして、プロバイダー グループを追加し、オプションで、それをプロバイダーに関連付けます。

ステップ 4 [RADIUS] で、必要に応じて次のセクションに値を入力します。

a) [Basic] タブで、[Database Conection Timeout] と [Retry Count] の値を入力します。

b) [Providers] タブで、[Add] をクリックして、プロバイダーを追加し、必要な設定情報を入力します。
上矢印と下矢印を使用して、プロバイダーの順序を変更できます。

c) [Groups] タブで、[Add] をクリックして、プロバイダー グループを追加し、オプションで、それをプロバイダーに関連付けます。

ステップ 5 [Authentication Domains] で、必要に応じて次のセクションに値を入力します。

a) [Add] をクリックして、親グループから継承された設定をオーバーライドする、選択したユーザ作成ドメイン グループの認証ポリシーを作成します。

b) 認証ドメインの名前を入力します。
この名前には、1 ～ 16 文字の英数字を使用できます。 優先する認証プロトコルとして RADIUS を使用するシステムの場合、認証ドメイン名はユーザ名の一部と見なされ、ローカルに作成されたユーザ名の 32 文字の制限に対して考慮されます。 Cisco UCS はフォーマット用に 5 文字を挿入するため、認証はユーザ名とドメイン名を組み合わせた合計が 27 文字を超えると失敗します。

c) [Web Session Refresh Period(Seconds)] に、選択した Cisco UCS Central ドメイン グループに含まれる Cisco UCS ドメインにアクセスしているユーザの更新要求間の最大許容時間を入力します。
この時間制限を超えると、Cisco UCS Manager は Web セッションを非アクティブと見なしますが、そのセッションを終了することはありません。

60 ～ 172800 の整数を指定します。 デフォルトは 600 秒です。

d) [Web Session Timeout(Seconds)] に、最後の更新要求後から Cisco UCS Manager で Web セッションが終了したと見なされるまでの最大経過時間を入力します。 この時間制限を超えると、Cisco UCS Manager は自動的に Web セッションを終了します。
60 ～ 172800 の整数を指定します。 デフォルトは 7200 秒です。

e) ドメイン内のユーザに適用される [Authentication Realm] を選択します。
次のいずれかになります。

- [LDAP]：ユーザを Cisco UCS Central で指定された LDAP サーバ上で定義する必要があります。
- [Local]：ユーザ アカウントを Cisco UCS Central または Cisco UCS ドメイン内でローカルに定義する必要があります。
- [RADIUS]：ユーザを Cisco UCS Central で指定された RADIUS サーバ上で定義する必要があります。
- [TACACS+]：ユーザを Cisco UCS Central で指定された TACACS+ サーバ上で定義する必要があります。

ステップ 6 [Save（保存）] をクリックします。

SNMP ポリシー

Cisco UCS Central は、SNMP トラップと SNMP ユーザの定義（通常のパスワードとプライバシー パスワード、md5 または sha の認証タイプ、および暗号化タイプの DES と AES-128 を使用）を有効または無効にするグローバル SNMP ポリシーをサポートします。 登録済み Cisco UCS ドメインでは、そのクライアントのポリシー解決コントロール内で SNMP ポリシーをグローバルに定義するようにしている場合、すべての SNMP ポリシーについて Cisco UCS Central への登録に従うことになります。

SNMP エージェント機能は、Cisco UCS Central をリモートで監視できる能力を提供します。 また、Cisco UCS Central のホスト IP を変更してから、新しい IP 上で SNMP エージェントを再起動することもできます。 SNMP は、アクティブとスタンバイの両方の Cisco UCS Central サーバ上で動作し、その両方で設定が保持されます。 Cisco UCS Central は、オペレーティング システム管理情報ベース（MIB）のみへの読み取り専用アクセスを提供します。Cisco UCS Central CLI 経由で、SNMP v1、v2c 用のコミュニティ ストリングを設定したり、SNMPv3 ユーザを作成または削除したりできます。

SNMP 機能の概要

SNMP フレームワークは 3 つの部分で構成されます。

- SNMP マネージャ：SNMP を使用してネットワーク デバイスのアクティビティを制御し、モニタリングするシステム
- SNMP エージェント：管理対象デバイスである Cisco UCS Central 内部のソフトウェア コンポーネントで、Cisco UCS Central に関するデータを保持し、必要に応じてそのデータを SNMP に報告します。 Cisco UCS Central には、エージェントと、MIB のコレクションが組み込まれています。 SNMP エージェントを有効にして、マネージャとエージェント間のリレーションシップを構築するには、Cisco UCS Central で SNMP を有効にして設定します。
- 管理情報ベース（MIB）：SNMP エージェント上の管理対象オブジェクトのコレクション。 Cisco UCS Central は、OS MIB のみをサポートします。

Cisco UCS Central は、SNMPv1、SNMPv2c、および SNMPv3 をサポートします。 SNMPv1 および SNMPv2c はどちらも、コミュニティベース形式のセキュリティを使用します。 次の RFC で SNMP が規定されています。

- RFC 3410（http://tools.ietf.org/html/rfc3410）
- RFC 3411（http://tools.ietf.org/html/rfc3411）
- RFC 3412（http://tools.ietf.org/html/rfc3412）
- RFC 3413（http://tools.ietf.org/html/rfc3413）
- RFC 3414（http://tools.ietf.org/html/rfc3414）
- RFC 3415（http://tools.ietf.org/html/rfc3415）
- RFC 3416（http://tools.ietf.org/html/rfc3416）

- RFC 3417（http://tools.ietf.org/html/rfc3417）
- RFC 3418（http://tools.ietf.org/html/rfc3418）
- RFC 3584（http://tools.ietf.org/html/rfc3584）

SNMP 通知

SNMP の重要な機能の 1 つは、SNMP エージェントから通知を生成できることです。 これらの通知では、要求を SNMP マネージャから送信する必要はありません。 通知は、不正なユーザ認証、再起動、接続の切断、隣接ルータとの接続の切断、その他の重要なイベントを表示します。

Cisco UCS Central は、SNMP 通知をトラップとして生成します。 SNMP マネージャはトラップの受信時に確認応答を送信せず、Cisco UCS Central はトラップが受信されたかどうかを確認できないため、トラップは信頼できません。

SNMP セキュリティ機能

SNMPv3 は、ネットワーク経由のフレームの認証と暗号化を組み合わせることによって、デバイスへのセキュア アクセスを実現します。 SNMPv3 は、設定済みユーザによる管理動作のみを許可し、SNMP メッセージを暗号化します。 SNMPv3 ユーザベース セキュリティ モデル（USM） は SNMP メッセージレベル セキュリティを参照し、次のサービスを提供します。

- メッセージの完全性：メッセージが不正な方法で変更または破壊されていないことを保証します。また、データ シーケンスが、通常発生するものよりも高い頻度で変更されていないことを保証します。
- メッセージ発信元の認証：受信データを発信したユーザのアイデンティティが確認されたことを保証します。
- メッセージの機密性および暗号化：不正なユーザ、エンティティ、またはプロセスからの情報の利用や開示を行えないようにします。

SNMP セキュリティ レベルおよび権限

SNMPv1、SNMPv2c、および SNMPv3 はそれぞれ別のセキュリティ モデルを表します。 セキュリティ モデルは、選択したセキュリティ レベルと結合され、SNMP メッセージの処理中に適用されるセキュリティ メカニズムを決定します。

セキュリティ レベルは、SNMP トラップに関連付けられているメッセージを表示するために必要な特権を決定します。 権限レベルは、メッセージが開示されないよう保護または認証の必要があるかどうかを決定します。 サポートされるセキュリティ レベルは、セキュリティ モデルが設定されているかによって異なります。 SNMP セキュリティ レベルは、次の権限の 1 つ以上をサポートします。

- noAuthNoPriv：認証なし、暗号化なし
- authNoPriv：認証あり、暗号化なし
- authPriv：認証あり、暗号化あり

SNMPv3 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。 セキュリティ モデルは、ユーザおよびユーザが属するロールを設定する認証方式です。 セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。 セキュリティ モデルとセキュリティ レベルの組み合わせにより、SNMP パケット処理中に採用されるセキュリティ メカニズムが決まります。

SNMP セキュリティ モデルおよびセキュリティ レベル

次の表に、Cisco UCS Central でサポートされる SNMP セキュリティ モデルとセキュリティ レベルの組み合わせを示します。

表 *2* : ***SNMP*** セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	結果
v1	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
v2c	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
v3	noAuthNoPriv	ユーザ名	No	ユーザ名の照合を使用して認証します。
v3	authNoPriv	HMAC-MD5 または HMAC-SHA	No	Hash-Based Message Authentication Code（HMAC）メッセージ ダイジェスト 5（MD5）アルゴリズムまたは HMAC Secure Hash Algorithm（SHA）アルゴリズムに基づいて認証します。

モデル	レベル	認証	暗号化	結果
v3	authPriv	HMAC-MD5 または HMAC-SHA	DES	HMAC-MD5 アルゴリズムまたは HMAC-SHA アルゴリズムに基づいて認証します。データ暗号規格（DES）の 56 ビット暗号化、および暗号ブロック連鎖（CBC）DES（DES-56）標準に基づいた認証を提供します。

Cisco UCS Central での SNMP サポート

MIB のサポート

Cisco UCS Central は、OS MIB への読み取り専用アクセスをサポートします。 MIB に対する設定操作は使用できません。 次の MIB が Cisco UCS Central でサポートされます。

- SNMP MIB-2 システム
- HOST-RESOURCES-MIB
  - hrSystem
  - hrStorage
  - hrDevice
  - hrSWRun
  - hrSWRunPerf
- UCD-SNMP-MIB
  - メモリ
  - dskTable
  - systemStats
  - fileTable
- SNMP MIB-2 インターフェイス
  - ifTable
- IP-MIB

- SNMP-FRAMEWORK-MIB
  - snmpEngine
- IF-MIB
- DISMAN-EVENT-MIB
- SNMP MIB-2 snmp

（注） Cisco UCS Central は、IPV6 と Cisco UCS Central MIB に対するサポートを提供しません、

関連トピック

SNMP のイネーブル化, （33 ページ）
SNMP ユーザの作成と編集, （34 ページ）
SNMP トラップの作成と編集, （34 ページ）

SNMP のイネーブル化

ステップ 1 メニュー バーで、[Operations] アイコンをクリックして、[SNMP] を選択します。

- タスク バーで「Manage UCS Central SNMP」と入力して Enter キーを押すことによって、SNMP を選択できます。

これにより、[Manage UCS Central SNMP] ダイアログボックスが開きます。

ステップ 2 [Basic] で、次のフィールドに値を入力します。

ステップ 3 [Community/User Name] に、デフォルトの SNMP v1 または v2c コミュニティ名または SNMPv3 ユーザ名を入力します。

ステップ 4 [System Contact] に、SNMP 実装のシステム担当者を入力します。
電子メール アドレス、名前、電話番号など、255 文字までの文字列を入力します。

ステップ 5 [System Location] に、SNMP エージェント（サーバ）が動作するホストの場所を入力します。
最大 510 文字の英数字文字列を入力します。

ステップ 6 [Save（保存）] をクリックします。

次の作業

SNMP トラップおよびユーザを作成します。

SNMP トラップの作成と編集

SNMP トラップを作成したら、必要に応じて、SNMP トラップ情報を編集できます。

ステップ 1 メニュー バーで、[Operations] アイコンをクリックして、[SNMP] を選択します。
これにより、[Manage UCS Central SNMP] ダイアログボックスが開きます。

ステップ 2 [Trap Host Name/IP Address] で、トラップを受信する SNMP ホストの IP アドレスを入力します。

ステップ 3 [SNMP Trap Properties] 領域で、次の手順を実行します。

ステップ 4 [Community/User Name] に、システムがトラップを SNMP ホストに送信するときに追加される SNMP v1 または v2c コミュニティ名、あるいは、SNMPv3 ユーザ名を入力します。 これは、SNMP サービスに設定されたコミュニティまたはユーザ名と同じである必要があります。
1 ～ 32 文字の英数字文字列を入力します。 @（アット マーク）、\（バックスラッシュ）、"（二重引用符）、?（疑問符）または空欄スペース は使用しないでください。

ステップ 5 [Port] に、システムがトラップ用に SNMP ホストと通信するポートを入力します。
1 ～ 65535 の整数を入力します。 デフォルト ポートは 162 です。

ステップ 6 [V1]、[V2C]、または [V3] をクリックして、SNMP のバージョンを選択します。

ステップ 7 [Trap] をクリックして、SNMP トラップの [Type] を選択します。

ステップ 8 [V3Privilege] を定義するために、次のいずれかを選択します。

ステップ 9 [Save（保存）] をクリックします。

- [auth]：認証されますが、暗号化されません
- [Noauth]：認証または暗号化なし
- [Priv]：認証あり、暗号化あり

次の作業

SNMP ユーザを作成する。

SNMP ユーザの作成と編集

SNMP ユーザを作成したら、必要に応じて、SNMP ユーザ情報を編集できます。

ステップ 1 メニュー バーで、[Operations] アイコンをクリックして、[SNMP] を選択します。
これにより、[Manage UCS Central SNMP] ダイアログボックスが開きます。

ステップ 2 [Manage UCS Central SNMP] ページで、[SNMP User] をクリックします。

ステップ 3 プラス記号をクリックして、SNMP ユーザを作成します。

ステップ 4 SNMP ユーザに割り当てるユーザ名を入力します。
32 文字までの文字または数字を入力します。 名前は文字で始まる必要があり、_（アンダースコア）、.（ピリオド）、@（アット マーク）、および -（ハイフン）も指定できます。

ステップ 5 [SNMP User Properties] で、次の手順を実行します。

ステップ 6 [Authentication Type] で、認証タイプを選択します。 次のいずれかになります。

- MDS
- SHA

ステップ 7 [AES-128 Encryption] を有効にします。 有効にした場合は、このユーザが AES-128 暗号化を使用します。

ステップ 8 ユーザのパスワードを入力します。

ステップ 9 このユーザのプライバシー パスワードを入力します。

ステップ 10 [Save（保存）] をクリックします。

第 5 章

ファームウェア管理

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

Cisco UCS Central を使用すれば、すべての登録された Cisco UCS ドメインと Cisco UCS Mini ドメインのすべてのファームウェアコンポーネントを管理できます。すべてのファームウェア更新のステータスが、[Domains] セクションに表示されます。 次のいずれかになります。

- [Firmware Ready]：ファームウェアは正常に更新されています。
- [In Progress]：ファームウェア更新が現在進行中です。
- [Pending User Ack]：ファームウェアを更新する前に、[Pending Activities] ページでユーザ承認が必要です。 保留アクティビティの確認と承認，（53 ページ）を参照してください。

（注） Cisco UCS Central から Cisco UCS ドメインのファームウェアを管理するには、Cisco UCS Manager でグローバル ファームウェア管理オプションをイネーブルにする必要があります。 グローバル ファームウェア管理オプションは、Cisco UCS Manager を Cisco UCS Central に登録するときにイネーブルにできます。 また、管理要件に基づいてグローバル管理オプションのオン/オフを切り替えることもできます。

Cisco UCS ドメインは、Cisco UCS Central のドメイン グループに管理目的で分類されます。 ファームウェアは、ドメイン グループ レベルで各ドメイン グループごとに別個に管理することも、ドメイン グループのルートからドメイン グループ全体に対して管理することもできます。 Cisco UCS Central には、次の Cisco UCS ドメインのファームウェア パッケージを管理するオプションがあります。

- **機能カタログ**：ドメイン グループごとに機能カタログを 1 つ使用します。 特定のドメイン グループに登録されたすべての Cisco UCS ドメインによって、ドメイン グループで定義された機能カタログが使用されます。
- **インフラストラクチャ ファームウェア**：ドメイン グループごとにインフラストラクチャ ファームウェア ポリシーを 1 つ使用します。 特定のドメイン グループに登録されたすべての Cisco UCS ドメインによって、ドメイン グループで定義された同じインフラストラクチャ ファームウェア バージョンが使用されます。

イメージ ライブラリ

Cisco UCS Central のイメージ ライブラリには、Cisco.com から Cisco UCS Central のローカル ファイル システムとリモート ファイル システムにダウンロードされたすべてのファームウェア イメージのリストが表示されます。 これらのファームウェア イメージは、ファームウェア ポリシーの作成に使用できます。

グローバル設定に関して実行できることは次のとおりです。

- ファームウェア イメージを使用してポリシーを作成する。
- イメージを選択して、[Delete] アイコンをクリックすることによって、イメージ ライブラリからダウンロードされたイメージを削除する。

（注） 削除しようとしているファームウェア イメージがスケジュールされたポリシーから参照されている場合は、削除操作が失敗します。 このポリシーはイメージ ライブラリから削除できません。

- [Flash] アイコンをクリックすることによって、ファームウェア イメージと Cisco.com 上のイメージを同期させます。

ファームウェア バンドルのインポート

Cisco.comからファームウェア バンドルをダウンロードして、ローカルデスクトップまたはサポートされているリモート ファイル システムに保存されていることを確認してください。

ステップ 1 メニュー バーで、[Operations] アイコンをクリックして、[Firmware] を選択します。

ステップ 2 [Firmware] ページで、[Operations] アイコンをクリックして、[Import Firmware Bundle] を選択します。これにより、[Import Firmware Bundle] ダイアログボックスが開きます。

ステップ 3 ローカル システムにファームウェア バンドルを含む BIN ファイルが存在する場合は、

a) [FW Bundle Location] で、[Local] をクリックします。
b) [File Name] フィールドで、ファイル アイコンをクリックしてローカル ブラウザを開きます。

c) ファイルの場所から、BIN ファイルを選択して、[Import] をクリックします。

ステップ 4 リモート ファイル システムにファームウェア バンドルが存在する場合は、

（注） リモート ファイル システムのホスト名、ユーザ名、およびパスワードがわかっていることを確認してください。

a) [FW Bundle Location] で、[Remote] をクリックします。
これにより、サポートされているファイル転送プロトコルが表示されます。

b) ファイルをインポートするオプションのいずれかを選択して、フィールドに必要な情報を入力し、[Import] をクリックします。
たとえば、リモート サーバ上の BIN ファイル `ucs-k9-bundle-infra.2.2.3a.A.bin` を使用する場合は、絶対パス /home/cisco-ucs-central/firmware/ucs-k9-bundle-infra.2.2.3a.A.bin を入力します。

次の作業

ファームウェア バンドルを適切なポリシーに追加して、アップグレードを実行します。

アップグレードが完了したら、Cisco UCS Central からファームウェア バンドルを削除できますが、関連するポリシーから先に削除する必要があります。

Cisco.com からの自動ファームウェア更新同期起動の有効化

Cisco.com 上の最新のファームウェア バンドルにアクセスするには、有効な Cisco.com ユーザ名とパスワードを持っている必要があります。

ステップ 1 タスク バーで、「Sync Firmware Updates from Cisco.com」と入力して、Enter キーを押します。
これにより、[Sync Firmware Updates from Cisco.com] ダイアログボックスが開きます。

ステップ 2 該当するフィールドに Cisco.com ユーザ名とパスワードを入力します。

ステップ 3 Cisco UCS Central に新しいファームウェア更新を自動的にダウンロードさせる場合：

a) [Sync FW Updates Periodically] フィールドで、[Enable] をクリックします。

b) [Frequency] フィールドで、必要な頻度を選択します。

（注） このフィールドで [On Demand] を選択した場合は、Cisco UCS Central が自動的に新しいファームウェア更新をダウンロードしません。 代わりに、このダイアログ ボックスの [Sync] ボタンを使用して手動でダウンロードする必要があります。

ステップ 4 システムから HTTP 経由で Cisco.com にアクセスできるようにする場合は、[HTTP Proxy To Access Cisco.com] フィールドで [Enabled] を選択して、該当するフィールドに HTTP 接続情報を入力します。

（注） この機能には、Cisco UCS Central が Cisco.com へのネットワーク アクセスを備えている必要があります。 必要に応じて、プロキシ サーバ設定を有効にして適用してください。

ステップ 5 [Sync] をクリックします。

Cisco UCS ドメイン グループのインフラストラクチャ ファームウェア更新のスケジューリング

ドメイン グループ内のすべてのサーバのインフラストラクチャ ファームウェア更新をスケジュールできます。

ステップ 1 タスク バーで、「Schedule Infra Firmware Update - Classic」と入力して、Enter キーを押します。
これにより、[Schedule Infra Firmware Update - Classic] ダイアログボックスが開きます。

ステップ 2 [Domain Group for UCS Infra Update] ドロップダウン リストで、ドメイン グループを選択します。
Cisco UCS Central に、ファームウェア アップグレードの影響を受けるドメインの数と、それらのドメインの Cisco UCS Manager バージョンが表示されます。

ステップ 3 [UCS Infra Update Version] ドロップダウン リストで、使用するファームウェア バージョンを選択します。

ステップ 4 （任意） [Catalog Version] ドロップダウン リストで、カタログ バージョンを選択します。

ステップ 5 [FW Update Maintenance Window] フィールドで、メンテナンス時間帯を選択します。

ステップ 6 [User Acknowledgement Required To Install] フィールドで、サーバのリブートにユーザの承認が必要かどうかを選択します。

- [Enabled]：選択したドメイン グループ内のサーバがリブートする前に、ユーザがリブート要求を手動で承認する必要があります。
- [Disabled]：選択されたドメイン グループ内のサーバは、必要に応じて更新中に自動的にリブートされます。

ステップ 7 [Schedule] をクリックします。
[Firmware] ページでファームウェア更新を監視できます。ファームウェア管理, （37 ページ）を参照してください。

Cisco UCS Mini ドメイン グループのインフラストラクチャ ファームウェア更新のスケジューリング

ドメイン グループ内のすべてのサーバのインフラストラクチャ ファームウェア更新をスケジュールできます。

ステップ 1 タスク バーで、「Schedule Infra Firmware Update - Mini」と入力して、Enter キーを押します。
これにより、[Schedule Infra Firmware Update - Mini] ダイアログボックスが開きます。

ステップ 2 [Domain Group for UCS Infra Update] ドロップダウン リストで、ドメイン グループを選択します。
Cisco UCS Central に、ファームウェア アップグレードの影響を受けるドメインの数と、それらのドメインの Cisco UCS Manager バージョンが表示されます。

ステップ 3 [UCS Infra Update Version] ドロップダウン リストで、使用するファームウェア バージョンを選択します。

ステップ 4 （任意） [Catalog Version] ドロップダウン リストで、カタログ バージョンを選択します。

ステップ 5 [FW Update Maintenance Window] フィールドで、メンテナンス時間帯を選択します。

ステップ 6 [User Acknowledgement Required To Install] フィールドで、サーバのリブートにユーザの承認が必要かどうかを選択します。

- [Enabled]：選択したドメイン グループ内のサーバがリブートする前に、ユーザがリブート要求を手動で承認する必要があります。
- [Disabled]：選択されたドメイン グループ内のサーバは、必要に応じて更新中に自動的にリブートされます。

ステップ 7 [Schedule] をクリックします。
[Firmware] ページでファームウェア更新を監視できます。ファームウェア管理, （37 ページ）を参照してください。

Cisco UCS ドメイン グループのインフラストラクチャ ファームウェア スケジュールの削除

ステップ 1 タスク バーで、「Remove Infra Firmware Schedule - Classic」と入力して、Enter キーを押します。
これにより、[Remove Infra Firmware Schedule - Classic] ダイアログボックスが開きます。

ステップ 2 [Domain Group for UCS Infra Update] ドロップダウン リストで、ドメイン グループを選択します。

Cisco UCS Central が自動的に [UCS Infra Update Version]、[Catalog Version]、および [FW Update Maintenance Window] の各フィールドに値を設定します。

ステップ 3 [Remove] をクリックします。

Cisco UCS Mini ドメイン グループのインフラストラクチャ ファームウェア スケジュールの削除

ステップ 1 タスク バーで、「Remove Infra Firmware Schedule - Mini」と入力して、Enter キーを押します。
これにより、[Remove Infra Firmware Schedule - Mini] ダイアログボックスが開きます。

ステップ 2 [Domain Group for UCS Infra Update] ドロップダウン リストで、ドメイン グループを選択します。
Cisco UCS Central が自動的に [UCS Infra Update Version]、[Catalog Version]、および [FW Update Maintenance Window] の各フィールドに値を設定します。

ステップ 3 [Remove] をクリックします。

ホスト ファームウェア パッケージ ポリシーの作成または編集

ステップ 1 タスク バーで、「Create Host Firmware Package Policy」と入力して、Enter キーを押します。
これにより、[Create Host Firmware Package Policy] ダイアログボックスが開きます。

ステップ 2 [Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
ポリシー名は大文字と小文字が区別されます。

ステップ 4 環境の要件に応じて、[Blade Version] 、[Rack Version] 、または [Modular Version] を選択します。

ステップ 5 [Create] をクリックします。

第 6 章

システム管理

この章は、次の内容で構成されています。

UCS Central システム ポリシーの設定

[Manage UCS Central System Policies] ダイアログボックスで、障害、syslog、およびコア ダンプ エクスポートのプロパティと設定値を指定できます。

ステップ 1 [System Settings] アイコンから、[System Policies] を選択します。
これにより、[Manage UCS Central System Policies] ダイアログボックスが開きます。

ステップ 2 設定するセクションのアイコンをクリックします。

- [Fault] セクションでは、[Manage UCS Central Fault Policy] ダイアログボックスと同じタスクを実行できます。 詳細については、UCS Central 障害ポリシーの管理，（44 ページ）を参照してください。
- [Syslog] セクションでは、[Manage UCS Central Syslog] ダイアログボックスと同じタスクを実行できます。 詳細については、UCS Central Syslog の管理，（45 ページ）を参照してください。
- [Core Dump Export] セクションでは、[Manage UCS Central Core Dump Export] ダイアログボックスと同じタスクを実行できます。 詳細については、 UCS Central コア ダンプ エクスポートの管理，（47 ページ）を参照してください。

ステップ 3 セクションごとに必要なフィールドに値を入力します。

ステップ 4 [Save（保存）] をクリックします。

関連トピック

UCS Central 障害ポリシーの管理, （44 ページ）
UCS Central Syslog の管理, （45 ページ）
UCS Central コア ダンプ エクスポートの管理, （47 ページ）

UCS Central 障害ポリシーの管理

ステップ 1 タスク バーで、「Manage UCS Central Fault Policy」と入力して、Enter キーを押します。
これにより、[Manage UCS Central Fault Policy] ダイアログボックスが開きます。

ステップ 2 [Fault] で、次のフィールドに値を入力します。

（注） [Initial Severity] フィールドと [Action on Acknowledgment] フィールドは読み取り専用のため、変更できません。

1. [Flapping Interval (Seconds)] フィールドに時間を秒単位で入力します。

   障害が発生し、すぐに何度かクリアされると、フラッピングが発生します。 これを防止するため、Cisco UCS Central では、最後に状態が変更されてからこの時間が経過するまで、障害が発生しても状態は変更されません。

   フラッピング間隔中に同じ条件が再発生した場合は、障害がアクティブ状態に戻ります。 フラッピング間隔中に同じ条件が再発生しない場合は、障害がクリアされます。 その時点でどうなるかは、[Action on Clear] フィールドの設定によって異なります。

2. [Soaking Interval] で、[None] を選択するか、カスタム ソーキング間隔を選択します。

3. [Clear Interval] で、Cisco UCS Central が障害をその経過時間に基づいて自動的にクリア済みとしてマークするかどうかを選択します。

   [None] を選択した場合は、障害が自動的にクリアされません。 [Custom Interval] を選択した場合は、Cisco UCS が自動的に関連する間隔フィールドで指定された時間後に障害メッセージを消去します。

4. [Action on Clear] で、障害がクリアされたときのシステムの動作を選択します。

   [Retain Cleared Faults] を選択した場合は、クリアされた障害が [Retention Interval] で指定された時間だけ保存されます。 [Delete Cleared Faults] を選択した場合は、クリアされた障害が即座に削除されます。

5. [Action on Clear] が [Retain Cleared Faults] に設定されている場合は、[Retention Interval] で、クリア済みとしてマークされた障害を Cisco UCS で保存する時間の長さを指定します。

[Forever] を選択した場合は、Cisco UCS が経過時間に関係なくすべてのクリア済みの障害メッセージを保存します。 [Custom Interval] を選択した場合は、Cisco UCS が関連する間隔フィールドで指定された時間だけクリア済みの障害メッセージを保存します。

ステップ 3 [Save] をクリックします。

関連トピック

UCS Central システム ポリシーの設定, （43 ページ）
UCS Central Syslog の管理, （45 ページ）
UCS Central コア ダンプ エクスポートの管理, （47 ページ）

UCS Central Syslog の管理

ステップ 1 タスク バーで、「Manage UCS Central Syslog」と入力して、Enter キーを押します。
これにより、[Manage UCS Central Syslog] ダイアログボックスが開きます。

ステップ 2 [Syslog Sources] で、ログ ファイルを収集するソースごとに [Enabled] を選択します。
次のいずれかになります。

- 障害
- 監査
- イベント

ステップ 3 [Local Destination] で、syslog メッセージを追加して表示可能な場所を指定します。 次のいずれかになります。

- [Console]：有効にした場合は、syslog メッセージがコンソールに表示されるだけでなく、ログに追加されます。 表示するメッセージのログ レベルを選択します。
- [Monitor]：有効にした場合は、syslog メッセージがモニタに表示されるだけでなく、ログに追加されます。 表示するメッセージのログ レベルを選択します。
- [Log File]：有効にした場合は、syslog メッセージがログ ファイルに保存されます。 無効にした場合は、syslog メッセージが保存されません。 ログ レベル、ファイル名、および最大ファイル サイズを選択します。

システムに保存するメッセージの最も低いレベルを選択します。 システムはそのレベル以上のメッセージを保存します。 ログ レベルは次のいずれかになります。

- Critical (UCSM Critical)

- Alert
- Emergency
- Error (UCSM Major)
- Warning (UCSM Minor)
- Notification (UCSM Warning)
- Information
- Debug

ステップ 4 [Remote Destination] で、プライマリ、セカンダリ、またはターシャリのどのサーバに syslog メッセージを保存するかを指定します。
リモート宛先ごとに次の情報を指定します。

- [Logging Level]：システムに保存する最も低いメッセージ レベルを選択します。 リモート ファイルにそのレベル以上のメッセージが保存されます。 次のいずれかになります。
  - Critical (UCSM Critical)
  - Alert
  - Emergency
  - Error (UCSM Major)
  - Warning (UCSM Minor)
  - Notification (UCSM Warning)
  - Information
  - Debug
- [Facility]：リモート宛先に関連付けられた機能。
- [Host Name/IPAddress]：リモート ログ ファイルが存在するホスト名または IP アドレス。 IPv4 または IPv6 アドレス以外のホスト名を使用している場合は、Cisco UCS Central で DNS サーバを設定する必要があります。

ステップ 5 [Save] をクリックします。

関連トピック

UCS Central システム ポリシーの設定, （43 ページ）
UCS Central 障害ポリシーの管理, （44 ページ）
UCS Central コア ダンプ エクスポートの管理, （47 ページ）

UCS Central コア ダンプ エクスポートの管理

Cisco UCS は、Core File Exporter を使用して、コア ファイルが生成されるとすぐにそれらを TFTP 経由でネットワーク上の指定された場所にエクスポートします。 この機能を使用すれば、コア ファイルを tar 形式でエクスポートすることができます。

ステップ 1 タスク バーで、「Manage UCS Central Core Dump Export」と入力して、Enter キーを押します。
これにより、[Manage UCS Central Core Dump Export] ダイアログボックスが開きます。

ステップ 2 [Enable] をクリックして、コア ファイルをエクスポートします。

ステップ 3 （任意） コア ファイルを保存するために使用するリモート サーバに関する説明を入力します。

ステップ 4 [Frequency]、[Maximum No. of Files]、[Remote Copy]、および [Protocol] の各フィールドはデフォルトで設定されています。

ステップ 5 （任意） [Absolute Remote Path] に、コア ファイルをリモート サーバにエクスポートするときに使用するパスを入力します。

ステップ 6 [Remote Server Host Name/IP Address] に、TFTP 経由で接続するホスト名または IP アドレスを入力します。

ステップ 7 （任意） [TFTP Port] に、TFTP 経由でコア ファイルをエクスポートするときに使用するポート番号を入力します。 デフォルトのポート番号は 69 です。

ステップ 8 [Save（保存）] をクリックします。

関連トピック

UCS Central システム ポリシーの設定, （43 ページ）
UCS Central 障害ポリシーの管理, （44 ページ）
UCS Central Syslog の管理, （45 ページ）

UCS Central システム プロファイルの管理

ステップ 1 [System Settings] アイコンから、[System Profile] を選択します。
これにより、[Manage UCS Central System Profile] ダイアログボックスが開きます。

ステップ 2 [UCS Central] セクションで、[UCS Central System Name]、[Mode]、および仮想 IPv4 アドレスと仮想 IPv6 アドレスを表示できます。
これらの値は、最初に Cisco UCS Central を設定したときに生成されます。 システム名とモードは変更できません。

ステップ 3 [Interfaces] で、次の管理ノードを確認または変更します。

- プライマリ ノード（IPv4）
- プライマリ ノード（IPv6）
- セカンダリ ノード（IPv4）
- セカンダリ ノード（IPv6）

ステップ 4 [Date & Time] で、タイム ゾーンを選択して、NTP サーバを追加します。

ステップ 5 [DNS] で、Cisco UCS Central ドメイン名を入力して、DNS サーバを追加します。

ステップ 6 [Remote Access] で、キー リングを選択します。

ステップ 7 [Trusted Points] で、[Add] をクリックして、新しいトラスト ポイントと証明書チェーンを追加します。

ステップ 8 [Certificates] では、既存のキー リングを表示したり、新しいキー リングと証明書要求を作成したりできます。

ステップ 9 [Save] をクリックします。

関連トピック

UCS Central NTP サーバの管理, （49 ページ）
UCS Central 管理ノードの管理, （48 ページ）
UCS Central DNS サーバの管理, （49 ページ）

UCS Central 管理ノードの管理

ステップ 1 タスク バーで、「Manage UCS Central Management Node」と入力して、Enter キーを押します。
これにより、[Manage UCS Central Management Node] ダイアログボックスが開きます。

ステップ 2 [Management Node] で、設定するノードの名前をクリックします。

ステップ 3 [IP Address]、[Subnet Mask]、および [Default Gateway] の値を入力します。

ステップ 4 [Save（保存）] をクリックします。

関連トピック

UCS Central システム プロファイルの管理, （47 ページ）
UCS Central NTP サーバの管理, （49 ページ）
UCS Central DNS サーバの管理, （49 ページ）

UCS Central NTP サーバの管理

ステップ 1 タスク バーで、「Manage UCS Central NTP Servers」と入力して、Enter キーを押します。
これにより、[Manage UCS Central NTP Servers] ダイアログボックスが開きます。

ステップ 2 [Time Zone] で、ドメインのタイム ゾーンを選択します。

ステップ 3 [NTP Servers] で、[Add] をクリックして新しい NTP サーバを追加するか、[Delete] をクリックして既存のサーバを削除します。

ステップ 4 [Save（保存）] をクリックします。

関連トピック

UCS Central システム プロファイルの管理, （47 ページ）
UCS Central 管理ノードの管理, （48 ページ）
UCS Central DNS サーバの管理, （49 ページ）

UCS Central DNS サーバの管理

ステップ 1 タスク バーで、「Manage UCS Central DNS Servers」と入力して Enter キーを押します。
これにより、[Manage UCS Central DNS Servers] ダイアログボックスが開きます。

ステップ 2 [UCS Central Domain Name] に、Cisco UCS Central ドメインの名前を入力します。

ステップ 3 [DNS Servers] で、[Add] をクリックして新しい DNS サーバを追加するか、[Delete] をクリックして既存のサーバを削除します。

ステップ 4 [Save（保存）] をクリックします。

関連トピック

UCS Central システム プロファイルの管理, （47 ページ）
UCS Central NTP サーバの管理, （49 ページ）
UCS Central 管理ノードの管理, （48 ページ）

ドメイン グループ システム ポリシーの管理

ステップ 1 ルートの [Domain Group] ページに移動します。

ステップ 2 [Settings] アイコンをクリックして、[System Profile] を選択します。

ステップ 3 [Fault] で、必要なフィールドに値を入力します。
詳細については、UCS Central 障害ポリシーの管理, （44 ページ）を参照してください。

ステップ 4 [Syslog] で、必要なフィールドに値を入力します。
詳細については、UCS Central Syslog の管理, （45 ページ）を参照してください。

ステップ 5 [Core Dump] で、必要なフィールドに値を入力します。
詳細については、UCS Central コア ダンプ エクスポートの管理, （47 ページ）を参照してください。

ステップ 6 [Interfaces] で、[Interface Monitoring Policy] を有効にするかどうかを選択します。

ステップ 7 [Enabled] を選択した場合は、必要に応じてインターフェイス モニタリング情報を入力します。

ステップ 8 [Equipment] で、[Power Redundancy] と [Power Allocation Method] を選択して、[ID Soaking Interval] を入力します。

ステップ 9 [System Events] で、必要なフィールドに値を入力して、システム イベント ログの収集方法を決定します。

ステップ 10 [Save] をクリックします。

ドメイン グループ システム プロファイルの管理

ステップ 1 ルートの [Domain Group] ページに移動します。

ステップ 2 [Settings] アイコンをクリックして、[System Profile] を選択します。

ステップ 3 [Date & Time] で、タイム ゾーンを選択して、NTP サーバを追加します。

ステップ 4 [DNS] で、UCS Central ドメイン名を入力して、DNS サーバを追加します。

ステップ 5 [Remote Access] で、HTTPS と HTTPS ポートを入力して、キー リングを選択します。

ステップ 6 [Trusted Points] で、[Add] をクリックして、トラスト ポイントを作成し、証明書チェーンを追加します。

ステップ 7 [Save] をクリックします。

テクニカル サポート ファイル

Cisco UCS Central と登録された Cisco UCS ドメインに関するテクニカル サポート ファイルを生成できます。 リモート テクニカル サポートの収集には以下が含まれます。

- テクニカル サポートの生成：Cisco UCS Central または登録された UCS ドメインのそれぞれに関するテクニカル サポート ファイルを生成できます。
- テクニカル サポート ファイルのダウンロード：作成したテクニカル サポート ファイルをダウンロードして情報を確認します。

（注） テクニカル サポート ファイルをダウンロードできるのは、Cisco UCS Central GUI からだけです。

テクニカル サポート ファイルの生成

ステップ 1 メニュー バーで、[Operation] アイコンをクリックして、[Tech Support] を選択します。

ステップ 2 [Domains] で、[UCS Central] またはテクニカル サポート ファイルを生成するドメインを選択します。これにより、使用可能なテクニカル サポート ファイルと生成メニュー オプションが表示されます。

ステップ 3 フラッシュ アイコンをクリックして、テクニカル サポート ファイルを生成します。

ステップ 4 ポップアップ確認ダイアログボックスで、[Yes] をクリックします。

ステップ 5 収集が進行中に、リスト ページにテクニカル サポート ファイルの収集ステータスが表示されます。 プロセスが完了すると、収集時間、ファイル名、および可用性ステータスが表示されます。

テクニカル サポート ファイルのダウンロード

ステップ 1 メニュー バーで、[Operation] アイコンをクリックして、[Tech Support] を選択します。
ステップ 2 [Domains] で、[UCS Central] またはテクニカル サポート ファイルを生成するドメインを選択します。
ステップ 3 右ペインに、選択したシステムで利用可能なテクニカル サポート ファイルのリストが表示されます。
ステップ 4 ダウンロードするファイルをクリックして選択します。
ステップ 5 メニュー バーで、[Download] アイコンをクリックします。
ステップ 6 ダウンロード ダイアログボックスで、[Save] をクリックして、テクニカル サポート ファイルをローカル ダウンロード フォルダに保存します。

システムの障害とログの監視

保留アクティビティ

Cisco UCS ドメインで遅延展開を設定すると、Cisco UCS Central ですべての保留アクティビティを表示することができます。 ユーザの確認応答を待っているアクティビティとスケジュール済みのアクティビティのすべてを確認できます。

Cisco UCS ドメインに保留アクティビティが存在する場合は、管理者特権を持っているユーザがログインしたときに Cisco UCS Central GUI からそのことが通知されます。

Cisco UCS Central には、すべての保留アクティビティに関する情報が表示されます。これには、次の内容が含まれます。

- 展開され、サーバと関連付けられるサービス プロファイルの名前
- 展開の影響を受けるサーバ
- 展開により発生する中断
- 展開によって実行される変更
- アクティビティが承認されているかどうか

アクティビティを承認することもできます。

特定の保留中アクティビティがサーバに適用されるメンテナンス時間を指定することはできません。 メンテナンス時間は、保留アクティビティの数と、サービスプロファイルに割り当てられたメンテナンス ポリシーによって異なります。 ただし、管理者特権を持っているユーザは、アクティビティがユーザの確認応答を待っているのかメンテナンス時間を待っ[ているのかに関係なく、手動で保留アクティビティを開始して、その場でサーバをリブートできます。

Cisco UCS Central GUI で保留アクティビティを表示するには、メニュー バーの [Alerts] アイコンをクリックします。

重要　保留アクティビティがローカル メンテナンス ポリシーとローカル スケジューラを使用したローカル サービス プロファイルによって引き起こされた場合は、ログに表示されません。 このような保留アクティビティは、Cisco UCS Manager から承認される必要があります。

保留アクティビティの確認と承認

ステップ 1　メニュー バーで、[Alerts] アイコンをクリックします。

ステップ 2　[Pending Activities] を選択します。

ステップ 3　[Pending Activities] で、保留中のアクティビティをメモします。
[Filters] 領域のチェックボックスを使用して、アクティビティを絞り込むことができます。

ステップ 4　[Acknowledge] をクリックして保留アクティビティを承認します。

システム障害

Cisco UCS Central は、Cisco UCS Central のシステム障害を収集して、そのすべてを [Fault Logs] ページに表示します。 これらのシステム障害ログを表示するには、[Alerts] アイコンをクリックして、[System Faults] を選択します。 [Faults Logs] ページでは、障害のタイプと重大度レベルに関する情報が表示され、システム障害を監視して認識したり、表示する障害を絞り込んだりすることができます。

障害テーブルには、障害ごとに次の情報が表示されます。

- [Code]：障害に関連付けられた ID
- [Timestamp]：障害が発生した日付と時刻
- [Type]：障害の発生元
- [Cause]：障害の原因
- [Affected Object]：この障害の影響を受けるコンポーネント
- [Fault Details]：障害の詳細
- [Severity]：障害の重大度
- [Action]：障害に必要なアクション

収集された情報を管理するには、UCS Central システム ポリシーの設定, （43 ページ）を参照してください。

UCS ドメインの障害

Cisco UCS Central は、UCS ドメインの [Faults Log] ページに、登録されたCisco UCS ドメインからの障害を収集して表示します。 障害はタイプと重大度レベル別に表示されます。 障害タイプをクリックすると、障害が発生した正確な Cisco UCS ドメインを展開して表示できます。 UCS ドメイン障害ログは次のようにカテゴリ別に表示されます。

- [Fault Level]：プロファイルをトリガーする障害レベル。 次のいずれかになります。
  - [Critical]：1 つ以上のコンポーネントに重大な問題があります。 これらの問題を調査し、すぐに修正する必要があります。
  - [Major]：1 つ以上のコンポーネントに深刻な問題があります。 これらの問題を調査し、すぐに修正する必要があります。
  - [Minor]：1 つ以上のコンポーネントにシステム パフォーマンスに悪影響を及ぼす可能性のある問題があります。 これらの問題を調査し、重大な問題や緊急の問題に発展する前にできるだけ早く修正する必要があります。
  - [Warning]：1 つ以上のコンポーネントに問題が解消されなければシステム パフォーマンスに悪影響を及ぼす可能性のある潜在的な問題があります。 これらの問題を調査し、問題が悪化する前にできるだけ早く修正する必要があります。
  - [Healthy]：ドメイン内のどのコンポーネントにも障害がありません。
  - [Unknown]：ドメイン内のどのコンポーネントにも障害がありません。
- [No Of Domains]：それぞれの重大度レベルで障害が発生したドメインの数。
- [Domain]：障害が発生したドメイン。 タイプをクリックすると、そのタイプの障害が 1 つ以上発生している Cisco UCS ドメインと障害の詳細が表示されます。
- [Critical]：Cisco UCS ドメイン内の選択したタイプの重大障害の件数。
- [Major]：Cisco UCS ドメイン内の選択したタイプのメジャー障害の件数。
- [Minor]：Cisco UCS ドメイン内の選択したタイプのマイナー障害の件数。
- [Warning]：Cisco UCS ドメイン内の選択したタイプの警告障害の件数。

このテーブルは、[UCS Domain Faults] ページでドメインを選択したときにだけ表示されます。

- [Filter]：テーブル内のデータをフィルタ処理できます。
- [ID]：障害に関連付けられた一意の識別子。
- [Timestamp]：障害が発生した日付と時刻。
- [Type]：障害の発生場所に関する情報。

- [Cause]：障害の原因の簡単な説明。
- [Affected Object]：この問題の影響を受けるコンポーネント。
- [Fault Details]：ログ メッセージに関する詳細情報。
- [Severity]：障害の重大度を示すアイコンが表示されます。 テーブルの下にアイコン キーが表示されます。

イベント ログ

Cisco UCS Central は、ユーザがログインしたときやシステムでエラーが発生したときなど、システムで発生したイベントを収集して表示します。 このようなイベントが発生すると、システムがそのイベントを**イベント ログ**に記録して表示します。 このイベント ログを確認するには、メニュー バーで [Alerts] アイコンをクリックして、[Events] を選択します。 イベント ログには以下に関する情報が記録されます。

- [ID]：障害を引き起こしたイベントに関連付けられた一意の識別子
- [Timestamp]：イベントが発生した日付と時刻
- [Trig. By]：イベントに関連付けられたユーザのタイプ
- [Affected Object]：イベントの影響を受けるコンポーネント

監査ログ

監査ログでは、Cisco UCS Central の設定変更の包括的なリストを表示できます。 Cisco UCS Central GUI または Cisco UCS Central CLI で作成、編集、または削除タスクに関する設定変更を実施したときに、Cisco UCS Central が監査ログを生成します。 設定に関連した情報に加えて、以下に関する情報が監査ログに記録されます。

- アクセスされたリソース。
- イベントが発生した日付と時刻。
- ログ メッセージに関連付けられた一意の識別子。
- 監査ログが生成されるアクションをトリガーしたユーザ。 これは、内部セッションの場合と Cisco UCS Central GUI または Cisco UCS Central CLI を使用して変更を加えた外部ユーザの場合があります。
- アクションをトリガーしたソース。
- 影響を受けるコンポーネント。

コア ダンプ

システムがクラッシュするエラーが発生した場合に、コア ダンプ ファイルが作成されます。 このコア ダンプ ファイルには、エラーが発生する前のシステムの状態やシステムがクラッシュした時刻などに関する情報が含まれています。 コア ダンプ ファイルを表示するには、メニュー バーで [Alerts] アイコンをクリックして、[Core Dumps] を選択します。 [Core Dumps] ログ テーブルで、次の情報を確認できます。

- [Timestamp]：コア ダンプ ファイルが作成された日時。
- [Name]：コア ダンプ ファイルの完全名。
- [Description]：コア ダンプ ファイルのタイプ。

アクティブ セッション

Cisco UCS Central でリモート ユーザとローカル ユーザのアクティブ セッションを表示して、サーバからそれらのセッションを終了することができます。 アクティブセッションを表示するには、メニュー バーで [Alerts] アイコンをクリックして、[Sessions] を選択します。 [Active Sessions] ログ テーブルで、次の情報を確認することができます。

- [ID]：ユーザがログインした端末のタイプ。
- [Timestamp]：ユーザがログインした日付と時刻。
- [User]：ユーザ名。
- [Type]：ユーザがログインした端末のタイプ。
- [Host]：ユーザがログインした IP アドレス。
- [Status]：セッションが現在アクティブかどうか。
- [Actions]：[Terminate] をクリックすると、選択したセッションが終了します。

内部サービス

内部サービス ログは、さまざまなプロバイダーとそれらのプロバイダーに関連付けられた Cisco UCS Central のバージョンに関する情報を提供します。 内部サービスを表示するには、メニュー バーで [Alerts] アイコンをクリックして、[Sessions] を選択します。

[Internal Services] ページの [Services] セクションで、次の情報を表示できます。

- [Name]：プロバイダーのタイプ。
- [Last Poll]：Cisco UCS Central がプロバイダーを最後にポーリングした日付と時刻。
- [IP Address]：プロバイダーに関連付けられた IP アドレス。
- [Version]：プロバイダーに関連付けられた Cisco UCS Central のバージョン。

- [Status]：プロバイダーの稼働状態。

[Internal Services] ページの [Clean Up] セクションで、次の情報を表示できます。

- [Domain]：ドメイン名。
- [Last Poll]：Cisco UCS Central がプロバイダーを最後にポーリングした日付と時刻。
- [Lost Visibility]：Cisco UCS Central がプロバイダーを認識できなくなった時点。
- [Clean Up]：[Clean Up] をクリックすると、Cisco UCS Central からこの Cisco UCS ドメインのすべての参照が削除されます。

（注） ドメインは、Cisco UCS Central に再登録しないかぎり、Cisco UCS Central で再び管理することはできません。

第 7 章

ドメインと組織

この章は、次の内容で構成されています。

ドメイン グループ

Cisco UCS Central は、複数の Cisco UCS ドメインを管理するための Cisco UCS ドメイン グループの階層を作成します。 Cisco UCS Central には、次のドメイン グループのカテゴリがあります。

- **ドメイン グループ**：複数の Cisco UCS ドメインを含むグループ。 管理を容易にするため、1 つのドメインの下に同様の Cisco UCS ドメインをグループ化できます。
- **グループ化されていないドメイン**：新しい Cisco UCS ドメインが Cisco UCS Central に登録されると、グループ化されていないドメインに追加されます。 グループ化されていないドメインを任意のドメイン グループに割り当てることができます。

ドメイン グループ ポリシーが作成されており、登録された新しい Cisco UCS ドメインがそのポリシーで定義された資格条件を満たしている場合は、そのドメインがポリシーで指定されたドメイン グループに自動的に配置されます。 それ以外の場合は、グループ化されていないドメイン カテゴリに配置されます。 このグループ化されていないドメインを、任意のドメイン グループに割り当てることができます。

各 Cisco UCS ドメインは、1 つのドメイン グループにのみ割り当てることができます。 Cisco UCS ドメインのメンバーシップは、任意の時点で割り当てまたは再割り当てすることができます。 Cisco UCS ドメインをドメイン グループに割り当てると、Cisco UCS ドメインは、ドメイン グループに対して指定されたすべての管理ポリシーを継承します。

Cisco UCS ドメインをドメイン グループに追加する前に、Cisco UCS ドメイン内でポリシー解決制御をローカルに変更してください。 これにより、その Cisco UCS ドメインに固有のサービス プロファイルおよびメンテナンス ポリシーが誤って上書きされるのを防止します。 Cisco UCS ドメインの自動検出をイネーブルにしている場合でも、ローカル ポリシー解決をイネーブルにすると、ポリシーが誤って上書きされることから Cisco UCS ドメインを保護します。

重要

- すべての M シリーズ モジュラ サーバ ドメイン用の別のドメイン グループを作成する必要があります。 また、モジュラ サーバ ドメイン グループが階層型ではないことを確認してください。
- Cisco UCS Central で、M シリーズ モジュラ ドメイン用の別のインフラストラクチャ ファームウェア ポリシーを作成する必要があります。 インフラストラクチャ ファームウェア ポリシーはモジュラ サーバごとに一意である必要があります。 これにより、他のドメイン グループとのファームウェア ポリシー解決が防止されます。

ドメイン グループの作成または編集

ステップ 1 タスク バーで、「Create Domain Group」と入力して、Enter キーを押します。
これにより、[Create Domain Group] ダイアログボックスが開きます。

ステップ 2 [Basic] で、[Domain Group Location] をクリックして、ドメイン グループを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
大文字と小文字が区別されます。

ステップ 4 [Qualification] で、Cisco UCS Manager ドメインを識別するために使用する [Qualification Policies] を選択します。
資格ポリシーを満たすすべてのドメインが自動的にドメイン グループに追加されます。

ステップ 5 [Domains] で、ドメイン グループに追加する Cisco UCS Manager ドメインを選択します。
M シリーズ モジュラ サーバのドメインは、UCS Classic（B シリーズ）ドメインまたは UCS Mini ドメインを含むドメイン グループに追加しないでください。

ステップ 6 [Create] をクリックします。

ドメイン グループへのドメインの追加

ステップ 1 [Domain Group] アイコンをクリックして、Cisco UCS Manager ドメインを追加するドメイン グループを選択します。

ステップ 2 [Edit] アイコンをクリックします。
選択したドメインの [Edit] ダイアログボックスが表示されます。

ステップ 3 必要に応じて説明と資格ポリシーを更新します。

ステップ 4 [Domains] をクリックして、ドメイン グループに追加する Cisco UCS Manager ドメインを選択します。
（注） Mシリーズモジュラ サーバのドメインは、UCS Classic（Bシリーズ）ドメインまたはUCS Mini ドメインを含むドメイン グループに追加しないでください。

ステップ 5 [Save] をクリックします。

ドメイン グループ SNMP の管理

ステップ 1 タスク バーで、「Manage Domain Group SNMP」と入力して、Enter キーを押します。
これにより、[Manage Domain Group SNMP] ダイアログボックスが開きます。

ステップ 2 [Basic] で、[Enabled] をクリックしてから、[Community/User Name] を入力します。
Cisco UCS には、トラップを SNMP ホストに送信するときの SNMP v1 または v2c コミュニティ名または SNMP v3 ユーザ名が付属しています。 これは [SNMP Traps] に設定されたコミュニティまたはユーザ名と同じにする必要があります。

ステップ 3 オプションの [System Contact] と [System Location] を入力します。

ステップ 4 [SNMP Traps] で、[Add] をクリックして、次の手順を実行します。

a) [Basic] セクションと同じ [Community/User Name] を入力します。
b) [Port] を入力して、SNMP の [Version]、[Type]、および [V3 Privilege] の値を選択します。

ステップ 5 [SNMP Users] で、[Add] をクリックして、次の手順を実行します。

a) [SNMP User Name] を入力します。
b) [Authentication Type] を選択し、[AES-128 Encryption] を有効にするかどうかを選択します。
c) パスワードとプライバシー パスワードの値を入力して、確認します。

ステップ 6 [Save] をクリックします。

ドメイン グループ資格ポリシー

ドメイン グループ ポリシーを使用すれば、新しい Cisco UCS ドメインを自動的にドメイン グループに配置することができます。 管理要件に応じて、さまざまな Cisco UCS ドメインの所有者、サイト、および IP アドレスに基づいて資格条件を作成できます。 新しい Cisco UCS ドメインが登録されると、Cisco UCS Central が、ドメイン グループ資格ポリシーで事前に定義された資格条件に基づいてドメインを分析し、そのドメインを管理用の特定のドメインに配置します。

ドメイン グループ資格ポリシーの作成または編集

ステップ 1 タスク バーで、「Create Domain Group Qualification Policy」と入力して、Enter キーを押します。
これにより、[Create Domain Group Qualification Policy] ダイアログボックスが開きます。

ステップ 2 [Basic] で、[Organization] をクリックして、ドメイン グループ資格ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
ポリシー名は大文字と小文字が区別されます。

ステップ 4 [Owner] で、所有者名と正規表現を入力します。

ステップ 5 [Site] で、サイト名と正規表現を入力します。

ステップ 6 [IP Address] で、IP アドレスの範囲を追加します。

ステップ 7 [Create] をクリックします。

組織

マニュアルの構成

[Organization] ページを使用すれば、登録された Cisco UCS ドメイン内に存在する組織で作成された論理エンティティを表示できます。

次のアイコンのいずれかをクリックすると、特定のページが表示されます。

- [Service Profiles]：組織内のすべてのサービス プロファイルが表示されます。
- [Service Profile Templates]：組織内のすべてのサービス プロファイル テンプレートが表示されます。
- [Pools]：組織内のすべてのプールが表示されます。
- [Policies]：組織内のすべてのポリシーが表示されます。

組織の説明の更新

組織を作成したら、その説明を更新できます。

ステップ 1 [Organization] ページで、[Edit] アイコンをクリックします。
これにより、[Edit Organization] ダイアログボックスが開きます。

ステップ 2 組織の [Description] を入力します。

ステップ 3 [Save] をクリックします。

インベントリ

ドメイン テーブル ビュー

[Domains Table View] ページには、Cisco UCS Central に登録されたドメインに関する次の情報が表示されます。

ドメイン	ハードウェア	設定	ステータス
この列には、登録されたドメインに関する次の情報が表示されます。 • 関連するドメイン名とサイト • ドメイン グループの場所 • 管理 IP アドレス • 所有者	この列には、登録されたドメインに関する次のハードウェア情報が表示されます。 • ファブリック インターコネクト モデル番号とクラスタ状態（HA またはスタンドアロン） • シャーシと FEX の数 • ブレード サーバとラック サーバの数 • ストレージに使用可能なブレード サーバの数 • Cisco UCS M シリーズ モジュラ サーバ用のカートリッジの数	この列には、登録されたドメインに関する次の設定が表示されます。 • プラットフォーム ファミリ • ファームウェアのバージョン • ファームウェアのステータス	この列には、登録されたドメインに関する次のステータスが表示されます。 • 全体のステータス • 最低障害レベル • 試用期限切れまたはステータス

ドメイン グループの詳細

[Domain Group] ページで、ドメイン グループに関連付けられたエンティティに関する情報を表示できます。 これには以下が含まれます。

- ドメイン
- ファブリック インターコネクト
- シャーシ
- サーバ
- FEX
- vLAN
- vSAN

[Settings] アイコンをクリックすると、次のタスクを実行できます。

- システム プロファイルまたはシステム ポリシーの作成。
- ユーザ、認証、SNMP、および Call Home の設定の管理。
- ドメイン グループの編集と、ユーザ作成ドメイン グループの削除。

（注） ドメイン グループ ルートは削除できません。

Cisco UCS ドメイン メイン ビュー

[Cisco UCS Domain] ページには、選択した Cisco UCS ドメインに関する次の情報が表示されます。

- [Basic]：選択された Cisco UCS ドメインの全体的ステータス、ファームウェア、使用可能なリソース、障害サマリー、および管理詳細に関する情報が表示されます。

  また、UCS Central サブスクリプションを保留または承認したり、ドメインのメンバーシップを再評価したりできます。

- [FI]：1 つのドメインに関連付けられたファブリック インターコネクト（FI）の数、FI の全体的ステータス、ハードウェア詳細、およびファームウェア詳細が表示されます。

  FI 内のコンポーネントのステータスに関する詳細を表示するには、リストで FI をクリックします。

- [Chassis]：1 つのドメインに関連付けられたシャーシの数、シャーシの全体的ステータス、ハードウェア詳細、および設定詳細が表示されます。シャーシ内のコンポーネントのステータスの詳細については、リストでシャーシをクリックします。

- [FEX]：1 つのドメインに関連付けられた FEX の数、FEX の全体的ステータス、ハードウェア詳細、および設定詳細が表示されます。FEX 内のコンポーネントのステータスの詳細については、リストで FEX をクリックします。

- [Servers]：1 つのドメイン内のサーバの台数と使用可能なサーバの台数が表示されます。サーバの全体的ステータス、ハードウェア詳細、および設定詳細については、[Go to Servers Table] をクリックします。

[Cisco UCS Domain] ページでは、次の操作を実行できます。

- 選択した Cisco UCS ドメインの Cisco UCS Manager GUI を起動する。
- ドメインの全体的ステータスが OK の場合に UCS Central サブスクリプションを保留にする。
- ドメインの全体的ステータスが保留中の場合に UCS Central サブスクリプションをアクティブにする。
- メンバーシップを再評価する。

ファブリック インターコネクト

[Fabric Interconnect]（FI）ページには、登録された Cisco UCS ドメインに関連付けられた FI に関する次の情報が表示されます。

ファブリックインターコネクト	ハードウェア	FW	ステータス
この列には、ファブリックインターコネクトに関する次の情報が表示されます。 • 関連するドメイン名と FI ID • ドメイン グループの場所 • ドメインの IP アドレス	この列には、ファブリックインターコネクトに関する次のハードウェア情報が表示されます。 • FIのモデル番号とタイプ • シリアル番号 • 固定モジュール ポートと拡張モジュール ポートの数 • イーサネット チャネル ポートとファブリック チャネル ポートの数	この列には、ファブリックインターコネクトに関する次のファームウェア詳細が表示されます。 • ファームウェアのバージョン • ファームウェアのステータス	この列には、ファブリックインターコネクトに関する次のステータスが表示されます。 • 全体のステータス • 最低障害レベル

ファブリック インターコネクト メイン ビュー

[Fabric Interconnect Main View] ページには、登録された Cisco UCS ドメイン内の選択したファブリック インターコネクト（FI）とそのコンポーネントに関する次の情報が表示されます。

- [Basic]：ドメイン内の FI の概要、ハードウェア詳細、ファームウェア バージョン、使用中および使用可能なポート（イーサネットまたは FC）の数、管理 IP、および障害サマリーの詳細が表示されます。
- [Fixed Mod.]：FIに設置された固定モジュールの全体的ステータス、ファームウェア、ハードウェア、プロパティ、および障害サマリーの詳細が表示されます。
- [Exp. Mod.]：FIに設置された拡張モジュールの全体的ステータス、ファームウェア、ハードウェア、プロパティ、および障害サマリーの詳細が表示されます。
- [Fans]：ファンの全体的ステータスとハードウェア詳細が表示されます。
- [PSUs]：PSUの全体的ステータス、障害サマリー、およびハードウェア詳細が表示されます。

[Toggle Locator LED] を選択することによって、シャーシのロケータ LED を点灯または消灯させることができます。

サーバ テーブル ビュー

[Servers] ページには、登録された UCS ドメインに関連付けられたサーバに関する次のような情報が表示されます。

サーバ	ハードウェア	設定	ステータス
この列には、サーバに関する次の情報が表示されます。 • 関連ドメイン名、シャーシ ID、およびスロット ID • ドメイン グループの場所 • 管理 IP アドレス	この列には、サーバに関する次のハードウェア情報が表示されます。 • ブレード サーバ モデル • CPUのコア数とマザーボード上の RAM の合計 • シリアル番号 • CPU の数と速度	この列には、サーバに関する次の設定が表示されます。 • サービス プロファイル名 • サービス プロファイル組織の場所 • ファームウェアのバージョン • ファームウェアのステータス	この列には、サーバに関する次のステータスが表示されます。 • 全体のステータス • 最低障害レベル • 電源ステータス • 使用停止サーバ。 使用停止サーバは再稼動できます。

サーバ詳細ページ

サーバ詳細ページを使用すれば、Cisco UCS ドメイン内のすべてのサーバを管理および監視できます。

（注） サーバ タイプによって、オプションが異なります。

選択したサーバとそのコンポーネントに関する次の情報を表示できます。

- [Basic]：選択したサーバの関連サービス プロファイル、障害の概要、ハードウェアの詳細、およびファームウェアの詳細が表示されます。
- [Motherboard]：マザーボードの全体的ステータスとハードウェアの詳細が表示されます。
- [CPUs]：サーバ内のすべてのCPUのリストが表示されます。 プロセッサをクリックすると、そのプロセッサの全体的ステータス、ハードウェアの詳細、およびその他の詳細が表示されます。
- [Memory]：選択したサーバで使用可能なメモリのリストが表示されます。 メモリをクリックすると、現在の全体的ステータスとその他の詳細が表示されます。

- [Adaptors]：選択したサーバ内のアダプタの詳細が表示されます。 アダプタをクリックすると、全体的ステータス、電源ステータス、およびその他の製品詳細が表示されます。
- [Storage]：選択したサーバ内のストレージのリストが表示されます。 ディスクをクリックすると、現在の全体的ステータス、ハードウェアの詳細、およびコントローラの詳細が表示されます。

また、次のサーバ関連タスクを実行することもできます。

- Cisco UCS Manager または **KVM コンソール**の起動
- サーバのリセット、回復、再認識、または使用停止
- ロケータ LED の切り替え

シャーシ

[Chassis] ページには、登録された Cisco UCS ドメインに関連付けられたシャーシに関する次の情報が表示されます。

シャーシ	ハードウェア	設定	ステータス
この列には、シャーシに関する次の情報が表示されます。 • 関連するドメイン名とシャーシ ID • ドメイン グループの場所 • ファブリック側	この列には、シャーシに関する次のハードウェア情報が表示されます。 • シャーシのモデル番号 • シャーシのシリアル番号 • ブレードまたはモジュラ サーバの数 • カートリッジの数	この列には、シャーシに関する次の設定が表示されます。 • 設定ステータス • 設定エラー カウント	この列には、シャーシに関する次のステータスが表示されます。 • 全体のステータス • 最低障害レベル • 電源ステータス • 温度ステータス • 解放されたシャーシ。 有効なシャーシ ID を指定することによって、シャーシを再稼動できます。

シャーシ メイン ビュー

[Chassis Main View] ページでは、Cisco UCS Central GUI を通して Cisco UCS ドメイン内のすべてのシャーシを管理および監視できます。

登録された Cisco UCS ドメイン内で選択したシャーシとそのコンポーネントに関する次の情報を確認できます。

- [Basic]：選択したシャーシ内のすべてのコンポーネントの全体的ステータスと概要、障害サマリー、設定エラー、およびハードウェア詳細が表示されます。
- [IOM Left]：左 IOM モジュールの全体的ステータス、ハードウェア詳細、および障害サマリーが表示されます。
- [IOM Right]：右 IOM モジュールの全体的ステータス、ハードウェア詳細、および障害サマリーが表示されます。
- [Servers]：このシャーシに関連付けられたサーバの全体的ステータス、ハードウェア詳細、およびファームウェア詳細が表示されます。 サーバを選択すると、そのページから UCS ドメイン内のサーバのサーバ詳細ビュー ページにリダイレクトされます。
- [Fans]：シャーシ内のファンのリストが表示されます。 ファンをクリックすると、そのモジュールに関する情報、全体的ステータス、およびハードウェア詳細が表示されます。
- [PSUs]：シャーシ内のすべての PSU のリストが表示されます。 PSU をクリックすると、その障害サマリーに関する情報、全体的ステータス、およびその他のプロパティ詳細が表示されます。

[Chassis Main View] ページで、次の手順を実行できます。

- シャーシの確認と解放。
- シャーシのロケータ LED の点灯または消灯。
- 選択したドメインの Cisco UCS Manager GUI の起動。

（注） Cisco UCS M シリーズ モジュラ サーバでは、シャーシに関連付けられたカートリッジ、ストレージ、および LUN に関する情報を表示することもできます。

FEX

[FEX] ページには、登録された Cisco UCS ドメインに関連付けられた FEX に関する次の情報が表示されます。

FEX	ハードウェア	設定	ステータス
この列には、FEX に関する次の情報が表示されます。 • 関連するドメイン名と FEX ID • ドメイン グループの場所 • ファブリック側	この列には、FEX に関する次のハードウェア情報が表示されます。 • モデル番号 • シリアル番号 • 使用可能なポート数	この列には、FEX に関する次の設定が表示されます。 • 設定ステータス • 設定エラー カウント	この列には、FEX に関する次のステータスが表示されます。 • 全体のステータス • 最低障害レベル • 電源ステータス • 温度ステータス • 解放された FEX。 有効な FEX ID を指定することによって、FEX を再稼動できます。

FEX メイン ビュー

Cisco UCS Central を使用すれば、Cisco UCS Central GUI および CLI の両方から登録された UCS ドメイン内の FEX を管理することができます。

登録された Cisco UCS ドメイン内の FEX とそのコンポーネントに関する次の情報を確認できます。

- [Basic]：UCS ドメイン内の FEX の障害サマリー、全体的ステータス、およびハードウェア詳細が表示されます。
- [IOM]：IOM の障害サマリー、全体的ステータス、およびプロパティが表示されます。
- [Servers]：FEX に接続されたラック サーバの数が表示されます。 サーバをクリックすると、そのサーバの全体的ステータス、ファームウェア詳細、およびハードウェア詳細に関する情報が表示されます。
- [Fans]：FEX 内のファンのリストが表示されます。 ファンをクリックすると、モジュール番号、全体的ステータス、およびハードウェア詳細に関する情報が表示されます。
- [PSUs]：FEX 内のすべての PSU のリストが表示されます。 PSU をクリックすると、障害サマリー、ステータス、プロパティ、および電源装置のステータスに関する詳細が表示されます。

[FEX Main View] ページで、次のタスクを実行できます。

- FEX の認識、解放、および再稼働。
- FEX 用のロケータ LED の点灯または消灯。

第 8 章

テンプレート

この章は、次の内容で構成されています。

テンプレート

システム内のテンプレートの完全なリストが表示されます。 [Template]、[Type]、[Usage Status]、または [Tenmplate Org] で並べ替えるフィルタを使用して、使用可能性と使用状況を確認できます。

サービス プロファイル テンプレート詳細ビュー

[Service Profile Template] ページには、サービス プロファイル テンプレートに関する詳細情報が表示されます。 そこから、次のことができます。

- 監査ログの表示
- サービス プロファイル テンプレートの削除、複製、または名前変更
- このサービス プロファイル テンプレートからのサービス プロファイルの作成
- ホスト インターフェイス配置の設定

サービス プロファイル テンプレートの作成または編集

既存のテンプレートを編集していて変更を加えた場合は、必ず、[Evaluate] をクリックして、そのテンプレートに加えた変更の影響を評価してください。

ステップ 1　タスク バーで、「Create Service Profile Template」と入力して、Enter キーを押します。

これにより、[Create Service Profile Template] ダイアログボックスが開きます。

ステップ 2 [Basic] で、サービス プロファイル テンプレートを作成する [Organization] を選択します。

a) [Name] 、[Description] 、および [User Label] を入力します。

b) [Template Instantiation Mode]、[Desired Power State Check on Association]、および [Compatability Check on Migration Using Server Pool] に関するオプションを選択します。

ステップ 3 [Identifiers] をクリックして、このサービス プロファイルの識別子を割り当てます。
それぞれの識別子をクリックします。 右側で、ドロップダウンをクリックして使用可能なプールを表示し、このサービス プロファイル テンプレートに必要なものを選択します。

ステップ 4 [Connectivity] をクリックして、このテンプレートの接続ポリシーと管理 vLAN を選択します。
SAN、LAN、およびダイナミック接続ポリシーと [Management vLAN] をクリックして、右側に詳細を表示します。 次に、ドロップダウンをクリックして使用可能なポリシーを表示するか、ポリシーを検索して、このサービス プロファイル テンプレートに必要なものを選択します。

ステップ 5 [Servers] をクリックして、右側のドロップダウンをクリックします。 このテンプレートを関連付けるサーバを選択または検索して割り当てます。

ステップ 6 [Storage] をクリックして、右側のドロップダウンをクリックします。 このテンプレートを関連付けるストレージ プロファイルを選択または検索して割り当てます。

ステップ 7 [Policies] をクリックします。
すべてのサービス プロファイル関連ポリシーをクリックし、右側のドロップダウン オプションを使用して、このテンプレートにポリシーを割り当てることができます。

vHBA テンプレートの作成または編集

特定の vHBA テンプレートを編集するには、検索バーで「vHBA Template」と入力して、編集する vHBA テンプレートを検索します。

（注） グローバル vHBA は Cisco UCS Manager で作成されたローカル サービス プロファイルで使用できます。

ステップ 1 タスク バーで、「Create vHBA Template」と入力して、Enter キーを押します。
これにより、[Create vHBA Template] ダイアログボックスが開きます。

ステップ 2 [Basic] で、vHBA テンプレートを作成する [Organization] を選択します。

a) [Name] と [Description] を入力します。

b) [Type] および [Fabric ID] のオプションを選択して、[Max Data Field Size(Bytes)] を入力します。

ステップ 3 [WWN Address Pool] をクリックして、WWN アドレスを選択します。

WWN アドレス プールを割り当てなかった場合は、システムがデフォルトを割り当てます。

ステップ 4 [vSANs] をクリックして、この vHBA テンプレートに使用する vSAN を追加します。

ステップ 5 [Policies] をクリックします。
ポリシーが割り当てられていない場合は、ポリシーとピン グループのぞれぞれをクリックします。 右側のドロップダウンをクリックして、関連するポリシーとピン グループを表示し、この vHBA テンプレートに必要なものを選択します。

ステップ 6 [Create] をクリックします。

vNIC テンプレートの作成または編集

特定の vNIC テンプレートを編集するには、検索バーに「vNIC Template」と入力して、編集する vNIC テンプレートを探します。

（注） Cisco UCS Manager で作成したローカル サービス プロファイルでグローバル vNIC を使用できます。

ステップ 1 タスク バーで、「Create vNIC Template」と入力して、Enter キーを押します。
これにより、[Create vNIC Template] ダイアログボックスが開きます。

ステップ 2 [Basic] で、vNIC テンプレートを作成する [Organization] を選択します。

a) [Name] と [Description] を入力します。

b) [Type]、[Fabric ID]、および [Fabric Failover] に関するオプションを選択し、[MTU] を入力します。

ステップ 3 [MAC Address] をクリックして、MAC アドレスを選択します。
MAC アドレス プールを割り当てなかった場合は、システムがデフォルトを割り当てます。

ステップ 4 [vLANs] をクリックして、この vNIC テンプレートに使用する vLAN を追加します。

ステップ 5 [Policies] をクリックします。
ポリシーが割り当てられていない場合は、それぞれのポリシーをクリックします。右側で、ドロップダウンをクリックして関連するポリシーを表示し、この vNIC テンプレートに必要なものを選択します。

ステップ 6 [Create] をクリックします。

第 9 章

サービス プロファイル

この章は、次の内容で構成されています。

サービス プロファイル

[Service Profiles] ページでは、Cisco UCS Central 内のすべてのサービス プロファイルのリストを表示したり、表示するサービス プロファイルを絞り込んだりすることができます。

サービス プロファイル詳細ビュー

[Service Profile] ページには、サービス プロファイルに関する詳細情報が表示されます。 そこから、次のことができます。

- ログと設定ステータスの表示
- このサービス プロファイルからのサービス プロファイル テンプレートの作成
- サービス プロファイルの削除、複製、または名前変更
- サーバの割り当てまたは割り当て解除
- ホスト インターフェイス配置の設定
- テンプレートへのバインド
- サーバのシャットダウン
- サーバのリセット
- KVM と UCS ドメインの起動

テンプレートからのサービス プロファイルの作成

ステップ 1 タスク バーで、「Create Service Profile from Template」と入力して、Enter キーを押します。
これにより、[Create Service Profile from Template] ダイアログボックスが開きます。

ステップ 2 [Service Profile Template to Instantiate] で、ドロップダウンをクリックして、使用可能なリストからサービス プロファイル テンプレートを選択します。

ステップ 3 [Organization] ドロップダウンで、このサービス プロファイルを作成する組織を選択します。

ステップ 4 [No of Service Profiles] で、このテンプレートを使用して作成するサービス プロファイルの数を指定します。

ステップ 5 [Service Profile Name Prefix] に、プレフィックスを入力します。

テンプレートへのサービス プロファイルのバインド

ステップ 1 [Service Profile] ページで、[Settings] アイコンをクリックします。

ステップ 2 [Bind To Template] をクリックします。
これにより、[Bind Service Profile] ダイアログボックスが開きます。

ステップ 3 [Service Profile Template to Instantiate] で、使用可能なリストからサービス プロファイル テンプレートを選択します。

ステップ 4 [Bind] をクリックします。

サービス プロファイルへのサーバの手動割り当て

ステップ 1 [Service Profile] ページで、[Settings] アイコンをクリックします。

ステップ 2 [Assign Server Manually] をクリックします。
これにより、[Assign Server Manually] ダイアログボックスが開きます。

ステップ 3 [Compatibility Check On Migration Using Manual Assignment] を有効にするかどうかを選択します。

ステップ 4 サービス プロファイルに割り当てるサーバを選択します。

ステップ 5 [Assign Server Manually] をクリックします。

サービス プロファイルまたはサービス プロファイル テンプレート上のインターフェイス配置の設定

ステップ 1 [Service Profile] ページまたは [Service Profile Template] ページで、[Settings] アイコンをクリックします。

ステップ 2 [Configure Interface Placement] をクリックします。
これにより、[Configure Host Interface Placement] ダイアログボックスが開きます。

ステップ 3 [Placement] で、[Manual Interface Placement] を有効にするかどうかを選択します。
[Disabled] を選択した場合は、システムが自動的に PCI の順序に基づいてインターフェイスを割り当てます。

ステップ 4 [Enabled] を選択した場合は、vHBA または vNIC を追加します。

ステップ 5 [Preference] で、仮想スロットごとに [Virtual Slot Selection Preference] を選択します。

（注） このフィールドは、サービス プロファイル テンプレートにのみ表示されます。

次のいずれかになります。

- [all]：設定されたすべての vNIC と vHBA を割り当てることができます。 これはデフォルトです。
- [assigned-only]：vNIC と vHBA を明示的に割り当てる必要があります。
- [exclude-dynamic]：ダイナミック vNIC および vHBA を割り当てることができません。
- [exclude-unassigned]：未割り当ての vNIC および vHBA を割り当てることができません。
- [exclude-usnic]：usNIC vNIC を割り当てることができません。

ステップ 6 [PCI Order] で、上矢印と下矢印をクリックして順序を調整します。

（注） [Manual Interface Placement] が有効になっている場合は、PCI 順序が読み取り専用になります。

ステップ 7 [Configure Host Interface Placement] をクリックします。

サービス プロファイルの障害

Cisco UCS Central は、[Service Profile Fault Logs] ページに、すべての Cisco UCS Central サービス プロファイル障害を収集して表示します。 サービス プロファイル障害を表示するには、[Service Profile] 詳細ページの [Fault Summary] セクションで [Faults] アイコンをクリックします。 [Faults Logs]ページでは、障害のタイプと重大度レベルに関する情報が表示され、システム障害を監視して認識したり、表示する障害を絞り込んだりすることができます。

障害テーブルには、障害ごとに次の情報が表示されます。

- [Code]：障害に関連付けられた ID
- [Timestamp]：障害が発生した日付と時刻
- [Type]：障害の発生元
- [Cause]：障害の原因
- [Affected Object]：この障害の影響を受けるコンポーネント
- [Fault Details]：障害の詳細
- [Severity]：障害の重大度
- [Action]：障害に必要なアクション

収集された情報を管理するには、UCS Central システム ポリシーの設定, （43 ページ）を参照してください。

サービス プロファイル サーバ障害

Cisco UCS Central は、サービス プロファイルに関連付けられたすべてのサーバ障害を収集して表示します。 サーバ障害を表示するには、[Service Profile] 詳細ページの [Server Fault Summary] セクションで [Faults] アイコンをクリックします。 [Faults Logs] ページでは、障害のタイプと重大度レベルに関する情報が表示され、システム障害を監視して認識したり、表示する障害を絞り込んだりすることができます。

障害テーブルには、障害ごとに次の情報が表示されます。

- [Code]：障害に関連付けられた ID
- [Timestamp]：障害が発生した日付と時刻
- [Type]：障害の発生元
- [Cause]：障害の原因
- [Affected Object]：この障害の影響を受けるコンポーネント
- [Fault Details]：障害の詳細
- [Severity]：障害の重大度
- [Action]：障害に必要なアクション

収集された情報を管理するには、UCS Central システム ポリシーの設定, （43 ページ）を参照してください。

サービス プロファイル イベント ログ

選択されたサービス プロファイルのイベント ログが表示されます。 これには次の情報を含めることができます。

- [ID]：障害を引き起こしたイベントに関連付けられた一意の識別子
- [Timestamp]：イベントが発生した日付と時刻
- [Trig. By]：イベントに関連付けられたユーザのタイプ
- [Affected Object]：イベントの影響を受けるコンポーネント

サービス プロファイル監査ログ

選択されたサービス プロファイルの監査ログが表示されます。 これには以下が含まれます。

- アクセスされたリソース。
- イベントが発生した日付と時刻。
- ログ メッセージに関連付けられた固有識別子。
- 監査ログが生成されるアクションをトリガーしたユーザ。 これは、内部セッションの場合と Cisco UCS Central GUI または Cisco UCS Central CLI を使用して変更を加えた外部ユーザの場合があります。
- アクションをトリガーしたソース。
- 影響を受けたコンポーネント。

第 10 章

ポリシー

この章は、次の内容で構成されています。

Cisco UCS Central と Cisco UCS ドメインのポリシー

Cisco UCS Central でグローバル ポリシーを作成して管理し、それらを 1 つ以上の Cisco UCS ドメイン 用のサービス プロファイルまたはサービス プロファイル テンプレートに含めることができます。 グローバル ポリシーを含むサービス プロファイルとサービス プロファイル テンプレートは次のいずれかにすることができます。

- 1 つの Cisco UCS ドメイン内の Cisco UCS Manager によって作成され、管理されているローカル サービス プロファイルまたはサービス プロファイル テンプレート。 ローカル サービス プロファイルは、そのドメイン内のサーバにしか関連付けることができません。 グローバル ポリシーをローカル サービス プロファイルに含めると、Cisco UCS Manager がそのポリシーのローカル読み取り専用コピーを作成します。
- Cisco UCS Central によって作成され、管理されているグローバル サービス プロファイルまたはサービス プロファイル テンプレート。 1 つ以上の登録された Cisco UCS ドメイン内のサーバとグローバル サービス プロファイルを関連付けることができます。

グローバル ポリシーは Cisco UCS Central でしか変更することができません。 この変更は、グローバル ポリシーを含むすべてのサービス プロファイルとサービス プロファイル テンプレートに影響します。 すべてのグローバル ポリシーが Cisco UCS Manager では読み取り専用です。

IPv6 アドレスを使用した 1 つのドメイン グループ内ですべての使用可能なポリシーを設定できます。 これらのポリシーは、Cisco UCS Central GUI の [Operations Management] タブに配置されます。

この機能は、Cisco UCS Central からこれらのポリシーをインポート中に IPv6 アドレスを使用する Cisco UCS Manager を支援します。

Cisco UCS Manager と Cisco UCS Central 間のポリシー解決

Cisco UCS Central で登録する各 Cisco UCS ドメイン では、特定のポリシーおよび設定を管理するアプリケーションを選択できます。 このポリシー解決は、同じ Cisco UCS Central に登録したすべての Cisco UCS ドメイン で同じである必要はありません。

これらのポリシーおよび設定を解決するには、次のオプションを使用します。

- [Local]：ポリシーまたは設定は、Cisco UCS Manager によって決定および管理されます。
- [Global]：ポリシーまたは設定は、Cisco UCS Central によって決定および管理されます。

次のテーブルには、Cisco UCS Manager または Cisco UCS Central のいずれかで管理するように選択できるポリシーと設定のリストを示します。

名前	説明
[Infrastructure & Catalog Firmware]	機能カタログとインフラストラクチャ ファームウェア ポリシーが、ローカルで定義されるかまたは Cisco UCS Central から取得されるかを決定します。
[TimeZone Management]	日付と時刻がローカルまたは Cisco UCS Central のどちらで定義されるかを決定します。
[Communication Services]	HTTP、CIM XML、Telnet、SNMP、Web セッション制限、管理インターフェイス モニタリング ポリシー設定を、ローカルまたは Cisco UCS Central のどちらで定義するかを決定します。
[GlobalFault Policy]	グローバル障害ポリシーがローカルまたは Cisco UCS Central のどちらで定義されるかを決定します。
[User Management]	認証およびネイティブ ドメイン、LDAP、RADIUS、TACACS+、トラストポイント、ロケールおよびユーザ ロールをローカルまたは Cisco UCS Central のどちらで定義するかを決定します。
[DNS Management]	DNS サーバがローカルまたは Cisco UCS Central のどちらで定義されるかを決定します。
[Backup & Export Policies]	Full State バックアップ ポリシーおよび All Configuration エクスポート ポリシーが、ローカルまたは Cisco UCS Central のどちらで定義されるかを決定します。
[Monitoring]	Call Home、Syslog、TFTP Core Exporter 設定が、ローカルまたは Cisco UCS Central のどちらで定義されるかを決定します。
[SEL Policy]	管理対象エンドポイントがローカルまたは Cisco UCS Central のどちらで定義されるかを決定します。

名前	説明
[Power Management]	電源管理がローカルまたは Cisco UCS Central のどちらで定義されるかを決定します。
[Power Supply Unit]	電源モジュールがローカルまたは Cisco UCS Central のどちらで定義されるかを決定します。

ポリシー解決変更の結果

Cisco UCS ドメインを登録するときに、ポリシーをローカルまたはグローバル解決用に設定します。 Cisco UCS ドメインの登録時、あるいは、その登録または設定の変更時の動作は、ドメイングループが割り当てられているかどうかなどの複数の要因によって異なります。

次の表に、ポリシーのタイプごとに予期されるポリシー解決動作について説明します。

ポリシーと設定	Policy Source		Cisco UCS Central への登録時の Cisco UCS Manager の動作		登録変更時の Cisco UCS Manager の動作	
	Cisco UCS Central	Cisco UCS Manager	ドメイン グループの割り当て解除	ドメイン グループの割り当て	ドメイン グループからの割り当て解除	Cisco UCS Central からの登録解除
Call Home	該当なし Cisco UCS Manager のみ	割り当てられたドメイン グループ	ローカル	ローカル/リモート	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される
SNMP コンフィギュレーション	該当なし Cisco UCS Manager のみ	割り当てられたドメイン グループ	ローカル	ローカル/リモート	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される
HTTP	該当なし Cisco UCS Manager のみ	割り当てられたドメイン グループ	ローカル	ローカル/リモート	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される
Telnet	該当なし Cisco UCS Manager のみ	割り当てられたドメイン グループ	ローカル	ローカル/リモート	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される
CIM XML	該当なし Cisco UCS Manager のみ	割り当てられたドメイン グループ	ローカル	ローカル/リモート	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される

ポリシーと設定	Policy Source		Cisco UCS Central への登録時の Cisco UCS Manager の動作		登録変更時の Cisco UCS Manager の動作	
	Cisco UCS Central	Cisco UCS Manager	ドメイン グループの割り当て解除	ドメイン グループの割り当て	ドメイン グループからの割り当て解除	Cisco UCS Central からの登録解除
管理インターフェイス モニタリング ポリシー	該当なし Cisco UCS Manager のみ	割り当てられたドメイン グループ	ローカル	ローカル/リモート	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される
電力割り当てポリシー	該当なし Cisco UCS Manager のみ	割り当てられたドメイン グループ	ローカル	ローカル/リモート	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される
電源ポリシー（別名 PSU ポリシー）	該当なし Cisco UCS Manager のみ	割り当てられたドメイン グループ	ローカル	ローカル/リモート	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される
SEL ポリシー	該当なし Cisco UCS Manager のみ	割り当てられたドメイン グループ	ローカル	ローカル/リモート	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される
認証ドメイン	該当なし Cisco UCS Manager のみ	割り当てられたドメイン グループ	ローカル	ローカル/リモート	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される
LDAP	ドメイン グループ ルート	割り当てられたドメイン グループ	ローカル	ローカル/リモート	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される
LDAP プロバイダー グループとグループ マップ	該当なし Cisco UCS Manager のみ	割り当てられたドメイン グループ	ローカル	ローカル/リモート	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される
プロバイダー グループを含む TACACS	該当なし Cisco UCS Manager のみ	割り当てられたドメイン グループ	ローカル	ローカル/リモート	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される
プロバイダー グループを含む RADIUS	該当なし Cisco UCS Manager のみ	割り当てられたドメイン グループ	ローカル	ローカル/リモート	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される

ポリシーと設定	Policy Source		Cisco UCS Central への登録時の Cisco UCS Manager の動作		登録変更時の Cisco UCS Manager の動作	
	Cisco UCS Central	Cisco UCS Manager	ドメイン グループの割り当て解除	ドメイン グループの割り当て	ドメイン グループからの割り当て解除	Cisco UCS Central からの登録解除
SSH（読み取り専用）	ドメイン グループ ルート	割り当てられたドメイン グループ	ローカル	ローカル/リモート	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される
DNS	ドメイン グループ ルート	割り当てられたドメイン グループ	ローカル	ローカル/リモート	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される
タイム ゾーン	ドメイン グループ ルート	割り当てられたドメイン グループ	ローカル	ローカル/リモート	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される
Web セッション	ドメイン グループ ルート	割り当てられたドメイン グループ	ローカル	ローカル/リモート	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される
Fault	ドメイン グループ ルート	割り当てられたドメイン グループ	ローカル	ローカル/リモート	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される
コア エクスポート	ドメイン グループ ルート	割り当てられたドメイン グループ	ローカル	ローカル/リモート	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される
Syslog	ドメイン グループ ルート	割り当てられたドメイン グループ	ローカル	ローカル/リモート	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される
グローバル Backup/Export ポリシー	ドメイン グループ ルート	割り当てられたドメイン グループ	ローカル	ローカル/リモート	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される
デフォルト認証	ドメイン グループ ルート	割り当てられたドメイン グループ	ローカル	ローカル/リモート	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される
コンソール認証	ドメイン グループ ルート	割り当てられたドメイン グループ	ローカル	ローカルまたはリモートにできる	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される

ポリシーと設定	Policy Source		Cisco UCS Central への登録時の Cisco UCS Manager の動作		登録変更時の Cisco UCS Manager の動作	
	Cisco UCS Central	Cisco UCS Manager	ドメイン グループの割り当て解除	ドメイン グループの割り当て	ドメイン グループからの割り当て解除	Cisco UCS Central からの登録解除
ロール	ドメイン グループ ルート	割り当てられたドメイン グループ	ローカル	ローカル/複合（ローカルに代わるリモート）	リモート ポリシーを削除	ローカル ポリシーに変換される
ロケール - 組織ロケール	ドメイン グループ ルート	割り当てられたドメイン グループ	ローカル	ローカル/複合（ローカルに代わるリモート）	リモート ポリシーを削除	ローカル ポリシーに変換される
トラスト ポイント	ドメイン グループ ルート	割り当てられたドメイン グループ	ローカル	ローカル/複合（ローカルに代わるリモート）	リモート ポリシーを削除	ローカル ポリシーに変換される
ファームウェア ダウンロード ポリシー	ドメイン グループ ルート	該当なし	該当なし	該当なし	該当なし	該当なし
ID ソーキング ポリシー	ドメイン グループ ルート	該当なし	該当なし	該当なし	該当なし	該当なし
ロケール - ドメイン グループ ロケール	ドメイン グループ ルート	該当なし	該当なし	該当なし	該当なし	該当なし
インフラストラクチャ ファームウェア パック	該当なし	割り当てられたドメイン グループ	ローカル	ローカル/リモート（リモートが存在する場合）	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される
カタログ	該当なし	割り当てられたドメイン グループ	ローカル	ローカル/リモート（リモートが存在する場合）	最後に確認されたポリシー状態を維持	ローカル ポリシーに変換される

ポリシーと設定	Policy Source		Cisco UCS Central への登録時の Cisco UCS Manager の動作		登録変更時の Cisco UCS Manager の動作	
	Cisco UCS Central	Cisco UCS Manager	ドメイン グループの割り当て解除	ドメイン グループの割り当て	ドメイン グループからの割り当て解除	Cisco UCS Central からの登録解除
メンテナンス ポリシー スケジュール ホスト ファームウェア パック	該当なし	割り当てられたドメイン グループ	ポリシー解決でのサービス プロファイル変更の結果, （87 ページ） を参照してください。	ポリシー解決でのサービス プロファイル変更の結果, （87 ページ） を参照してください。	リモート ポリシーを削除	ローカル ポリシーに変換される
メンテナンス ポリシー スケジュール ホスト ファームウェア パック	該当なし	割り当てられたドメイン グループ	ポリシー解決でのサービス プロファイル変更の結果, （87 ページ） を参照してください。	ポリシー解決でのサービス プロファイル変更の結果, （87 ページ） を参照してください。	リモート ポリシーを削除	ローカル ポリシーに変換される
メンテナンス ポリシー スケジュール ホスト ファームウェア パック	該当なし	割り当てられたドメイン グループ	ポリシー解決でのサービス プロファイル変更の結果, （87 ページ） を参照してください。	ポリシー解決でのサービス プロファイル変更の結果, （87 ページ） を参照してください。	リモート ポリシーを削除	ローカル ポリシーに変換される

ポリシー解決でのサービス プロファイル変更の結果

ポリシーによっては、そのポリシーを含む 1 つ以上のサービス プロファイルが更新されているかどうかもポリシー解決動作に影響します。

次の表に、このようなポリシーに対して予期されるポリシー解決動作について説明します。

ポリシー	Cisco UCS Central への登録時の Cisco UCS Manager の動作		Cisco UCS Central への登録後に割り当てられたドメイン グループ
	ドメイン グループの割り当て解除/ドメイン グループの割り当て		
	サービス プロファイルが変更されない	サービス プロファイルが変更される	
メンテナンス ポリシー	ローカル	ローカル、ただし、すべての「デフォルト」ポリシーがドメイン グループ割り当て時に更新される	ローカル/リモート（登録後に「デフォルト」に解決された場合）
スケジュール	ローカル	ローカル、ただし、すべての「デフォルト」ポリシーがドメイン グループ割り当て時に更新される	ローカル/リモート（登録後に「デフォルト」に解決された場合）
ホスト ファームウェア パッケージ	ローカル	ローカル、ただし、すべての「デフォルト」ポリシーがドメイン グループ割り当て時に更新される	ローカル/リモート（登録後に「デフォルト」に解決された場合）

ブート ポリシー

ブート ポリシーは、BIOS セットアップ メニューのブート順序をオーバーライドして、以下を決定します。

- ブート デバイスの選択
- サーバのブート元である場所
- ブート デバイスの起動順序

たとえば、ローカル ディスクや CD-ROM（VMedia）などのローカル デバイスから関連するサーバを選択するか、または SAN ブートもしくは LAN（PXE）ブートを選択することができます。

1 つ以上のサービス プロファイルに関連付けることができる名前付きブート ポリシーを作成するか、特定のサービス プロファイルに対するブート ポリシーを作成できます。 ブート ポリシーを有効にするには、ブート ポリシーをサービス プロファイルに含め、このサービス プロファイルをサーバに関連付ける必要があります。 サービス プロファイルにブート ポリシーを含めなかった場合は、UCS ドメインがデフォルト ブート ポリシーを適用します。

（注） ブート ポリシーに対する変更は、そのブート ポリシーを含む最新のサービス プロファイル テンプレートを使用して作成されたすべてのサービス プロファイルに伝播します。 BIOS にブート順序情報を再書き込みするためのサービス プロファイルとサーバとの再アソシエーションは自動的にトリガーされます。

ブート ポリシーの作成または編集

ステップ 1 タスク バーで、「Create Boot Policy」と入力して、Enter キーを押します。
これにより、[Create Boot Policy] ダイアログボックスが開きます。

ステップ 2 ドロップダウン リストから組織を選択してから、ポリシーの一意の名前とオプションの説明を入力します。

ステップ 3 （任意） ブート順序の変更後にこのブート ポリシーを使用するすべてのサーバをリブートする場合は、[Reboot on Boot Order Change] に対して [Enabled] をクリックします。
他社製の VIC アダプタが実装されたサーバに適用されるブート ポリシーの場合、[Reboot on Boot Order Change] が無効になっている場合でも、SAN デバイスが追加、削除、または順序変更され、ブート ポリシーの変更が保存されるたびにサーバがリブートします。

ステップ 4 （任意） [Boot Order] セクションの vNIC、vHBA、または iSCSI vNIC のいずれかがサービス プロファイル内のサーバ設定と一致したときに設定エラーを表示する場合は、[Enforce Interface Name] に対して [Enabled] をクリックします。

ステップ 5 [Boot Mode] で、[Legacy] または [Unified Extensible Firmware Interface (UEFI)] をクリックします。

ステップ 6 [Boot Order] アイコンをクリックして、次の手順を実行します。

a) [Add] ボタンをクリックして、ブート オプションを追加します。
b) ブート オプションに必要なプロパティを更新します。
c) 上矢印と下矢印を使用してブート順序を調整します。

（注） HTML5 GUI で iSCSI ブート用のブート ポリシーを作成した場合は、HTML5 GUI でしかそのブート ポリシーを更新できません。

ステップ 7 [Save] をクリックします。

BIOS ポリシー

BIOS ポリシーは、サーバまたはサーバ グループの BIOS 設定値の指定を自動化します。 ルート組織内のすべてのサーバに対して使用可能なグローバル BIOS ポリシーを作成するか、サブ組織の階層に対してだけ使用可能な BIOS ポリシーを作成できます。

BIOS ポリシーを使用するには、次の手順を実行します。

1. Cisco UCS Central で BIOS ポリシーを作成します。
2. BIOS ポリシーを 1 つ以上のサービス プロファイルに割り当てます。
3. サービス プロファイルをサーバと関連付けます。

サービス プロファイルの関連付け時に、Cisco UCS Central によってサーバ上の BIOS 設定が BIOS ポリシー内の設定と一致するように変更されます。 BIOS ポリシーを作成せず、BIOS ポリシーをサービス プロファイルに割り当てていない場合は、サーバの BIOS 設定にそのサーバ プラットフォームのデフォルトが使用されます。

関連トピック

デフォルトの BIOS 設定, （91 ページ）
基本 BIOS 設定, （92 ページ）
ブート オプションの BIOS 設定, （107 ページ）
コンソール , （111 ページ）
Intel Directed I/O BIOS 設定, （100 ページ）
プロセッサの BIOS 設定, （94 ページ）
RAS メモリの BIOS 設定, （102 ページ）
サーバ管理, （108 ページ）
USB の BIOS 設定, （104 ページ）

BIOS ポリシーの作成または編集

ステップ 1 タスク バーで、「Create BIOS Policy」と入力して、Enter キーを押します。
これにより、[Create BIOS Policy] ダイアログボックスが開きます。

ステップ 2 [Basic] で、[Organization] をクリックして、ブート ポリシーを作成する場所を選択します。

a) [Name] とオプションの [Description] を入力します。
ポリシー名は大文字と小文字が区別されます。

b) （任意） 必要に応じてその他のフィールドに値を入力します。
詳細については、基本 BIOS 設定, （92 ページ）を参照してください。

ステップ 3 [Processor] で、必要に応じてフィールドに値を入力します。
詳細については、プロセッサの BIOS 設定, （94 ページ）を参照してください。

ステップ 4 [I/O] で、必要に応じてフィールドに値を入力します。
詳細については、Intel Directed I/O BIOS 設定, （100 ページ）を参照してください。

ステップ 5 [RAS Memory] で、必要に応じてフィールドに値を入力します。
詳細については、RAS メモリの BIOS 設定, （102 ページ）を参照してください。

ステップ 6 [USB] で、必要に応じてフィールドに値を入力します。
詳細については、USB の BIOS 設定, （104 ページ）を参照してください。

ステップ 7 [PCI] で、必要に応じてフィールドに値を入力します。
詳細については、PCIを参照してください。

ステップ 8 [Boot Options] で、必要に応じてフィールドに値を入力します。
詳細については、ブート オプションの BIOS 設定, （107 ページ）を参照してください。

ステップ 9 [Server Manager] で、必要に応じてフィールドに値を入力します。
詳細については、サーバ管理, （108 ページ）を参照してください。

ステップ 10 [Console] で、必要に応じてフィールドに値を入力します。
詳細については、コンソール , （111 ページ）を参照してください。

ステップ 11 [Create] をクリックします。

デフォルトの BIOS 設定

Cisco UCS Central には、Cisco UCS によってサポートされるサーバのタイプごとに 1 セットずつのデフォルト BIOS 設定が付属しています。 デフォルト BIOS 設定は、ルート組織だけで使用でき、グローバルです。 Cisco UCS でサポートされている各サーバ プラットフォームには、1 セットの BIOS 設定だけを適用できます。 デフォルト BIOS 設定は変更できますが、デフォルト BIOS 設定の追加セットの作成はできません。

デフォルト BIOS 設定の各セットは、サポートされているサーバの特定のタイプに合わせて設計されており、サービス プロファイルに BIOS ポリシーが含まれていない、特定のタイプのすべてのサーバに適用されます。

Cisco UCS 実装にサーバ特定の設定によって満たされない特定の要件があるのでない限り、Cisco UCS ドメインのサーバの各タイプ用に設計されたデフォルト BIOS 設定を使用するよう推奨します。

Cisco UCS Central により、これらのサーバ プラットフォーム固有の BIOS 設定が次のように適用されます。

- サーバに関連付けられたサービス プロファイルには、BIOS ポリシーはインクルードされません。
- BIOS ポリシーには、特定の設定に対するプラットフォーム デフォルトのオプションが設定されます。

Cisco UCS Central によって提供されるデフォルトの BIOS 設定は変更できます。 ただし、デフォルトの BIOS 設定に対する変更は、その特定のタイプまたはプラットフォームのすべてのサーバに適用されます。 特定のサーバの BIOS 設定だけを変更する場合は、BIOS ポリシーを使用することを推奨します。

基本 BIOS 設定

次の表に、BIOS ポリシーまたはデフォルト BIOS 設定を介して実行できるメイン サーバ BIOS 設定の一覧を示します。

名前	説明
Name	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
Description	ポリシーの説明。 ポリシーが使用される場所と条件についての情報を含めることを推奨します。
Owner	次のいずれかになります。 • [Local]：このポリシーは、Cisco UCS ドメイン内のサービス プロファイルとサービス プロファイル テンプレートでのみ使用できます。 • [Pending Global]：このポリシーの制御は、Cisco UCS Centralに移行中です。 移行が完了すると、このポリシーは Cisco UCS Centralに登録されているすべての Cisco UCS ドメインで使用可能になります。 • [Global]：このポリシーは、Cisco UCS Centralで管理されます。 このポリシーを変更する場合は、必ず Cisco UCS Centralを使用して変更してください。
Reboot on BIOS Settings Change	1 つ以上の BIOS 設定を変更した後、サーバをリブートするタイミング。 この設定を有効にした場合、サーバのサービス プロファイルのメンテナンス ポリシーに従ってリブートされます。 たとえば、メンテナンス ポリシーでユーザの確認応答が必要な場合、サーバはリブートされず、ユーザが保留中のアクティビティを確認するまで BIOS の変更は適用されません。 この設定をイネーブルにしない場合、BIOS の変更は、別のサーバ設定変更の結果であれ手動リブートであれ、次回のサーバのリブート時まで適用されません。

名前	説明
Quiet Boot	BIOS が Power On Self-Test（POST）中に表示する内容。次のいずれかになります。 • [disabled]：BIOS はブート中にすべてのメッセージとオプション ROM 情報を表示します。 • [enabled]：BIOS はロゴ画面を表示しますが、ブート中にメッセージやオプション ROM 情報を表示しません。 • [Platform Default][platform-default]：BIOS は、サーバタイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。
Post Error Pause	POST 中にサーバで重大なエラーが発生した場合の処理。次のいずれかになります。 • [disabled]：BIOS は、サーバの起動を試行し続けます。 • [enabled]：POST 中に重大なエラーが発生した場合、BIOS はサーバのブート試行を一時停止し、エラーマネージャを開きます。 • [Platform Default][platform-default]：BIOS は、サーバタイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。
Resume Ac On Power Loss	予期しない電力損失後に電力が復帰したときにサーバがどのように動作するかを決定します。 次のいずれかになります。 • [stay-off]：手動で電源をオンにするまでサーバの電源がオフになります。 • [last-state]：サーバの電源がオンになり、システムが最後の状態を復元しようとします。 • [reset]：サーバの電源がオンになり、自動的にリセットされます。 • [Platform Default][platform-default]：BIOS は、サーバタイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
Front Panel Lockout	前面パネルの電源ボタンとリセット ボタンがサーバによって無視されるかどうかを決定します。 次のいずれかになります。 • [disabled]：前面パネルの電源ボタンとリセットボタンはアクティブであり、サーバに影響を与えるために使用できます。 • [enabled]：電源ボタンとリセット ボタンはロックアウトされます。 サーバをリセットしたり、電源をオンにしたりできるのは、CIMC GUI からだけです。 • [Platform Default][platform-default]：BIOS は、サーバタイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。

プロセッサの BIOS 設定

次の表に、BIOS ポリシーまたはデフォルト BIOS 設定を介して実行できるプロセッサ BIOS 設定の一覧を示します。

名前	説明
Turbo Boost	プロセッサで Intel Turbo Boost Technology を使用するかどうか。このテクノロジーでは、仕様よりも低い電力、温度、または電圧でプロセッサが動作していると、自動的にそのプロセッサの周波数が上がります。 次のいずれかになります。 • [disabled]：プロセッサは周波数を自動的に上昇させません。 • [enabled]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。 • [Platform Default][platform-default]：BIOS は、サーバタイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
Enhanced Intel Speedstep	プロセッサで Enhanced Intel SpeedStep Technology を使用するかどうか。このテクノロジーでは、プロセッサの電圧やコア周波数をシステムが動的に調整できます。 このテクノロジーにより、平均電力消費量と平均熱発生量が減少する可能性があります。 次のいずれかになります。 • [disabled]：プロセッサの電圧または周波数を動的に調整しません。 • [enabled]：プロセッサで Enhanced Intel SpeedStep Technology が使用され、サポートされているすべてのスリープ状態でさらに電力を節約することが可能になります。 • [Platform Default][platform-default]：BIOS は、サーバタイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。
Hyper Threading	プロセッサで Intel Hyper-Threading Technology を使用するかどうか。このテクノロジーでは、マルチスレッド ソフトウェア アプリケーションのスレッドを各プロセッサ内で並列に実行できます。 次のいずれかになります。 • [disabled]：プロセッサでのハイパースレッディングを禁止します。 • [enabled]：プロセッサでの複数スレッドの並列実行を許可します。 • [Platform Default][platform-default]：BIOS は、サーバタイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。

名前	説明
Core Multi Processing	パッケージ内の CPU ごとの論理プロセッサ コアの状態を設定します。 この設定を無効にした場合は、Intel Hyper Threading Technology も無効になります。 次のいずれかになります。 • [all]：すべての論理プロセッサ コアの多重処理を有効にします。 • [1] から [n]：サーバで実行可能な CPU ごとの論理プロセッサ コアの数を指定します。マルチプロセッシングを無効にして、サーバで動作する CPU ごとの論理プロセッサ コアを 1 つだけにするには、[1] を選択します。 • [Platform Default][platform-default]：BIOS は、サーバ タイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。
Execute Disabled Bit	サーバのメモリ領域を分類し、アプリケーション コードを実行可能な場所を指定します。 この分類の結果、悪意のあるワームがバッファにコードを挿入しようとした場合、プロセッサでコードの実行をディセーブルにします。 この設定は、損害、ワームの増殖、および特定クラスの悪意のあるバッファ オーバーフロー攻撃を防止するのに役立ちます。 次のいずれかになります。 • [Disabled]：プロセッサはメモリ領域を分類しません。 • [Enabled]：プロセッサはメモリ領域を分類します。 • [Platform Default][platform-default]：BIOS は、サーバ タイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。

名前	説明
Virtualization Technology (VT)	プロセッサで Intel Virtualization Technology を使用するかどうか。このテクノロジーでは、1 つのプラットフォームで、複数のオペレーティング システムとアプリケーションをそれぞれ独立したパーティション内で実行できます。 次のいずれかになります。 • [disabled]：プロセッサでのバーチャライゼーションを禁止します。 • [enabled]：プロセッサで、複数のオペレーティングシステムをそれぞれ独立したパーティション内で実行できます。 • [Platform Default][platform-default]：BIOS は、サーバタイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。 （注） このオプションを変更した場合は、設定を有効にするためにサーバの電源を再投入する必要があります。
Direct Cache Access	プロセッサで、データを I/O デバイスから直接プロセッサ キャッシュに入れることにより、I/O パフォーマンスを向上させることができます。 この設定はキャッシュミスを減らすのに役立ちます。 次のいずれかになります。 • [Disabled]：I/O デバイスからのデータは、プロセッサのキャッシュに直接配置されません。 • [Enabled]：I/O デバイスからのデータは、プロセッサのキャッシュに直接配置されます。 • [Platform Default][platform-default]：BIOS は、サーバタイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
Processor C State	アイドル期間中にシステムが省電力モードに入ることができるかどうか。 次のいずれかになります。 • [disabled]：システムは、アイドル時にも高パフォーマンス状態を維持します。 • [enabled]：システムは DIMM や CPU などのシステム コンポーネントへの電力を低減できます。 • [Platform Default][platform-default]：BIOS は、サーバタイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。
Processor C1E	C1 に入ってプロセッサが最低周波数に遷移できるようにします。 この設定は、サーバをリブートするまで有効になりません。 次のいずれかになります。 • [disabled]：CPU は C1 状態のとき最大周波数で動作し続けます。 • [enabled]：CPU は最小周波数に移行します。 このオプションでは、C1 状態での最大電力量が削減されます。 • [Platform Default][platform-default]：BIOS は、サーバタイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
Processor C3 Report	プロセッサからオペレーティング システムに C3 レポートを送信するかどうか。 次のいずれかになります。 • [disabled]：プロセッサから C3 レポートを送信しません。 • [acpi-c2]：プロセッサは Advanced Configuration and Power Interface（ACPI）C2 形式を使用して C3 レポートを送信します。 • [acpi-c3]：ACPI C3 フォーマットを使用してプロセッサから C3 レポートを送信します。 • [Platform Default][platform-default]：BIOS は、サーバタイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。 Cisco UCS B440 サーバでは、[BIOS Setup] メニューでこれらのオプションの [enabled] と [disabled] が使用されます。 [acpi-c2] または [acpi-c2] を指定すると、このサーバではそのオプションの BIOS 値に [enabled] が設定されます。
Processor C6 Report	プロセッサからオペレーティング システムに C6 レポートを送信するかどうか。 次のいずれかになります。 • [disabled]：プロセッサから C6 レポートを送信しません。 • [enabled]：プロセッサから C6 レポートを送信します。 • [Platform Default][platform-default]：BIOS は、サーバタイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。
Processor C7 Report	プロセッサからオペレーティング システムに C7 レポートを送信するかどうか。 次のいずれかになります。 • [disabled]：プロセッサから C7 レポートを送信しません。 • [enabled]：プロセッサから C7 レポートを送信します。 • [Platform Default][platform-default]：BIOS は、サーバタイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
CPU Performance	サーバの CPU パフォーマンス プロファイルを設定します。 次のいずれかになります。 • [enterprise]：M3 サーバに対して、すべてのプリフェッチャとデータの再利用がイネーブルになります。 M1 および M2 サーバについては、データの再利用と DCU IP プリフェッチャはイネーブルになり、他のすべてのプリフェッチャはディセーブルになります。 • [high-throughput]：データの再利用と DCU IP プリフェッチャはイネーブルになり、他のすべてのプリフェッチャはディセーブルになります。 • [hpc]：プリフェッチャはすべてイネーブルになり、データの再利用はディセーブルになります。 この設定はハイ パフォーマンス コンピューティングとも呼ばれます。 • [Platform Default][platform-default]：BIOS は、サーバタイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。
Max Variable MTRR Setting	平均修復時間（MTRR）変数の数を選択できます。 次のいずれかになります。 • [auto-max]：BIOS はプロセッサのデフォルト値を使用します。 • [8]：BIOS は MTRR 変数に指定された数を使用します。 • [Platform Default][platform-default]：BIOS は、サーバタイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。

Intel Directed I/O BIOS 設定

次の表に、BIOS ポリシーまたはデフォルト BIOS 設定を介して実行できる Intel Directed I/O BIOS 設定の一覧を示します。

名前	説明
VIrtualization Technology (VT)for Directed IO	Intel Virtualization Technology for Directed I/O（VT-d）をプロセッサで使用するかどうか。 次のいずれかのオプションを選択できます。 • [disabled]：プロセッサでバーチャライゼーションテクノロジーを使用しません。 • [enabled]：プロセッサでバーチャライゼーションテクノロジーを使用します。 • [Platform Default][platform-default]：BIOS は、サーバタイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。 （注） 他の Intel Directed I/O BIOS 設定を変更する場合は、このオプションをイネーブルにする必要があります。
Interrupt Remap	プロセッサで Intel VT-d Interrupt Remapping をサポートするかどうか。 次のいずれかのオプションを選択できます。 • [disabled]：プロセッサでリマッピングをサポートしません。 • [enabled]：プロセッサで VT-d Interrupt Remapping を必要に応じて使用します。 • [Platform Default][platform-default]：BIOS は、サーバタイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。
Coherency Support	プロセッサで Intel VT-d Coherency をサポートするかどうか。 次のいずれかのオプションを選択できます。 • [disabled]：プロセッサでコヒーレンシをサポートしません。 • [enabled]：プロセッサで VT-d Coherency を必要に応じて使用します。 • [Platform Default][platform-default]：BIOS は、サーバタイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
Address Translation Services (ATS) Support	プロセッサで Intel VT-d Address Translation Services（ATS）をサポートするかどうか。 次のいずれかのオプションを選択できます。 • [disabled]：プロセッサで ATS をサポートしません。 • [enabled]：プロセッサで VT-d ATS を必要に応じて使用します。 • [Platform Default][platform-default]：BIOS は、サーバタイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。
Pass Through DMA Support	プロセッサで Intel VT-d Pass-through DMA をサポートするかどうか。 次のいずれかのオプションを選択できます。 • [disabled]：プロセッサでパススルー DMA をサポートしません。 • [enabled]：プロセッサで VT-d Pass-through DMA を必要に応じて使用します。 • [Platform Default][platform-default]：BIOS は、サーバタイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。

RAS メモリの BIOS 設定

次の表に、BIOS ポリシーまたはデフォルト BIOS 設定を介して実行できる RAS メモリの BIOS 設定の一覧を示します。

名前	説明
NUMA	BIOS で NUMA をサポートするかどうか。 次のいずれかになります。 • [disabled]：BIOS で NUMA をサポートしません。 • [enabled]：BIOS は NUMA に対応したオペレーティング システムに必要な ACPI テーブルを含みます。このオプションをイネーブルにした場合は、一部のプラットフォームでシステムのソケット間メモリインターリーブをディセーブルにする必要があります。 • [Platform Default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
LV DDR Mode	低電圧と高周波数のどちらのメモリ動作をシステムで優先するか。 次のいずれかになります。 • [power-saving-mode]：低電圧のメモリ動作が高周波数のメモリ動作よりも優先されます。 このモードでは、電圧を低く維持するために、メモリの周波数が低下する可能性があります。 • [performance-mode]：高周波数の動作が低電圧の動作よりも優先されます。 • [Platform Default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
DRAM Refresh Rate	内部メモリ用の更新間隔レート。 次のいずれかになります。 • 1x • 2x • 3x • 4x • auto • [Platform Default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
Memory RAS Config	サーバに対するメモリの Reliability, Availability, and Serviceability（RAS）の設定方法。 次のいずれかになります。 • [maximum performance]：システムのパフォーマンスが最適化されます。 • [mirroring]：システムのメモリの半分をバックアップとして使用することにより、システムの信頼性が最適化されます。 • [lockstep]：サーバ内の DIMM ペアが、同一のタイプ、サイズ、および構成を持ち、SMI チャネルにまたがって装着されている場合、ロックステップモードをイネーブルにして、メモリ アクセス遅延の最小化およびパフォーマンスの向上を実現できます。B440 サーバでは [lockstep] がデフォルトでイネーブルになっています。 • [Platform Default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

USB の BIOS 設定

次の表に、BIOS ポリシーまたはデフォルト BIOS 設定を介して実行できる USB BIOS 設定の一覧を示します。

名前	説明
Make Device Non Bootable	サーバが USB デバイスからブートできるかどうか。 次のいずれかになります。 • [disabled]：サーバは USB デバイスからブートできます。 • [enabled]：サーバは USB デバイスからブートできません。 • [Platform Default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
USB Front Panel Access Lock	USB 前面パネル ロックは、USB ポートへの前面パネル アクセスをイネーブルまたはディセーブルにするために設定されます。 次のいずれかになります。 • disabled • enabled • [Platform Default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
Legacy USB Support	
USB Idle Power Optimizing Setting	USB EHCI のアイドル時電力消費を減らすために USB システムにアイドル時電力最適化設定を使用するかどうか。 この設定で選択した値によって、パフォーマンスが影響を受けることがあります。 次のいずれかになります。 • [high-performance]：最適なパフォーマンスを電力節約より優先するため、USB システムのアイドル時電力最適化設定はディセーブルにされます。 このオプションを選択すると、パフォーマンスが大幅に向上します。 サイトにサーバの電源制限がない場合はこのオプションを選択することを推奨します。 • [lower-idle-power]：電力節約を最適なパフォーマンスより優先するため、USB システムのアイドル時電力最適化設定はイネーブルにされます。 • [Platform Default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

LOM および PCIe スロットの BIOS 設定

次の表に、BIOS ポリシーまたはデフォルト BIOS 設定を介して実行できる USB BIOS 設定の一覧を示します。

名前	説明
[All Onboard LOM Ports]	すべての LOM ポートがイネーブルであるか、ディセーブルであるか。 次のいずれかになります。 • [Disabled]：すべての LOM ポートがディセーブルです。 • [Enabled]：すべての LOM ポートがイネーブルです。 • [Platform Default][platform-default]：BIOS は、サーバ タイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。
[LOM Port *n* OptionROM] ト	*n* で指定された LOM ポートでオプション ROM を使用できるかどうか。 次のいずれかになります。 • [Disabled]：拡張スロット *n* を使用できません。 • [Enabled]：拡張スロット *n* を使用できます。 • [UEFI-Only]：拡張スロット *n* を UEFI でのみ使用できます。 • [Legacy-Only]：拡張スロット *n* をレガシーでのみ使用できます。 • [Platform Default][platform-default]：BIOS は、サーバ タイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。
[PCIe Slot:SAS OptionROM]	オプション ROM が SAS ポートで使用できるかどうか。 次のいずれかになります。 • [Disabled]：拡張スロットを使用できません。 • [Enabled]：拡張スロットを使用できます。 • [UEFI-Only]：拡張スロットは UEFIでのみ使用できます。 • [Legacy-Only]：拡張スロットはレガシーでのみ使用できます。 • [Platform Default][platform-default]：BIOS は、サーバ タイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[PCIe Slot:*n* Link Speed]	このオプションでは、PCIe スロット *n* に取り付けられたアダプタ カードの最大速度を制限することができます。 次のいずれかになります。 • [gen1]：最大速度が 2.5 GT/s（ギガ転送/秒）になります。 • [gen2]：最大速度が 5 GT/s になります。 • [gen3]：最大速度が 8 GT/s になります。 • [auto]：最高速度は自動的に設定されます。 • [Disabled]：最大速度は制限されません。 • [Platform Default][platform-default]：BIOS は、サーバ タイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。

ブート オプションの BIOS 設定

次の表に、BIOS ポリシーまたはデフォルト BIOS 設定を介して実行できるブート オプション BIOS 設定の一覧を示します。

名前	説明
Boot Option Retry	BIOS でユーザ入力を待機せずに非 EFI ベースのブート オプションを再試行するかどうか。 次のいずれかになります。 • [Disabled]：NON-EFI ベースのブート オプションを再試行する前にユーザ入力を待ちます。 • [Enabled]：ユーザ入力を待たずに NON-EFI ベースのブート オプションを継続的に試行します。 • [Platform Default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
Onboard SCU Storage Support	オンボード ソフトウェア RAID コントローラをサーバに使用できるかどうか。 次のいずれかになります。 • [disabled]：ソフトウェア RAID コントローラを使用できません。 • [enabled]：ソフトウェア RAID コントローラを使用できます。 • [Platform Default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
Intel Entry SAS RAID	Intel SAS Entry RAID モジュールがイネーブルかどうか。次のいずれかになります。 • [disabled]：Intel SAS Entry RAID モジュールはディセーブルです。 • [enabled]：Intel SAS Entry RAID モジュールはイネーブルです。 • [Platform Default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
Intel Entry SAS RAID Module	Intel SAS Entry RAID モジュールがどのように設定されるか。 次のいずれかになります。 • [it-ir-raid]：Intel IT/IR RAID を使用するよう RAID モジュールを設定します。 • [intel-esrtii]：Intel Embedded Server RAID Technology II を使用するよう RAID モジュールを設定します。 • [Platform Default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

サーバ管理

次の表に、BIOS ポリシーまたはデフォルト BIOS 設定を介して実行できるサーバ管理 BIOS 設定の一覧を示します。

名前	説明
Assert NMI on SERR	システムエラー（SERR）の発生時に、BIOSがマスク不能割り込み（NMI）を生成し、エラーをログに記録するかどうか。 次のいずれかになります。 • [Disabled]：BIOSはSERRが発生したときにNMIを生成せず、エラーを記録しません。 • [Enabled]：BIOSはSERRが発生するとNMIを生成し、エラーを記録します。 [Assert NMI on Perr]をイネーブルにするには、この設定をイネーブルにする必要があります。 • [Platform Default]：BIOSは、サーバタイプとベンダーのBIOSデフォルト値に含まれるこの属性の値を使用します。
Assert NMI on PERR	プロセッサバスパリティエラー（PERR）の発生時に、BIOSがマスク不能割り込み（NMI）を生成し、エラーをログに記録するかどうか。 次のいずれかになります。 • [Disabled]：BIOSはPERRが発生したときにNMIを生成せず、エラーを記録しません。 • [Enabled]：BIOSはPERRが発生するとNMIを生成し、エラーを記録します。 この設定を使用するには、[Assert NMI on Serr]をイネーブルにする必要があります。 • [Platform Default]：BIOSは、サーバタイプとベンダーのBIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
OS Boot Watchdog Timer	BIOS が定義済みのタイム アウト値を持つウォッチドッグ タイマーをプログラムするかどうか。 タイマーが切れる前にオペレーティング システムのブートを完了しない場合、CIMC はシステムをリセットし、エラーがログに記録されます。 次のいずれかになります。 • [Disabled]：サーバ ブートにかかる時間を追跡するためのウォッチドッグ タイマーを使用しません。 • [Enabled]：サーバ ブートにかかる時間をウォッチドッグ タイマーで追跡します。 サーバが事前に定義した時間内にブートしない場合、CIMC はシステムをリセットし、エラーを記録します。 • [Platform Default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 この機能には、オペレーティング システムのサポートまたは Intel 管理ソフトウェアが必要です。
OS Boot Watchdog Timer Timeout	BIOS でウォッチドッグ タイマーの設定に使用されるタイムアウト値。 次のいずれかになります。 • [5-minutes]：ウォッチドッグ タイマーは OS ブート開始から 5 分後に期限切れになります。 • [10-minutes]：ウォッチドッグ タイマーは OS ブート開始から 10 分後に期限切れになります。 • [15-minutes]：ウォッチドッグ タイマーは OS ブート開始から 15 分後に期限切れになります。 • [20-minutes]：ウォッチドッグ タイマーは OS ブート開始から 20 分後に期限切れになります。 • [Platform Default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 このオプションは、[OS Boot Watchdog Timer] をイネーブルにした場合にだけ利用できます。

コンソール

名前	説明
Legacy OS Redirect	シリアル ポートでレガシーなオペレーティング システム（DOS など）からのリダイレクションをイネーブルにするかどうか。 次のいずれかになります。 • [disabled]：コンソール リダイレクションがイネーブルになっているシリアル ポートはレガシー オペレーティング システムから非表示になります。 • [enabled]：コンソール リダイレクションがイネーブルになっているシリアル ポートはレガシー オペレーティング システムに表示されます。 • [Platform Default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
Console Redirection	POST および BIOS のブート中に、シリアル ポートをコンソール リダイレクションに使用できるようにします。 BIOS のブートが完了し、オペレーティング システムがサーバを担当すると、コンソール リダイレクションは関連がなくなり、無効になります。 次のいずれかになります。 • [disabled]：POST 中にコンソール リダイレクションは発生しません。 • [serial-port-a]：POST 中のコンソール リダイレクションのためシリアル ポート A をイネーブルにします。 このオプションはブレード サーバおよびラック マウント サーバに対して有効です。 • [serial-port-b]：POST 中のコンソール リダイレクションのためシリアル ポート B をイネーブルにし、サーバ管理タスク実行を許可します。 このオプションは、ラック マウント サーバでのみ有効です。 • [Platform Default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 （注） このオプションをイネーブルにする場合は、POST 中に表示される Quiet Boot のロゴ画面もディセーブルにします。

名前	説明
BAUD Rate	シリアル ポートの伝送速度として使用されるボー レート。 [Console Redirection] をディセーブルにした場合は、このオプションを使用できません。 次のいずれかになります。 • [9600]：ボー レート 9600 が使用されます。 • [19200]：ボー レート 19200 が使用されます。 • [38400]：ボー レート 38400 が使用されます。 • [57600]：ボー レート 57600 が使用されます。 • [115200]：ボー レート 115200 が使用されます。 • [Platform Default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。
Terminal Type	コンソール リダイレクションに使用される文字フォーマットのタイプ。 次のいずれかになります。 • [pc-ansi]：PC-ANSI 端末字体が使用されます。 • [VT100]：サポートされている VT-100 ビデオ端末とその文字セットが使用されます。 • [vt100-plus]：サポートされている vt100-plus ビデオ端末とその文字セットが使用されます。 • [vt-utf8]：UTF-8 文字セットを持つビデオ端末が使用されます。 • [Platform Default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。

名前	説明
Flow Control	フロー制御にハンドシェイク プロトコルを使用するかどうか。 送信要求/クリア ツー センド（RTS/CTS）を使用すると、隠れた端末問題が原因で発生する可能性があるフレーム コリジョンを減らすことができます。 次のいずれかになります。 • [none]：フロー制御は使用されません。 • [rts-cts]：フロー制御に RTS/CTS が使用されます。 • [Platform Default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。

イーサネット アダプタ ポリシー

イーサネットアダプタポリシーは、アダプタのトラフィック処理方法など、アダプタのホスト側の動作を制御します。 たとえば、このようなポリシーを使用して、次のデフォルト設定を変更できます。

- キュー
- 割り込み処理
- パフォーマンス拡張
- RSS ハッシュ
- 2 つのファブリック インターコネクトによるクラスタ構成におけるフェールオーバー

オペレーティング システム固有のアダプタ ポリシー

Cisco UCSには、デフォルトで、イーサネット アダプタ ポリシーのセットが用意されています。これらのポリシーには、サポートされている各サーバオペレーティングシステムにおける推奨設定が含まれています。 オペレーティング システムはこれらのポリシーに影響されます。 通常、ストレージベンダーはデフォルト以外のアダプタ設定を要求します。ベンダーが提供しているサポート リストで必須設定の詳細を確認できます。

（注） 該当するオペレーティング システムには、これらのポリシーの値を使用することを推奨します。 シスコのテクニカル サポートで指示されない限り、デフォルトのポリシーの値は変更しないでください。

デフォルトの Windows アダプタ ポリシーを使用するのではなく、Windows オペレーティング システム用のイーサネット アダプタ ポリシーを作成する場合は、次の式を使用して Windows で動作する値を計算する必要があります。

完了キュー = 送信キュー + 受信キュー
割り込み回数 = (完了キュー + 2) 以上である 2 のべき乗の最小値

たとえば、送信キューが 1 で受信キューが 8 の場合、

完了キュー = 1 + 8 = 9

割り込み回数 = (9 + 2) 以上の 2 のべき乗の最小値 = 16

イーサネット アダプタ ポリシーの作成と編集

ステップ 1 タスク バーで、「Create Ethernet Adapter Policy」と入力して、Enter キーを押します。
これにより、[Create Ethernet Adapter Policy] ダイアログボックスが開きます。

ステップ 2 [Basic] で、[Organization] ドロップダウン リストから、イーサネット アダプタ ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。

ステップ 4 [Resources] で、次の手順を実行します。

a) [Transmit Queues] で、割り当てる送信キュー リソースの数を入力します。
b) [Transmit Queue Ring Size] に、送信キュー内の記述子の数を入力します。
c) [Receive Queues] に、割り当てる受信キュー リソースの数を入力します。
d) [Receive Queues Ring Size] で、受信キュー内の記述子の数を入力します。
e) [Completion Queues] で、割り当てる完了キュー リソースの数を入力します。 一般的に、割り当てる完了キュー リソースの数は、送信キュー リソースの数と受信キュー リソースの数の合計と一致する必要があります。
f) [Interrupts] に、割り当てる割り込みリソースの数を入力します。 通常、この値は、完了キュー リソースの数と同じにします。

ステップ 5 [Settings] で、次の手順を実行します。

a) [Transmit Checksum Offloading]、[Receive Checksum Offloading]、[TCP Segmentation Offloading]、および [Large TCP Receive Offloading] を有効にするかどうかを選択します。
b) [Interrupt Mode] を選択します。
c) [Interrupt Timer] 値をマイクロ秒単位で入力します。
d) [Interrupt Coalescing Type] を選択します。

e) [Failback Timeout] を秒単位で入力します。

ステップ 6 [Create] をクリックします。

IPMI アクセス プロファイル

IPMI アクセス プロファイル ポリシーを使用すれば、IP アドレスを使用して IPMI コマンドを直接サーバに送信できるどうかを指定できます。 たとえば、Cisco IMC からセンサー データを取得するためのコマンドを送信することができます。 このポリシーは、サーバでローカルに認証可能なユーザ名とパスワードを含むIPMIアクセス、およびこのアクセスが読み取り専用か、読み取りと書き込みであるかを定義します。

このポリシーはサービスプロファイルに組み込む必要があります。また。このサービスプロファイルを有効にするには、サーバに関連付ける必要があります。

IPMI アクセス プロファイルの作成と編集

IPMI アクセス プロファイルには IPMI ユーザが必要です。 IPMI ユーザは、IPMI アクセス プロファイルの作成時に作成することも、既存の IPMI アクセス プロファイルに追加することもできます。

IPMI アクセス プロファイル ポリシーのパラメータを変更するには、[All policies] ページでポリシーを選択してから、[Edit] アイコンをクリックします。

ステップ 1 タスク バーで、「Create IPMI Access Profile Policy」と入力して、Enter キーを押します。
これにより、[Create IPMI Access Profile Policy] ダイアログボックスが開きます。

ステップ 2 [Basic] で、[Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
ポリシー名は大文字と小文字が区別されます。

ステップ 4 （任意） [IPMI Users] で、IPMI ユーザ名を選択して、パスワードを入力し、パスワードを確認します。

ステップ 5 読み取り専用と管理用のどちらの [Serial over LAN Access] を許可するかを選択します。

ステップ 6 [Create] をクリックします。

次の作業

サービス プロファイルまたはサービス プロファイル テンプレートに IPMI プロファイルを含めます。

Serial over LAN ポリシー

Srial over LAN ポリシーは、ポリシーを使用するサービス プロファイルに関連付けられたすべてのサーバに対する Serial over LAN 接続を設定します。 デフォルトでは、Serial over LAN 接続はディセーブルにされています。

Serial over LAN ポリシーを実装する場合、IPMI プロファイルを作成することも推奨します。

このポリシーはサービスプロファイルに組み込む必要があります。また。このサービスプロファイルを有効にするには、サーバに関連付ける必要があります。

Serial over LAN ポリシーの作成と編集

ステップ 1 タスク バーで、「Create Serial Over LAN (SOL) Policy」と入力して、Enter キーを押します。
これにより、[Create Serial Over LAN (SOL) Policy] ダイアログボックスが開きます。

ステップ 2 [Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 ポリシーの [Name] とオプションの [Description] を入力します。

ステップ 4 [Baud Rate] の値を選択します。

ステップ 5 [Enable] をクリックして、Serial over LAN 接続を許可します。

ステップ 6 [Create] をクリックします。

Serial over LAN ポリシーの削除

はじめる前に

ステップ 1 [show search tables] バーで、[Policies] をクリックします。
該当する組織名に達するまでルート ノードを展開することによって、[Show Org Navigation] バーから組織またはサブ組織レベルのポリシーを表示できます。 **ルート組織**ページで、[Go to All Policies Table] をクリックします。

これにより、[All Policies] ページが開きます。

ステップ 2 削除するポリシーを検索します。
次のいずれかの方法でポリシーを検索できます。

- ポリシーのリストを参照します。
- [Search] アイコンをクリックして、ポリシー名を入力します。
- [Filter] 列から [Serial over LAN] を選択します。

ステップ 3 [Org] 列で、ポリシーをクリックします。
これにより、選択された [SOL policy] ページが開きます。

ステップ 4 [SOL policy] ページで、[Delete] アイコンをクリックします。
ポリシーの削除の確認を促すダイアログボックスが表示されます。

ステップ 5 [Delete] をクリックします。

次の作業

ダイナミック vNIC 接続ポリシー

ダイナミック vNIC 接続ポリシーは、VM とダイナミック vNIC の間の接続を設定する方式を決定します。 VM がインストール済みでダイナミック vNIC が設定された VIC アダプタを使用しているサーバを含む Cisco UCS ドメインには、このポリシーが必要です。

各ダイナミック vNIC 接続ポリシーには、イーサネット アダプタ ポリシーが含まれており、ポリシーを含むサービス プロファイルに関連付けられた任意のサーバに対して設定できる vNIC の数を指定します。

（注） サーバの移行：

- ダイナミック vNIC または別の移行ツールを使用して設定されたサーバを移行する場合は、vNIC で使用されるダイナミック インターフェイスで障害が発生して、Cisco UCS Central からその障害が通知されます。
- サーバが復旧すると、Cisco UCS Central はサーバに新しいダイナミック vNIC を割り当てます。 ダイナミック vNIC 上のトラフィックを監視している場合、監視元を再設定する必要があります。

ダイナミック vNIC 接続ポリシーの作成または編集

ステップ 1 タスク バーで、「Create Dynamic vNIC Connection Policy」と入力して、Enter キーを押します。
これにより、[Create Dynamic vNIC Connection Policy] ダイアログボックスが開きます。

ステップ 2 [Organization] をクリックして、ダイナミック vNIC 接続ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
ポリシー名は大文字と小文字が区別されます。

ステップ 4 作成するダイナミック vNICS の数を入力します。

ステップ 5 使用する保護モードを選択します。

ステップ 6 このポリシーに関連付けるアダプタ プロファイルを選択します。
[Ethernet Adapter] ドロップダウン リストに含めるプロファイルがすでに存在する必要があります。

ステップ 7 [Create] をクリックします。

ファイバ チャネル アダプタ ポリシー

ファイバ チャネル アダプタ ポリシーは、アダプタのトラフィック処理方法など、ホスト側のアダプタの動作を制御します。 たとえば、このようなポリシーを使用して、次のデフォルト設定を変更できます。

- キュー
- 割り込み処理
- パフォーマンス拡張
- RSS ハッシュ
- 2 つのファブリック インターコネクトによるクラスタ構成におけるフェールオーバー

（注） ファイバ チャネル アダプタ ポリシーの場合は、Cisco UCS Central で表示される値が QLogic SANsurfer などのアプリケーションで表示される値と一致しない場合があります。 たとえば、次の値は、SANsurfer と Cisco UCS Central で一致しない可能性があります。

- ターゲットごとの最大 LUN：SANsurfer の最大 LUN は 256 であり、この数値を超える値は表示されません。 Cisco UCS Central でサポートされている最大 LUN 数はこれよりも大きくなっています。
- リンク ダウン タイムアウト：SANsurfer では、リンク ダウンのタイムアウトしきい値を秒単位で設定します。 Cisco UCS Central では、この値をミリ秒で設定します。 そのため、Cisco UCS Central で 5500 ミリ秒の値は、SANsurfer では 5 秒として表示されます。
- 最大データ フィールド サイズ：SANsurfer で許可される値は 512、1024、および 2048 です。 Cisco UCS Central では、任意のサイズの値を設定できます。 したがって、Cisco UCS Central で 900 と設定された値は、SANsurfer では 512 として表示されます。

オペレーティング システム固有のアダプタ ポリシー

Cisco UCSには、デフォルトで、ファイバ チャネル アダプタ ポリシーのセットが用意されています。 これらのポリシーには、サポートされている各サーバ オペレーティング システムにおける

推奨設定が含まれています。 オペレーティング システムはこれらのポリシーに影響されます。通常、ストレージベンダーはデフォルト以外のアダプタ設定を要求します。ベンダーが提供しているサポート リストで必須設定の詳細を確認できます。

（注） 該当するオペレーティング システムには、これらのポリシーの値を使用することを推奨します。 シスコのテクニカル サポートで指示されない限り、デフォルトのポリシーの値は変更しないでください。

ファイバ チャネル アダプタ ポリシーの作成または編集

ステップ 1 タスク バーで、「Create Fibre Channel Adapter Policy」と入力して、Enter キーを押します。
これにより、[Create Fibre Channel Adapter Policy] ダイアログボックスが開きます。

ステップ 2 [Basic] で、[Organization] をクリックして、このポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
ポリシー名は大文字と小文字が区別されます。

ステップ 4 [Resources] で、必要に応じてフィールドに値を入力します。

ステップ 5 [Settings] で、必要に応じてフィールドに値を入力します。

ステップ 6 [Create] をクリックします。

ホスト ファームウェア パッケージ ポリシー

ホスト ファームウェア パッケージ ポリシーを使用すれば、ホスト ファームウェア パッケージ（ホスト ファームウェア パックとも呼ばれる）を構成するファームウェア バージョンのセットを指定することができます。

ホスト ファームウェア パッケージ ポリシーの作成または編集

ステップ 1 タスク バーで、「Create Host Firmware Package Policy」と入力して、Enter キーを押します。
これにより、[Create Host Firmware Package Policy] ダイアログボックスが開きます。

ステップ 2 [Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
ポリシー名は大文字と小文字が区別されます。

ステップ 4 環境の要件に応じて、[Blade Version] 、[Rack Version] 、または [Modular Version] を選択します。

ステップ 5 [Create] をクリックします。

ホスト インターフェイス配置ポリシー

ホストインターフェイス配置ポリシーを使用すれば、vNIC と vHBA のユーザ指定仮想ネットワーク インターフェイス接続（vCon）の配置を指定することができます。

ホストインターフェイス配置ポリシーを作成するには、ホストインターフェイス配置ポリシーの作成または編集, （120 ページ）を参照してください。 既存のポリシーの詳細が、[Host Interface Placement Policy] ページに表示されます。

ホスト インターフェイス配置ポリシーの作成または編集

ステップ 1 タスク バーで、「Create Host Interface Placement Policy」と入力して、Enter キーを押します。
これにより、[Create Host Interface Placement Policy] ダイアログボックスが開きます。

ステップ 2 [Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
ポリシー名は大文字と小文字が区別されます。

ステップ 4 [Virtual Slot Mapping Scheme] を選択します。
次のいずれかになります。

- [Linear Ordered]：仮想スロットが順番に割り当てられます。
- [Round Robin]：仮想スロットが順次割り当てられます。

ステップ 5 仮想スロットごとに [Virtual Slot Selection Preference] を選択します。
次のいずれかになります。

- [all]：設定されたすべての vNIC と vHBA を割り当てることができます。 これはデフォルトです。
- [assigned-only]：vNIC と vHBA を明示的に割り当てる必要があります。
- [exclude-dynamic]：ダイナミック vNIC および vHBA を割り当てることができません。
- [exclude-unassigned]：未割り当ての vNIC および vHBA を割り当てることができません。
- [exclude-usnic]：usNIC vNIC を割り当てることができません。

ステップ 6 [Create] をクリックします。

iSCSI アダプタ ポリシー

iSCSI アダプタ ポリシーの作成または編集

ステップ 1 タスク バーで、「Create iSCSI Adapter Policy」と入力して、Enter キーを押します。
これにより、[Create iSCSI Adapter Policy] ダイアログボックスが開きます。

ステップ 2 [Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
大文字と小文字が区別されます。

ステップ 4 [Connection Timeout]、[LUN Busy Retry Count]、および [DHCP Timeout] の値を入力します。

ステップ 5 [TCP Timestamp]、[HBA Mode]、および [Boot To Target] を有効にするかどうかを選択します。

ステップ 6 [Create] をクリックします。

iSCSI 認証プロファイルの作成または編集

ステップ 1 タスク バーで、「Create iSCSI Authentication Profile」と入力して、Enter キーを押します。
これにより、[Create iSCSI Authentication Profile] ダイアログボックスが開きます。

ステップ 2 [Basic] で、[Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
大文字と小文字が区別されます。

ステップ 4 [User ID] を入力します。

ステップ 5 パスワードを入力して確認します。

ステップ 6 [Create] をクリックします。

LAN 接続ポリシー

LAN 接続ポリシーは、ネットワークのサーバと LAN の間の接続およびネットワーク通信リソースを決定します。 このポリシーは、プールを使用して MAC アドレスをサーバに割り当て、サーバがネットワークとの通信に使用する vNIC を識別します。

（注） また、このポリシーは、サービス プロファイルとサービス プロファイル テンプレートに含まれており、複数のサーバの設定に使用できます。 そのため、接続ポリシー内で静的な ID を使用することは推奨されません。

LAN 接続ポリシーの作成または編集

ステップ 1 タスク バーで、「Create LAN Connectivity Policy」と入力して、Enter キーを押します。
これにより、[Create LAN Connectivity Policy] ダイアログボックスが開きます。

ステップ 2 [Basic] で、[Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
大文字と小文字が区別されます。

ステップ 4 [vNICs] に、「vNIC」と入力して、適切なプロパティ値を入力します。

ステップ 5 [iSCSI vNICs] に、「iSCSI vNIC」と入力して、適切なプロパティ値を入力します。
（注） HTML5 GUI で LAN 接続ポリシーを作成する場合は、ポリシー内の iSCSI vNICS に対して設定する iSCSI vNIC パラメータを HTML5 GUI でしか更新できません。

ステップ 6 [Create] をクリックします。

ローカル ディスク ポリシー

このポリシーは、ローカル ドライブのオンボード RAID コントローラを通じて、サーバ上にインストールされているオプションの SAS ローカル ドライブを設定します。 このポリシーでは、ローカルディスク設定ポリシーをインクルードしているサービスプロファイルに関連付けられたすべてのサーバに対してローカル ディスク モードを設定できます。

ローカル ディスク モードには次のものがあります。

- 任意構成
- ローカル ストレージなし
- RAID なし
- RAID 1 ミラー
- RAID 10 ミラー & ストライプ
- RAID 0 ストライプ
- RAID 6 ストライプ化デュアルパリティ

- RAID 60 ストライプ デュアル パリティ ストライプ
- RAID 5 ストライプ パリティ
- RAID 50 ストライプ パリティ ストライプ

ローカル ディスク ポリシーの作成または編集

ステップ 1 タスク バーで、「Create Local Disk Policy」と入力して、Enter キーを押します。
これにより、[Create Local Disk Policy] ダイアログボックスが開きます。

ステップ 2 [Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
大文字と小文字が区別されます。

ステップ 4 [Mode] で、ローカル ディスクの設定モードを選択します。

ステップ 5 [Configuration Protection]、[FlexFlash]、および [FlexFlash RAID Reporting] を有効にするか、無効にするかを選択します。

ステップ 6 [Create] をクリックします。

メンテナンス ポリシー

登録されたドメイン内のサーバに関連付けられたサービス プロファイルを変更したら、サーバをリブートする必要があります。 メンテナンス ポリシーによって Cisco UCS Central がリブート要求にどのように対処するかが決定されます。

メンテナンスポリシーを作成して、リブート要件を指定することによって、サービスプロファイルを変更せずに自動的にサーバがリブートされないことを確認できます。 メンテナンスポリシーに関する次のオプションのいずれかを指定できます。

- [Immediately]：サービス プロファイルを変更すると、その変更が即座に適用されます。
- [User Acknowledgment]：管理者特権を持っているユーザがシステム内の変更を承認後に変更が適用されます。
- [Schedule]：スケジュール内で指定された日付と時刻に基づいて変更が適用されます。

スケジュールを指定した場合は、メンテナンス ポリシーを作成すると、スケジュールによって最初の利用可能なメンテナンス時間中に変更が適用されます。

（注） メンテナンス ポリシーでは、関連付けられたサービス プロファイルに設定変更が加えられた場合に、サーバの即時リブートは回避できますが、 次のアクションの即時実行は回避されません。

- 関連付けられたサービス プロファイルのシステムからの削除
- サーバ プロファイルのサーバからの関連付けの解除
- サービス ポリシーを使用しないファームウェア アップグレードの直接インストール
- サーバのリセット

メンテナンス ポリシーの作成または編集

ステップ 1 タスク バーで、「Create Maintenance Policy」と入力して、Enter キーを押します。
これにより、[Create Maintenance Policy] ダイアログボックスが開きます。

ステップ 2 [Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
大文字と小文字が区別されます。

ステップ 4 リブートが必要な変更を適用するタイミングを選択します。
次のいずれかになります。

- [User Acknowledgement]：設定の変更をユーザが承認する必要があり、リブートを確認する必要があります。
- [Schedule]：設定の変更が選択されたスケジュールに基づいて適用されます。 新しいスケジュールを値のリストに追加するには、スケジュールの作成または編集, （125 ページ）を参照してください。
- [Save]：設定の変更が保存直後に適用され、リブートが実行されます。

ステップ 5 [Create] をクリックします。

スケジュールの作成または編集

（注） 繰り返し実行か、ワンタイム実行かに関係なく、単純なスケジュールには、ユーザの承認を必要とするオプションはありません。 ユーザの承認が必要な場合は、高度なスケジュールを選択する必要があります。

ステップ 1 タスク バーで、「Create Schedule」と入力して、Enter キーを押します。
これにより、[Create Schedule] ダイアログボックスが開きます。

ステップ 2 [Basic] で、[Name] とオプションの [Description] を入力します。

ステップ 3 スケジュールを [Recurring]、[One Time]、または [Advanced] のどれにするのかを選択します。
[Advanced] の場合は、ユーザの承認が必要かどうかを選択します。

ステップ 4 [Schedule] で、次の手順を実行します。

a) [Recurring] スケジュールの場合は、開始日、頻度、時刻、およびその他のプロパティを選択します。
b) [One Time] スケジュールの場合は、開始日、時刻、およびその他のプロパティを選択します。
c) [Advanced] スケジュールの場合は、スケジュールの名前を入力して、ワンタイム スケジュールを使用するのか、繰り返しスケジュールを使用するのかを選択し、その他のプロパティの値を選択します。

ステップ 5 [Create] をクリックします。

ネットワーク制御ポリシー

このポリシーは Cisco UCS ドメインのネットワーク制御を設定するもので、次の設定も含まれます。

- Cisco Discovery Protocol（CDP）の有効化/無効化
- エンドホスト モードで使用できるアップリンク ポートが存在しない場合の、仮想インターフェイス（VIF）の動作方法
- 関連付けられているボーダー ポートの障害時に、リモート イーサネット インターフェイス、vEthernet インターフェイス、または vFibre チャネル インターフェイスで Cisco UCS Central が実行するアクション
- ファブリック インターコネクトへのパケット送信時に、異なる MAC アドレスをサーバが使用できるかどうか
- MAC 登録を VNIC ごとに実行するか、またはすべての VLAN に対して実行するか

[アップリンクのアクションに失敗しました] プロパティ

デフォルトでは、ネットワーク制御ポリシー内の [アップリンクのアクションに失敗しました] プロパティは、リンクダウンの値を使用して設定されます。 Cisco UCS M81KR 仮想インターフェイス カードなどのアダプタの場合、このデフォルトの動作では、関連付けられたボーダ ポートに障害が発生した場合に、Cisco UCS Central に対して vEthernet または vFibre チャネル インターフェイスをダウンさせるように指示します。 Cisco UCS CNA M72KR-Q や Cisco UCS CNA M72KR-E などの、イーサネットと FCoE トラフィックの両方をサポートする VM-FEX 非対応の統合型ネットワーク アダプタを使用する Cisco UCS システムの場合、このデフォルトの動作では、関連付けられたボーダ ポートに障害が発生した場合に、Cisco UCS Central に対してリモート イーサネット インターフェイスをダウンさせるように指示します。 このシナリオでは、リモート イーサネット インターフェイスにバインドされている vFibre チャネル インターフェイスもダウンします。

（注） このセクションに記載されている VM-FEX 非対応の統合型ネットワーク アダプタのタイプが実装に含まれ、そのアダプタがイーサネットと FCoE の両方のトラフィックを処理することが予想される場合は、警告の値を使用して [アップリンクのアクションに失敗しました] プロパティを設定することをお勧めします。 ただし、この設定にすると、ボーダ ポートがダウンした場合に、イーサネット チーミング ドライバでリンク障害を検出できなくなる場合があります。

MAC 登録モード

MAC アドレスは、ネイティブ VLAN でのみデフォルトでインストールされます。これにより、ほとんどの実装で VLAN ポート数が最大になります。

（注） トランキング ドライバがホスト上で実行され、インターフェイスがプロミスキャス モードになっている場合、Mac 登録モードをすべての VLAN に設定することをお勧めします。

ネットワーク制御ポリシーの作成または編集

ステップ 1 タスク バーで、「Create Network Control Policy」と入力して、Enter キーを押します。
これにより、[Create Network Control Policy] ダイアログボックスが開きます。

ステップ 2 [Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
大文字と小文字が区別されます。

ステップ 4 [Cisco Discovery Protocol (CDP)] を有効にするかどうかを選択します。

ステップ 5 [Action on Uplink Failure] 、[MAC Address Registration] 、および [MAC Address Forging] の値を選択します。

ステップ 6 [Create] をクリックします。

電源制御ポリシー

Cisco UCS Central で電源制御ポリシーを作成してそれをサービス プロファイルに含めることによって、登録された Cisco UCS ドメイン内のブレード サーバに対する電力割り当て制御をシステムで管理させることができます。

Cisco UCS は、ブレード タイプや構成と一緒に電力制御ポリシー内の優先順位設定を使用して、シャーシ内のブレードごとの初期電力割り当てを計算します。

通常の動作中、シャーシ内のアクティブなブレードは、同じシャーシ内のアイドル ブレードから電力を借りることができます。 すべてのブレードがアクティブで、電力制限に到達すると、高優先順位の電力制御ポリシーのサービス プロファイルが、優先順位の低い電力制御ポリシーのサービス プロファイルより優先されます。 優先順位は 1 ～ 10 の段階にランク付けされ、1 が優先順位最高、10 が優先順位最低を表します。 デフォルトのプライオリティは 5 です。

ミッション クリティカル アプリケーションには、no-cap という特殊な優先順位も使用できます。優先順位を no-cap に設定すると、Cisco UCS が特定のサーバの未使用の電力を利用できなくなります。 この設定により、サーバにはそのサーバ タイプに可能な電力の最大容量が割り当てられます。

電源制御ポリシーの作成または編集

ステップ 1 タスク バーで、「Create Power Control Policy」と入力して、Enter キーを押します。
これにより、[Create Power Control Policy] ダイアログボックスが開きます。

ステップ 2 [Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
大文字と小文字が区別されます。

ステップ 4 [Power Capping] を有効にするかどうかを選択します。

ステップ 5 [Enabled] を選択した場合は、スライダを使用して [Power Group Priority] を選択します。
優先順位は 1 ～ 10 の段階にランク付けされ、1 が優先順位最高、10 が優先順位最低を表します。 デフォルトのプライオリティは 5 です。

ステップ 6 [Create] をクリックします。

Quality Of Service ポリシー

Quality Of Service（QoS）ポリシーは、vNIC または vHBA に向けた発信トラフィックにシステム クラスを割り当てます。 このシステム クラスにより、このトラフィックに対する Quality Of Service が決定されます。 一部のアダプタでは、発信トラフィックでバーストやレートなど追加の制御を指定することもできます。

vNIC ポリシー、または vHBA ポリシーに QoS ポリシーをインクルードし、その後、このポリシーをサービス プロファイルにインクルードして、vNIC または vHBA を設定する必要があります。

Quality of Service ポリシーの作成または編集

ステップ 1 タスク バーで、「Create Quality of Service (QOS) Policy」と入力して、Enter キーを押します。
これにより、[Create Quality of Service (QOS) Policy] ダイアログボックスが開きます。

ステップ 2 [Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
大文字と小文字が区別されます。

- [Egress] 領域で、[Priority] を選択して、[Burst(Bytes)] と [Rate(Kbps)] を入力し、[Host Control] を選択します。

ステップ 4 [Egress Priority] を選択します。

ステップ 5 [Host Control Class of Service (CoS)] を有効にするかどうかを選択します。

ステップ 6 [Egress Burst Size] を入力して、出力平均トラフィック レートを選択します。

ステップ 7 [Create] をクリックします。

SAN 接続ポリシー

SAN 接続ポリシーは、ネットワーク上のサーバと SAN の間の接続およびネットワーク通信リソースを決定します。 このポリシーは、プールを使用して WWN および WWPN をサーバに割り当て、サーバがネットワークと通信するために使用する vHBA を識別します。

（注） また、このポリシーは、サービス プロファイルとサービス プロファイル テンプレートに含まれており、複数のサーバの設定に使用できます。 そのため、接続ポリシー内で静的な ID を使用することは推奨されません。

SAN 接続ポリシーの作成または編集

ステップ 1 タスク バーで、「Create SAN Connectivity Policy」と入力して、Enter キーを押します。
これにより、[Create SAN Connectivity Policy] ダイアログボックスが開きます。

ステップ 2 [Basic] で、[Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
大文字と小文字が区別されます。

ステップ 4 [Identifiers] で、WWNN プールを選択します。
詳細については、WWN プールの作成と編集, （142 ページ）を参照してください。

ステップ 5 [vHBAs] で、1 つ以上の vHBA を作成して、プロパティを選択します。
vHBA を手動で作成することも、vHBA テンプレートを使用することもできます。

ステップ 6 [Create] をクリックします。

スクラブ ポリシー

Cisco UCS Central では、検出プロセス中、サーバが再認識された場合、またはサーバがサービス プロファイルとの関連付けを解除された場合に、サーバ上のローカル データと BIOS 設定がどうなるかを決定するスクラブ ポリシーを作成できます。

（注） ローカル ディスク スクラブ ポリシーは、Cisco UCS Manager によって管理されるハード ドライブにのみ適用され、USB ドライブなど他のデバイスには適用されません。

スクラブ ポリシーの設定によっては、そのようなときに次の処理が行われます。

ディスク スクラブ

ローカル ドライブのデータに対しては、アソシエーションが解除されるときに、次のいずれかが発生します。

- イネーブルの場合、ローカル ドライブ上のすべてのデータが破棄されます。
- ディセーブルの場合、ローカル ドライブ上のすべてのデータが保持されます（ローカル ストレージ設定を含む）。

BIOS 設定スクラブ

BIOS 設定に対しては、スクラブ ポリシーを含むサービス プロファイルがサーバからアソシエーション解除されるときに、次のいずれかが発生します。

- イネーブルの場合、サーバのすべての BIOS 設定が消去され、そのサーバ タイプとベンダーに合わせた BIOS のデフォルトにリセットされます。
- ディセーブルの場合、サーバの既存の BIOS 設定が保持されます。

FlexFlash スクラブ

FlexFlash スクラブにより、新規またはデグレード SD カードの組み合わせ、FlexFlash メタデータの設定エラーの解決、およびパーティションが 4 つの旧式 SD カードから単一パーティション SD カードへの移行が可能になります。 SD カードに対しては、スクラブ ポリシーを含むサービス プロファイルがサーバからアソシエーション解除されるとき、またはサーバが再認識されるときに、次のいずれかが発生します。

- イネーブルの場合、SD カードの HV パーティションは PNUOS フォーマット ユーティリティによりフォーマットされます。 SD カードが 2 つある場合、そのカードは RAID-1 ペアされており、両方のカードの HV パーティションは有効とマークされます。 スロット 1 のカードはプライマリとマークされ、スロット 2 のカードはセカンダリとしてマークされます。
- ディセーブルの場合、既存の SD カード設定が保持されます。

（注）
- FlexFlash スクラブを行うと SD カードの HV パーティションが消去されるため、FlexFlash スクラブを実行する前に推奨されるホスト オペレーティング システム ユーティリティを使用して SD カードの完全バックアップを行うことを推奨します。
- サービス プロファイルのメタデータ設定不具合を解決するには、FlexFlash スクラブを実行する前にローカル ディスク設定ポリシーの FlexFlash をディセーブルにし、サーバが再認識された後に FlexFlash をイネーブルにする必要があります。
- ペアリングが完了、またはメタデータ不具合が解決したらすぐにスクラブ ポリシーをディセーブルにします。

スクラブ ポリシーの作成または編集

ステップ 1 タスク バーで、「Create Scrub Policy」と入力して、Enter キーを押します。
これにより、[Create Scrub Policy] ダイアログボックスが開きます。

ステップ 2 [Basic] で、[Organization] をクリックして、ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
大文字と小文字が区別されます。

ステップ 4 有効にするスクラブ ポリシーを選択します。

ステップ 5 [Create] をクリックします。

vMedia ポリシー

vMedia ポリシーは、リモート vMedia デバイスのマッピング情報を設定するために使用します。 1 つの vMedia ポリシーで、CD 用と HDD 用の 2 つの vMedia デバイスとマッピングを使用できます。 1 つの ISO と 1 つの IMG を同時に設定できます。 CD ドライブに対する ISO 設定のマッピング。 HDD デバイスに対する IMG 設定のマッピング。

（注） デバイスをリモート フォルダにマッピングする場合は、IMG を作成し、HDD デバイスとしてマッピングします。

Cisco UCS Central から、リモート UCS サーバ用の vMedia デバイス ISO イメージをプロビジョニングできます。 スクリプト可能 vMedia を使用して、リモート サーバ上で IMG イメージと ISO イメージをプログラム的にマウントすることができます。 CIMC マウント vMedia を使用すれば、メディア接続に関する追加要件なしで、データセンター内の他のマウント メディア間で通信できるようになります。 スクリプト可能 vMedia を使用すれば、ブラウザを使用せずに仮想メディア デバイスを制御して、手動で各 Cisco UCS サーバを個別にマッピングできます。

スクリプト可能 vMedia は、NFS、CIFS、HTTP、および HTTPS の共有など、複数の共有タイプをサポートします。 スクリプト可能 vMedia は BIOS 設定を通して有効にし、Web GUI および CLI インターフェイスを介して設定します。 スクリプト可能 vMedia を使用して、登録された Cisco UCS ドメイン内で次の操作を実行できます。

- 特定の vMedia デバイスからのブート
- マウント共有からローカル ディスクへのファイルのコピー
- OS ドライバのインストールと更新

（注） スクリプト可能 vMedia のサポートは、CIMC マップド デバイスにのみ適用されます。 既存の KVM ベースの vMedia デバイスはサポートされません。

vMedia ポリシーの作成または編集

vMedia ポリシーを作成して、それとサービス プロファイルを関連付けることができます。

ステップ 1 タスク バーで、「Create vMedia Policy」と入力して、Enter キーを押します。
これにより、[Create vMedia Policy] ダイアログボックスが開きます。

ステップ 2 [Basic] で、[Organization] をクリックして、この vMedia ポリシーを作成する場所を選択します。

a) [Name] とオプションの [Description] を入力します。
ポリシー名は大文字と小文字が区別されます。

b) （任意） [Retry on Mount Failure] に対して [Enabled] または [Disabled] を選択します。
[Enabled] の場合は、マウント エラーが発生しても vMedia がマウントを継続します。

ステップ 3 （任意） [HDD] をクリックして、次の手順を実行します。

a) [Mount Name] を入力します。
b) [Protocol] を選択して、必要なプロトコル情報を入力します。
c) [Generate File name from Service Profile Name] で、[Enabled] または [Disabled] をクリックします。
[Enabled] の場合は、自動的に IMG 名としてサービス プロファイル名が使用されます。 サービス プロファイルと同じ名前の IMG ファイルが必要なパスで入手できる必要があります。 [Disabled] を選択した場合は、ポリシーで使用する必要のあるリモート IMG ファイル名を入力します。

ステップ 4 （任意） [CDD] をクリックして、次の手順を実行します。

a) [Mount Name] を入力します。
b) [Protocol] を選択して、必要なプロトコル情報を入力します。
c) [Generate File name from Service Profile Name] で、[Enabled] または [Disabled] をクリックします。
[Enabled] の場合は、自動的に ISO 名としてサービス プロファイル名が使用されます。 サービス プロファイルと同じ名前の ISO ファイルが必要なパスで入手できる必要があります。 [Disabled] を選択した場合は、ポリシーで使用する必要のあるリモート ISO ファイル名を入力します。

ステップ 5 [Create] をクリックします。

次の作業

vMedia ポリシーとサービス プロファイルを関連付けます。

Call Home ポリシー

Cisco UCS Central は、Call Home プロファイルで定義されているすべての電子メール受信者に特定の Cisco UCS Manager のイベントを通知するためのグローバル Call Home ポリシーをサポートしています（このリリースでは、Cisco UCS Central に対する Call Home はサポートされていません）。プロファイルは、アラート通知（フル テキスト、ショート テキスト、または XML 形式で最大値に定義されたメッセージ サイズ）を受信する電子メール受信者のリスト、および通知をトリガーするためのアラート条件を定義します。

アラート通知は、アラート レベル（やや重大、比較的重大でない、通常、通知、および警告）、および通知をトリガーするイベント（診断、環境、インベントリ、ライセンス、およびその他の事前定義されたイベント）を識別する選択されたアラート グループに基づいて、事前定義されたコンテンツ付きで送信されます。 個別の電子メール受信者は、既存のプロファイルに個別に追加される可能性があります。 登録済み Cisco UCS ドメイン では、そのクライアントのポリシー解決コントロール内でセキュリティ ポリシーを定義するようにしている場合、すべての Call Home ポリシーについて Cisco UCS Central への登録に従うことになります。

Call Home の設定

Call Home ポリシーは、ドメイン グループ ルート下にあるドメイン グループから作成されます。ドメイン グループ ルート下にある Call Home ポリシーは、システムによってすでに作成されており、設定できる状態です。

手順の概要

1. [Domain Group] ページに移動します。
2. [Settings] アイコンをクリックして、[Call Home Settings] を選択します。
3. [Basic] で、[Enabled] をクリックして、Call Home 機能を有効にし、必要な情報を入力します。
4. [Profiles] で、[Add] をクリックして、新しいプロファイルを作成するか、既存のプロファイルを編集します。
5. [Alerts] で、[Add] または [Delete] をクリックして、送信するアラートをトリガーするイベントを管理します。
6. [Save] をクリックします。

手順の詳細

ステップ 1 [Domain Group] ページに移動します。

ステップ 2 [Settings] アイコンをクリックして、[Call Home Settings] を選択します。

ステップ 3 [Basic] で、[Enabled] をクリックして、Call Home 機能を有効にし、必要な情報を入力します。

ステップ 4 [Profiles] で、[Add] をクリックして、新しいプロファイルを作成するか、既存のプロファイルを編集します。

ステップ 5 [Alerts] で、[Add] または [Delete] をクリックして、送信するアラートをトリガーするイベントを管理します。

ステップ 6 [Save] をクリックします。

第 11 章

ID プール

この章は、次の内容で構成されています。

ID ユニバース

[ID Universe] には、システムで使用可能なプール、ID のコレクション、あるいは物理または論理リソースが表示されます。すべてのプールは、サービスプロファイルの柔軟性を高め、ユーザがシステム リソースを中央で集中管理できるようにするものです。 Cisco UCS Central で定義されたプールはグローバル プールと呼ばれ、Cisco UCS ドメイン間で共有できます。 グローバル プールは、Cisco UCS Central に登録された Cisco UCS ドメイン全体で集中型 ID 管理を可能にします。 Cisco UCS Central から Cisco UCS Manager に ID プールを割り当てることにより、ID がどこでどのようにして使用されるかを追跡し、競合を防止し、また競合が発生した場合に通知を受けることができます。 Cisco UCS Manager でローカルに定義されたプールは、ドメイン プールと呼ばれます。

（注） 異なるプールに同じ ID が存在できますが、割り当てることができるのは一度だけです。 同じプールの 2 つのブロックは、同じ ID を保有できません。

MAC アドレスなどの ID 情報をプールし、特定のアプリケーションをホストするサーバに範囲を事前に割り当てることができます。 たとえば、MAC アドレス、UUID、および WWN の同じ範囲内にある Cisco UCS ドメインにわたってすべてのデータベース サーバを設定できます。

[ID Universe] ページで、プールのタイプごとの ID の総数を確認できます。総数は [Available]、[In Use]、または [Conflict] です。 [Resource] をクリックすると、その ID とそれが使用されている場所に関する詳細情報を確認できます。

IP プール

IP プールは、IP アドレスの集合です。 次のいずれかの方法で、Cisco UCS Central で IP プールを使用できます。

- Cisco UCS Manager サーバの外部管理。
- iSCSI ブート イニシエータ。
- Cisco UCS Manager の外部管理および iSCSI ブート イニシエータの両方。

（注） サーバまたはサービス プロファイルのスタティック IP アドレスとして割り当てられている IP アドレスが、IP プールに含まれていてはなりません。

同じ IP アドレスが 2 つの異なる Cisco UCS ドメインに割り当てられた場合は、障害が発生します。 同じ IP アドレスを使用する場合は、[scope] プロパティを使用して、ブロック内の IP アドレスがパブリックとプライベートのどちらであるかを指定できます。

- [public]：ブロック内の IP アドレスを 1 つの登録済み Cisco UCS ドメインのみに割り当てることができます。
- [private]：ブロック内の IP アドレスを複数の Cisco UCS ドメインに割り当てることができます。

Cisco UCS Central は、デフォルトでパブリック IP プールを作成します。

グローバル IP プールは、同様の地理的な場所で使用する必要があります。 IP アドレッシング スキームが異なる場合は、これらのサイトに同じ IP プールを使用できません。

Cisco UCS Central は、IP プール内の IPv4 ブロックと IPv6 ブロックの作成と削除をサポートします。 ただし、iSCSI ブート イニシエータは IPv4 ブロックしかサポートしません。

IQN プール

IQN プールは、Cisco UCS ドメイン内の iSCSI vNIC によって発信側 ID として使用される iSCSI 修飾名（IQN）の集合です。 Cisco UCS Central で作成された IQN プールは、Cisco UCS ドメイン間で共有できます。

IQN プール メンバーの形式は、*prefix*:*suffix*:*number*であり、接頭辞、接尾辞、および番号のブロック（範囲）を指定できます。

IQN プールは、番号の範囲とサフィックスは異なるものの、同じプレフィックスを共有する複数の IQN ブロックを含むことができます。

MAC プール

MAC プールは、ネットワーク ID（MAC アドレス）の集まりです。MAC アドレスはレイヤ 2 環境では一意で、サーバの vNIC に割り当てることができます。 Cisco UCS Central で作成された MAC プールは、Cisco UCS ドメイン間で共有できます。 サービス プロファイルで MAC プールを使用する場合は、サービス プロファイルに関連付けられたサーバで使用できるように MAC アドレスを手動で設定する必要はありません。

マルチテナント機能を実装しているシステムでは、組織階層を使用して、この MAC プールが特定のアプリケーションまたはビジネス サービスでのみ使用できるようにすることができます。 Cisco UCS Central は名前解決ポリシーを使用してプールから MAC アドレスを割り当てます。

サーバに MAC アドレスを割り当てるには、vNIC ポリシーに MAC プールをインクルードする必要があります。 その後、この vNIC ポリシーは、このサーバに割り当てられたサービス プロファイルに含められます。

独自の MAC アドレスを指定することもできますし、シスコにより提供された MAC アドレスのグループを使用することもできます。

UUID 接尾辞プール

UUID 接尾辞プールは、サーバへの割り当てに使用できる SMBIOS UUID の集まりです。 UUID の接頭辞を構成する先頭の桁の数字は固定です。 残りの桁である UUID サフィックスは変数値です。 UUID 接尾辞プールは、競合を避けるため、その特定のプールを使用するサービス プロファイルに関連付けられたサーバごとに、これらの変数値が固有であることを保証します。

サービス プロファイルで UUID 接尾辞プールを使用する場合、サービス プロファイルに関連付けられたサーバの UUID を手動で設定する必要はありません。 Cisco UCS Central からのグローバル UUID 接尾辞プールを Cisco UCS Central または Cisco UCS Manager 内のサービス プロファイルに割り当てることにより、それらを Cisco UCS ドメイン間で共有できます。

WWN プール

WWN プールは、Cisco UCS ドメイン内のファイバ チャネル vHBA で使用される WWN の集合です。 Cisco UCS Central で作成された WWN プールは、Cisco UCS ドメイン間で共有できます。 次の独立したプールを作成します。

- サーバに割り当てられる WW ノード名
- vHBA に割り当てられる WW ポート名
- WW ノード名と WW ポート名の両方

重要

WWN プールは、20:00:00:00:00:00:00:00 ～ 20:FF:FF:FF:FF:FF:FF:FF、または 50:00:00:00:00:00:00:00 ～ 5F:FF:FF:FF:FF:FF:FF:FF の範囲内の WWNN または WWPN だけを含めることができます。 その他の WWN 範囲はすべて予約されています。 SAN ファブリックで Cisco UCS WWNN と WWPN を確実に一意にするには、プールのすべてのブロックに 20:00:00:25:B5:XX:XX:XX の WWN プレフィックスを使用することをお勧めします

サービス プロファイルで WWN プールを使用する場合は、サービス プロファイルに関連付けられたサーバで使用される WWN を手動で設定する必要はありません。 複数のテナントを実装するシステムでは、WWN プールを使用して、各組織で使用される WWN を制御できます。

WWN をブロック単位でプールに割り当てます。

WWNN プール

ワールド ワイド ノード名（WWNN）プールは、WW ノード名だけを含む WWN プールです。サービス プロファイルに WWNN のプールを含める場合、関連付けられたサーバには、そのプールから WWNN が割り当てられます。

WWPN プール

ワールドワイドポート名（WWPN）プールは、WW ポート名だけを含む WWN プールです。サービス プロファイルに WWPN のプールを含める場合、関連付けられたサーバの各 vHBA 上のポートには、そのプールから WWPN が割り当てられます。

WWxN プール

WWxN プールは、WW ノード名および WW ポート名の両方を含む WWN プールです。 ノードごとに WWxN プールで作成されるポート数を指定できます。 WWxN プールのプール サイズは、ノードごとのポートに 1 を加えた数の倍数である必要があります。 たとえば、ノードごとに 7 個のポートがある場合、プールサイズは8の倍数である必要があります。 ノードごとに63個のポートがある場合、プール サイズは、64 の倍数である必要があります。

すべてのプール

システム内の ID プールの完全なリストが表示されます。 [Utilization Status] 、[Org] 、または [ID Type] で並べ替えるフィルタを使用して使用可能性と使用状況を確認できます。

IP プールの作成と編集

IP プールを作成したら、選択した IP プールの総括ページで [Edit] アイコンを選択することによって、それを編集することができます。 IP プールを選択するには、[All Pools] ページにアクセスして、編集する IP プールを選択します。 このページから、選択した IP プールの総括ページにリダイレクトされます。

ステップ 1 タスク バーで、「Create IP Pool」と入力して、Enter キーを押します。
これにより、[Create IP Pool] ダイアログボックスが開きます。

ステップ 2 [Basic] で、次の手順を実行します。

a) [Organization] ドロップダウン リストから、IP プールを作成またはアクセスする組織またはサブ組織を選択します。

b) プールの名前と説明を入力します。

ステップ 3 それぞれの IP ブロックをクリックして、IP アドレス（IPv4 または IPv6）のブロックを作成し、次の手順を実行します。

a) プラス記号をクリックして、選択したプール内の 1 つ以上の IP アドレスのブロックを作成します。

b) それぞれの IP ブロック開始列に、ブロック内の最初の IPv4 または IPv6 アドレスを入力します。

c) [Size] 列に、プール内の IP アドレスの総数を入力します。

ステップ 4 [Apply] アイコンをクリックします。
ページに追加のフィールドが表示されます。

ステップ 5 [Basic] で、次のフィールドに値を入力します。

1. ブロック内の IPv4 または IPv6 アドレスに関連付けられたサブネット マスクを入力します。
2. ブロック内の IPv4 または IPv6 アドレスに関連付けられたデフォルト ゲートウェイを入力します。
3. この IPv4 または IPv6 アドレスのブロックでアクセスするプライマリ DNS サーバを入力します。
4. この IPv4 または IPv6 アドレスのブロックでアクセスするセカンダリ DNS サーバを入力します。
5. ブロック内の IP アドレスを Cisco UCS Central に登録された 1 つ以上の Cisco UCS ドメインに割り当てることができるかどうかを選択します。 次のいずれかになります。
   - [public]：ブロック内の IP アドレスを 1 つの登録済み Cisco UCS ドメインにのみ割り当てることができます。
   - [private]：ブロック内の IP アドレスを複数の Cisco UCS ドメインに割り当てることができます。

（注） ブロックを保存した後、ブロック内の IP アドレスのスコープを変更することはできません。

ステップ 6 [IPv4] または [IPv6] アドレスで、プール内の IP アドレスの数、割り当てられた IP アドレスの数、および重複する IP アドレスの数をグラフで表示できます。

ステップ 7 [Access Control] で、[ID Range Access Control Policy] ドロップダウン リストから、この IP アドレス ブロックに関連付けるポリシーを選択します。

ステップ 8 [Create] をクリックします。

次の作業

IQN プールの作成と編集

（注） ほとんどの場合、最大 iSCSI 修飾名（IQN）サイズ（プレフィックス＋サフィックス＋その他の文字）は 223 文字です。 Cisco UCS NIC M51KR-B アダプタを使用する場合、IQN サイズを 128 文字に制限する必要があります。

IQN プールを作成したら、選択した IQN プールの総括ページで [Edit] アイコンを選択することによって、それを編集することができます。 IQN プールを選択するには、[All Pools] ページにアクセスして、編集する IQN プールを選択します。 ページから、選択した IQN プールの総括ページにリダイレクトされます。

ステップ 1 タスク バーで、「Create IQN Pool」と入力して、Enter キーを押します。
これにより、[Create IQN Pool] ダイアログボックスが開きます。

ステップ 2 [Basic] で、次の手順を実行します。

a) [Organization] ドロップダウン リストから、IQN プールを作成またはアクセスする組織またはサブ組織を選択します。
b) IQN プールの名前と説明を入力します。
c) このプール用に作成された IQN ブロックのプレフィックスを入力します。

ステップ 3 [Suffix Blocks] で、次の手順を実行します。

a) プラス アイコンをクリックして、選択したプールで 1 つ以上の IQN サフィックスのブロックを作成します。
b) [Suffix Block] 列に、この IQN のブロックのサフィックスを入力します。
c) [Start] 列に、ブロック内の最初の IQN サフィックスを入力します。
d) [Size] 列に、ブロック内の IQN サフィックスの総数を入力します。

ステップ 4 [Apply] アイコンをクリックします。

ステップ 5 [Create] をクリックします。

次の作業

サービス プロファイルまたはサービス プロファイル テンプレートに IQN サフィックス プールを含めます。

MAC プールの作成と編集

MAC プールを作成したら、選択した MAC プールの総括ページで [Edit] アイコンを選択することによって、それを編集することができます。 MAC プールを選択するには、[All Pools] ページにアクセスして、編集する MAC プールを選択します。 ページから、選択した MAC プールの総括ページにリダイレクトされます。

ステップ 1 タスク バーで、「Create MAC Pool」を入力して、Enter キーを押します。
これにより、[Create MAC Pool] ダイアログボックスが開きます。

ステップ 2 [Basic] で、次の手順を実行します。

a) [Organization] ドロップダウン リストからは、MAC プールを作成またはアクセスする組織またはサブ組織を選択します。
b) プールの名前と説明を入力します。

ステップ 3 [MAC Blocks] で、次の手順を実行します。

a) プラス アイコンをクリックして、MAC アドレス ブロックを作成します。
b) [MAC Block Start] 列に、ブロック内の最初の MAC アドレスを入力します。
c) [Size] 列に、ブロック内の MAC アドレスの数を入力します。
d) [Apply] アイコンをクリックします。
MAC プールに関連したその他のフィールドが表示されます。
e) [MAC Addresses] で、プール内の MAC アドレスの数、割り当てられた MAC アドレスの数、重複する MAC アドレス、および MAC サマリーをグラフで表示できます。
f) [Access Control] で、このブロックに適用する ID 範囲アクセス コントロール ポリシーを選択します。ポリシーが存在しない場合は、タスク バーで「Create ID Range Access Control Policy」と入力することによって、ポリシーを作成することができます。

ステップ 4 [Create] をクリックします。

次の作業

MAC プールは、vNIC テンプレートにインクルードします。

UUID サフィックス プールの作成と編集

UUID プールを作成したら、選択した UUID プールの総括ページで [Edit] アイコンを選択することによって、それを編集することができます。 UUID プールを選択するには、[All Pools] ページにア

クセスして、編集する UUID プールを選択します。 このページから、選択した UUID プールの総括ページにリダイレクトされます。

ステップ 1 タスク バーで、「Create UUID Pool」と入力して、Enter キーを押します。
これにより、[Create UUID Pool] ダイアログボックスが開きます。

ステップ 2 [Basic] で、次の手順を実行します。

a) [Organization] ドロップダウン リストから、UUID プールを作成またはアクセスする組織またはサブ組織を選択します。
b) プールの名前と説明を入力します。
c) このプール用に作成された UUID ブロックのサフィックスを入力します。

ステップ 3 [Suffix Blocks] で、次の手順を実行します。

a) [Create] アイコンをクリックします。
b) [Suffix Block] 列に、この UUID のブロックのサフィックスを入力します。
c) [Start] 列に、ブロック内の最初の UUID サフィックスを入力します。
d) [Size] 列に、ブロック内の UUID の総数を入力します。
e) [Apply] アイコンをクリックします。
UUID プールに関連したその他のフィールドが表示されます。
f) [UUIDs] では、プール内の UUID アドレスの数、割り当てられた UUID アドレスの数、重複する UUID アドレス、および UUID サマリーをグラフで表示できます。
g) [Access Control] で、このブロックに適用する ID 範囲アクセス コントロール ポリシーを選択します。ポリシーが存在しない場合は、タスク バーで「Create ID Range Access Control Policy」と入力することによって、ポリシーを作成することができます。

ステップ 4 [Create] をクリックします。

次の作業

UUID サフィックス プールをサービス プロファイルまたはサービス プロファイル テンプレートに含めます。

WWN プールの作成と編集

WWN プールを作成したら、選択した WWN プールの総括ページで [Edit] アイコンを選択することによって、それを編集することができます。 WWN プールを選択するには、[All Pools] ページにアクセスして、編集する WWN プールを選択します。 このページから、選択した WWN プールの総括ページにリダイレクトされます。

ステップ 1 タスク バーで、「Create WWN Pool」と入力して、Enter キーを押します。

これにより、[Create WWN Pool] ダイアログボックスが開きます。

ステップ 2 [Basic] で、次の手順を実行します。

a) [Organization] をクリックして、プールを作成する場所を選択します。
b) WWN プールの名前と説明を入力します。
c) [World Wide Name (WWN) Used For] 領域で、次のいずれかを選択します。

- [Port (WWPN)]：プールが WWNN と WWPN の両方に使用されます。
- [Node (WWNN)]：プールが WWNN に使用されます。
- [Both (WWxN)]：プールが WWNN に使用されます。

ステップ 3 [WWN Blocks] で、次の手順を実行します。

a) [Create] アイコンをクリックします。
b) [WWN Block Start] 列に、ブロック内の最初の WWN イニシエータを入力します。
c) [Size] 列に、プール内の WWN イニシエータの総数を入力します。
d) [Apply] アイコンをクリックします。
WWN プールに関連したその他のフィールドが表示されます。
e) [WWNs] タブをクリックすると、プール内の WWN アドレスの数、割り当てられた WWN アドレスの数、重複する MAC アドレス、および WWN サマリーをグラフで表示できます。
f) [Access Control] で、このブロックに適用する ID 範囲アクセス コントロール ポリシーを選択します。ポリシーが存在しない場合は、タスク バーで「Create ID Range Access Control Policy」と入力することによって、ポリシーを作成することができます。

ステップ 4 [Create] をクリックします。
（注） 別のプールを作成する場合は、5 秒以上待つ必要があります。

次の作業

- WWPN プールは、vHBA テンプレートにインクルードします。
- サービス プロファイルまたはサービス プロファイル テンプレートに WWNN プールを含めます。
- サービス プロファイルまたはサービス プロファイル テンプレートに WWxN プールを含めます。

プールの削除

プールを削除すると、Cisco UCS Central が Cisco UCS Manager で vNIC または vHBA に割り当てられたアドレスを（そのプールから）再割り当てしません。 削除されたプールのすべての割り当て済みブロックは、次のいずれかが起きるまで、割り当てられた vNIC または vHBA に残ります。

- 関連付けられたサービス プロファイルが削除された場合。
- アドレスが割り当てられた vNIC または vHBA が削除された場合。
- vNIC または vHBA が異なるプールに割り当てられた場合。

はじめる前に

ステップ 1 ナビゲーション バーで、[Operations] アイコンをクリックして、[Pools] を選択します。
これにより、[All Pools] ダイアログボックスが開きます。

ステップ 2 [Pool name] 列で、削除するプールを選択します。
次のいずれかの方法でプールを検索できます。

- プールのリストを参照します。
- [Search] アイコンをクリックして、プール名を入力します。
- [Filter] 列からプール タイプを選択します。

ステップ 3 [Org] 列で、プールをクリックします。
これにより、選択されたプールの総括ページが開きます。

ステップ 4 削除アイコンをクリックします。
Cisco UCS Central GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

サーバ プール

サーバプールは複数のサーバで構成されています。 これらのサーバは通常、同じ特性を持っています。 これらの特性は、シャーシ内の位置であったり、サーバ タイプ、メモリ容量、ローカル ストレージ、CPUのタイプ、ローカル ドライブ設定などの属性だったりします。 サーバを手動でサーバ プールに割り当てることも、サーバ プール ポリシーとサーバ プール ポリシー資格情報を使用して割り当てを自動化することもできます。

システムが組織を通じて、マルチテナント機能を実装している場合、特定の組織で使用されるサーバ プールを1つ以上、指定できます。 たとえば、CPU を2個搭載したサーバをすべて含むプールをマーケティング組織に割り当て、メモリのサイズが 64GB のサーバをすべて、財務組織に割り当てることができます。

サーバ プールには、システム内のどのシャーシにあるサーバでも入れることができます。 1つのサーバは複数のサーバ プールに属することができます。

特定のサーバ プールを選択すると、そのプールに関する個別の詳細を表示できます。これには、プール内のサーバ数と関連する資格ポリシーが含まれます。

サーバ プールの作成または編集

ステップ 1 タスク バーで、「Create Server Pool」と入力して、Enter キーを押します。
これにより、[Create Server Pool] ダイアログボックスが開きます。

ステップ 2 [Basic] で、[Organization] をクリックして、サーバ プールを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。

ステップ 4 [Qualification] で、[Add] をクリックして新しい資格ポリシーを追加するか、[Delete] をクリックして既存のポリシーを削除します。
詳細については、サーバ プール資格ポリシーの作成または編集, （146 ページ）を参照してください。

ステップ 5 [Servers] で、プールに含めるサーバを追加します。

ステップ 6 [Create] をクリックします。

サーバ プール資格ポリシー

サーバプール資格ポリシーは、検出プロセス中に実施されたサーバインベントリに基づいてサーバを認定します。 ポリシー内で、サーバが選択基準を満たしているどうかを判断するための資格情報または個別のルールを設定できます。 たとえば、データセンタープールのサーバの最小メモリ容量を指定するルールを作成できます。

資格情報は、サーバプールポリシーだけではなく、その他のポリシーでも、サーバを配置するために使用されます。 たとえば、サーバがある資格ポリシーの基準を満たしている場合、このサーバを 1 つ以上のサーバ プールに追加したり、自動的にサービス プロファイルと関連付けたりできます。

サーバ プール ポリシー資格情報を使用すると、次の基準に従ってサーバを資格認定できます。

- アダプタのタイプ
- シャーシの場所
- メモリのタイプと設定
- 電源グループ
- CPU のコア数、タイプ、および設定
- ストレージの設定と容量
- サーバのモデル

実装によっては、サーバプールポリシー資格情報を使用して、次を含む複数のポリシーを設定する必要があります。

- 自動構成ポリシー
- シャーシ ディスカバリ ポリシー
- サーバ ディスカバリ ポリシー
- サーバ継承ポリシー
- サーバ プール ポリシー

サーバ プール資格ポリシーの作成または編集

ステップ 1 タスク バーで、「Create Server Pool Qualification Policy」と入力して、Enter キーを押します。
これにより、[Create Server Pool Qualification Policy] ダイアログボックスが開きます。

ステップ 2 [Basic] で、[Organization] をクリックして、サーバ プール資格ポリシーを作成する場所を選択します。

ステップ 3 [Name] と、オプションの [Description] と [Server Model/PID] を入力します。

ステップ 4 （任意） [Domain] に、ドメイン グループ名を入力して、必須フィールドに値を入力します。
詳細については、ドメイン グループの作成または編集, （60 ページ）を参照してください。

ステップ 5 [Hardware] で、プロセッサ、メモリ、ストレージ、およびアダプタ別の資格情報を有効にするかどうかを選択します。

ステップ 6 [Create] をクリックします。

第 12 章

グローバル VLAN および VSAN

この章は、次の内容で構成されています。

グローバル VLAN

Cisco UCS Central を使用すれば、ドメイン グループ ルートまたはドメイン グループ レベルで LAN クラウド内にグローバル VLAN を定義することができます。 1 回の操作で単一の VLAN または複数の VLAN を作成できます。

グローバル VLAN 解決が、グローバル サービス プロファイルの展開前に、Cisco UCS Central で実施されます。 グローバル サービス プロファイルがグローバル VLAN を参照しているが、その VLAN が存在しない場合は、Cisco UCS ドメインでのグローバル サービス プロファイルの展開がリソース不足により失敗します。 Cisco UCS Central で作成されたすべてのグローバル VLAN がそのグローバル サービス プロファイルの展開前に解決されている必要があります。

グローバル VLAN は、グローバル VLAN への参照を含むグローバル サービス プロファイルがその UCS ドメイン内に展開されていない場合でも、Cisco UCS Manager で使用できます。

（注） また、グローバル VLAN は、それを参照しているグローバル サービス プロファイルが削除されても、削除されません。

グローバル VLAN は、Cisco UCS Manager から削除できません。 グローバル VLAN を Cisco UCS Manager から削除する場合は、VLAN をローカライズしてから削除する必要があります。

VLAN 組織権限

Cisco UCS Central で設定されたすべての VLAN が、作成された組織に共通です。 組織に権限を割り当てないかぎり、組織の一部である Cisco UCS Manager インスタンスがリソースを消費することはできません。 組織権限を VLAN に割り当てると、VLAN が組織から見えるようになり、その

組織の一部である Cisco UCS Manager インスタンスによって保持されているサービス プロファイルで参照できるようになります。

VLAN 名前解決は、各ドメイン グループの階層内で実施されます。 複数のドメイン グループ内に同じ名前の VLAN が存在する場合は、組織権限がドメイン グループ全体の同じ名前のすべての VLAN に適用されます。

VLAN 組織権限は、作成、変更、または削除することができます。

（注） VLAN 組織権限は、必ずそれを作成した同じ組織から削除してください。 Cisco UCS Central GUI で、この VLAN が関連付けられている組織の構造を表示できます。 ただし、Cisco UCS Central CLI のサブ組織レベルでは、VLAN 組織権限関連付け階層を表示できないため、Cisco UCS Central CLI のサブ組織レベルで VLAN を削除しようとすると、削除操作が失敗します。

VLAN の作成または編集

ドメイン グループ ルートまたは特定のドメイン グループ レベルで VLAN を作成し、VLAN にアクセス可能な組織を指定できます。

選択した VLAN の [VLAN ID] 、[Multicast Policy] 、およびコントロールに対するアクセスを編集できます。 ドメイン グループ内で VLAN を作成すると、[Domain Group Location] または [VLAN Name] を変更できなくなります。

ステップ 1 タスク バーで、「Create VLAN」と入力して、Enter キーを押します。
これにより、[Create VLAN] ダイアログボックスが開きます。

ステップ 2 [Basic] で、[Domain Group Location] をクリックして、この VLAN を作成する場所を選択します。

ステップ 3 この VLAN の [Name] を入力します。
VLAN 名は大文字と小文字が区別されます。

重要 Cisco UCS Central で VLAN を作成するときに default という名前を使用しないでください。 グローバル デフォルト VLAN を作成する場合は、名前に globalDefault を使用できます。

ステップ 4 [VLAN ID] を入力します。
VLAN ID には次の値を入力できます。

- 1 ～ 3967

  （注） 登録された Cisco UCS ドメインに UCS Manager バージョン 2.2(4) 以降が存在する場合は、ID の範囲を 1 ～ 4027 にすることができます。

- 4048 ～ 4093
- すでに他のドメイン グループで定義されている他の VLAN ID とのオーバーラップ

ステップ 5 （任意） [Check VLAN Name Overlap] と [Check VLAN ID Overlap] をクリックして、オーバーラップを特定します。

ステップ 6 （任意） [Multicast Policy] とこの VLAN を関連付ける場合は、マルチキャスト ポリシー名を入力します。Cisco UCS Central がマルチキャスト ポリシーを特定して、それをバックエンドで VLAN にアタッチします。

ステップ 7 [Access Control] で、プラス記号をクリックして、使用可能な組織を表示します。

ステップ 8 組織を選択して、チェックマークをクリックし、選択した組織をこの VLAN の [Permitted Orgs] として適用します。

ステップ 9 [Aliased VLANs] で、既存の VLAN を表示して、同じ名前の VLAN が存在するかどうかを確認できます。

ステップ 10 [Create] をクリックします。

VLAN 範囲の作成または編集

ステップ 1 タスク バーで、「Create VLAN Range」と入力して、Enter キーを押します。
これにより、[Create VLAN Range] ダイアログボックスが開きます。

ステップ 2 [Basic] で、[Domain Group Location] をクリックして、この VLAN を作成する場所を選択します。

ステップ 3 この VLAN 範囲の [Name Prefix] を入力します。

ステップ 4 [VLAN ID] を入力します。
VLAN ID には次の値を入力できます。

- 1 ～ 3967
- 4048 ～ 4093
- すでに他のドメイン グループで定義されている他の VLAN ID とのオーバーラップ

例：
たとえば、ID が 4、22、40、41、42、および 43 の 6 つの VLAN を作成するには、「4, 22, 40-43」と入力します。

ステップ 5 （任意） [Check VLAN Name Overlap] と [Check VLAN ID Overlap] をクリックして、オーバーラップを特定します。

ステップ 6 （任意） [Multicast Policy] とこの VLAN を関連付ける場合は、マルチキャスト ポリシー名を入力します。Cisco UCS Central がマルチキャスト ポリシーを特定して、それをバックエンドで VLAN にアタッチします。

ステップ 7 [Access Control] で、プラス記号をクリックして、使用可能な組織を表示します。

ステップ 8 組織を選択して、チェックマークをクリックし、選択した組織をこの VLAN の [Permitted Orgs] として適用します。

ステップ 9 [Aliased VLANs] で、既存の VLAN を表示して、同じ名前の VLAN が存在するかどうかを確認できます。

ステップ 10 [Create] をクリックします。

グローバル VSAN

Cisco UCS Central を使用すれば、SAN クラウド、ドメイン グループ ルート、またはドメイン グループ レベルでグローバル VSAN を定義することができます。 Cisco UCS Central で作成されたグローバル VSAN は、それが作成されたファブリック インターコネクト固有です。 VSAN は、ファブリック A とファブリック B のどちらかまたはその両方に割り当てることができます。 グローバル VSAN は、Cisco UCS Central で共通の VSAN ではありません。

グローバル VSAN の解決は、それを参照しているグローバル サービス プロファイルの Cisco UCS Manager への展開前に、Cisco UCS Central で実施されます。 グローバル サービス プロファイルがグローバル VSAN を参照しているが、その VSAN が存在しない場合は、グローバル サービス プロファイルの Cisco UCS Manager への展開がリソース不足により失敗します。 Cisco UCS Central で作成されたすべてのグローバル VSAN がそのグローバル サービス プロファイルの展開前に解決されている必要があります。

グローバル VSAN は、グローバル VSAN への参照を含むグローバル サービス プロファイルがその UCS ドメイン内に展開されていない場合でも、Cisco UCS Manager で使用できます。 また、グローバル VSAN は、それを参照しているグローバル サービス プロファイルが削除されても、削除されません。

Cisco UCS Manager インスタンスで使用可能なグローバル サービス プロファイルから参照されているグローバル VSAN は、明示的にドメイン グループから削除されないかぎり、そのまま使用できます。 Cisco UCS Manager で、グローバル VSAN をローカライズして、ローカル VSAN として機能させることができます。 グローバル VSAN がローカライズされていない場合は、Cisco UCS Manager から削除できません。

VSAN の作成または編集

次の予約された範囲のものを除いて、1 ～ 4093 の ID で VSAN を作成できます。

- Cisco UCS ドメイン FC スイッチ モードを使用する予定の場合は、ID が 3040 ～ 4078 の範囲にある VSAN を設定しないでください。
- Cisco UCS ドメイン FC エンドホスト モードを使用する予定の場合は、ID が 3840 ～ 4079 の範囲にある VSAN を設定しないでください。

重要 SAN クラウドの FCoE VLAN と LAN クラウドの VLAN の ID が同じであってはなりません。VSAN 内の FCoE vLAN と vLAN で同じ ID を使用すると、その VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害とトラフィックの中断が発生します。 FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

VSAN は、ドメイン グループ ルートまたは特定のドメインで作成することができます。 また、VSAN は、ファブリック A とファブリック B のどちらかまたはその両方に割り当てることができます。 VSAN を両方のファブリックに割り当てる場合は、その両方に別々の VSAN ID と FCoE vLAN ID を設定する必要があります。

VSAN を作成したら、必要に応じて、[Fabric Zoning]、[Fabric] 割り当て、[VSAN ID]、および [FCoE vLAN ID] を編集できます。

ステップ 1 タスク バーで、「Create VSAN」と入力して、Enter キーを押します。
これにより、[Create vSAN] ダイアログボックスが開きます。

ステップ 2 [Domain Group Location] をクリックして、この VSAN を作成する場所を選択します。

ステップ 3 [Name] を入力します。
VSAN 名は大文字と小文字が区別されます。

重要 Cisco UCS Central で VSAN を作成するときは、default という名前を使用しないでください。 グローバル デフォルト VSAN を作成する場合は、名前として globalDefault を使用できます。

ステップ 4 （任意） [FC Zoning Settings] パネルの [Enabled] オプション ボタンを選択して、ファイバ チャネル ゾーン分割を有効にします。
ファイバ チャネル ゾーン分割は次のどちらかにすることができます。

- [disabled]：アップストリーム スイッチがファイバ チャネル ゾーン分割を設定して制御するか、ファイバ チャネル ゾーン分割がこの VSAN 上に実装されません。
- [enabled]：Cisco UCS Manager が VSAN の展開時にファイバ チャネル ゾーン分割を設定して制御します。

（注） ファイバ チャネル ゾーン分割はデフォルトで無効にされます。

ステップ 5 この VSAN を割り当てるファブリックを選択します。
VSAN を両方のファブリックに割り当てる場合は、両方のファブリックの VSAN ID と FCoE vLAN ID を入力します。 選択した VSAN の ID を割り当てない場合。

ステップ 6 [Create] をクリックします。

第 13 章

ストレージ プロファイル

この章は、次の内容で構成されています。

ストレージ プロファイル

Cisco UCS M シリーズ モジュラ サーバでは、ストレージがシャーシごとに集中管理され、この集中管理されたストレージがシャーシ内のすべてのサーバで共有されます。ストレージプロファイルを使用すれば、次の操作を実行できます。

- 複数の仮想ドライブを設定して、仮想ドライブで使用される物理ドライブを選択する。
- 仮想ドライブのストレージ容量を設定する。
- ディスク グループ内のディスクの台数、タイプ、および役割を設定する。
- サービス プロファイルとストレージ プロファイルを関連付ける。

ストレージ プロファイルの作成または編集

ステップ 1 タスク バーで、「Create Storage Profile」と入力して、Enter キーを押します。
これにより、[Create Storage Profile] ダイアログボックスが開きます。

ステップ 2 [Basic] で、[Organization] をクリックして、ストレージ プロファイルを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
大文字と小文字が区別されます。

ステップ 4 [Local Luns] で、次の手順を実行します。

a) [Add] をクリックして、新しいローカル LUN を追加します。

b) [Basic] タブで、GB 単位のサイズを入力します。
c) [Disk Group] タブで、[Disk Group Configuration Policy] を選択します。
上矢印と下矢印を使用して、ローカル LUN の順序を変更できます。

ステップ 5 [Create] をクリックします。

ディスク グループ設定ポリシー

シャーシ内のサーバは、そのシャーシ内で集中管理されたストレージを使用することができます。ストレージに使用するディスクを選択して設定できます。 これらの物理ディスクの論理集合をディスク グループと言います。 ディスク グループを使用すれば、ローカル ディスクを整理できます。 ストレージ コントローラがディスク グループの作成と設定を制御します。

ディスク グループ設定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たものです。このポリシーで、ディスク グループに使用する RAID レベルを指定します。 また、ディスク グループのディスクの手動選択または自動選択とディスクのロールも指定します。

ディスク グループ設定ポリシーの作成または編集

ステップ 1 タスク バーで、「Create Disk Group Configuration Policy」と入力して、Enter キーを押します。
これにより、[Create Disk Group Configuration Policy] ダイアログボックスが開きます。

ステップ 2 [Basic] で、[Organization] をクリックして、ディスク グループ設定ポリシーを作成する場所を選択します。

ステップ 3 [Name] とオプションの [Description] を入力します。
大文字と小文字が区別されます。

ステップ 4 [Raid Level] を選択します。
次のいずれかになります。

- プラットフォームのデフォルト
- Simple
- RAID
- RAID 0 ストライプ
- RAID 1 ミラー
- RAID 5 ストライプ パリティ
- RAID 6 ストライプ化デュアルパリティ
- RAID 10 ミラー & ストライプ

- RAID 50 ストライプ パリティ & ストライプ
- RAID 60 ストライプ デュアル パリティ & ストライプ

ステップ 5 [Disk Group] で、[Drive Type] を選択して、ドライブ情報の値を入力し、残りのディスクを使用するかどうかを選択します。

ステップ 6 [Virtual Drive] アイコンで、必要に応じてフィールドに値を入力します。

ステップ 7 [Create] をクリックします。

第 14 章

バックアップと復元

この章は、次の内容で構成されています。

バックアップと復元

Cisco UCS Central を使用すれば、Cisco UCS Central と登録された UCS ドメインをバックアップして復元することができます。バックアップおよび復元ポリシーをスケジュールすることも、Cisco UCS Central または選択したドメインの即時オンデマンド バックアップを実行することもできます。

[Backup & Restore] ページから、Cisco UCS Central と登録された Cisco UCS ドメインの完全状態バックアップをスケジュールできます。 Cisco UCS ドメインの場合は、完全状態バックアップ ポリシーをローカルに作成することもできます。

スケジュールされたバックアップ ポリシーはデフォルトで無効にされます。 Cisco UCS Central または登録された UCS ドメインをバックアップする場合は、両方のバックアップ状態を有効にする必要があります。 バックアップ プロセスが、サーバまたはネットワーク トラフィックを中断または変更することはありません。 バックアップは、ドメインが起動されて動作している間に実行できます。 バックアップ操作では、管理プレーンからの情報が保存されます。

リモートで設定されたポリシーは、バックアップに関して、Cisco UCS Manager によって内部的にマウントされた Cisco UCS Central リポジトリを使用するように制限されます。

定期バックアップをスケジュールすると、バックアップ リポジトリがデータの収集を開始できます。 バックアップ アーカイブを管理するために、保存されているバックアップ バージョンの最大数を指定できます。 ポリシー指定を使用して、Cisco UCS ドメインごとに保持するバックアップ数を指定します。

（注） この最大数は、リモートの場所に保存可能なバックアップ イメージ ファイルの数に影響しません。

Cisco UCS Central GUI から Cisco UCS ドメインごとのバックアップのリストを表示したり、保存されたまたは未使用のバックアップ ディレクトリと設定を削除したりできます。

重要

- バックアップ操作とインポート操作を作成し、実行するには、管理ロールを持つユーザ アカウントが必要です。
- バックアップは、Cisco UCS ドメイン（バックアップが取得された）の登録が解除されてからしか削除できません。

バックアップ イメージ ファイル

次の場所にデータベースまたはコンフィギュレーションバックアップ ファイルを保存できます。

- **ローカル ファイル システム**：ローカル ファイル システム内。
- **リモートの場所**：TFTP、FTP、SCP、SFTP などのプロトコルを使用したリモートの場所。

重要 イメージ ファイルをリモートの場所に保存するためのオプションを使ってグローバル バックアップ ポリシーを指定するには、Cisco UCS Manager リリース 2.2(2x) 以降を Cisco UCS Central に登録する必要があります。

バックアップをスケジュールするときに、システムに保存するバックアップ ファイルの最大数を指定することもできます。

設定の復元

Cisco UCS Central の完全状態バックアップを復元できるのはセットアップ中だけです。 詳細については、該当する『*Cisco UCS Central Installation and Upgrade Guide*』を参照してください。

Cisco UCS Manager では、初期設定中にファブリック インターコネクトのコンソールから完全状態バックアップ設定を復元できます。

バックアップ操作の考慮事項と推奨事項

バックアップ操作を作成する前に、次のことを考慮してください。

バックアップの場所

バックアップ場所とは、Cisco UCS Central でバックアップ ファイルをエクスポートするネットワーク上の宛先またはフォルダのことです。 バックアップ操作は、バックアップ ファイルを保存する場所ごとに 1 つしか保持できません。

バックアップ ファイル上書きの可能性

ファイル名を変更しないでバックアップ操作を再実行すると、サーバ上にすでに存在するファイルが Cisco UCS Central によって上書きされます。 既存のバックアップ ファイルが上書きされるのを回避するには、バックアップ操作内のファイル名を変更するか、既存のファイルを別の場所にコピーします。

バックアップの複数のタイプ

同じ場所に対して複数種類のバックアップを実行し、エクスポートできます。 バックアップ操作を再実行する前に、バックアップ タイプを変更する必要があります。 バックアップ タイプの識別を容易にし、また既存のバックアップ ファイルが上書きされるのを回避するために、ファイル名を変更することを推奨します。

スケジュール バックアップ

バックアップ操作を前もって作成し、そのバックアップの実行準備が整うまで管理状態をディセーブルのままにしておくことはできます。 Cisco UCS Central は、バックアップ操作の管理状態がイネーブルに設定されるまで、バックアップ操作を実行したり、コンフィギュレーション ファイルを保存したり、エクスポートしたりしません。

増分バックアップ

Cisco UCS Manager または Cisco UCS Central の増分バックアップを実行できません。

完全な状態のバックアップの暗号化

パスワードなどの機密情報がクリア テキストでエクスポートされることがないように、完全な状態のバックアップは暗号化されます。

Cisco UCS Central の完全状態バックアップのスケジューリング

はじめる前に

リモートの場所を指定する場合は、その場所が存在することを確認してください。 バックアップ ファイルをリモートの場所に保存するためには、次の情報を準備しておく必要があります。

- 絶対リモート パス。 たとえば、転送プロトコルが SCP の場合：`scp://user@<ip>/x/y/z`
- リモート サーバのホスト名または IP アドレス
- リモート サーバのユーザ名とパスワード

ステップ 1 タスク バーで、「Schedule Central Backup」と入力して、Enter キーを押します。
これにより、[Schedule Central Backup] ダイアログボックスが開きます。

ステップ 2 （任意） [Description] フィールドに、このバックアップ ポリシーの説明を入力します。

ステップ 3 [Schedule] ドロップダウンから、このバックアップのスケジュールを選択します。 次のいずれかになります。

- [One Time Schedules]：バックアップはスケジュールされた日付と時刻にのみ行われます。
- [Recurring Schedules]：バックアップはスケジュールされた頻度で行われます。

（注） この完全状態バックアップと事前定義されたスケジュールを関連付ける必要があります。 スケジュールを作成するには、スケジュールの作成または編集, （125 ページ）を参照してください。

ステップ 4 [Maximum No of Backup Files] フィールドで、システムに保存するバックアップ ファイルの数を指定します。
バックアップ ファイルの最大数に達すると、最も古いバックアップ ファイルが最も新しいバックアップ ファイルで上書きされます。

ステップ 5 （任意） バックアップ ファイルをリモートの場所に保存する場合は、[Remote Copy] フィールドで、[Enabled] をクリックします。
次のフィールドに値を入力して、リモートの場所に関する情報を追加します。

名前	説明
Transfer Protocol	転送プロトコルを選択します。 次のいずれかを指定できます。 • FTP • SFTP • TFTP • SCP
[Absolute Remote Path] フィールド	絶対リモート パス。
[Remote Server Host Name/IP Address] フィールド	リモート サーバの IP アドレス。
[User Name] フィールド	リモート サーバのユーザ名。
[Password] フィールド	リモート サーバのパスワード。

Cisco UCS ドメインの完全状態バックアップのスケジューリング

登録された Cisco UCS ドメインの完全状態バックアップはドメイン グループ レベルでしか作成できません。

はじめる前に

リモートの場所を指定する場合は、その場所が存在することを確認してください。 バックアップ ファイルをリモートの場所に保存するためには、次の情報を準備しておく必要があります。

- 絶対リモート パス。 たとえば、転送プロトコルが SCP の場合：`scp://user@<ip>/x/y/z`
- リモート サーバのホスト名または IP アドレス
- リモート サーバのユーザ名とパスワード

ステップ 1 [Domain Group] ドロップダウン オプションをクリックして、完全状態バックアップをスケジュールするドメイン グループを選択します。
この選択によって、[Schedule] オプションと [No of Backup Files] オプションが表示されます。

ステップ 2 [Schedule] ドロップダウンから、このバックアップのスケジュールを選択します。 次のいずれかを指定できます。

- [Simple]：1 つのワンタイム実行または繰り返し実行を作成します。
- [Advanced]：複数のワンタイム実行または繰り返し実行を作成します。

（注） この完全状態バックアップと事前定義されたスケジュールを関連付ける必要があります。

ステップ 3 [Maximum No of Backup Files] フィールドで、システムに保存するバックアップ ファイルの数を指定します。

ステップ 4 （任意） バックアップ ファイルをリモートの場所に保存する場合は、[Remote Copy] フィールドで、[Enabled] をクリックします。
次のフィールドに値を入力して、リモートの場所に関する情報を追加します。

名前	説明
Transfer Protocol	転送プロトコルを選択します。 次のいずれかを指定できます。 • FTP • SFTP • TFTP • SCP
[Absolute Remote Path] フィールド	絶対リモート パス。
[Remote Server Host Name/IP Address] フィールド	リモート サーバの IP アドレス。
[User Name] フィールド	リモート サーバのユーザ名。

名前	説明
[Password] フィールド	リモート サーバのパスワード。

オンデマンド完全状態バックアップの作成

いつでも Cisco UCS Central の完全状態バックアップを作成して、ファイルをローカルの場所とリモートの場所の両方に保存できます。 ただし、登録済みの Cisco UCS ドメインでは、バックアップをリモートの場所でしか作成することができません。

はじめる前に

オンデマンドバックアップ ファイルをリモートの場所に保存するためには、次の情報を準備しておく必要があります。

- 絶対リモート パス。 たとえば、転送プロトコルが SCP の場合：
  `scp://user@ipaddress/x/y/backup_filename.tgz`
- リモート サーバのホスト名または IP アドレス
- リモート サーバのユーザ名とパスワード

ステップ 1 メニュー バーで、[Operations] アイコンをクリックして、[Backup & Restore] を選択します。

ステップ 2 [UCS Central] をクリックするか、ドメイン グループを選択します。

ステップ 3 [Backup] アイコンをクリックします。
これにより、[Create Backup] ダイアログボックスが開きます。

ステップ 4 Cisco UCS Central の完全状態バックアップの場合は、[Remote Copy] を有効にするか、無効にするかを選択します。
[Disabled] を選択した場合は、ローカル バックアップ コピーが作成され、ステップ 6 に進むことができます。

ステップ 5 [Transfer Protocol] を選択して、必要なリモートの場所に関する情報を入力します。

ステップ 6 [Create] をクリックします。

完全状態バックアップ ファイルが、指定されたリモートの場所に作成され、保存されます。 Cisco UCS ドメインのバックアップ状態を確認するには、ドメイン グループ名をクリックします。

（注） Cisco UCS Central または Cisco UCS Manager のオンデマンド完全状態バックアップが失敗すると、次のエラー メッセージが表示されます。
End point timed out. Check for IP, password, space or access related issues.
このエラーを修正するには、設定を再送信します。 再送信が成功すると、バックアップ ファイルがバックアップ リポジトリ内に作成されます。

Cisco UCS ドメインの完全状態バックアップの削除

後述する手順に加えて、次のシナリオで完全状態バックアップを無効化/削除することができます。

- ルート ドメイン グループ ポリシーを削除すると、バックアップ/エクスポート ポリシーが無効になります。
- サブドメイン グループ ポリシーを削除すると、バックアップ/エクスポート ポリシーが削除されます。

ステップ 1 メニュー バーで、[Operations] アイコンをクリックして、[Backup & Restore] を選択します。

ステップ 2 [Schedule] アイコンをクリックして、[Remove Domain Backup Schedule] を選択します。
これにより、[Remove Domain Backup Schedule] ダイアログボックスが開きます。

ステップ 3 バックアップを削除する [Domain Group] を選択します。

ステップ 4 選択後に表示されるフィールド内の情報を調べて、これが削除するバックアップ スケジュールであることを確認します。

ステップ 5 [Remove] をクリックします。

Cisco UCS Central の完全状態バックアップの削除

後述する手順に加えて、次のシナリオでは、Cisco UCS Central の完全状態バックアップを無効化または削除することができます。

- Cisco UCS Central ポリシーを削除すると、バックアップ/エクスポート ポリシーが無効になります。

ステップ 1 メニュー バーで、[Operations] アイコンをクリックして、[Backup & Restore] を選択します。

ステップ 2 [Schedule] アイコンをクリックして、[Remove Central Backup Schedule] を選択します。

これにより、[Remove Central Backup Schedule] ダイアログボックスが開きます。

ステップ 3 表示されたフィールド内の情報を調べ、それが削除するバックアップ スケジュールであることを確認します。

ステップ 4 [Remove] をクリックします。

Cisco UCS Central のバックアップ ファイルの表示

ステップ 1 メニュー バーで、[Backup & Restore] を選択します。

ステップ 2 [Domains] で、Cisco UCS Central ドメインを選択して、Cisco UCS Central スコープを入力します。

ステップ 3 右側のペインで、すべての Cisco UCS Central バックアップ ファイルのリストを確認します。 バックアップ ファイルごとに、ステータス、最終バックアップ日付、スケジュール、最大ファイル数、およびリモート コピーの場所を表示できます。

第 15 章

設定のエクスポートとインポート

この章は、次の内容で構成されています。

設定のエクスポートとインポート

[Export & Import] から、Cisco UCS Central と登録された Cisco UCS ドメインの設定バックアップをスケジュールすることができます。エクスポートまたはインポートポリシーをスケジュールすることも、Cisco UCS Central または選択したドメインの即時オンデマンド設定エクスポートを実行することもできます。 Cisco UCS ドメインの場合は、オンデマンド バックアップがすべてリモートに保存されます。 バックアップをスケジュールする場合は、ローカルまたはリモートに保存できます。

（注） HTML5 GUI では、全設定バックアップと完全状態バックアップのみがサポートされます。 論理設定バックアップとシステム設定バックアップを使用する場合は、Java ベースの GUI を使用してください。

スケジュールされたバックアップ ポリシーはデフォルトで無効にされます。 Cisco UCS Central または登録された Cisco UCS ドメインをバックアップする場合は、両方のバックアップ状態を有効にする必要があります。 バックアップ プロセスがサーバまたはネットワーク トラフィックを中断または変更することはありません。 バックアップは、ドメインが起動されて動作している間に実行できます。 バックアップ操作では、管理プレーンからの情報が保存されます。

リモートで設定されたポリシーは、バックアップに関して、Cisco UCS Manager によって内部的にマウントされた Cisco UCS Central リポジトリを使用するように制限されます。

定期バックアップをスケジュールすると、バックアップ リポジトリがデータの収集を開始できます。 バックアップ アーカイブを管理するために、保存されているバックアップ バージョンの最大数を指定できます。 ポリシー指定を使用して、Cisco UCS ドメインごとに保持するバックアップ数を指定します。

（注） この最大数は、リモートの場所に保存可能なバックアップ イメージ ファイルの数に影響しません。

Cisco UCS Central GUI から各 Cisco UCS ドメインのバックアップのリストを表示できます（Cisco UCS Central のバックアップ ファイルの表示, （164 ページ）を参照してください。また、保存されたまたは未使用のバックアップ ディレクトリと設定を削除することもできます）。

重要
- バックアップ操作とインポート操作を作成し、実行するには、管理ロールを持つユーザ アカウントが必要です。
- バックアップは、Cisco UCS ドメイン（バックアップが取得された）の登録が解除されてからしか削除できません。

バックアップ イメージ ファイル

次の場所にデータベースまたはコンフィギュレーション バックアップ ファイルを保存できます。

- **ローカル ファイル システム**：ローカル ファイル システム内。
- **リモートの場所**：TFTP、FTP、SCP、SFTP などのプロトコルを使用したリモートの場所。

重要 イメージ ファイルをリモートの場所に保存するためのオプションを使ってグローバル バックアップ ポリシーを指定するには、登録された Cisco UCS ドメイン内に Cisco UCS Manager リリース 2.2(2x) が存在する必要があります。Cisco UCS ドメイン内に Cisco UCS Manager リリース 2.2(2x) が存在しない場合は、リモート バックアップを使用したグローバル バックアップ ポリシーが機能しません。

バックアップをスケジュールするときに、システムに保存するバックアップ ファイルの最大数を指定することもできます。

設定のインポート

バックアップ リポジトリに保存された設定を使用して、管理対象の Cisco UCS ドメインのいずれかをインポートして設定できます。 TFTP プロトコルを使用して、バックアップ設定にアクセスします。

Cisco UCS Central の設定エクスポートのスケジューリング

はじめる前に

リモートの場所を指定する場合は、その場所が存在することを確認してください。 バックアップ ファイルをリモートの場所に保存するためには、次の情報を準備しておく必要があります。

- 絶対リモート パス。 たとえば、転送プロトコルが SCP の場合：`scp://user@<ip>/x/y/z`
- リモート サーバのホスト名または IP アドレス
- リモート サーバのユーザ名とパスワード

ステップ 1 メニュー バーで、[Operations] アイコンをクリックして、[Export & Import] を選択します。

ステップ 2 [Config Export & Import] ページで、[UCS Central] をクリックします。

ステップ 3 [Schedule] アイコンをクリックして、[Schedule Central Export] を選択します。
これにより、[Schedule Central Configuration Export] ダイアログボックスが開きます。

ステップ 4 （任意） [Description] フィールドに、このバックアップ ポリシーの説明を入力します。

ステップ 5 [Schedule] ドロップダウンをクリックして、このバックアップのスケジュールを選択します。
（注） この設定バックアップと事前定義のスケジュールを関連付ける必要があります。

ステップ 6 [Maximum No of Backup Files] フィールドで、システムに保存するバックアップ ファイルの数を指定します。

ステップ 7 （任意） バックアップ ファイルをリモートの場所に保存する場合は、[Remote Copy] フィールドで、[Enabled] をクリックして、必要なリモートの場所に関する情報を入力します。

Cisco UCS ドメインの設定エクスポートのスケジューリング

登録された Cisco UCS ドメインの設定バックアップは、ドメイン グループ レベルでのみ作成できます。

はじめる前に

リモートの場所を指定する場合は、その場所が存在することを確認してください。 バックアップ ファイルをリモートの場所に保存するためには、次の情報を準備しておく必要があります。

- 絶対リモート パス。 たとえば、転送プロトコルが SCP の場合：`scp://user@<ip>/x/y/z`
- リモート サーバのホスト名または IP アドレス

- リモート サーバのユーザ名とパスワード

ステップ 1 [Domain Group] ドロップダウン オプションをクリックして、設定バックアップをスケジュールするドメイン グループを選択します。
この選択により、[Schedule] オプションと [No. of Backup Files] オプションが表示されます。

ステップ 2 [Schedule] ドロップダウンをクリックして、このバックアップのスケジュールを選択します。
（注） この設定バックアップと事前定義のスケジュールを関連付ける必要があります。

ステップ 3 [Maximum No of Backup Files] フィールドで、システムに保存するバックアップ ファイルの数を指定します。

ステップ 4 （任意） バックアップ ファイルをリモートの場所に保存する場合は、[Remote Copy] フィールドで、[Enabled] をクリックします。
表示されたフィールドに、必要なリモートの場所の関連情報を入力します。

ステップ 5 [Schedule] をクリックします。

UCS Central の設定バックアップのエクスポート

はじめる前に

リモートの場所を指定する場合は、その場所が存在することを確認してください。 バックアップ ファイルをリモートの場所に保存するためには、次の情報を準備しておく必要があります。

- 絶対リモート パス。 たとえば、転送プロトコルが SCP の場合：`scp://user@<ip>/x/y/z`
- リモート サーバのホスト名または IP アドレス
- リモート サーバのユーザ名とパスワード

ステップ 1 [Config Export & Import] ページで、[UCS Central] をクリックします。

ステップ 2 エクスポートするバックアップ ファイルを選択します。

ステップ 3 [Config Export] アイコンをクリックします。

ステップ 4 バックアップ ファイルをリモートの場所に保存する場合は、[Remote Copy] フィールドで、[Enabled] をクリックします。
[Disabled] が選択された場合は、ファイルがローカルに保存されます。

ステップ 5 リモートの場所については、[Transfer Protocol] を選択して、表示されたフィールドに必要なリモートの場所に関する情報を入力します。

ステップ 6 [Export] をクリックします。

ドメインの設定オンデマンド バックアップのエクスポート

登録された Cisco UCS ドメインの設定バックアップは、ドメイン グループ レベルでのみ作成できます。

はじめる前に

オンデマンド バックアップが使用できるのはリモートの場所だけです。 ローカル Cisco UCS ドメインでは、オンデマンド バックアップがサポートされません。 バックアップ ファイルをリモートの場所に保存するためには、次の情報を準備しておく必要があります。

- 絶対リモート パス。 たとえば、転送プロトコルが SCP の場合：`scp://user@<ip>/x/y/z`
- リモート サーバのホスト名または IP アドレス
- リモート サーバのユーザ名とパスワード

ステップ 1 [Config Export & Import] ページで、ドメインを選択します。

ステップ 2 エクスポートするバックアップ ファイルを選択します。

ステップ 3 [Config Export] アイコンをクリックします。

ステップ 4 [Transfer Protocol] を選択して、表示されたフィールドに必要なリモートの場所に関する情報を入力します。

ステップ 5 [Export] をクリックします。

Cisco UCS Central の設定のインポート

別の Cisco UCS Central から設定をインポートすることも、ローカルまたはリモートの場所にエクスポートした xml ファイルをインポートすることもできます。

ステップ 1 メニュー バーで、[Operations] アイコンをクリックして、[Export & Import] を選択します。

ステップ 2 [Config Export & Import] ページで、[UCS Central] をクリックします。

ステップ 3 [Config Import] アイコンをクリックします。

これにより、[Import Central Backup] ダイアログボックスが開きます。

ステップ 4 [Behavior on Configuration Import] で、要件に基づいて次のオプションのいずれかを選択します。

オプション	説明
Replace	インポートしたファイル内のオブジェクトごとに、現在の設定内の対応するオブジェクトを置き換えます。
Merge	インポートしたファイル内の設定情報と既存の設定情報をマージします。 競合が存在する場合は、現在の設定内の情報がインポートした設定ファイル内の情報に置き換えられます。

ステップ 5 [Config File Location] で、すべての設定を Cisco UCS Central にインポートする場所を選択します。
以下を選択した場合：

- [UCS Central]：[Config File] ドロップダウンから設定バックアップを選択します。
- [Local]：ファイルの場所を参照して、ファイルを選択します。
  （注） このバックアップ XML ファイルはローカルに存在します。
- [Remote]：リモート サーバ関連情報とファイル パスを入力します。
  （注） このバックアップ XML ファイルはリモート サーバ上に存在します。

ステップ 6 [Import] をクリックします。
Cisco UCS Central のインポートが失敗した場合は、次のエラー メッセージが表示されます。
End point timed out. Check for IP, password, space or access related issues.
このエラーを修正するには、設定を再送信します。 再送信が成功すると、インポート プロセスが開始されます。

Cisco UCS ドメインの設定のインポート

（注） Cisco UCS ドメインが一時停止状態にある、表示されない、または切断されている場合は、インポート設定機能が無効になります。

はじめる前に

バックアップポリシーを使用して、全設定バックアップファイルが作成されていることを確認します。

ステップ 1 メニュー バーで、[Operations] アイコンをクリックして、[Export & Import] を選択します。

ステップ 2 [Config Export & Import] ページで、バックアップをインポートするドメインをクリックします。

ステップ 3 [Config Import] アイコンをクリックします。
これにより、[Import Domain Config Backup] ダイアログボックスが開きます。

ステップ 4 [Behavior on Configuration Import] で、要件に基づいて [Replace] または [Merge] を選択します。

オプション	説明
Replace	インポートしたファイル内のオブジェクトごとに、現在の設定内の対応するオブジェクトを置き換えます。
Merge	インポートしたファイル内の設定情報と既存の設定情報をマージします。 競合が存在する場合は、現在の設定内の情報がインポートした設定ファイル内の情報に置き換えられます。

ステップ 5 [Import From] ドロップダウンで、すべての設定をこのドメインにインポートするドメインを選択します。
ここでの選択肢は、[Config File] ドロップダウンに表示されます。

ステップ 6 [Config File] ドロップダウンをクリックして、設定ファイルを選択します。

ステップ 7 [Import] をクリックします。

Cisco UCS Central の設定エクスポート スケジュールの削除

ステップ 1 [Config Export & Import] ページで、[Schedule] アイコンをクリックします。

ステップ 2 [Remove Central Export Schedule] アイコンを選択します。

ステップ 3 スケジュール内のエントリを確認します。
（注） Cisco UCS Central のスケジュールは 1 つだけです。

ステップ 4 [Remove] をクリックします。

Cisco UCS ドメインの設定エクスポート スケジュールの削除

後述の手順に加えて、次のシナリオでは、Cisco UCS Central の完全状態バックアップを無効化または削除できます。

- サブドメイン グループ ポリシーを削除すると、バックアップ/エクスポート ポリシーが削除されます。
- 中央またはルート ドメイン グループ ポリシーを削除すると、バックアップ/エクスポート ポリシーが無効になります。

ステップ 1 [Config Export & Import] ページで、[Schedule] アイコンをクリックします。
ステップ 2 [Remove Domain Export Schedule] アイコンを選択します。
ステップ 3 設定バックアップを削除するドメイン グループを選択します。
ステップ 4 削除するスケジュールを選択します。
ステップ 5 [Remove] をクリックします。

Cisco UCS Central のバックアップ ファイルの表示

ステップ 1 メニュー バーで、[Backup & Restore] を選択します。
ステップ 2 [Domains] で、Cisco UCS Central ドメインを選択して、Cisco UCS Central スコープを入力します。
ステップ 3 右側のペインで、すべての Cisco UCS Central バックアップ ファイルのリストを確認します。 バックアップ ファイルごとに、ステータス、最終バックアップ日付、スケジュール、最大ファイル数、およびリモート コピーの場所を表示できます。